VISCHER

Memorandum

An: Hansruedi Born, Amt für Informatik, Kanton Zürich

Von: David Rosenthal, Sarah Bischof, VISCHER AG

Datum: 24. März 2022

Betrifft: Berechnung des ausländischen Lawful Access / US CLOUD Act

---

I. AUSGANGSLAGE

1 Der Kanton Zürich beabsichtigt, gewisse bisher auf internen Servern betriebene Office-Anwendungen von Microsoft in eine Cloud-basierte Umgebung zu überführen und dort von Microsoft betreiben zu lassen (**M365**). Die Datenbearbeitungen selbst ändern sich nicht. Was sich ändert ist der Betreiber der IT-Infrastruktur. Dies ist neu Microsoft mit ihren Rechenzentren in der Schweiz.

2 Konkret geht es um folgende Anwendungen:

- Office-Anwendungen (Word, Excel, Powerpoint, OneNote etc.)*
- E-Mail (Exchange Online)
- Kommunikation (Teams)
- Fileserver-Verzeichnisse und Intranet (Sharepoint Online)*
- Persönliche Laufwerke (OneDrive for Business)*
- Planner**
- Whiteboard**

* In diesen Fällen findet eine Erweiterung, nicht aber ein Abbau der bestehenden lokalen Ressourcen statt, d.h. diese Anwendungen werden weiterhin auch lokal ("on premise") benutzt.

** Diese Anwendungen finden auf Rechenzentren in Europa statt.

3 Die Dokumente mit Geschäftsfalldaten verbleiben vorerst im bisherigen Geschäftsverwaltungssystem, welche weiterhin auf internen Servern betrieben werden; es ist derzeit nicht geplant, Geschäftsverwaltungssysteme oder Fachapplikationen in die Cloud zu verschieben. Werden Dokumente in diesen Anwendungen erstellt oder von dort geöffnet, geschieht auch dies lokal, d.h. Word, Excel und Powerpoint laufen auch in diesen Fällen lokal und nicht in der Cloud.

4 Zur Umsetzung des Vorhabens wurden mit Microsoft zusätzliche Vertragsbedingungen verhandelt. Im Rahmen der Vorabkontrolle nach dem Gesetz über die Information und den Datenschutz des Kantons Zürich (IDG) fanden zudem Gespräche mit der Datenschutzbeauftragten des Kantons Zürich statt.

5 In diesem Rahmen wurde festgelegt, dass vor einem Entscheid des Regierungsrats zur Umsetzung des Vorhabens eine Abklärung über das damit verbundene Risiko eines Zugriffs durch US-Behörden gestützt auf den CLOUD Act vorgenommen werden muss, d.h. ermittelt werden soll, wie wahrscheinlich es ist, dass US-Behörden auf dem Weg über Microsoft an die vom Kanton Zürich in der Cloud zu speichernden Daten gelangen können und es auch tun werden.

II. ERGEBNIS

6 Durchgeführt wurde die Risikobeurteilung auf der Basis einer von uns entwickelten statistischen Methode, die heute bei diversen Schweizer Banken und anderen Berufs- und Amtsgeheimnisträgern zum Einsatz kommt. An der Beurteilung beteiligt waren diverse Vertreter des Kantons Zürich. Berücksichtigt wurden die vom Kanton Zürich vorgesehenen technischen und organisatorischen Massnahmen zur Absicherung der Daten in der Microsoft Cloud.

7 Die Risikobeurteilung kam zum Ergebnis, dass die prognostizierte Wahrscheinlichkeit eines erfolgreichen ausländischen Behördenzugriffs (sog. *Lawful Access*) in Bezug auf **Geschäftsfalldaten** (d.h. Daten aus hoheitlichen Geschäften, zum Begriff vgl. N 38) in der Betrachtungsperiode von fünf Jahren bei **0.74 Prozent** liegt. Bei diesem Wert braucht es 1'552 Jahre, damit es mit einer Wahrscheinlichkeit von 90 Prozent statistisch gesehen (bei gleichbleibender Wahrscheinlichkeit) mindestens ein Mal zu einem erfolgreichen *Lawful Access* kommt. Genügt eine Wahrscheinlichkeit von 50 Prozent, ist dies alle 467 Jahre mindestens ein Mal der Fall.

8 Bei **normalen Daten** (vgl. N 38) kam die Risikobeurteilung zum Ergebnis, dass die Eintrittswahrscheinlichkeit bei **0.95 Prozent** liegt. Bis eine Wahrscheinlichkeit von 90 Prozent erreicht sind, müssen also 1'206 Jahre vergehen bzw. 363 Jahre, bis die Wahrscheinlichkeit 50 Prozent erreicht. Die Eintrittswahrscheinlichkeit ist höher, weil diese Daten i.d.R. weniger gut verschlüsselt sind als die Geschäftsfalldaten. Keine eigene Beurteilung erfolgte für die Anwendungen *Planner* und *Whiteboard*, obwohl sie auf Rechenzentren in Europa, nicht der Schweiz laufen; es wird angenommen, dass sie keine für einen *Lawful Access* relevante Daten enthalten (erfahrungsgemäss wäre das Risiko jedoch vergleichbar).

9 Demnach erscheint es aufgrund der erfolgten Risikobeurteilung beim Vorhaben M365 als **höchst unwahrscheinlich**, dass US-Behörden über Microsoft auf vom Kanton Zürich in der Cloud gespeicherte Daten ohne Einwilligung des Kantons im Klartext zugreifen können und werden.

10 Die konkrete Berechnung ist dem beiliegenden Excel zu entnehmen.

III. DISKUSSION

A. Rechtliche Relevanz

11 Die Möglichkeit eines ausländischen Lawful Access ist für das Vorhaben aus zweierlei Gründen von Relevanz. Erstens kann ein solcher Lawful Access zu einer Verletzung des Berufs- bzw. Amtsgeheimnisses erfolgen, da im Falle eines Lawful Access über den ausländischen Provider (d.h. unter Umgehung des Schweizer Rechts- und Amtshilfewegs) eine Offenbarung von geheimnisgeschützten Informationen erfolgt. Zweitens kann ein solcher Lawful Access eine Verletzung des Schweizer Datenschutzrechts bzw. des hier einschlägigen IDG darstellen, falls dieser Lawful Access nicht den hiesigen Anforderungen an einen rechtmässigen Zugriff durch den Staat genügt

12 Dieser Umstand führte während längerer Zeit dazu, dass die Meinung vertreten wurde, dass Berufs- und Amtsgeheimnisträger ihre Daten nicht oder nur unter sehr strengen Voraussetzungen in die Cloud geben dürften.[1] Ähnliches wurde von gewissen (ausländischen) Datenschutzbehörden vertreten.[2] Hierbei ist zu berücksichtigen, dass bei Angeboten wie der Microsoft Cloud die Daten der Kunden zwar mitunter in der Schweiz gespeichert werden, ein Zugriff auf diese aus dem Kreis des Providers und seiner Konzerngesellschaften aber auch aus anderen Ländern und so insbesondere aus den USA möglich ist.

13 Mittlerweile wird generell eine differenziertere Meinung vertreten, wodurch Berufs- und Amtsgeheimnisträgern die Nutzung von Cloud-Diensten unter nicht mehr ganz so strengen Auflagen möglich ist.[3] Allerdings muss ein Berufs- oder Amtsgeheimnisträger, um seinen Sorgfaltspflichten im Rahmen einer Auslagerung in die Cloud nachzukommen, weiterhin abklären, wie hoch das Risiko eines ausländischen Lawful Access im konkreten Fall tatsächlich ist und bei einem nicht mehr akzeptablen Risiko auf die Auslagerung verzichten oder das Risiko hinreichend beschränkende Massnahmen ergreifen. Ist ein ausländischer Lawful Access angesichts der konkret getroffenen Schutzmassnahmen höchstwahrscheinlich ausgeschlossen, wird das Restrisiko in der Regel als akzeptabel gelten.[4]

14 Dieselbe Position vertreten inzwischen auch die Mehrheit der EU-Datenschutzbehörden und der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte. Sie verlangen vor einem Export von Perso-

---

[1] Vgl. unter anderem WOLFGANG WOHLERS, Auslagerung einer Datenbearbeitung und Berufsgeheimnis (Art. 321 StGB), Zürich/Basel/Genf 2016.

[2] So noch der Europäische Datenschutz-Ausschuss (EDSA) in seiner Empfehlung 01/2020 vom 10. November 2020 ("Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data").

[3] Vgl. unter anderem CHRISTIAN SCHWARZENEGGER/FLORENT THOUVENIN/BURKHARD STILLER, Gutachten zur Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte, Zürich, Fassung vom 1. November 2019.

[4] DAVID ROSENTHAL, Mit Berufsgeheimnissen in die Cloud, So geht es trotz US CLOUD Act, in: Jusletter vom 10. August 2020, Rz. 103 ff., abrufbar unter www.rosenthal.ch.

nendaten in ein Land ohne angemessenen Datenschutz, wozu auch die Möglichkeit des Fernzugriffs gehört, die Durchführung eines *Transfer Impact Assessments* (**TIA**), d.h. einer Beurteilung der Wahrscheinlichkeit eines datenschutzrechtlich unzulässigen ausländischen Lawful Access.[5] Kann der Datenexporteur aufzeigen, dass er "keinen Grund zur Annahme" hat, dass es angesichts der getroffenen Schutzmassnahmen zu einem datenschutzrechtlich unbefugten Lawful Access kommt, ist ein Export zulässig.[6] Dies ergibt sich inzwischen auch aus Art. 14 der in der Schweiz ebenfalls akzeptierten EU-Standardvertragsklauseln.

B. Situation in Bezug auf die USA

15 In Bezug auf die USA ergibt sich hieraus ein differenziertes Bild.

16 Das Berufs- und Amtsgeheimnis verlangt eine Verhinderung jeglicher Art von ausländischem Lawful Access gegenüber dem Provider. In diese Kategorie gehören in den USA insbesondere behördliche Herausgabebefehle, die dort gestützt auf *US Stored Communications Act* (**SCA**) gegenüber einem in den USA ansässigen Cloud-Provider erfolgen kann. Im Rahmen des 2018 erlassenen *US Clarifying Lawful Overseas Use of Data Act* (**CLOUD Act**) ist dabei klargestellt worden, dass solche Herausgabebefehle auch dann zulässig sind, wenn der in den USA ansässige Provider die von ihm (gültigerweise) herausverlangten Daten zur Herausgabe von einem Rechenzentrum ausserhalb der USA abrufen muss. Der CLOUD Act stellte allerdings nur klar, was schon zuvor immer galt und von den US-Gerichten auch so praktiziert worden war. Die Regelung entspricht überdies Art. 18 Abs. 1 des Übereinkommens über die Cyberkriminalität des Europarats,[7] steht also im Einklang mit europäischem Recht.

17 Aus diesem Grund verlangt das Datenschutzrecht in der Schweiz und der EU keine Beurteilung eines derartigen Lawful Access. Aus datenschutzrechtlicher Sicht beurteilt werden muss hingegen die Section 702 des *US Foreign Intelligence Surveillance Act* (**FISA**) sowie der Executive Order (**EO**) 12.333. Die beiden Bestimmungen erlauben den US-Behörden einerseits die ausländische Kabel- und Funkaufklärung und andererseits eine Massenüberwachung von durch US-Provider abgewickelte Kommunikation von Nicht-US-Personen. Im Rahmen seines "Schrems II"-Entscheids kam der Europäische Gerichtshofs (EuGH) am 16. Juli 2020 (C-311/18) zum Schluss, dass diese beiden Bestimmungen mangels einer Rechtsweggarantie nach europäischem Verständnis

---

[5] Europäischer Datenschutz-Ausschuss (EDSA) in der finalen Fassung seiner Empfehlung 01/2020 vom 18. Juni 2021 ("Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data"); Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB), Anleitung für die Prüfung der Zulässigkeit von Datenübermittlungen mit Auslandbezug (nach Art. 6 Abs. 2 lit. a DSG) vom 18. Juni 2021.

[6] Vgl. die Ausführungen zu TIAs in DAVID ROSENTHAL, FAQ zu den neuen Standardvertragsklauseln (SCC) für Datenübermittlungen in unsichere Drittstaaten, aktuelle Fassung abrufbar unter https://www.rosenthal.ch/downloads/VISCHER-faq-scc.pdf.

[7] SR 0.311.43.

den Anforderungen des EU-Datenschutzrechts nicht entsprechen. Der EDÖB schloss sich dieser Beurteilung in der Folge an.

18 Sind Berufs- und Amtsgeheimnis *und* Datenschutz betroffen, muss im Falle der USA das Restrisiko sowohl eines Lawful Access durch US-Behörden auf Basis des CLOUD Acts bzw. SCA als auch nach Section 702 FISA und EO 12.333 beurteilt werden.

19 Keine Rolle spielt hingegen der *US Providing Appropriate Tools to Restrict, Intercept and Obstruct Terrorism Act* aus dem Jahre 2001 (**PATRIOT Act**). Er ist nicht mehr in Kraft.

C. Bestimmung des Restrisikos eines Lawful Access

1. Verwendete Methode

20 Für die Bestimmung des Restrisikos eines ausländischen Lawful Access wurde die Berechnungsmethode von DAVID ROSENTHAL verwendet. Sie wurde ursprünglich für eine Schweizer Grossbank erarbeitet, im Sommer 2020 unter einer freien Lizenz im Rahmen einer wissenschaftlichen Abhandlung zum Berufsgeheimnis publiziert[8] und wird heute von diversen Berufs- und Amtsgeheimnisträgern in der Schweiz und im Ausland eingesetzt, um für Cloud-Vorhaben in strukturierter Form die Eintrittswahrscheinlichkeit eines erfolgreichen Lawful Access durch eine ausländische Behörde zu ermitteln. Auch die *International Association of Privacy Professionals* (**IAPP**) übernahm die Methode.[9] Sie beinhaltet auch ein TIA.

21 Die Methode basiert im Kern auf der Überlegung, dass ein Lawful Access durch eine ausländische Behörde auf Daten in der Cloud nur dann erfolgreich sein kann, wenn eine ganze Reihe von Bedingungen kumulativ erfüllt sind. Für die Zwecke der Beurteilung wurden diese Bedingungen herausgearbeitet. Es müssen bestimmte technische Voraussetzungen gegeben sein, gewisse faktische Bedingungen und gewisse rechtliche Anforderungen. Hierzu wurde ein strukturierter Prozess geschaffen, in dessen Rahmen jede dieser Bedingungen bzw. die Wahrscheinlichkeit deren Erfüllung einzeln bewertet werden muss. Mit Hilfe einer Kalkulation werden die Einzelbewertungen statistisch verknüpft und aus ihr für die jeweils festzulegende Beurteilungsperiode eine gesamthafte Eintrittswahrscheinlichkeit berechnet. Daraus kann das Restrisiko abgeleitet[10] oder – anders formuliert – die Wirksamkeit der getroffenen Vorkehrungen gegen einen Lawful Access beurteilt werden.

22 Das Ergebnis bleibt zwar eine reine Prognose, aber insbesondere, wenn sie in einer Gruppe mit Vertretern verschiedener Kompetenzen und

---

[8] Ausführliche Erläuterungen zum Lawful Access Risiko und dem Berechnungsmodell finden Sie hier: ROSENTHAL, Mit Berufsgeheimnissen in die Cloud, So geht es trotz US CLOUD Act, in: Jusletter vom 10. August 2020.

[9] https://datenrecht.ch/transfer-impact-assessments-iapp-veroeffentlicht-zwei-formulare-von-david-rosenthal/.

[10] Risiko = Eintrittswahrscheinlichkeit x Höhe des zu erwartenden Schadens (der hier als maximal angenommen wird).

Fachbereiche erstellt wird, reduziert diese strukturierte und schematische Vorgehensweise Verrauschungen und Verzerrungen wesentlich. Das so ermittelte prädiktive Urteil ist daher objektiver und weniger zufällig als bei anderen Methoden.

23 Eine weitere Besonderheit der Methode liegt darin, dass die Einzelbewertungen nicht genau sein müssen. Ob die Chance, dass ein Lawful Access mit einer bestimmten technischen Massnahme verhindert werden kann, geschätzt bei 40, 50 oder 60 Prozent liegt, spielt für das Endergebnis in aller Regel keine entscheidende Rolle. Es sind also keine absoluten Aussagen nötig sind, d.h. es ist keine Gewissheit erforderlich, ob eine bestimmte Eintrittsbedingung erfüllt ist (in aller Regel wird auch nie Gewissheit bestehen). Trotzdem gelangt die Methode zu einer Aussage.

24 Umgesetzt wird die Methode mit Hilfe eines Excel-Dokuments, das in der Gruppe gemeinsam befüllt wird.[11]

2. Beurteilungsschritte

25 Die Berechnung der Eintrittswahrscheinlichkeit eines ausländischen Lawful Access in der Cloud erfolgt in fünf Schritten:

- Im **ersten Schritt** werden die Rahmenbedingungen für die Beurteilung definiert, so insbesondere für welche Daten die Beurteilung durchgeführt wird und für welchen Beurteilungszeitraum. Der Beurteilungszeitraum ist wichtig, weil keine Aussage für die Ewigkeit gemacht werden kann, sondern nur für einige Jahre. Danach oder bei veränderten Umständen ist die Risikobeurteilung zu wiederholen.
- Im **zweiten Schritt** wird ermittelt, wie oft die relevanten ausländischen Behörden überhaupt ein Interesse haben könnten, an die Daten des betreffenden Betriebs zu gelangen. Dies wird in der Regel anhand von Erfahrungen aus der Vergangenheit eingeschätzt. Es geht hier noch *nicht* um die Cloud. In diesem Schritt wird auch berücksichtigt, wie viele dieser Fälle auf dem Weg der Rechts- oder Amtshilfe erledigt werden können, denn wenn ausländische Behörden auf diesem Weg an ihre Daten gelangen, brauchen sie nicht den (aufwändigeren) Weg über den Provider anzutreten. Ergebnis ist die Zahl der Fälle, in denen sich die Frage des Lawful Access über den Cloud-Provider im Beurteilungszeitraum überhaupt stellen wird.
- Im **dritten Schritt** wird ermittelt, welche Erfolgschancen ein Lawful Access über den Cloud-Provider hat. Im Fokus sind hier anlassbezogene Zugriffsversuche, d.h. die Situation, in welcher eine ausländische Behörde gezielt an die Daten eines Betriebs gelangen will und sich darum an dessen Provider hält. Hier wird ei-

---

[11] https://www.rosenthal.ch/downloads/Rosenthal_Cloud_Lawful_Access_Risk_Assessment.xlsx.

nerseits berücksichtigt, ob der Provider überhaupt auf die Daten im Klartext in der gewünschten Form zugreifen könnte, wenn er wollte, und andererseits, ob bzw. wie erfolgreich er sich angesichts der konkreten Umstände gegen den Zugriff rechtlich wehren kann, wozu er in der Regel verpflichtet ist (dazu nachfolgend). Es müssen insgesamt sieben Voraussetzungen erfüllt sein.[12]

- Im **vierten Schritt** wird beurteilt, wie hoch die Wahrscheinlichkeit ist, dass der Provider im Rahmen einer Massenüberwachung (die anders als der anlassbezogene Lawful Access nicht gezielt gegen den Betrieb erfolgt) auch auf Daten des Betriebs zugreifen würde. Auch hier werden verschiedene Faktoren berücksichtigt. Dieser vierte Schritt entspricht im Falle der USA dem von den Datenschutzbehörden verlangten TIA.
- Im **fünften Schritt** werden die so ermittelten Eintrittswahrscheinlichkeiten zusammengerechnet und entsprechend dargestellt.

26 Die Beurteilung kann je für unterschiedliche Kategorien von Daten und Risikoprofilen und damit mehrfach durchgeführt werden. Wird eine bestimmte Datenkategorie zum Beispiel durch eine zusätzliche technische Massnahme besonders geschützt, sollte sie separat beurteilt werden, weil diese Massnahme Einfluss auf die Eintrittswahrscheinlichkeit eines ausländischen Lawful Access haben wird. Auch das Interesse ausländischer Behörden an bestimmten Daten wird je nach Kategorie unterschiedlich sein.

D. Exkurs: Rechtliche Argumente im Rahmen des CLOUD Act

27 In der öffentlichen Wahrnehmung erscheint der CLOUD Act als für Berufs- und Amtsgeheimnisträger besonders bedrohlich, weil gemeinhin angenommen wird, US-Behörden könnten gestützt auf diesen Erlass auf alle Daten zugreifen, die irgendwo auf der Welt in einer Cloud mit US-Bezug gespeichert sind. Dies ist unzutreffend.

28 Ein in den USA ansässiger Provider kann überhaupt nur zur Herausgabe gemäss dem CLOUD Act bzw. SCA verpflichtet werden, wenn er die angefragten Daten besitzt oder kontrolliert ("Possession, Custody or Control"). Hierzu existiert in den USA eine ausführliche, langjährige Praxis.[13]

29 "Besitz" fällt bei europäischen Clouds in der Regel weg, weil die Daten in diesen Fällen ausschliesslich in Rechenzentren gespeichert werden,

---

[12] ROSENTHAL, Mit Berufsgeheimnissen in die Cloud, So geht es trotz US CLOUD Act, in: Jusletter vom 10. August 2020, Rz. 109.

[13] Detailliert hierzu: JUSTIN HEMMINGS, SREENIDHI SRINIVASAN, PETER SWIRE, "Defining the Scope of "Possession, Custody or Control" for Privacy Issues and the CLOUD Act, in: Journal of National Security Law & Policy, Januar 2020, abrufbar unter unter https://ssrn.com/abstract=3469808.

die von europäischen Gesellschaften betrieben werden. Sie und nicht ihre allfälligen US-Muttergesellschaften haben die Daten im Besitz.

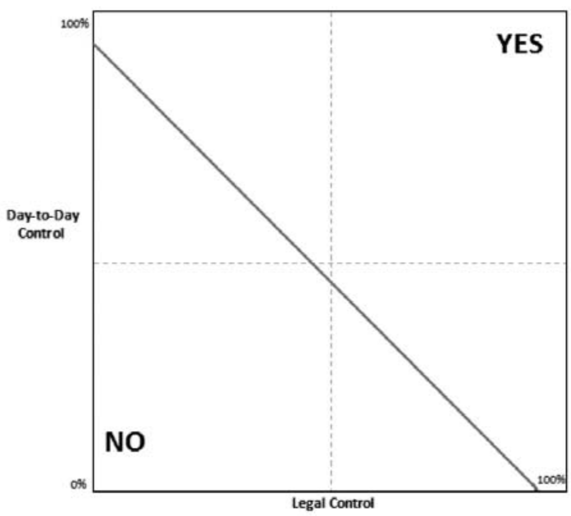
30 "Kontrolle" kann entweder gegeben sein, wenn der Provider im Tagesgeschäft Zugang zu den Daten im Klartext hat ("day-to-day-control") oder wenn er einen Anspruch auf die Daten im Klartext hat, und zwar nicht nur, um einen Herausgabebefehl einer US-Behörde beantworten zu können ("legal control").

31 Die folgende Grafik von HEMMINGS/SRINIVASAN/SWIRE stellt bildlich dar, in welchen Fällen US-Gerichte von Kontrolle eines Providers ausgehen und ihn zur Herausgabe der Daten verpflichten. Die Grafik basiert auf den zwei Voraussetzungen der "day-to-day-control" und der "legal control", welche auf einer X- und Y-Achse dargestellt werden; die Grafik und die darin dargestellte Beurteilung, ab wann die Kontrolle des Providers bejaht wird, ist das Ergebnis einer Analyse der Rechtsprechung von US-Gerichten in Bezug auf die Voraussetzung der "Possession, Custody or Control" vor Inkrafttreten des CLOUD Act.

32 Die Autoren kommen im Rahmen ihrer Analyse zum Schluss, dass der CLOUD Act in erster Linie die geltende Rechtsprechung in den USA bezüglich die Herausgabe von nicht in den USA gespeicherten, elektronischen Beweisen bestätigte, die Kompetenzen der Behörden aber nicht ausweitete. Folglich hat die Grafik auch im Zusammenhang mit der Beurteilung, wann im Rahmen des CLOUD Acts von der Kontrolle des Providers ausgegangen wird, Gültigkeit.

33 Der Bereich über der schrägen Linie zeigt an, wann Kontrolle von den US-Gerichten bejaht wird:[14]

Figure 2:
Line Roughly Describing Where Courts Find Possession, Custody, or Control



14 HEMMINGS/SRINIVASAN/SWIRE, "Defining the Scope of "Possession, Custody or Control" for Privacy Issues and the CLOUD Act, in: Journal of National Security Law & Policy, Januar 2020, S. 4.

34 Technische und organisatorische bzw. vertragliche Massnahmen können den Zugang des Providers auf die Daten in tatsächlicher und auch in rechtlicher Hinsicht einschränken. Werden Daten beispielsweise verschlüsselt, so dass die Mitarbeiter des Providers für sein Tagesgeschäft (d.h. nicht für den Notfall) aufgrund der organisatorischen Vorkehrungen keinen Zugang zum entsprechenden Schlüssel haben, wird nach unserem Verständnis in der Regel keine "day-to-day-control" seitens des Providers vorliegen; dass er sich im Notfall oder durch Umgehung von Schutzmassnahmen trotzdem Zugang verschaffen könnte, ist unbeachtlich. Entsprechend müsste auf der Y-Achse unseres Erachtens ein Punkt im unteren Bereich gesetzt werden. Vertragliche Absprachen, wie etwa das "Customer Lockbox"-Verfahren[15] von Microsoft, können zudem benutzt werden um zu bewirken, dass der Provider aus der Sicht eines US-Gerichts über möglichst keine "legal control" verfügt (auch wenn ein Zugriff technisch allenfalls möglich wäre). Hier müsste der Punkt auf der X-Achse also deutlich links gesetzt werden. Damit aber läge keine "Kontrolle" mehr vor, oder die Chance, dass ein Gericht eine solche annimmt, ist zumindest deutlich reduziert.

35 Selbst wenn sich der Provider also für den Notfall oder im Falle einer gesetzlichen Pflicht einen Zugang zu den Daten seiner Kunden vorbehält, wird er im Falle eines Herausgabebefehls geltend machen können (und vertraglich müssen), dass er jedenfalls im Tagesgeschäft keinen Zugang zu und auch keinen Anspruch auf die Daten hat und den Befehl auf diese Weise mangels "Possession, Custody or Control" abwehren. Die Erfolgschance einer solchen Verteidigungsstrategie wird im Rahmen der Methode entsprechend berücksichtigt.

36 Berücksichtigt werden können von ihr überdies auch andere rechtliche Argumente zur Abwehr von Herausgabebefehlen unter dem CLOUD Act. Werden beispielsweise die Daten des Kunden im Territorium der Schweiz gespeichert, können sich die Mitarbeiter des Providers im Falle einer Herausgabe an einen ausländischen Staat nach Art. 271 des Schweizer Strafgesetzbuchs (StGB) strafbar machen. Dies wiederum kann ein Provider in den USA geltend machen, um einen Herausgabebefehl abzuwehren: US-Gerichte sind angehalten, in solchen Fällen eine Interessenabwägung durchzuführen. Nach unserer Erfahrung respektieren US-Behörden in solchen Fällen Art. 271 StGB regelmässig, wenn ihnen gezeigt werden kann, dass die Voraussetzungen zur Anwendung dieser Strafnorm tatsächlich gegeben sind und Strafbarkeit

---

15 Dieses Verfahren ist ein vertragliches Versprechen von Microsoft an ihre Kunden, nur dann auf die in der Cloud gespeicherten Daten im Klartext zuzugreifen, wenn der Kunde hierfür seine Einwilligung erteilt hat (z.B. im Supportfall). Technisch wäre der Zugriff von Microsoft zwar auch ohne diese Einwilligung möglich. Microsoft würde dadurch aber den Vertrag mit dem Kunden verletzen, soweit sie nicht rechtlich gezwungen sind, Zugriff zu gewähren. Die Pflicht Zugriff zu gewähren hängt aber wiederum davon ab, worauf auch ohne rechtliche Verpflichtung im Tagesgeschäft zugreift (vgl. N 27 ff.). Weitere Informationen zu "Customer Lockbox" können auf der Website von Microsoft gefunden werden: https://docs.microsoft.com/en-us/microsoft-365/compliance/customer-lockbox-requests?view=o365-worldwide.

droht. Auch dieser Punkt wird in der Methode abgebildet und fliesst in die Beurteilung mit ein.

E. Risikobestimmung des Kantons Zürich

1. Durchführung der Risikobeurteilungen

37 Die Wahrscheinlichkeit eines ausländischen Lawful Access im Falle des Vorhabens "M365" wurde vom Kanton Zürich in einem Workshop einer interdisziplinären Gruppe von Fachleuten bestimmt. Vertreten waren technische Experten, aber auch juristische Mitarbeiter und weitere Vertreter aus dem Amt für Informatik, der Staatsanwaltschaft, dem kantonalen Steueramt, der Staatskanzlei und der Kantonspolizei. Vor und nach diesem Workshop fanden für einzelne Aspekte gesonderte Besprechungen statt.

38 Aufgrund der Tatsache, dass für gewisse E-Mails eine zusätzliche Verschlüsselung vorgesehen ist, wurden zwei verschiedene Risikobeurteilungen durchgeführt:

- **Geschäftsfalldaten:** Dies sind Daten, die für vorliegend einem erhöhten Schutzbedarf unterliegen, wie insbesondere Falldaten aus der Geschäftsverwaltung (z.B., wenn über Geschäfte kommuniziert oder Akten ausgetauscht werden); zum Begriff des Geschäftsfalls vgl. auch § 2–6 der Verordnung über die Informationsverwaltung und -sicherheit (IVSV, LS 170.8). Die Fallakten selbst werden zwar weiterhin im Geschäftsverwaltungssystem abgelegt (welches sich nicht in der Cloud befindet) und lokal bearbeitet (d.h. nicht in den Online-Versionen der Office-Anwendungen), ein Versand über E-Mail oder ein Austausch dazu ist jedoch möglich. Die Mitarbeiter werden durch entsprechende Weisungen und Reglemente verpflichtet, in diesen Fällen die S/MIME-Verschlüsselung zu aktivieren. Für Microsoft weiterhin erkennbar sind der Betreff des E-Mails sowie Sender und Empfänger, nicht jedoch der Inhalt des E-Mails.
- **Normale Daten:** Gemeint sind alle anderen Daten, so beispielsweise Daten aus Projekten, dem Personalwesen, der internen Organisation oder aus politischen Geschäften. In diesen Fällen werden die Mitarbeiter nicht verpflichtet sein, eine S/MIME Verschlüsselung einzusetzen (sie können dies aber jederzeit tun, wo sie dies als angezeigt erachten oder dies fallspezifisch angewiesen wäre). Solche Daten können auch auf Speicherlaufwerken in der Cloud abgelegt sein.

39 Für die vorliegende Risikobeurteilung wurde bewusst nicht auf die Kategorie der "besonderen" Personendaten, wie sie das Gesetz über die Information und den Datenschutz (IDG, LS 170.4) definiert, abgestellt. Der Grund ist, dass es vorliegend nicht um die Beurteilung der Datensicherheit oder des Datenschutzes im herkömmlichen Sinne geht, sondern um das (Sonder-)Risiko eines ausländischen Lawful Access durch US-Behörden. Beim CLOUD Act ist zusätzlich zu beachten, dass dieser

nur (aber immerhin) zur Verhütung, Ermittlung, Aufklärung oder Verfolgung schwerer Straftaten ("serious crimes") zur Verfügung steht.[16] Diesem Risiko des Lawful Access sind "besondere" Personendaten nicht in erhöhtem Masse ausgesetzt, denn das Interesse der US-Behörde richtet sich beim CLOUD Act nach der Relevanz für die verfolgten Straffällen und nicht nach der Kategorie der Daten. Die Risikofaktoren sind somit bei besonderen und normalen Personendaten dieselben, weshalb bei der vorliegenden Risikobeurteilung nicht danach differenziert wird. Unterschieden wird stattdessen zwischen Geschäftsfalldaten und allen anderen Daten, da US-Behörden sich vor allem für erstere interessieren werden und sie auch sonst eines besonderen Schutzes bedürfen, da sie in Ausübung hoheitlicher Befugnisse und nötigenfalls zwangsweise erhoben werden – gleichgültig, ob sie "besonders" sind oder nicht. Auch aus Sicht der betroffenen Person geht im Falle eines Lawful Access durch US-Behörden für ein US-Strafverfahren von besonderen Personendaten nicht per se ein höheres Risiko aus. Für eine betroffene Person kann eine Offenlegung "normaler" Personendaten (z.B. Angaben über eine Tathandlung oder eine gemachte Äusserung) im Gegenteil sogar gravierendere Folgen haben als von "besonderen" Personendaten (z.B. Angabe zu einer Krankheit oder Parteizugehörigkeit). Entscheidendes Kriterium ist vielmehr die Fallrelevanz. Der Schutz vor dem Zugriff durch andere unbefugte Dritte (externe oder interne Angreifer) bzw. das diesbezügliche Risiko ist hier wiederum *nicht* Gegenstand der Beurteilung.

2. Erläuterungen zu der durchschnittlichen Anzahl Rechtshilfeersuchen

40 Für die Prognose der Anzahl Fälle, in welchen die US-Behörden ein Interesse an den Daten des Kantons Zürich haben könnten, wurde auf Zahlen zurückgegriffen, die das Bundesamt für Justiz (**BJ**) auf Rückfrage des Kanton Zürichs zusammengestellt hat.

41 Die folgende Tabelle zeigt auf, wie viele Rechtshilfeersuchen von US-Behörden in den Jahren 2018-2021 beim BJ eingingen und wie viele dieser Rechtshilfeersuchen den Kanton Zürich betrafen. Dabei wurden ausschliesslich jene Rechtshilfeersuchen berücksichtigt, mit welchen US-Behörden eine strafrechtliche Beweiserhebung beantragten; unberücksichtigt blieben Fälle über Auslieferungsverfahren und Verfahren, mit welchen um Herausgabe von in der Schweiz gesperrten Vermögenswerten an die USA ersucht wurde, weil diese nicht auf die Herausgabe von Daten zielen und daher auch ein ausländischer Lawful Access gegenüber dem Provider für die US-Behörden nicht zum Ziel führen würde. Nicht berücksichtigt wurden Rechtshilfeersuchen in Zivilsachen, da in diesen Angelegenheiten der CLOUD Act nicht zur Verfügung steht. Aus diesem Grund wurden auch keine Amtshilfeverfahren be-

---

[16] Vgl. etwa den Bericht des Bundesamts für Justiz vom 17. September 2021 zum US CLOUD Act (https://www.bj.admin.ch/bj/de/home/publiservice/publikationen/berichte-gutachten/2021-09-17.html), S. 4.

rücksichtigt. Alle Fälle, in denen die Schweiz Amtshilfe *gewährt*, fallen für einen ausländischen Lawful Acccess über einen Provider ohnehin ausser Betracht, weil es in diesen Fällen keinen Anlass gibt, diesen für die Behörde wesentlich aufwändigeren und unsicheren Weg zu beschreiten. Wo keine Amtshilfe gewährt wird, muss der Fall aus Sicht des US-Rechts (auch) strafrechtlicher Natur sein, d.h. ein "serious crime" darstellen, damit den US-Behörden ein Zugriff nach CLOUD Act überhaupt zugänglich ist. Ist dies der Fall, stellt sich wiederum mindestens prinzipiell die Frage einer Rechtshilfe in Strafsachen, auch wenn die Schweiz sie im Einzelfall schlussendlich nicht gewährt. Diese Fälle in Strafsachen sind als Ausgangspunkt der Risikobeurteilung berücksichtigt worden, und zwar unabhängig davon, ob Rechtshilfe letztendlich gewährt wurde.

Jahr	**Gesamtanzahl Rechtshilfeersuchen von US-Behörden in Strafsachen**	**Anzahl Ersuchen, die den Kanton Zürich betrafen**
2018	67	8
2019	64	8
2020	88	10
2021	94	11
Durchschnitt	**78.25**	**9.25**

42 Von diesen jährlich beim BJ eingehenden Rechtshilfeersuchen werden rund 1-3 abgelehnt. Diese niedrige Zahl lässt sich damit erklären, dass der Rechtshilfe-Kanal zwischen der Schweiz und den USA sehr gut eingespielt ist und funktioniert. US-Behörden suchen daher in Fällen, in denen die Rechtshilfefähigkeit fraglich erscheint, vorgängig das Gespräch mit der Zentralstelle USA des BJ, weil diese für die Ausführung von US-Rechtshilfeersuchen auf dem gesamten Gebiet der Schweiz zuständig ist. Bei einer ablehnenden Einschätzung des BJ verzichtet das U.S. Department of Justice (**DoJ**), welches in den USA als zentrale Stelle für entsprechende Rechtshilfeersuchen zuständig ist, regelmässig auf die Einreichung eines formellen Ersuchens.

43 Gemäss Aussagen des BJ wurden in den Jahren 2018-2021 jährlich schätzungsweise 1-3 Rechtshilfeersuchen (d.h. im Durchschnitt 2) nicht gestellt, da dem DoJ aufgrund von Vorgesprächen mit dem BJ klar wurde, dass sie mit einem solchen keinen Erfolg haben würden. Damit erhöht sich die durchschnittliche Anzahl Fälle pro Jahr, in denen US-Behörden zum Zweck der strafrechtlichen Beweiserhebung über den Rechtsweg versucht haben, Daten von der Schweiz zu erlangen,

auf 80.25; die entsprechende Anzahl Fälle, die sich auf Daten des Kantons Zürich bezogen, erhöht sich auf 9.46 (80.25 x 0.1182).

44 Der Kanton geht davon aus, dass sich diese Werte in Zukunft nicht bzw. nicht massgeblich verändern werden. Für die Risikoberechnung wurde daher davon ausgegangen, dass US-Behörden im Schnitt in 10 Fällen pro Jahr versuchen werden oder zumindest erwägen, über den Rechtsweg zum Zweck der strafrechtlichen Beweiserhebung an Daten des Kantons Zürichs zu gelangen, auch wenn die Rechtshilfe nicht zur Verfügung steht oder gewährt wird. Für diese "Restanz" wird letztlich erwogen, wie wahrscheinlich es ist, dass US-Behörden über den CLOUD Act Zugang zu in der Cloud gespeicherten Daten des Kantons Zürich im Klartext erhalten.

3. Technische und organisatorische Massnahmen

45 Bei der Schätzung der Werte und Prognosen wurden ferner die vom Kanton Zürich für das Vorhaben M365 geplanten technischen und organisatorischen Massnahmen berücksichtigt. Zu diesen Massnahmen gehören unter anderem die folgenden:

- Alle Daten des Kantons werden ausschliesslich in der Schweiz gespeichert ("data at rest"), d.h. in den Schweizer Rechenzentren von Microsoft.
- Alle Daten des Kantons werden während ihrer Übermittlung ("data in transit") und während ihrer Speicherung ("data at rest") verschlüsselt.
- Die Schlüssel der gespeicherten Daten werden in einem von Microsoft betriebenen Schlüsselspeicher aufbewahrt, auf welchen grundsätzlich nur die Mitarbeiter des Kantons Zugriff haben, welche vom Kanton im Verzeichnis mit der entsprechenden Berechtigung eingetragen worden sind, wobei sich die "Masterkopie" dieses Verzeichnisses in den Händen des Kantons befindet und das Verzeichnis für diesen stets einsehbar ist.
- Mitarbeitern des Providers wiederum ist der Zugriff auf die wesentlichen, in der Cloud gespeicherten Daten des Kunden nur mit ausdrücklicher Einzelfreigabe des Kunden erlaubt (z.B. in Supportfällen).
- Werden Geschäftsfalldaten über E-Mail versendet, wird der Inhalt der jeweiligen E-Mail (nicht ihr Kopf) mittels S/MIME "end-to-end" verschlüsselt, so dass Microsoft bereits technisch keinen Zugang zum Inhalt im Klartext hat und auch nicht über den Schlüssel verfügt.
- Dem Provider ist die Bearbeitung der Daten des Kunden grundsätzlich nur für die Zwecke des Kunden und zur Erbringung von Leistungen an den Kunden erlaubt, ebenso verpflichtet er sich zur Einhaltung des Schweizer Rechts; eine Offenlegung gegenüber

ausländischen Behörden ist nur und erst zulässig, wenn der Provider nach ausländischem Recht dazu verpflichtet ist.

4. Ergebnisse

46 Die Ergebnisse der Risikobeurteilungen wurden in einem Excel mit zwei Arbeitsblättern dokumentiert und von allen Beteiligten gesichtet und verabschiedet. Das Excel enthält auch eine Begründung der jeweils angenommenen Werte.

Cloud-Computing: Risikobeurteilung eines Lawful Access durch ausländische Behörden

Template: Version 5.04 (1. September 2021)

Eine Version als DSGVO TIA gibt es hier:

Bogen zur Beurteilung eines einzelnen Lands

Autor: David Rosenthal (www.rosenthal.ch)

Schritt 1: Ausgangslage der Risikobeurteilung definieren

a)	Unternehmen:	**Kanton Zürich**	Datum:	3. und 16. Dezember 2021 (Beurteilungssitzungen), Fassung vom 22. Januar 2022
b)	Daten, die vor dem Behördenzugriff zu schützen sind und um die es hier geht:	**Geschäftsfalldaten (per S/MIME verschlüsselt)** (zur Begriffsdefinition vgl. das erläuternde Memorandum)	Mitwirkende:	Hansruedi Born (Amt für Informatik), Tanja Bucher (Staatsanwaltschaft), Stephan Beky (Amt für Informatik, Rechtsdienst), Jörg Ochsner (Amt für Informatik, IT-Sicherheit und Datenschutz), Andreas von Moos (Kantonales Steueramt), Esther Hefti (Staatskanzlei, Rechtsdienst), Philipp Grabher (CISO), Serdar Günal Rütsche (Kantonspolizei Zürich, Cybercrime)
c)	Cloud-Anwendung, mit welcher die Daten bearbeitet werden sollen:[5]	**M365**	Rechtsberater:	David Rosenthal, Sarah Bischof, VISCHER AG
d)	Betrachtungszeitraum der Risikobeurteilung in Jahren:	**5**	Verantwortlich:	Hansruedi Born
e)	Relevante ausländische Rechtsordnung:	**USA**		

Schritt 2: Wahrscheinlichkeit, dass eine ausländische Behörde Anspruch auf die Daten hat und ihn gegen den Provider durchsetzen will[1]

		Wahrscheinlichkeit pro Fall* **	Fälle pro Jahr	Fälle verbleibend	Begründung
a)	Anzahl der Fälle pro Jahr, in welchen eine Behörde im Land im Betrachtungszeitraum schätzungsweise versuchen wird, auf dem Rechtsweg an relevante Daten zu gelangen[2]		10.00		*Grundlage für diese Zahl war (a) der Durchschnittswert aller US-Rechtshilfeersuchen (zum Zweck der strafrechtlichen Beweiserhebung) aus den Jahren 2018-2021 an die Schweiz (78.25) und (b) der Anteil der Fälle, die Daten aus dem Kanton Zürich betreffen (9.25 Fälle, 11.82%). Die Zahlen stammen vom Bundesamt für Justiz (16.12.2021), da solche Rechtshilfeersuchen zentral über diese Stelle eingehen (und nicht direkt beim Kanton Zürich). Von den jährlich eingehenden Rechtshilfeersuchen lehnt das BJ pro Jahr schätzungsweise 1-3 Ersuchen ab. Schätzungsweise werden im Jahr 1-3 (also im Durchschnitt 2) Ersuchen gar nicht gestellt, weil dem U.S. Department of Justice (DoJ), welches in den USA als zentrale Stelle für solche Ersuchen zuständig ist, aufgrund von Vorgesprächen mit dem BJ klar wird, dass sie keine Chance haben. Damit erhöht sich die durchschnittliche Anzahl Fälle pro Jahr, in denen US-Behörden in den Jahren 2018-2021 auf dem Rechtsweg zum Zweck der strafrechtlichen Beweiserhebung versucht haben, Daten von der Schweiz zu erlangen, auf 80.25; die entsprechende Anzahl Fälle, die sich auf Daten des Kantons Zürich bezogen, erhöht sich auf 9.46 (80.25 x 0.1182). Wir gehen davon aus, dass sich diese Werte in Zukunft nicht bzw. nicht massgeblich verändern werden. Wir nehmen daher an, dass US-Behörden im Schnitt in 10 Fällen pro Jahr versuchen werden, über den Rechtsweg zum Zweck der strafrechtlichen Beweiserhebung Daten des Kantons Zürichs zu erlangen. Rechtshilfeersuchen in Zivilsachen wurden hier der Einfachheit halber (entgegen der Fragestellung) bereits auf dieser Stufe nicht mehr berücksichtigt, da der US CLOUD Act hier keine Zugriffe erlaubt. Amtshilfeersuchen wurden aus demselben Grund hier nicht mitgezählt. Soweit sie gewährt werden, stellt sich die Frage des Lawful Access gar nicht erst. Werden sie nicht gewährt, muss auch nach US-Recht zugleich eine (schwerwiegende) Straftat vorliegen, damit ein Lawful Access nach US CLOUD Act möglich ist. Wir erachteten es daher als zielführend, uns von Anfang an auf strafrechtliche Fälle zu fokussieren, hier aber auch jene Fälle zu berücksichtigen, in denen die Schweiz keine Rechtshilfe in Strafsachen gewährt, sei es durch Ablehnung eines Gesuchs, sei es, weil die US-Behörden bereits nach einem informellen Austausch zum Schluss kommen, dass ein Gesuch keine Chance hat. Das sind gemäss BJ nur wenige Fälle. Wir haben die Zahl zusätzlich mehr als aufgerundet.*
b)	Anteil der Fälle, in welchen die Herausgabe der Verfolgung von Fällen dient, die im betreffenden Staat einen Herausgabebefehl grundsätzlich auch gegenüber einem Provider erlauben	50%	5.00		*Herausgabebefehle der US-Behörden gegenüber US-Providern nach dem US CLOUD Act sind nur dann rechtmässig, wenn es sich um ein Verfahren zur Aufklärung einer schwerwiegenden Straftat ("serious crime") handelt. Nicht bei allen Fällen, in denen US-Behörden auf dem Rechtshilfeweg an Daten gelangen möchten, wird es sich um solche Straftaten handeln. Ferner sind hier nur Fälle zu berücksichtigen, in denen die US-Behörden wissen, dass es sich um Daten des Kantons Zürich handelt. Denn wenn ein Rechtshilfeersuchen abgelehnt wird, werden sie nicht erfahren, welchen Kanton es betraf, d.h. sie müssten im Falle eines Zugriffs auf den Provider bereits wissen, dass es sich um einen Zürich betreffenden Fall handelt. Nur dann aber steht den US-Behörden der US CLOUD Act gegenüber Microsoft mit Bezug auf die Instanz des Kantons Zürich offen, da sie aufzeigen müssen, dass diese die von ihnen gesuchten Daten enthält (keine Fishing Expeditions). Hierbei ist auch zu beachten, dass die Geschäftsverwaltung nicht in der Cloud sein wird, d.h. dass die US-Behörden in der Regel keine Anhaltspunkte haben, dass sich für ihren Fall relevante Daten in der Cloud des Kantons Zürich befinden werden. Wir nehmen an, dass daher weit weniger als die Hälfte der Fälle die Anforderungen des US CLOUD Act erfüllen werden, gleichgültig, wer der Provider ist und welche Massnahmen zur Verhinderung eines Lawful Access getroffen wurden.*
c)	Wahrscheinlichkeit, dass es in den verbleibenden Fällen gelingt, die Behörde nach ihrem eigenen Recht oder sonst von ihrem Vorhaben, an die Daten im Klartext zu gelangen, abzubringen[3]	0%	5.00		*Wir gehen für vorliegende Zwecke davon aus, dass wir nicht in der Lage sein werden, uns gegen eine Herausgabeforderung nach Massgabe des US-Rechts wehren zu können. Den Umstand, dass eine Herausgabeforderung völkerrechtlich problematisch ist, berücksichtigen wir an dieser Stelle nicht.*
d)	Wahrscheinlichkeit, dass in den verbleibenden Fällen die Daten in der einen oder anderen Weise geliefert werden (z.B. mit Einwilligung oder über Rechts- oder Amtshilfe)[4]	95%	0.25		*Der Rechtshilfe-Kanal zwischen den USA und der Schweiz ist sehr gut eingespielt und funktioniert. Pro Jahr werden nur schätzungsweise 1-3 Ersuchen abgelehnt; weitere schätzungsweise 1-3 Ersuchen werden nach entsprechenden Vorgesprächen nicht gestellt. Daraus ergibt sich, dass von den oben genannten Fällen im Schnitt etwas über 95% erfolgreich sind und die US-Behörden auf diesem Weg an ihre Daten gelangen. Wir gehen nicht davon aus, dass sich dieser Wert im Betrachtungszeitraum verschlechtern wird, d.h. die US-Behörden werden in weniger als 5 Prozent der Fälle nicht mit entsprechenden Datenlieferungen befriedigt werden können.*
e)	Wahrscheinlichkeit, dass die Behörde in den verbleibenden Fällen die Daten trotzdem für so wichtig erachtet, dass sie einen anderen Weg suchen wird, um an sie heranzukommen	25%	0.06	0.06	*Kommen die US-Behörden auf dem Weg der Rechtshilfe nicht zum Zug, versuchen sie erfahrungsgemäss in der Regel, auf dem Wege eines Zivilverfahrens oder sonst über die beteiligten Personen an die von ihnen gewünschten Daten zu gelangen. Der Weg über den Provider und gestützt auf den US CLOUD Act dauert auch dann, wenn er erfolgreich ist, vergleichsweise lange, weil sich die Provider zur Wehr setzen müssen und werden. Hinzu kommt, dass ein "Angriff" auf die Computersysteme eines souveränen fremden Staats massive politische Konsequenzen nach sich ziehen dürfte, was die Hemmschwelle der US-Behörden zusätzlich hochsetzen dürfte. Wir gehen trotzdem für vorliegende Berechnung vorsichtigerweise davon aus, dass in einem von vier Fällen, in welchen die US-Behörden auf dem Weg der Strafrechtshilfe nicht an die Daten gelangt sind, sie es über den Provider versuchen werden.*
	Anzahl der Fälle pro Jahr, in welchen sich die Frage eines lawful access durch eine ausländische Behörde stellt			0.06	
	Anzahl Fälle im Betrachtungszeitraum			0.31	

Schritt 3: Wahrscheinlichkeit, dass eine ausländische Behörde den Anspruch über den Provider erfolgreich durchsetzt

Für die vorliegende Beurteilung herangezogene Rechtsgrundlage: US CLOUD Act (inklusive Stored Communications Act; der PATRIOT Act ist hingegen in den USA nicht mehr in Kraft)

	Voraussetzung für einen Taterfolg[5]	Wahrscheinlichkeit pro Fall[6][9] * **			Begründung
a)	Wahrscheinlichkeit, dass die Behörde um den vom Unternehmen beigezogenen Provider und dessen Subunternehmern weiss (Voraussetzung Nr. 1)	100%		100%	*Es wird allgemein bekannt sein, dass der Kanton Zürich die Cloud von Microsoft benutzt. Daher werden die US-Behörden wissen, von welchem Provider sie die Daten herausverlangen müssen.*
b)	Wahrscheinlichkeit, dass ein Mitarbeiter des Providers oder seiner Subunternehmer während eines Support-Falls Einsicht in Daten im Klartext erhält ... (Voraussetzung Nr. 2)	5%	0.25%		*Wir alleine bestimmen, in welchen Supportfällen die Mitarbeiter des Providers Zugang zu unseren Daten im Klartext erhalten und werden dies nur wo zwingend nötig verlangen und erlauben; die erste Ansprechperson in Supportfällen wird die interne IT Abteilung der Verwaltung sein, weshalb die Anzahl Supportfälle, die an Microsoft weitergeleitet werden muss, minim sein wird. Hinzu kommt, dass die hier relevanten Geschäftsfalldaten mittels S/MIME End-to-End-verschlüsselt sein werden, d.h. Microsoft selbst beim Zugriff auf die Mailbox eines Mitarbeiters des Kantons den Inhalt der E-Mail nicht sehen wird. Die Geschäftsverwaltungsdaten werden in lokal betriebenen Geschäftsverwaltungssystemen und Fachapplikationen und nicht auf den Sharedrives gespeichert. Somit ist die Wahrscheinlichkeit, dass Microsoft die Daten im Klartext sieht, äusserst gering.*
	... und dabei nach den von der Behörde gewünschten Daten suchen, sie finden und sie für sich kopieren kann (Voraussetzung Nr. 3)	5%			*Wenn der Provider Zugang im Supportfall erhalten würde, würde er nur Zugriff auf jene Daten erhalten, die für die Behandlung des konkreten Supportfalls nötig sind. Er kann dabei nicht nach anderen Daten suchen. Behördenanfragen beziehen sich jedoch immer auf bestimmte Daten. Die Wahrscheinlichkeit, dass die Daten, die der Provider sieht (z.B. die unverschlüsselte E-Mail eines Benutzers) gerade jenen entsprechen, die die Behörde vom Provider verlangt, ist minim.*
c)	Wahrscheinlichkeit, dass Mitarbeiter des Providers, seiner Subunternehmer oder des Mutterhauses trotz der getroffenen technischen Gegenmassnahmen[14] rein technisch (auch) ausserhalb eines Support-Falls (z.B. mit Administratorenrechten) Zugriff auf Daten im Klartext nehmen oder sich einen solchen Zugang zu Daten verschaffen können, so z.B. durch unbemerkten Einbau einer Hintertür oder das "Hacken" des eigenen Systems (ungeachtet dessen, ob sie dies dürfen) ... (Voraussetzung Nr. 2)	10%	8.00%	8%	*Daten zu amtlichen Geschäften werden in lokal betriebenen Geschäftsverwaltungssystemen und Fachapplikationen abgelegt, und nicht in der Cloud. Es ist unseren Mitarbeitern verboten, diese Daten auf Sharepoint oder OneDrive (also in der Cloud) abzulegen. Was hingegen vorkommen kann ist ein Austausch via E-Mail. Für die vorliegende Betrachtung sind daher ausschliesslich Daten relevant, die über Exchange versendet werden. In diesem Falle sind die Mitarbeiter angewiesen, die E-Mails via S/MIME zu verschlüsseln, d.h. der Inhalt der E-Mail wird bereits auf dem Endgerät des Benutzers verschlüsselt und befindet sich somit ausschliesslich verschlüsselt in der Cloud. Auch mit externen Stellen wird in solchen Fällen in der Regel verschlüsselt kommuniziert (End-to-End). In der Cloud selbst werden alle Daten wiederum verschlüsselt, solange sie nicht gebraucht werden ("data at rest"). Der Schlüssel wird in einer ersten Phase noch von Microsoft verwaltet ("Microsoft managed key"). Später ist angedacht, dass die Schlüssel-Verwaltung durch uns erfolgt ("Bring-you-own-key", "Customer managed key"). Auf diesen Schlüssel erhalten systembedingt in der Regel nur die im Azure Active Directory aufgeführten Benutzer Zugriff. Das Azure Active Directory wird wiederum laufend vom Active Directory Verzeichnisdienst gespiesen und kontrolliert, bei welchem die Masterkopie auf den Rechnern des Kantons Zürich liegt. Dieser letzte Schutz könnte Microsoft technisch gesehen umgehen, die S/MIME-Verschlüsselung hingegen höchstwahrscheinlich nicht, da sie keinen Zugang zu den Schlüsseln verfügt ("Hold-your-own-key").*
	... und dabei in der Lage sind, nach den von der Behörde gewünschten Daten zu suchen, diese zu finden und für sich zu kopieren (Voraussetzung Nr. 4)	80%			*Ein Zugang alleine nutzt nicht; der Provider müsste auch nach den von den Behörden verlangten Daten suchen und diese als solche aus dem System herauskopieren können. Auch wenn die Inhalte der E-Mails mit Geschäftsfalldaten verschlüsselt sind, wäre es jedoch denkbar, dass der Provider von den Behörden verlangte E-Mails aufgrund der Angaben zu den Sendern und Empfängern sowie der Betreffzeile ermitteln könnte (z.B. aufgrund einer vorbekannten Fallnummer in der Betreffzeile). Wir gehen von einer relativ hohen Wahrscheinlichkeit aus, dass eine solche Suche erfolgreich wäre, sollte Microsoft dazu gezwungen sein.*
d)	Wahrscheinlichkeit, dass der Provider, der Subunternehmer bzw. das Mutterhaus sich im Zuständigkeitsbereich der Behörde befindet (Voraussetzung Nr. 4)	100%		100%	*Der Provider behält sich vor, die Dienstleistung auch aus den USA zu erbringen, wo sich die Microsoft Corp. befindet. Damit ist mindestens einer der Subunternehmer des Providers im Zuständigkeitsbereich der US-Behörden und daher grundsätzlich unter dem US CLOUD Act verpflichtet.*

e)	Wahrscheinlichkeit, dass die Behörde trotz bestehender, beschränkter Zugriffsmöglichkeiten und trotz der getroffenen technischen und organisatorischen Gegenmassnahmen[14)] dem Provider, seinem Subunternehmer bzw. dem Mutterhaus befehlen darf, sich Zugang zu den Daten zu verschaffen und ihr diese im Klartext herauszugeben[7)] (Voraussetzung Nr.5)	40%	40%	*Der US CLOUD Act zwingt den Provider nicht, sämtliche technischen Methoden auszuschöpfen, um an von den US-Behörden verlangte Daten zu gelangen. Er ist nur verpflichtet, jene Daten herauszugeben, die in seinem Besitz sind oder welche er kontrolliert ("Custody, Possession, Control"). Insbesondere ist er nicht verpflicht, Zugriffssperren auf seinen Systemen zu umgehen oder Verschlüsselungsschlüssel herauszugeben. Im vorliegenden Fall sind die Daten in einem Schweizer, von einer hiesigen Gesellschaft betriebenen Rechenzentrum gespeichert und somit nicht im Besitz der Microsoft Corp. in den USA. Es ist aber davon auszugehen, dass diese Fernzugriff auf die Daten haben kann. Es ist also zu beurteilen, wie wahrscheinlich dies als "Control" gewertet werden kann. Hierzu gibt es eine ausführliche Praxis in den USA. "Control" kann entweder gegeben sein, wenn im Tagesgeschäft ein faktischer Zugang zu den Daten im Klartext besteht ("day-to-day control"), oder wenn die Gesellschaft selbst Anspruch auf einen Zugang zu den Daten im Klartext hat und zwar nicht bloss für die Zwecke der US-Behörden ("legal control"). Vgl. hierzu die Ausführungen Justin Hemmings, Sreenidhi Srinivasan, Peter Swire, "Defining the Scope of "Possession, Custody or Control" for Privacy Issues and the CLOUD Act, in: Journal of National Security Law & Policy, Januar 2020, abrufbar unter in https://bit.ly/3yFSuQG. Im vorliegenden Fall wird der Kanton Zürich das "Lockbox"-Verfahren einsetzen, in dessen Rahmen sich der Provider verpflichtet, nur dann Zugriff auf die Daten zu nehmen, wenn der Kunde dies erlaubt. Damit kann der Provider (und erst recht Microsoft Corp.) mit guten Gründen vertreten, über keine "legal control" zu verfügen. Aufgrund der S/MIME-Verschlüsselung hat er auch keine "day-to-day control"; er kann mit guten Gründen argumentieren, dass es ihm an einer solchen bereits aufgrund der Microsoft-eigenen Verschlüsselung fehlt, weil diese dafür sorgt, dass im Tagesgeschäft nur die im Azure Active Directory eingetragenen Personen einen Zugang zu unverschlüsselten Daten erhalten, und Support-Zugriffe im Klartext nicht hierzu gehören. Im Azure Active Directory sind wiederum nur Mitarbeiter des Kantons eingetragen. Hinzu kommt, dass Microsoft Corp. nicht der primäre Dienstleister des Kantons ist, sondern Microsoft in Irland; Microsoft Corp. wird nur fallweise beigezogen, was den Grad an Kontrolle weiterhin mindert. Microsoft Corp. ist aufgrund der vereinbarten EU-Standardvertragsklauseln und den weiteren Datenschutzzusagen des Providers zudem verpflichtet, gegen Zugriffe durch US-Behörden rechtlich vorzugehen und diese Argumente vorzubringen. Die von uns geschätzte Wahrscheinlichkeit der erfolgreichen Abwehr eines Herausgabebefehls auf Basis solcher Argumente ist nicht sehr hoch, weil die mit Microsoft verhandelte Vereinbarung nicht in jeder Hinsicht optimal ausgestaltet ist, so namentlich, was die Geheimhaltungspflicht und den Schutz von Daten von juristischen Personen betrifft.*
f)	Wahrscheinlichkeit, dass wenn der ausländischen Behörde Daten herausgegeben würden, dies zur Strafbarkeit von Mitarbeitern des Providers oder eines seiner Subunternehmer führen würde, deren Verfolgung auch möglich und realistisch wäre und dies dazu führt, dass die Daten nicht herausgegeben werden oder nicht herausgegeben werden müssen[8)9)] (Voraussetzung Nr. 6)	85%	15%	*Selbst wenn ein Herausgabebefehl grundsätzlich erteilt werden dürfte, steht einer solchen immer noch Schweizer Recht entgegen: Die Daten befinden sich auf Schweizer Boden, da für die Speicherung die Rechenzentren des Providers in der Schweiz benutzt werden. Das bedeutet zum einen, dass das US-Gericht abwägen müsste, ob die US-Interessen trotzdem eine Herausgabe erfordern (nach unserer Erfahrungen ist dies bei den meisten Herausgabebegehren nicht der Fall). Zum anderen dürfen wir davon ausgehen, dass mindestens die Schweizer Mitarbeiter, die einer Strafbarkeit ausgesetzt sind, sich an das Schweizer Recht halten und die Herausgabe verhindern werden (Vertrauensgrundsatz). Beides zusammen führt zu einer hohen Wahrscheinlichkeit, dass die Herausgabe - falls grundsätzlich genehmigt - an diesen beiden Hürden scheitert. Hinzu kommt noch der Umstand, dass es sich im vorliegenden Fall nicht um Daten eines Privatunternehmens handelt, sondern um Daten eines souveränen ausländischen Staats und die Chancen hoch sind, dass selbst ein US-Gericht einen Herausgabebefehl als völkerrechtswidrig bzw. Verletzung des Grundsatzes der "international comity" erachten würde.*
g)	Wahrscheinlichkeit, dass es dem Unternehmen nicht gelingt, die verlangten Daten rechtzeitig in Sicherheit zu bringen bzw. dem Zugriff des Providers im Klartext zu entziehen (Voraussetzung Nr. 7)	90%	90%	*Es ist möglich, dass wir versuchen werden, Daten in Sicherheit zu bringen, sobald wir von einer Anfrage einer US-Behörde erfahren (z.B. weil die Behörde uns zuerst direkt anfragt). Allerdings ist dies mit gewissen Mühen verbunden und möglicherweise geht es um zu viele Daten. Die Wahrscheinlichkeit, dass wir die Daten rechtzeitig dem Provider entziehen können und so einen Zugriff vereiteln, erachten wir daher als nicht sehr hoch.*

Restrisiko eines erfolgreichen Lawful Access durch eine ausländische Behörde über den Provider (angesichts der Gegenmassnahmen[14)]): 0.44%

Schritt 4: Wahrscheinlichkeit eines Lawful Access durch eine ausländische Massenüberwachung[10)] *(= "Schrems II")*

Für die vorliegende Beurteilung herangezogene Rechtsgrundlage: Section 702 US Foreign Intelligence Surveillance Act (FISA), Executive Order (EO) 12.333

		Wahrscheinlichkeit in der Periode* **			Begründung
a)	Wahrscheinlichkeit, dass die hier relevanten Daten während der Übermittlung an den Provider oder an die Subunternehmer von Telekommunikationsprovidern im betreffenden Land im Rahmen einer Upstream-Überwachung der Internet-Backbones im Klartext eingesehen werden können	0%	0.00%		*Es werden weder von uns noch vom Provider über das Internet Daten in unverschlüsselter Form übermittelt. Daher können unsere Daten im Rahmen der Überwachung der Internet-Backbones durch die US-Nachrichtendienste nicht im Klartext in deren Hände fallen. Ein Lawful Access auf diesem Weg scheidet daher aus.*
b)	Wahrscheinlichkeit, dass die übermittelten Daten Inhalte umfassen, die von den Selektoren (d.h. nachrichtendienstliche Suchbegriffe wie bestimmte Empfänger oder Sender von elektronischer Kommunikation) erfasst werden	0%			*N/A*
c)	Wahrscheinlichkeit, dass der Provider oder ein Subunternehmer im betreffenden Land technisch in der Lage ist, die Daten im Klartext ohne Genehmigung des Kunden laufend nach Selektoren (d.h. nach Suchbegriffen wie bestimmte Empfänger oder Sender von elektronischer Kommunikation) im Rahmen einer Downstream-Überwachung von Online-Kommunikation zu durchsuchen[11)]	40%			*Wir kennen die Software des Providers zwar nicht, aber aufgrund der Verschlüsselung unserer Daten, der Vereinbarung, dass unsere Daten ausschliesslich in Europa gespeichert werden (d.h. von den USA lediglich ein Fernzugriff ohne Speicherung besteht), der Annahme, dass die Software des Providers auf den Rechenzentren in Europa über keine Hintertüren für eine solche Suche verfügt (dies würde gegen europäisches Recht und damit gegen den Vertrag verstossen), dem Umstand, dass auch die Audit-Berichte keine Hinweise auf entsprechende Funktionen enthalten (obwohl sie sicherheitsrelevant wären), gehen wir davon aus, dass es wenig wahrscheinlich ist, dass der Provider mit Bezug auf die hier relevanten Daten technisch in der Lage ist, eine solche Suche mit Bezug auf unsere Daten durchzuführen (einschliesslich laufender Entschlüsselung der Daten). Eine solche Suche wäre nur dann möglich, wenn - der Provider hierzu seine Software anpassen würde, was zwar grundsätzlich möglich wäre, aber in solchen Konstellationen nicht verlangt wird und technisch kaum unbemerkt möglich wäre (auch für die Prüfgesellschaften). Dann aber könnte sofort reagiert werden, da diese Überwachung nicht kundenspezifisch und grundsätzlich zukunftsgerichtet ist. - der Provider hierzu seine Verträge anpasst, um sich nicht dem Vorwurf der Vertragsverletzung auszusetzen, wovon auszugehen ist; er rechnet in unserem Fall offenbar auch nicht mit der Möglichkeit des Zugriffs, sonst hätte er seine Verträge anders abgefasst. Trotzdem sind wir hier vorsichtigerweise von einem sehr hohen Wert ausgegangen. Hinzu kommt in diesem spezifischen Fall, dass die Inhalte der E-Mails in Bezug auf Geschäftsfalldaten mittels S/MIME so verschlüsselt sein werden, dass der Provider diese gar nicht im Klartext lesen kann. Nicht verschlüsselt wären Angaben zum Betreff, zum Sender und Empfänger. Es könnte somit herausgefunden werden, wer mit wem kommuniziert, nicht jedoch der Inhalt. Auch mit den von Geschäftsfällen betroffenen Personen (und deren Anwälten oder sonstigen Stellvertretern) kommunizieren wir nur ausnahmsweise und nur mit deren Einwilligung per E-Mail. Auch diese Kommunikation erfolgt von unserer Seite her in aller Regel verschlüsselt. Trotzdem sind wir hier vorsichtigerweise von einem eher hohen Wert ausgegangen.*
d)	Wahrscheinlichkeit, dass der Provider oder ein Subunternehmer im betreffenden Land verpflichtet werden kann, eine solche Suche (auch) in den Daten des Unternehmens durchzuführen[12)]	30%	0.60%	0.60%	*Es sprechen gemäss unserer Analyse mehrere Punkte dagegen, dass der Provider nach US-Recht zu solchen Suchläufen in Bezug auf unsere Daten verpflichtet werden kann: - Erstens wird der in den USA ansässige Subunternehmer des Providers zwar als Electronic Communications Service Provider gelten und daher an sich Adressat solcher Befehle sein können. Es ist jedoch fraglich, ob er auch in Bezug auf seine Tätigkeit für das Unternehmen ein ECSP ist, da seine Aufgabe weder die Bereitstellung von Speicherplatz, noch die Bearbeitung von Daten noch die Ermöglichung von Kommunikation umfasst, sondern lediglich das Lösen bestimmter technischer Probleme, z.B. in Supportfällen. Die Gesellschaft, welche uns diese Dienste erbringt, hat ihren Sitz in Europa und ist daher nicht im Zuständigkeitsbereich der US-Behörden. In Europa (und nur dort) sind auch unsere hier relevanten Daten gespeichert. - Zweitens befinden sich unsere Daten auch nicht unter der Kontrolle des in den USA ansässigen Subunternehmers, was eine weitere Voraussetzung für die Pflicht zur Durchführung solcher Suchläufe ist. Wir verweisen auf die obigen Ausführungen. Der Provider wäre auch nicht befugt, Kopien der relevanten Daten in den USA auf dem Rechner des US-Subunternehmens zu speichern, damit sie unter seiner Kontrolle wären und durchsucht werden könnten, was aber Voraussetzung für die Durchführung einer Suche wäre. Der Provider garantiert in seinen Vertragsbedingungen ferner, den US-Behörden selbst keinen direkten Zugriff zu gewähren. - Drittens besteht eine hohe Wahrscheinlichkeit, dass die dem US-Subunternehmer allenfalls zugänglichen Daten per se von einem Zugriff im Rahmen von Section 702 FISA ausgeschlossen sind, da es sich um Daten handelt, die nicht durch ihn, sondern an ihn übermittelt werden, nämlich zur Erbringung einer Support-Dienstleistung. Somit handelt es sich um eine Kommunikation an eine "US Person", für welche die genannten nachrichtendienstlichen Suchläufe untersagt sind (vgl. hierzu die Ausführungen von Alan Charles Raul, "Why Schrems II Might Not Be a Problem for EU-U.S. Data Transfers", 21. Dezember, 2020, abrufbar unter https://bit.ly/3qHNMy7 und in voller Länge vom selben Autor unter https://bit.ly/2V9veez mit einem Nachtrag "Transferring EU Data To US After New Contractual Safeguards" of May 17, 2021, abrufbar unter https://bit.ly/3l12oHZ). - Viertens können unsere Daten auch Daten von "US Persons" enthalten. Da der Provider diese nicht unterscheiden kann, wird ihm der Zugriff auf unsere Daten unter Section 702 FISA auch aus diesem Grund verwehrt sein. - Fünftens hat der Provider, einschliesslich seines US-Subunternehmers, die Standardvertragsklauseln der Europäischen Kommission unterzeichnet und damit zugesichert, dass er selbst nicht der Ansicht ist, dass er im Rahmen von Section 702 FISA (oder EO 12.333) den Nachrichtendiensten Zugang zu unseren Daten gewährleisten muss. Es sind bisher auch keine solchen Fälle in mit unserer Situation vergleichbaren Konstellationen bekannt.*
e)	Wahrscheinlichkeit, dass die Daten Inhalte umfassen, die Gegenstand von nachrichtendienstlichen Suchaufträgen aus dem betreffenden Land sind[13)]	5%			*Wir nutzen einen Service des Providers, wie er ausschliesslich grösseren Unternehmen (und staatlichen Betrieben) für deren interne Zwecke zur Verfügung gestellt wird. Darin kommt zwar Kommunikation vor, doch handelt es sich dabei lediglich um geschäftliche Kommunikation des jeweiligen Unternehmens, mit dessen Bearbeitung der Provider beauftragt wird (im Rahmen einer Auftragsbearbeitung). Diese ist im Gegensatz zu privater Kommunikation via E-Mail und in sozialen Medien (wo der Provider Verantwortlicher ist) gemäss den einschlägigen Quellen nicht das Ziel nachrichtendienstlichen Informationsbeschaffung nach Section 702 FISA oder EO 12.333. Dies wird sowohl durch einen Bericht des Privacy and Civil Liberty Oversight Board (PCLOB) (https://bit.ly/3yeO7us), die Ausführungen der NSA (https://bit.ly/3dFalhk) und die Entscheide des die Zugriffe bewilligenden Foreign Intelligence Surveillance Court (FISC) (2019: https://bit.ly/3heBYQB) bestätigt, welche keinen Hinweis darauf enthalten, dass Corporate-E-Mail-Kommunikation je das Ziel von Suchaufträgen nach Section 702 FISA oder EO 12.333 wären. Auch nach Section 702 FISA geht es nur um Kommunikationsdienste, welche den gesuchten Personen erbracht werden, und nicht anderen (wie im vorliegenden Fall uns). Daher gehen wir davon aus, dass die Wahrscheinlichkeit, dass der Provider mit Bezug auf unsere Daten im Betrachtungszeitraum eine Überwachungsanordnung hat oder erhalten wird, sehr gering ist, selbst wenn er verpflichtet wäre, sie auszuführen.*

Restrisiko eines erfolgreichen Lawful Access durch einen ausländischen Nachrichtendienst ohne Rechtsweggarantie (angesichts der Gegenmassnahmen[14)]): 0.60%

Schritt 5: Gesamtbeurteilung

Wahrscheinlichkeit, dass sich die Frage eines Lawful Access über den Cloud-Provider überhaupt stellt (1 Fall in der Periode = 100%)	31.25%
Wahrscheinlichkeit, dass es in diesen Fällen trotz der Gegenmassnahmen[14)] zu einem erfolgreichen Lawful Access durch die betreffenden ausländischen Behörden kommt	0.44%
Wahrscheinlichkeit, dass es zusätzlich zu einem erfolgreichen Lawful Access durch einen ausländischen Nachrichtendienst ohne Rechtsweggarantie kommt (trotz der Gegenmassnahmen[14)])	0.60%
Gesamtwahrscheinlichkeit eines erfolgreichen Lawful Access über den Cloud-Provider in der Betrachtungsperiode:* **	0.74%
Umschreibung in Worten (basierend auf Hillson****):	Sehr tief
Soviele Jahre braucht es, damit es mit einer Wahrscheinlichkeit von **90 Prozent** mindestens ein Mal zu einem Lawful Access kommt:	1'552
Soviele Jahre braucht es, damit es mit einer Wahrscheinlichkeit von **50 Prozent** mindestens ein Mal zu einem Lawful Access kommt:	467

... unter der Annahme, dass die Wahrscheinlichkeit sich über Zeit weder erhöht noch reduziert (wie bei einem Münzwurf)

** Damit die statistischen Berechnungen stimmen, ist es wichtig, jeden Faktor für einen erfolgreichen Lawful Access nur ein Mal zu berücksichtigen. Beispiel: In Schritt 2 b) wird abgefragt, ob es sich um einen Fall handelt, der eine Behörde im betreffenden Land grundsätzlich berechtigt, die Herausgabe der Daten auch von einem Provider zu verlangen (z.B. weil es sich um die Verfolgung einer schweren Straftat handelt). Dieser Faktor darf darum später bei Schritt 3 e) bei der Frage der Berechtigung zum Lawful Access nicht mehr berücksichtigt werden, sondern nur noch die restlichen Voraussetzungen für einen solchen Zugriff, soweit sie nicht schon bei den vorherigen Fragen berücksichtigt worden sind.*

*** Gemeint ist die probabilistische Wahrscheinlichkeit (probability), nicht die Mutmasslichkeit (likelihood). Im Rahmen der Einschätzung ist also z.B. was folgt zu fragen: Wenn der Fall, den es zu beurteilen gilt, zehn Richtern vorgelegt würde, wieviele davon würden aufgrund der Umstände schätzungsweise davon überzeugt sein, dass die jeweilige Voraussetzung gegeben ist? Sind es lediglich vier von zehn, die voll oder gerade noch überzeugt sind, so beträgt die Wahrscheinlichkeit 40%. Das Resultat der statistischen Berechnungen ist letztendlich nur so gut, wie die Annahmen, die getroffen werden. In einer Risikobeurteilung ist es allerdings üblich, mit Annahmen zu arbeiten, sofern sie sich auf die konkreten Umstände beziehen, denn sie sind in der Regel das Einzige, was zur Verfügung steht. Das ändert sich erst, wenn Erfahrungswerte vorliegen. Es geht vorliegend auch nicht darum vorherzusagen, was tatsächlich wann geschehen wird, sondern nur, was die statistische Wahrscheinlichkeit ist, dass das Ereignis in der Beurteilungsperiode eintritt.*

**** Falls dieser Wert bei 100% oder mehr liegt, ist es statistisch sicher, dass dieser Fall eintritt; die nachfolgenden Berechnungen funktionieren dann nicht mehr; zu dieser Situation kann es kommen, wenn die Zahl der in der Betrachtungsperiode projizierten Fälle so gross ist, dass in mindestens einem Fall es statistisch gesehen zum Lawfull Access kommen muss.*

***** Skala: <5% = "Sehr tief", 5-10% = "Tief", 11-25 = "Mittel", 26-50% = "Hoch" und >50% = "Sehr hoch" (nach David Hillson, 2005, siehe https://www.pmi.org/learning/library/describing-probability-limitations-natural-language-7556).*

1) Unabhängig von der Cloud-Nutzung; es geht um die Frage, wie wahrscheinlich es ist, dass eine ausländische Behörde an die Daten des Unternehmens gelangen möchte (z.B. weil sie ein Strafverfahren gegen einen Kunden des Unternehmens oder eine Untersuchung gegen das Unternehmen selbst führt); es können die Werte für das betreffende Land bzw. die Region definiert werden; es geht hier nur um Verfahren, für welche eine Rechtsweggarantie besteht, d.h. der behördliche Anspruch letztlich einer gerichtlichen Kontrolle unterliegt (für die anderen vgl. Schritt 4).

2) Als Basis bietet sich eine Auswertung der Fälle bei einem Rückblick über denselben Betrachtungszeitraum wie die Risikoeinschätzung an; dabei sollte geprüft werden, ob es Gründe für eine Zunahme oder Abnahme der Wahrscheinlichkeit solcher Fälle für die Zukunft gibt (z.B. bessere technische Schutzmöglichkeiten, mehr Rechte für Behörden); zu berücksichtigen sind ausländische Verfahren sowohl gegen das Unternehmen als auch gegen Personen, über welche das Unternehmen Daten bearbeitet (z.B. Kunden), da beide dazu führen können, dass ausländische Behörden an Daten gelangen wollen.

3) Durch die Geltendmachung von Widerspruchsrechten, die nach dem ausländischen Recht auch für die Behörde verbindlich sind (z.B. ein Legal Privilege, Zeugnisverweigerungsrechte), oder durch Aufzeigen, dass der Herausgabeanspruch der Behörde aus anderen Gründen nicht berechtigt ist (z.B. weil die Forderung zuwenig begründet oder zu ungenau ist); hier sind bisherige Erfahrungswerte besonders wichtig; allerdings sollten hier nicht Aspekte der International Comity berücksichtigt werden (wie z.B. im Schweizer Recht Art. 271 StGB), da dies zu einer Doppelzählung führt, wenn der Ort der Speicherung der Daten diesbezüglich auch bei Voraussetzung Nr. 6 in Schritt 3 berücksichtigt wird.

4) Wo die ausländische Behörde erfolgreich die Amts- oder Rechtshilfe benutzt, können und müssen ihr die Daten geliefert werden und ein Risiko eines Lawful Access über den Provider entfällt naturgemäss in diesen Fällen; dies gilt auch dort, wo ein Unternehmen freiwillig und erlaubterweise die Daten liefert, z.B. weil das Einverständnis der betroffenen Person vorliegt oder diese es sogar verlangt; daher sind auch diese Fälle zu berücksichtigen und abzuziehen.

5) Taterfolg ist ein Herausgabebefehl einer ausländischen Behörde z.B. nach Art. 18 Abs. 1 CCC (oder einer anderen hier berücksichtigten Rechtsgrundlage), welcher zu einer seitens des Unternehmens strafbaren Offenbarung durch den Provider von Kundendaten im Klartext führt.

6) Falls ein Lawful Access aus mehreren Ländern droht, ist die höchste Wahrscheinlichkeit zu wählen, d.h. die Wahrscheinlichkeit für jenes Land, dessen Lawful Access Versuch am wahrscheinlichsten die Voraussetzung erfüllt.

7) Diese Voraussetzung ist i.d.R. dann gegeben, wenn die Behörde zeigen kann, dass die Daten im Klartext "im Besitz" oder "unter der Kontrolle" des Providers sind; ob Kontrolle über die Daten im Klartext besteht, bestimmt sich üblicherweise danach, ob der Provider *im üblichen Geschäftsgang* eine freie Zugriffsmöglichkeit hat ("day-to-day control") oder ob er die Daten herausverlangen kann ("legal control"); ob er zum Zugriff auch rechtlich befugt sein muss, ist umstritten; keine Kontrolle hat hingegen, wer sich ins eigene System "hacken" oder eine Hintertüre einbauen müsste; aus statistischen Gründen dürfen die Ursachen, die zur Reduktion der Eintrittswahrscheinlichkeit der Voraussetzungen Nr. 2-4 und Schritt 2 führen, hier *nicht mehr* gezählt werden; ergibt sich beispielsweise im Rahmen von Voraussetzung Nr. 2, dass aufgrund der technischen Massnahmen die Chance, dass der Provider auf die Daten im Klartext zugreifen kann, 50% ist, dann muss im Rahmen von Voraussetzung Nr. 5 gefragt werden, wie wahrscheinlich ein Gericht vom Provider verlangen wird, dass er die technischen Hindernisse und anderen Gegenmassnahmen (z.B. Zugriffsverbote für Mitarbeiter) überwindet oder ignoriert und die Daten liefert. Für eine Diskussion der Begriffs Besitz, Gewahrsam und Kontrolle im US-Recht siehe zum Beispiel Justin Hemmings, Sreenidhi Srinivasan, Peter Swire, Defining the Scope of "Possession, Custody, or Control" for Privacy Issues and the CLOUD Act, in: Journal of National Security Law & Policy, Vol. 10 No. 3 vom 23. Januar 2020 (https://bit.ly/3i2xfC9). Siehe auch Hogan Lovells' Demystifying the U.S. CLOUD Act: Assessing the law's compatibility with international norms and the GDPR of January 15, 2019 (https://bit.ly/3rLQfbp) mit einer Zusammenfassung der Standards des US-Rechts in Bezug auf den Begriff "Kontrolle".

8) Rechtsgrundlage wäre im Schweizer Recht namentlich die Verletzung von Art. 271 StGB ("Verbotene Handlungen für einen fremden Staat") und Berufsgeheimnispflichten (wie z.B. Art. 321 StGB), denen die Mitarbeiter des Providers oder eines Subunternehmers direkt unterworfen sind; dies hat zwei Folgen: Erstens kann es dazu führen, dass auch nach ausländischem Recht unter Beachtung der International Comity trotz allem nicht geliefert werden muss, und es kann zweitens dazu führen, dass im eigenen Land der Zugriff verhindert bzw. nicht gestattet wird, weil sie die zuständigen Personen (doch) an das Schweizer Recht halten, was nach dem Vertrauensprinzip von ihnen unter gewissen Voraussetzungen auch erwartet werden darf.

9) Die Voraussetzung wurde zur besseren Verständlichkeit umgekehrt formuliert (d.h. die angegebene Voraussetzung trägt dazu bei, dass der Zugriff trotz allem verhindert wird); daher muss der Prozentwert für die Berechnung der Gesamtwahrscheinlichkeit umgekehrt werden; aus statistischen Gründen dürfen die Ursachen, die zur Reduktion der Eintrittswahrscheinlichkeit der Voraussetzung Nr. 5 führen, hier nicht mehr berücksichtigt werden; die International Comity sollte daher z.B. nicht im Rahmen von Voraussetzung Nr. 5 geprüft werden, sondern im Rahmen von Voraussetzung Nr. 6.

10) Dies bezieht sich auf ausländische Gesetze, die eine Massenüberwachung erlauben, z. B. die vor- und nachgelagerte Überwachung von Internet-Backbones, Social-Media-Plattformen und öffentlichen E-Mail-Diensten, wie sie in den USA durch Abschnitt 702 des Foreign Intelligence Surveillance Act (FISA) und Executive Order (EO) 12.333 erlaubt ist. Diese Form des Lawful Access war Gegenstand der Entscheidung "Schrems II" des Europäischen Gerichtshofs vom 16. Juli 2020. Im Gegensatz zu der in Schritt 2 und 3 durchgeführten Analyse ist es nicht möglich, die Anzahl der erfolgreichen ausländischen behördlichen Herausgabebefehle während des Zeitraums einzuschätzen. Da es sich bei der Massenüberwachung um eine Form der fortlaufenden Überwachung handelt, muss beurteilt werden, wie wahrscheinlich es ist, dass die fraglichen Daten überhaupt Gegenstand der Überwachung werden, unabhängig davon, mit wievielen direkten Anfragen das Unternehmen in der Vergangenheit konfrontiert worden ist.

11) Dieser Wert muss grundsätzlich tiefer sein als der Wert im Rahmen von Voraussetzung Nr. 2 und 3 oben, da ein solcher Zugriff einen ständigen, systematischen Zugriff auf alle entsprechenden Inhalte erfordert; es wird dabei zudem in der Regel nicht verlangt, etwaige Verschlüsselungen zu brechen.

12) Im US-Recht setzt dies unter anderem voraus, dass es sich um einen "Electronic Communications Service Provider" handelt; der Begriff wird unter Section 702 FISA breit verstanden. Er umfasst neben klassischen Fernmeldedienstanbietern und Anbietern, die Daten für andere speichern oder verarbeiten (Cloud-Anbieter, E-Mail-Provider, Social Media-Provider), auch alle Unternehmen, welche ihren Benutzern sonst die Möglichkeit verschaffen, elektronische Kommunikation zu senden oder zu empfangen; davon sind theoretisch auch Unternehmen erfasst, welche ihren Mitarbeitern E-Mail-Dienste (wenn auch nur für geschäftliche Zwecke) zur Verfügung stellen; letztere sind allerdings anerkanntermassen nicht das Ziel solcher Suchaufträge (vgl. hierzu die Ausführungen von Alan Charles Raul, "Why Schrems II Might Not Be a Problem for EU-U.S. Data Transfers", 21. Dezember 2020, abrufbar unter https://bit.ly/3qHNMy7 und in voller Länge vom selben Autor unter https://bit.ly/2V9veez mit einem Nachtrag "Transferring EU Data To US After New Contractual Safeguards" vom 17. Mai 2021, abrufbar unter https://bit.ly/3l12oHZ).

13) Im Falle der Section 702 FISA sind das z.B. elektronisch über öffentlich zugängliche Dienste (wie E-Mail-Services für Privatpersonen und Social-Media-Plattformen) unter Dritten kommunizierte Internet-Inhalte.

14) Berücksichtigte Gegenmassnahmen seitens des Unternehmens bzw. des Providers sind:

1 Verschlüsselung der Inhalte sensibler E-Mails (d.h. die Geschäftsfalldaten enthalten) mit S/MIME; Provider hat keinen Zugang zum Schlüssel
2 Verschlüsselung aller Kundendaten "in transit" und "at rest"
3 Der Schlüssel zur Verschlüsselung "at rest" wird in einer ersten Phase in einem von Microsoft betriebenen "Key Vault" gespeichert
4 Der Schlüssel zur Verschlüsselung "at rest" wird in einer zweiten Phase in einem vom Kanton verwalteten "Key Vault" bei Microsoft gespeichert
5 Auf den Schlüssel im Key Vault haben grundsätzlich nur die Personen im Azure Active Directory Zugriff; dieses kontrolliert der Kunde
6 Auf den Schlüssel im Key Vault dürfen Mitarbeiter von Microsoft ohne Erlaubnis des Kunden keinen Zugriff nehmen ("Customer Lockbox")
7 Microsoft benötigt für den Support grundsätzlich keinen Zugriff auf Kundendaten im Klartext (First-Level-Support bleibt beim Kunden)
8 Kündigungsmöglichkeit bei erhöhtem Risiko eines Lawful Access (inkl. Abzug aller Daten ohne Rückbehalt durch den Provider nach der Beendigung);
9 Zusicherung des Providers, dass die Kundendaten nur in der gewählten "Geo" gespeichert werden (hier: Schweiz)
10 Vertraulichkeit aller im Rahmen der Leistungserbringung zur Kenntnis genommen Kundendaten (auch als Controller)
11 Pflicht des Providers, die Kundendaten nicht für eigene Zwecke einzusetzen; vorbehalten bleiben Rechtspflichten
12 Pflicht des Providers, sich gegen Herausgabebefehle gerichtlich soweit sinnvoll möglich zur Wehr zu setzen
13 Standardvertragsklauseln der Europäischen Kommission für Zugriffe aus den USA
14 Auftragsdatenverarbeitungsvertrag (ADV) nach Art. 28 DSGVO
15 Überbindung der Pflichten des Providers auf dessen Subunternehmer
16 Organisatorische Massnahmen beim Provider zur Verhinderung eines Zugriffs auf Kundendaten im Klartext durch den Subunternehmer
17 Organisatorische Massnahmen beim Provider zur Verhinderung eines Zugriffs auf Kundendaten im Klartext durch die Muttergesellschaft
18 Vertragliche Pflicht, Kundendaten auch vor der Muttergesellschaft geheimzuhalten, soweit sie kein Subunternehmer ist
19 Audit-Berichte, welche die Einhaltung der Massnahmen zur Datensicherheit bestätigen

Cloud-Computing: Risikobeurteilung eines Lawful Access durch ausländische Behörden

Template: Version 5.04 (1. September 2021)

Eine Version als DSGVO TIA gibt es hier:

Bogen zur Beurteilung eines einzelnen Lands

Autor: David Rosenthal (www.rosenthal.ch)

(Lizenz: Siehe unten)

Schritt 1: Ausgangslage der Risikobeurteilung definieren

a)	Unternehmen:	**Kanton Zürich**	Datum:	3. und 16. Dezember 2021 (Beurteilungssitzungen), Fassung vom 22. Januar 2022 (+red. Korr.)
b)	Daten, die vor dem Behördenzugriff zu schützen sind und um die es hier geht:	**Normale Daten** (zur Begriffsdefinition vgl. das erläuternde Memorandum)	Mitwirkende:	Hansruedi Born (Amt für Informatik), Tanja Bucher (Staatsanwaltschaft), Stephan Beky (Amt für Informatik, Rechtsdienst), Jörg Ochsner (Amt für Informatik, IT-Sicherheit und Datenschutz), Andreas von Moos (Kantonales Steueramt), Esther Hefti (Staatskanzlei, Rechtsdienst), Philipp Grabher (CISO), Serdar Günal Rütsche (Kantonspolizei Zürich, Cybercrime)
c)	Cloud-Anwendung, mit welcher die Daten bearbeitet werden sollen:[5)]	**M365**	Rechtsberater:	David Rosenthal, Sarah Bischof, VISCHER AG
d)	Betrachtungszeitraum der Risikobeurteilung in Jahren:	**5**	Verantwortlich:	Hansruedi Born
e)	Relevante ausländische Rechtsordnung:	**USA**		

Schritt 2: Wahrscheinlichkeit, dass eine ausländische Behörde Anspruch auf die Daten hat und ihn gegen den Provider durchsetzen will[1)]

		Wahrscheinlichkeit pro Fall* **	Fälle pro Jahr	Fälle verbleibend	Begründung
a)	Anzahl der Fälle pro Jahr, in welchen eine Behörde im Land im Betrachtungszeitraum schätzungsweise versuchen wird, auf dem Rechtsweg an relevante Daten zu gelangen[2)]		10.00		*Grundlage für diese Zahl war (a) der Durchschnittswert aller US-Rechtshilfeersuchen (zum Zweck der strafrechtlichen Beweiserhebung) aus den Jahren 2018-2021 an die Schweiz (78.25) und (b) der Anteil der Fälle, die Daten aus dem Kanton Zürich betreffen (9.25 Fälle, 11.82%). Die Zahlen stammen vom Bundesamt für Justiz (16.12.2021), da solche Rechtshilfeersuchen zentral über diese Stelle eingehen (und nicht direkt beim Kanton Zürich). Von den jährlich eingehenden Rechtshilfeersuchen lehnt das BJ pro Jahr schätzungsweise 1-3 Ersuchen ab. Schätzungsweise werden im Jahr 1-3 (also im Durchschnitt 2) Ersuchen gar nicht gestellt, weil dem U.S. Department of Justice (DoJ), welches in den USA als zentrale Stelle für solche Ersuchen zuständig ist, aufgrund von Vorgesprächen mit dem BJ klar wird, dass sie keine Chance haben. Damit erhöht sich die durchschnittliche Anzahl Fälle pro Jahr, in denen US-Behörden in den Jahren 2018-2021 auf dem Rechtsweg zum Zweck der strafrechtlichen Beweiserhebung versucht haben, Daten von der Schweiz zu erlangen, auf 80.25; die entsprechende Anzahl Fälle, die sich auf Daten des Kantons Zürich bezogen, erhöht sich auf 9.46 (80.25 x 0.1182). Wir gehen davon aus, dass sich diese Werte in Zukunft nicht bzw. nicht massgeblich verändern werden. Wir nehmen daher an, dass US-Behörden im Schnitt in 10 Fällen pro Jahr versuchen werden, über den Rechtsweg zum Zweck der strafrechtlichen Beweiserhebung Daten des Kantons Zürichs zu erlangen. Rechtshilfeersuchen in Zivilsachen wurden hier der Einfachheit halber (entgegen der Fragestellung) bereits auf dieser Stufe nicht mehr berücksichtigt, da der US CLOUD Act hier keine Zugriffe erlaubt. Amtshilfeersuchen wurden aus demselben Grund hier nicht mitgezählt. Soweit sie gewährt werden, stellt sich die Frage des Lawful Access gar nicht erst. Werden sie nicht gewährt, muss auch nach US-Recht zugleich eine (schwerwiegende) Straftat vorliegen, damit ein Lawful Access nach US CLOUD Act möglich ist. Wir erachteten es daher als zielführend, uns von Anfang an auf strafrechtliche Fälle zu fokussieren, hier aber auch jene Fälle zu berücksichtigen, in denen die Schweiz keine Rechtshilfe in Strafsachen gewährt, sei es durch Ablehnung eines Gesuchs, sei es, weil die US-Behörden bereits nach einem informellen Austausch zum Schluss kommen, dass ein Gesuch keine Chance hat. Das sind gemäss BJ nur wenige Fälle. Wir haben die Zahl zusätzlich mehr als aufgerundet.*
b)	Anteil der Fälle, in welchen die Herausgabe der Verfolgung von Fällen dient, die im betreffenden Staat einen Herausgabebefehl grundsätzlich auch gegenüber einem Provider erlauben	5%	0.50		*Bei den für die vorliegende Beurteilung relevanten Daten handelt es sich plangemäss um Daten, die keine Daten aus den einzelnen Geschäftsvorfälle zum Inhalt haben, sondern z.B. sonstige E-Mails zwischen den Mitarbeitern des Kantons Zürich, projektbezogene Dateien und andere geschäftliche und ggf. auch einzelne private Inhalte oder Anfragen von Bürgern, welche diese unverschlüsselt senden. Für Strafverfahren in den USA werden diese Daten in aller Regel nicht relevant sein, und erst recht nicht für schwere Straftaten ("serious crimes"), welche einen Zugriff via US CLOUD Act erlauben. Für ein solches US-Strafverfahren dürften sie nur dann von Interesse sein, wenn dieses Verfahren Mitarbeiter des Kantons Zürich selbst betrifft (z.B. weil die US-Behörden an die Mailbox eines Mitarbeiters XY der kantonalen Verwaltung gelangen wollen, weil sie sich davon Hinweise zur Aufdeckung einer US-Straftat erhoffen). Wird davon ausgegangen, dass im Kanton Zürich derzeit 1.5 Mio. Menschen wohnhaft sind und der Kanton Zürich über rund 35'000 Mitarbeitende verfügt, so ergibt das einen Anteil von 2.3% der Einwohner des Kantons Zürich, die beim Kanton beschäftigt sind. Da nicht anzunehmen ist, dass eine überdurchschnittliche Zahl der US-Strafverfahren diesen Anteil der Bevölkerung betrifft, liegt es hier nahe, höchstens den Wert von 2.3% zu nehmen. Auf einen weiteren Abschlag haben wir verzichtet, da die US-Behörden bei die Mitarbeiter des Kantons betreffenden Fälle annehmen werden, dass deren Daten auf den Systemen des Kantons Zürich sein werden. Immerhin wäre es denkbar, einen weiteren Abschlag vorzunehmen im Hinblick auf den Umstand, dass nicht alle Fälle eine schwere Straftat betreffen werden. Wir haben hier vorsichtigerweise trotzdem den doppelten Wert genommen, um etwaige andere Fallkonstellationen zu berücksichtigen.*
c)	Wahrscheinlichkeit, dass es in den verbleibenden Fällen gelingt, die Behörde nach ihrem eigenen Recht oder sonst von ihrem Vorhaben, an die Daten im Klartext zu gelangen, abzubringen[3)]	0%	0.50		*Wir gehen für vorliegende Zwecke davon aus, dass wir nicht in der Lage sein werden, uns gegen eine Herausgabeforderung nach Massgabe des US-Rechts wehren zu können. Den Umstand, dass eine Herausgabeforderung völkerrechtlich problematisch ist, berücksichtigen wir an dieser Stelle nicht.*
d)	Wahrscheinlichkeit, dass in den verbleibenden Fällen die Daten in der einen oder anderen Weise geliefert werden (z.B. mit Einwilligung oder über Rechts- oder Amtshilfe)[4)]	95%	0.03		*Der Rechtshilfe-Kanal zwischen den USA und der Schweiz ist sehr gut eingespielt und funktioniert. Pro Jahr werden nur schätzungsweise 1-3 Ersuchen abgelehnt; weitere schätzungsweise 1-3 Ersuchen werden nach entsprechenden Vorgesprächen nicht gestellt. Daraus ergibt sich, dass von den oben genannten Fällen im Schnitt etwas über 95% erfolgreich sind und die US-Behörden auf diesem Weg an ihre Daten gelangen. Wir gehen nicht davon aus, dass sich dieser Wert im Betrachtungszeitraum verschlechtern wird, d.h. die US-Behörden werden in weniger als 5 Prozent der Fälle nicht mit entsprechenden Datenlieferungen befriedigt werden können.*
e)	Wahrscheinlichkeit, dass die Behörde in den verbleibenden Fällen die Daten trotzdem für so wichtig erachtet, dass sie einen anderen Weg suchen wird, um an sie heranzukommen	25%	0.01	0.01	*Kommen die US-Behörden auf dem Weg der Rechtshilfe nicht zum Zug, versuchen sie erfahrungsgemäss in der Regel, auf dem Wege eines Zivilverfahrens oder sonst über die beteiligten Personen an die von ihnen gewünschten Daten zu gelangen. Der Weg über den Provider und gestützt auf den US CLOUD Act dauert auch dann, wenn er erfolgreich ist, vergleichsweise lange, weil sich die Provider zur Wehr setzen müssen und werden. Hinzu kommt, dass ein "Angriff" auf die Computersysteme eines souveränen fremden Staats massive politische Konsequenzen nach sich ziehen dürfte, was die Hemmschwelle der US-Behörden zusätzlich hochsetzen dürfte. Wir gehen trotzdem für vorliegende Berechnung vorsichtigerweise davon aus, dass in einem von vier Fällen, in welchen die US-Behörden auf dem Weg der Strafrechtshilfe nicht an die Daten gelangt sind, sie es über den Provider versuchen werden.*
	Anzahl der Fälle pro Jahr, in welchen sich die Frage eines lawful access durch eine ausländische Behörde stellt			0.01	
	Anzahl Fälle im Betrachtungszeitraum			0.03	

Schritt 3: Wahrscheinlichkeit, dass eine ausländische Behörde den Anspruch über den Provider erfolgreich durchsetzt

Für die vorliegende Beurteilung herangezogene Rechtsgrundlage: US CLOUD Act (inklusive Stored Communications Act; der PATRIOT Act ist hingegen in den USA nicht mehr in Kraft)

	Voraussetzung für einen Taterfolg[5)]	Wahrscheinlichkeit pro Fall[6)9)] * **			Begründung
a)	Wahrscheinlichkeit, dass die Behörde um den vom Unternehmen beigezogenen Provider und dessen Subunternehmern weiss (Voraussetzung Nr. 1)	100%		100%	*Es wird allgemein bekannt sein, dass der Kanton Zürich die Cloud von Microsoft benutzt. Daher werden die US-Behörden wissen, von welchem Provider sie die Daten herausverlangen müssen.*
b)	Wahrscheinlichkeit, dass ein Mitarbeiter des Providers oder seiner Subunternehmer während eines Support-Falls Einsicht in Daten im Klartext erhält ... (Voraussetzung Nr. 2)	100%	10.00%		*Wir können zwar bestimmen, in welchen Supportfällen die Mitarbeiter des Providers Zugang zu unseren Daten im Klartext erhalten und werden dies nur wo wirklich nötig erlauben, aber es wird Fälle geben, wo dies im Rahmen eines konkreten Supportfalls nötig ist und vorkommen wird. In diesen Fällen wird der Provider Zugriff auf die Daten in Klartext erhalten*
	... und dabei nach den von der Behörde gewünschten Daten suchen, sie finden und sie für sich kopieren kann (Voraussetzung Nr. 3)	10%			*Wenn der Provider Zugang im Supportfall erhält, erhält er Zugriff auf jene Daten, die für die Behandlung des Supportfalls nötig sind. Er kann dabei nicht einfach nach anderen Daten suchen. Behördenanfragen beziehen sich jedoch immer auf bestimmte Daten. Die Wahrscheinlichkeit, dass die Daten, die der Provider sieht (z.B. Inhalte der Mailbox eines bestimmten Benutzers) gerade jenen entsprechen, die die Behörde zuvor vom Provider herausverlangt hat, ist sehr gering.*
c)	Wahrscheinlichkeit, dass Mitarbeiter des Providers, seiner Subunternehmer oder des Mutterhauses trotz der getroffenen technischen Gegenmassnahmen[14)] rein technisch (auch) ausserhalb eines Support-Falls (z.B. mit Administratorenrechten) Zugriff auf Daten im Klartext nehmen oder sich einen solchen Zugang zu Daten verschaffen können, so z.B. durch unbemerkten Einbau einer Hintertür oder das "Hacken" des eigenen Systems (ungeachtet dessen, ob sie dies dürfen) ... (Voraussetzung Nr. 2)	100%	70.00%	73%	*Unsere Daten werden verschlüsselt abgelegt ("data at rest"). Der Schlüssel wird in einer ersten Phase noch von Microsoft verwaltet ("Microsoft managed key"). Später ist angedacht, dass die Schlüssel-Verwaltung durch uns erfolgt ("Bring-you-own-key", "Customer managed key"). Auf diesen Schlüssel erhalten systembedingt in der Regel nur die im Azure Active Directory aufgeführten Benutzer Zugriff. Das Azure Active Directory wird wiederum laufend vom Active Directory Verzeichnisdienst gespiesen und kontrolliert, bei welchem die Masterkopie auf den Rechnern des Kantons Zürich liegt. Rein technisch kann sich der Provider jedoch jederzeit Zugang zu diesem Schlüssel verschaffen, sei es über seine Administratoren-Zugänge, sei es durch Umgehung von Sicherheitsmechanismen, da die Software von Microsoft selbst stammt. Will der Provider also Zugang zu den Daten im Klartext erhalten, kann er diesen bei diesen Daten auch erhalten.*
	... und dabei in der Lage sind, nach den von der Behörde gewünschten Daten zu suchen, diese zu finden und für sich zu kopieren (Voraussetzung Nr. 4)	70%			*Ein Zugang alleine nutzt nicht; der Provider müsste auch nach den von den Behörden verlangten Daten suchen und diese als solche aus dem System herauskopieren können. Auch hier wird der Provider als Ersteller der Software viele Möglichkeiten haben, allerdings wird er hierzu wohl zusätzlich Programme entwickeln müssen, da solche Suchzugriffe für den Standardbetrieb nicht nötig sind oder aber protokolliert und dadurch für uns (oder andere betroffene Kunden) sichtbar würden. Da Herausgabebefehle konkrete Daten verlangen (z.B. bestimmte Inhalte von Sharepoint-Verzeichnissen oder Mailboxen) und Microsoft nicht unbedingt weiss, wie wir die Daten organisiert haben, erachten wir die Chance, dass sie die erforderlichen Daten lokalisieren kann, zwar für hoch, aber nicht 100%.*
d)	Wahrscheinlichkeit, dass der Provider, der Subunternehmer bzw. das Mutterhaus sich im Zuständigkeitsbereich der Behörde befindet (Voraussetzung Nr. 4)	100%		100%	*Der Provider behält sich vor, die Dienstleistung auch aus den USA zu erbringen, wo sich die Microsoft Corp. befindet. Damit ist mindestens einer der Subunternehmer des Providers im Zuständigkeitsbereich der US-Behörden und daher grundsätzlich unter dem US CLOUD Act verpflichtet.*

e)	Wahrscheinlichkeit, dass die Behörde trotz bestehender, beschränkter Zugriffsmöglichkeiten und trotz der getroffenen technischen und organisatorischen Gegenmassnahmen[14)] dem Provider, seinem Subunternehmer bzw. dem Mutterhaus befehlen darf, sich Zugang zu den Daten zu verschaffen und ihr diese im Klartext herauszugeben[7)] (Voraussetzung Nr.5)	65%	65%	*Der US CLOUD Act zwingt den Provider nicht, sämtliche technischen Methoden auszuschöpfen, um an von den US-Behörden verlangte Daten zu gelangen. Er ist nur verpflichtet, jene Daten herauszugeben, die in seinem Besitz sind oder welche er kontrolliert ("Custody, Possession, Control"). Insbesondere ist er nicht verpflicht, Zugriffssperren auf seinen Systemen zu umgehen oder Verschlüsselungsschlüsselherauszugeben. Im vorliegenden Fall sind die Daten in einem Schweizer, von einer hiesigen Gesellschaft betriebenen Rechenzentrum gespeichert und somit nicht im Besitz der Microsoft Corp. in den USA. Es ist aber davon auszugehen, dass diese Fernzugriff auf die Daten haben kann. Es ist also zu beurteilen, wie wahrscheinlich dies als "Control" gewertet werden kann. Hierzu gibt es eine ausführliche Praxis in den USA. "Control" kann entweder gegeben sein, wenn im Tagesgeschäft ein faktischer Zugang zu den Daten im Klartext besteht ("day-to-day control"), oder wenn die Gesellschaft selbst Anspruch auf einen Zugang zu den Daten im Klartext hat und zwar nicht bloss für die Zwecke der US-Behörden ("legal control"). Vgl. hierzu die Ausführungen Justin Hemmings, Sreenidhi Srinivasan, Peter Swire, "Defining the Scope of "Possession, Custody or Control" for Privacy Issues and the CLOUD Act, in: Journal of National Security Law & Policy, Januar 2020, abrufbar unter in https://bit.ly/3yFSuQG. Im vorliegenden Fall wird der Kanton Zürich das "Lockbox"-Verfahren einsetzen, in dessen Rahmen sich der Provider verpflichtet, nur dann Zugriff auf die Daten zu nehmen, wenn der Kunde dies erlaubt. Damit kann der Provider (und erst recht Microsoft Corp.) mit guten Gründen vertreten, über keine "legal control" zu verfügen. Anders als bei den Geschäftsfalldaten haben wir bei den vorliegenden Daten keinen zusätzlichen S/MIME-Verschlüsselungschutz, weshalb Microsoft bei der Abwehr von Herausgabeforderungen nicht geltend machen kann, die Inhalte seien ohnehin verschlüsselt. Microsoft kann aber mit guten Gründen argumentieren, dass es ihr an der erforderlichen "day-to-day control" bereits aufgrund der Microsoft-eigenen Verschlüsselung fehlt, weil diese dafür sorgt, dass im Tagesgeschäft nur die im Azure Active Directory eingetragenen Personen einen Zugang zu unverschlüsselten Daten erhalten, und Support-Zugriffe im Klartext nicht hierzu gehören. Im Azure Active Directory sind wiederum nur Mitarbeiter des Kantons eingetragen. Hinzu kommt, dass Microsoft Corp. nicht der primäre Dienstleister des Kantons ist, sondern Microsoft in Irland; Microsoft Corp. wird nur fallweise beigezogen, was den Grad an Kontrolle weiter mindert. Microsoft Corp. ist aufgrund der vereinbarten EU-Standardvertragsklauseln und den weiteren Datenschutzzusagen des Providers zudem verpflichtet, gegen Zugriffe durch US-Behörden rechtlich vorzugehen und diese Argumente vorzubringen. Wir gehen trotzdem davon aus, dass Microsoft im Falle einer gerichtlichen Überprüfung eines Herausgabebefehls weniger als vier von zehn US-Richtern überzeugen wird, dass Microsoft Corp. keine "control" über die von uns in der Cloud gespeicherten Klartext-Daten hat. Der Wert ist dabei wegen der fehlenden S/MIME-Verschlüsselung schlechter als bei den Geschäftsfalldaten (der Umstand, dass die nicht normalen Daten weniger häufig nachgefragt werden, ist in Schritt 2 berücksichtigt). Berücksichtigt haben wir auch, dass die mit Microsoft verhandelte Vereinbarung nicht in jeder Hinsicht optimal ausgestaltet ist, so namentlich, was die Geheimhaltungspflicht und den Schutz von Daten von juristischen Personen betrifft.*
f)	Wahrscheinlichkeit, dass wenn der ausländischen Behörde Daten herausgegeben würden, dies zur Strafbarkeit von Mitarbeitern des Providers oder eines seiner Subunternehmer führen würde, deren Verfolgung auch möglich und realistisch wäre und dies dazu führt, dass die Daten nicht herausgegeben werden oder nicht herausgegeben werden müssen[8)9)] (Voraussetzung Nr. 6)	85%	15%	*Selbst wenn ein Herausgabebefehl grundsätzlich erteilt werden dürfte, steht einer solchen immer noch Schweizer Recht entgegen: Die Daten befinden sich auf Schweizer Boden, da für die Speicherung die Rechenzentren des Providers in der Schweiz benutzt werden. Das bedeutet zum einen, dass das US-Gericht abwägen müsste, ob die US-Interessen trotzdem eine Herausgabe erfordern (nach unserer Erfahrungen ist dies bei den meisten Herausgabebegehren nicht der Fall). Zum anderen dürfen wir davon ausgehen, dass mindestens die Schweizer Mitarbeiter, die einer Strafbarkeit ausgesetzt sind, sich an das Schweizer Recht halten und die Herausgabe verhindern werden (Vertrauensgrundsatz). Beides zusammen führt zu einer hohen Wahrscheinlichkeit, dass die Herausgabe - falls grundsätzlich genehmigt - an diesen beiden Hürden scheitert. Hinzu kommt noch der Umstand, das es sich im vorliegenden Fall nicht um Daten eines Privatunternehmens handelt, sondern um Daten eines souveränen ausländischen Staats und die Chancen hoch sind, dass selbst ein US-Gericht einen Herausgabebefehl als völkerrechtswidrig bzw. Verletzung des Grundsatzes der "international comity" erachten würde.*
g)	Wahrscheinlichkeit, dass es dem Unternehmen nicht gelingt, die verlangten Daten rechtzeitig in Sicherheit zu bringen bzw. dem Zugriff des Providers im Klartext zu entziehen (Voraussetzung Nr. 7)	90%	90%	*Es ist möglich, dass wir versuchen werden, Daten in Sicherheit zu bringen, sobald wir von einer Anfrage einer US-Behörde erfahren (z.B. weil die Behörde uns zuerst direkt anfragt). Allerdings ist dies mit gewissen Mühen verbunden und möglicherweise geht es um zu viele Daten. Die Wahrscheinlichkeit, dass wir die Daten rechtzeitig dem Provider entziehen können und so einen Zugriff vereiteln, erachten wir daher als nicht sehr hoch.*

Restrisiko eines erfolgreichen Lawful Access durch eine ausländische Behörde über den Provider (angesichts der Gegenmassnahmen[14)]): 6.41%

Schritt 4: Wahrscheinlichkeit eines Lawful Access durch eine ausländische Massenüberwachung[10)] *(= "Schrems II")*

Für die vorliegende Beurteilung herangezogene Rechtsgrundlage: Section 702 US Foreign Intelligence Surveillance Act (FISA), Executive Order (EO) 12.333

		Wahrscheinlichkeit in der Periode* **			Begründung
a)	Wahrscheinlichkeit, dass die hier relevanten Daten während der Übermittlung an den Provider oder an die Subunternehmer von Telekommunikationsprovidern im betreffenden Land im Rahmen einer Upstream-Überwachung der Internet-Backbones im Klartext eingesehen werden können	0%	0.00%		*Es werden weder von uns noch vom Provider über das Internet Daten in unverschlüsselter Form übermittelt. Daher können unsere Daten im Rahmen der Überwachung der Internet-Backbones durch die US-Nachrichtendienste nicht im Klartext in deren Hände fallen. Ein Lawful Access auf diesem Weg scheidet daher aus.*
b)	Wahrscheinlichkeit, dass die übermittelten Daten Inhalte umfassen, die von den Selektoren (d.h. nachrichtendienstliche Suchbegriffe wie bestimmte Empfänger oder Sender von elektronischer Kommunikation) erfasst werden	0%			*N/A*
c)	Wahrscheinlichkeit, dass der Provider oder ein Subunternehmer im betreffenden Land technisch in der Lage ist, die Daten im Klartext ohne Genehmigung des Kunden laufend nach Selektoren (d.h. nach Suchbegriffen wie bestimmte Empfänger oder Sender von elektronischer Kommunikation) im Rahmen einer Downstream-Überwachung von Online-Kommunikation zu durchsuchen[11)]	50%			*Wir kennen die Software des Providers zwar nicht, aber aufgrund der Verschlüsselung unserer Daten, der Vereinbarung, dass unsere Daten ausschliesslich in Europa gespeichert werden (d.h. von den USA lediglich ein Fernzugriff ohne Speicherung besteht), der Annahme, dass die Software des Providers auf den Rechenzentren in Europa über keine Hintertüren für eine solche Suche verfügt (dies würde gegen europäisches Recht und damit gegen den Vertrag verstossen), dem Umstand, dass auch die Audit-Berichte keine Hinweise auf entsprechende Funktionen enthalten (obwohl sie sicherheitsrelevant wären), gehen wir davon aus, dass es wenig wahrscheinlich ist, dass der Provider mit Bezug auf die hier relevanten Daten technisch in der Lage ist, eine solche Suche mit Bezug auf unsere Daten durchzuführen (einschliesslich laufender Entschlüsselung der Daten). Eine solche Suche wäre nur dann möglich, wenn - der Provider hierzu seine Software anpassen würde, was zwar grundsätzlich möglich wäre, aber in solchen Konstellationen nicht verlangt wird und technisch kaum unbemerkt möglich wäre (auch für die Prüfgesellschaften). Dann aber könnte sofort reagiert werden, da diese Überwachung nicht kundenspezifisch und grundsätzlich zukunftsgerichtet ist. - der Provider hierzu seine Verträge anpasst, um sich nicht dem Vorwurf der Vertragsverletzung auszusetzen, wovon auszugehen ist; er rechnet in unserem Fall offenbar auch nicht mit der Möglichkeit des Zugriffs, sonst hätte er seine Verträge anders abgefasst. Trotzdem sind wir hier vorsichtigerweise von einem sehr hohen Wert ausgegangen.*
d)	Wahrscheinlichkeit, dass der Provider oder ein Subunternehmer im betreffenden Land verpflichtet werden kann, eine solche Suche (auch) in den Daten des Unternehmens durchzuführen[12)]	30%	0.75%	0.75%	*Es sprechen gemäss unserer Analyse mehrere Punkte dagegen, dass der Provider nach US-Recht zu solchen Suchläufen in Bezug auf unsere Daten verpflichtet werden kann: - Erstens wird der in den USA ansässige Subunternehmer des Providers zwar als Electronic Communications Service Provider gelten und daher an sich Adressat solcher Befehle sein können. Es ist jedoch fraglich, ob er auch in Bezug auf seine Tätigkeit für das Unternehmen ein ECSP ist, da seine Aufgabe weder die Bereitstellung von Speicherplatz, noch die Bearbeitung von Daten noch die Ermöglichung von Kommunikation umfasst, sondern lediglich das Lösen bestimmter technischer Probleme, z.B. in Supportfällen. Die Gesellschaft, welche uns diese Dienste erbringt, hat ihren Sitz in Europa und ist daher nicht im Zuständigkeitsbereich der US-Behörden. Dort (und nur dort) sind auch unsere hier relevanten Daten gespeichert. - Zweitens befinden sich unsere Daten auch nicht unter der Kontrolle des in den USA ansässigen Subunternehmers, was eine weitere Voraussetzung für die Pflicht zur Durchführung solcher Suchläufe ist. Wir verweisen auf die obigen Ausführungen. Der Provider wäre auch nicht befugt, Kopien der relevanten Daten in den USA auf dem Rechner des US-Subunternehmens zu speichern, damit sie unter seiner Kontrolle wären und durchsucht werden könnten, was aber Voraussetzung für die Durchführung einer Suche wäre. Der Provider garantiert in seinen Vertragsbedingungen ferner, den US-Behörden selbst keinen direkten Zugriff zu gewähren. - Drittens besteht eine hohe Wahrscheinlichkeit, dass die dem US-Subunternehmer allenfalls zugänglichen Daten per se von einem Zugriff im Rahmen von Section 702 FISA ausgeschlossen sind, da es sich um Daten handelt, die nicht durch ihn, sondern an ihn übermittelt werden, nämlich zur Erbringung einer Support-Dienstleistung. Somit handelt es sich um eine Kommunikation an eine "US Person", für welche die genannten nachrichtendienstlichen Suchläufe n untersagt sind (vgl. hierzu die Ausführungen von Alan Charles Raul, "Why Schrems II Might Not Be a Problem for EU-U.S. Data Transfers", 21. Dezember, 2020, abrufbar unter https://bit.ly/3qHNMy7 und in voller Länge vom selben Autor unter https://bit.ly/2V9veez mit einem Nachtrag "Transferring EU Data To US After New Contractual Safeguards" of May 17, 2021, abrufbar unter https://bit.ly/3l12oHZ). - Viertens können unsere Daten auch Daten von "US Persons" enthalten. Da der Provider diese nicht unterscheiden kann, wird ihm der Zugriff auf unsere Daten unter Section 702 FISA auch aus diesem Grund verwehrt sein. - Fünftens hat der Provider, einschliesslich seines US-Subunternehmers, die Standardvertragsklauseln der Europäischen Kommission unterzeichnet und damit zugesichert, dass er selbst nicht der Ansicht ist, dass er im Rahmen von Section 702 FISA (oder EO 12.333) den Nachrichtendiensten Zugang zu unseren Daten gewährleisten muss. Es sind bisher auch keine solchen Fälle in mit unserer Situation vergleichbaren Konstellationen bekannt.*
e)	Wahrscheinlichkeit, dass die Daten Inhalte umfassen, die Gegenstand von nachrichtendienstlichen Suchaufträgen aus dem betreffenden Land sind[13)]	5%			*Wir nutzen einen Service des Providers, wie er ausschliesslich grösseren Unternehmen (und staatlichen Betrieben) für deren internen Zwecke zur Verfügung gestellt wird. Darin kommt zwar Kommunikation vor, doch handelt es sich dabei lediglich um geschäftliche Kommunikation des jeweiligen Unternehmens, mit dessen Bearbeitung der Provider beauftragt wird (im Rahmen einer Auftragsbearbeitung). Diese ist im Gegensatz zu privater Kommunikation via E-Mail und in sozialen Medien (wo der Provider Verantwortlicher ist) gemäss den einschlägigen Quellen nicht das Ziel nachrichtendienstlichen Informationsbeschaffung nach Section 702 FISA oder EO 12.333. Dies wird sowohl durch einen Bericht des Privacy and Civil Liberty Oversight Board (PCLOB) (https://bit.ly/3yeO7us), die Ausführungen der NSA (https://bit.ly/3dFalhk) und die Entscheide des die Zugriffe bewilligenden Foreign Intelligence Surveillance Court (FISC) (2019: https://bit.ly/3heBYQB) bestätigt, welche keinen Hinweis darauf enthalten, dass Corporate-E-Mail-Kommunikation je das Ziel von Suchaufträgen nach Section 702 FISA oder EO 12.333 wären. Auch nach Section 702 FISA geht es nur um Kommunikationsdienste, welche den gesuchten Personen erbracht werden, und nicht anderen (wie im vorliegenden Fall uns). Daher gehen wir davon aus, dass die Wahrscheinlichkeit, dass der Provider mit Bezug auf unsere Daten im Betrachtungszeitraum eine Überwachungsanordnung hat oder erhalten wird, sehr gering ist, selbst wenn er verpflichtet wäre, sie auszuführen.*

Restrisiko eines erfolgreichen Lawful Access durch einen ausländischen Nachrichtendienst ohne Rechtsweggarantie (angesichts der Gegenmassnahmen[14)]): 0.75%

Schritt 5: Gesamtbeurteilung

Wahrscheinlichkeit, dass sich die Frage eines Lawful Access über den Cloud-Provider überhaupt stellt (1 Fall in der Periode = 100%)	3.13%
Wahrscheinlichkeit, dass es in diesen Fällen trotz der Gegenmassnahmen[14)] zu einem erfolgreichen Lawful Access durch die betreffenden ausländischen Behörden kommt	6.41%
Wahrscheinlichkeit, dass es zusätzlich zu einem erfolgreichen Lawful Access durch einen ausländischen Nachrichtendienst ohne Rechtsweggarantie kommt (trotz der Gegenmassnahmen[14)])	0.75%
Gesamtwahrscheinlichkeit eines erfolgreichen Lawful Access über den Cloud-Provider in der Betrachtungsperiode:* **	0.95%
Umschreibung in Worten (basierend auf Hillson****):	Sehr tief
Soviele Jahre braucht es, damit es mit einer Wahrscheinlichkeit von **90 Prozent** mindestens ein Mal zu einem Lawful Access kommt:	1’206
Soviele Jahre braucht es, damit es mit einer Wahrscheinlichkeit von **50 Prozent** mindestens ein Mal zu einem Lawful Access kommt:	363

... unter der Annahme, dass die Wahrscheinlichkeit sich über Zeit weder erhöht noch reduziert (wie bei einem Münzwurf)

** Damit die statistischen Berechnungen stimmen, ist es wichtig, jeden Faktor für einen erfolgreichen Lawful Access nur ein Mal zu berücksichtigen. Beispiel: In Schritt 2 b) wird abgefragt, ob es sich um einen Fall handelt, der eine Behörde im betreffenden Land grundsätzlich berechtigt, die Herausgabe der Daten auch von einem Provider zu verlangen (z.B. weil es sich um die Verfolgung einer schweren Straftat handelt). Dieser Faktor darf darum später bei Schritt 3 e) bei der Frage der Berechtigung zum Lawful Access nicht mehr berücksichtigt werden, sondern nur noch die restlichen Voraussetzungen für einen solchen Zugriff, soweit sie nicht schon bei den vorherigen Fragen berücksichtigt worden sind.*

*** Gemeint ist die probabilistische Wahrscheinlichkeit (probability), nicht die Mutmasslichkeit (likelihood). Im Rahmen der Einschätzung ist also z.B. was folgt zu fragen: Wenn der Fall, den es zu beurteilen gilt, zehn Richtern vorgelegt würde, wieviele davon würden aufgrund der Umstände schätzungsweise davon überzeugt sein, dass die jeweilige Voraussetzung gegeben ist? Sind es lediglich vier von zehn, die voll oder gerade noch überzeugt sind, so beträgt die Wahrscheinlichkeit 40%. Das Resultat der statistischen Berechnungen ist letztendlich nur so gut, wie die Annahmen, die getroffen werden. In einer Risikobeurteilung ist es allerdings üblich, mit Annahmen zu arbeiten, sofern sie sich auf die konkreten Umstände beziehen, denn sie sind in der Regel das Einzige, was zur Verfügung steht. Das ändert sich erst, wenn Erfahrungswerte vorliegen. Es geht vorliegend auch nicht darum vorherzusagen, was tatsächlich wann geschehen wird, sondern nur, was die statistische Wahrscheinlichkeit ist, dass das Ereignis in der Beurteilungsperiode eintritt.*

**** Falls dieser Wert bei 100% oder mehr liegt, ist es statistisch sicher, dass dieser Fall eintritt; die nachfolgenden Berechnungen funktionieren dann nicht mehr; zu dieser Situation kann es kommen, wenn die Zahl der in der Betrachtungsperiode projizierten Fälle so gross ist, dass in mindestens einem Fall es statistisch gesehen zum Lawfull Access kommen muss.*

***** Skala: <5% = "Sehr tief", 5-10% = "Tief", 11-25 = "Mittel", 26-50% = "Hoch" und >50% = "Sehr hoch" (nach David Hillson, 2005, siehe https://www.pmi.org/learning/library/describing-probability-limitations-natural-language-7556).*

[1)] Unabhängig von der Cloud-Nutzung; es geht um die Frage, wie wahrscheinlich es ist, dass eine ausländische Behörde an die Daten des Unternehmens gelangen möchte (z.B. weil sie ein Strafverfahren gegen einen Kunden des Unternehmens oder eine Untersuchung gegen das Unternehmen selbst führt); es können die Werte für das betreffende Land bzw. die Region definiert werden; es geht hier nur um Verfahren, für welche eine Rechtsweggarantie besteht, d.h. der behördliche Anspruch letztlich einer gerichtlichen Kontrolle unterliegt (für die anderen vgl. Schritt 4).

[2)] Als Basis bietet sich eine Auswertung der Fälle bei einem Rückblick über denselben Betrachtungszeitraum wie die Risikoeinschätzung an; dabei sollte geprüft werden, ob es Gründe für eine Zunahme oder Abnahme der Wahrscheinlichkeit solcher Fälle für die Zukunft gibt (z.B. bessere technische Schutzmöglichkeiten, mehr Rechte für Behörden); zu berücksichtigen sind ausländische Verfahren sowohl gegen das Unternehmen als auch gegen Personen, über welche das Unternehmen Daten bearbeitet (z.B. Kunden), da beide dazu führen können, dass ausländische Behörden an Daten gelangen wollen.

[3)] Durch die Geltendmachung von Widerspruchsrechten, die nach dem ausländischen Recht auch für die Behörde verbindlich sind (z.B. ein Legal Privilege, Zeugnisverweigerungsrechte), oder durch Aufzeigen, dass der Herausgabeanspruch der Behörde aus anderen Gründen nicht berechtigt ist (z.B. weil die Forderung zuwenig begründet oder zu ungenau ist); hier sind bisherige Erfahrungswerte besonders wichtig; allerdings sollten hier nicht Aspekte der International Comity berücksichtigt werden (wie z.B. im Schweizer Recht Art. 271 StGB), da dies zu einer Doppelzählung führt, wenn der Ort der Speicherung der Daten diesbezüglich auch bei Voraussetzung Nr. 6 in Schritt 3 berücksichtigt wird.

[4)] Wo die ausländische Behörde erfolgreich die Amts- oder Rechtshilfe benutzt, können und müssen ihr die Daten geliefert werden und ein Risiko eines Lawful Access über den Provider entfällt naturgemäss in diesen Fällen; dies gilt auch dort, wo ein Unternehmen freiwillig und erlaubterweise die Daten liefert, z.B. weil das Einverständnis der betroffenen Person vorliegt oder diese es sogar verlangt; daher sind auch diese Fälle zu berücksichtigen und abzuziehen.

[5)] Taterfolg ist ein Herausgabebefehl einer ausländischen Behörde z.B. nach Art. 18 Abs. 1 CCC (oder einer anderen hier berücksichtigten Rechtsgrundlage), welcher zu einer seitens des Unternehmens strafbaren Offenbarung durch den Provider von Kundendaten im Klartext führt.

[6)] Falls ein Lawful Access aus mehreren Ländern droht, ist die höchste Wahrscheinlichkeit zu wählen, d.h. die Wahrscheinlichkeit für jenes Land, dessen Lawful Access Versuch am wahrscheinlichsten die Voraussetzung erfüllt.

[7)] Diese Voraussetzung ist i.d.R. dann gegeben, wenn die Behörde zeigen kann, dass die Daten im Klartext "im Besitz" oder "unter der Kontrolle" des Providers sind; ob Kontrolle über die Daten im Klartext besteht, bestimmt sich üblicherweise danach, ob der Provider *im üblichen Geschäftsgang* eine freie Zugriffsmöglichkeit hat ("day-to-day control") oder ob er die Daten herausverlangen kann ("legal control"); ob er zum Zugriff auch rechtlich befugt sein muss, ist umstritten; keine Kontrolle hat hingegen, wer sich ins eigene System "hacken" oder eine Hintertüre einbauen müsste; aus statistischen Gründen dürfen die Ursachen, die zur Reduktion der Eintrittswahrscheinlichkeit der Voraussetzungen Nr. 2-4 und Schritt 2 führen, hier *nicht mehr* gezählt werden; ergibt sich beispielsweise im Rahmen von Voraussetzung Nr. 2, dass aufgrund der technischen Massnahmen die Chance, dass der Provider auf die Daten im Klartext zugreifen kann, 50% ist, dann muss im Rahmen von Voraussetzung Nr. 5 gefragt werden, wie wahrscheinlich ein Gericht vom Provider verlangen wird, dass er die technischen Hindernisse und anderen Gegenmassnahmen (z.B. Zugriffsverbote für Mitarbeiter) überwindet oder ignoriert und die Daten liefert. Für eine Diskussion der Begriffs Besitz, Gewahrsam und Kontrolle im US-Recht siehe zum Beispiel Justin Hemmings, Sreenidhi Srinivasan, Peter Swire, Defining the Scope of "Possession, Custody, or Control" for Privacy Issues and the CLOUD Act, in: Journal of National Security Law & Policy, Vol. 10 No. 3 vom 23. Januar 2020 (https://bit.ly/3i2xfC9). Siehe auch Hogan Lovells' Demystifying the U.S. CLOUD Act: Assessing the law's compatibility with international norms and the GDPR of January 15, 2019 (https://bit.ly/3rLQfbp) mit einer Zusammenfassung der Standards des US-Rechts in Bezug auf den Begriff "Kontrolle".

[8)] Rechtsgrundlage wäre im Schweizer Recht namentlich die Verletzung von Art. 271 StGB ("Verbotene Handlungen für einen fremden Staat") und Berufsgeheimnispflichten (wie z.B. Art. 321 StGB), denen die Mitarbeiter des Providers oder eines Subunternehmers direkt unterworfen sind; dies hat zwei Folgen: Erstens kann es dazu führen, dass auch nach ausländischem Recht unter Beachtung der International Comity trotz allem nicht geliefert werden muss, und es kann zweitens dazu führen, dass im eigenen Land der Zugriff verhindert bzw. nicht gestattet wird, weil sie die zuständigen Personen (doch) an das Schweizer Recht halten, was nach dem Vertrauensprinzip von ihnen unter gewissen Voraussetzungen auch erwartet werden darf.

[9)] Die Voraussetzung wurde zur besseren Verständlichkeit umgekehrt formuliert (d.h. die angegebene Voraussetzung trägt dazu bei, dass der Zugriff trotz allem verhindert wird); daher muss der Prozentwert für die Berechnung der Gesamtwahrscheinlichkeit umgekehrt werden; aus statistischen Gründen dürfen die Ursachen, die zur Reduktion der Eintrittswahrscheinlichkeit der Voraussetzung Nr. 5 führen, hier nicht mehr berücksichtigt werden; die International Comity sollte daher z.B. nicht im Rahmen von Voraussetzung Nr. 5 geprüft werden, sondern im Rahmen von Voraussetzung Nr. 6.

[10)] Dies bezieht sich auf ausländische Gesetze, die eine Massenüberwachung erlauben, z. B. die vor- und nachgelagerte Überwachung von Internet-Backbones, Social-Media-Plattformen und öffentlichen E-Mail-Diensten, wie sie in den USA durch Abschnitt 702 des Foreign Intelligence Surveillance Act (FISA) und Executive Order (EO) 12.333 erlaubt ist. Diese Form des Lawful Access war Gegenstand der Entscheidung "Schrems II" des Europäischen Gerichtshofs vom 16. Juli 2020. Im Gegensatz zu der in Schritt 2 und 3 durchgeführten Analyse ist es nicht möglich, die Anzahl der erfolgreichen ausländischen behördlichen Herausgabebefehle während des Zeitraums einzuschätzen. Da es sich bei der Massenüberwachung um eine Form der fortlaufenden Überwachung handelt, muss beurteilt werden, wie wahrscheinlich es ist, dass die fraglichen Daten überhaupt Gegenstand der Überwachung werden, unabhängig davon, mit wievielen direkten Anfragen das Unternehmen in der Vergangenheit konfrontiert worden ist.

[11)] Dieser Wert muss grundsätzlich tiefer sein als der Wert im Rahmen von Voraussetzung Nr. 2 und 3 oben, da ein solcher Zugriff einen ständigen, systematischen Zugriff auf alle entsprechenden Inhalte erfordert; es wird dabei zudem in der Regel nicht verlangt, etwaige Verschlüsselungen zu brechen.

[12)] Im US-Recht setzt dies unter anderem voraus, dass es sich um einen "Electronic Communications Service Provider" handelt; der Begriff wird unter Section 702 FISA breit verstanden. Er umfasst neben klassischen Fernmeldedienstanbietern und Anbietern, die Daten für andere speichern oder verarbeiten (Cloud-Anbieter, E-Mail-Provider, Social Media-Provider), auch alle Unternehmen, welche ihren Benutzern sonst die Möglichkeit verschaffen, elektronische Kommunikation zu senden oder zu empfangen; davon sind theoretisch auch Unternehmen erfasst, welche ihren Mitarbeitern E-Mail-Dienste (wenn auch nur für geschäftliche Zwecke) zur Verfügung stellen; letztere sind allerdings anerkanntermassen nicht das Ziel solcher Suchaufträge (vgl. hierzu die Ausführungen von Alan Charles Raul, "Why Schrems II Might Not Be a Problem for EU-U.S. Data Transfers", 21. Dezember 2020, abrufbar unter https://bit.ly/3qHNMy7 und in voller Länge vom selben Autor unter https://bit.ly/2V9veez mit einem Nachtrag "Transferring EU Data To US After New Contractual Safeguards" vom 17. Mai 2021, abrufbar unter https://bit.ly/3l12oHZ).

[13)] Im Falle der Section 702 FISA sind das z.B. elektronisch über öffentlich zugängliche Dienste (wie E-Mail-Services für Privatpersonen und Social-Media-Plattformen) unter Dritten kommunizierte Internet-Inhalte.

[14)] Berücksichtigte Gegenmassnahmen seitens des Unternehmens bzw. des Providers sind:

~~Verschlüsselung der Inhalte sensibler E-Mails mit S/MIME; Provider hat keinen Zugang zum Schlüssel~~

1 Verschlüsselung aller Kundendaten "in transit" und "at rest"
2 Der Schlüssel zur Verschlüsselung "at rest" wird in einer ersten Phase in einem von Microsoft betriebenen "Key Vault" gespeichert
3 Der Schlüssel zur Verschlüsselung "at rest" wird in einer zweiten Phase in einem vom Kanton verwalteten "Key Vault" bei Microsoft gespeichert
4 Auf den Schlüssel im Key Vault haben grundsätzlich nur die Personen im Azure Active Directory Zugriff; dieses kontrolliert der Kunde
5 Auf den Schlüssel im Key Vault dürfen Mitarbeiter von Microsoft ohne Erlaubnis des Kunden keinen Zugriff nehmen ("Customer Lockbox")
6 Microsoft benötigt für den Support grundsätzlich keinen Zugriff auf Kundendaten im Klartext (First-Level-Support bleibt beim Kunden)
7 Kündigungsmöglichkeit bei erhöhtem Risiko eines Lawful Access (inkl. Abzug aller Daten ohne Rückbehalt durch den Provider nach der Beendigung);
8 Zusicherung des Providers, dass die Kundendaten nur in der gewählten "Geo" gespeichert werden (hier: Schweiz)
9 Vertraulichkeit aller im Rahmen der Leistungserbringung zur Kenntnis genommen Kundendaten (auch als Controller)
10 Pflicht des Providers, die Kundendaten nicht für eigene Zwecke einzusetzen; vorbehalten bleiben Rechtspflichten
11 Pflicht des Providers, sich gegen Herausgabebefehle gerichtlich soweit sinnvoll möglich zur Wehr zu setzen
12 Standardvertragsklauseln der Europäischen Kommission für Zugriffe aus den USA
13 Auftragsdatenverarbeitungsvertrag (ADV) nach Art. 28 DSGVO
14 Überbindung der Pflichten des Providers auf dessen Subunternehmer
15 Organisatorische Massnahmen beim Provider zur Verhinderung eines Zugriffs auf Kundendaten im Klartext durch den Subunternehmer
16 Organisatorische Massnahmen beim Provider zur Verhinderung eines Zugriffs auf Kundendaten im Klartext durch die Muttergesellschaft
17 Vertragliche Pflicht, Kundendaten auch vor der Muttergesellschaft geheimzuhalten, soweit sie kein Subunternehmer ist
18 Audit-Berichte, welche die Einhaltung der Massnahmen zur Datensicherheit bestätigen

VORBEHALT: Diese Tabellenkalkulation und Risikobeurteilungsmethode steht Ihnen ohne jede Gewähr zur Verfügung. Sie nutzen Sie "wie besehen" auf eigenes Risiko, da sie Fehler enthalten kann. Sie steht Ihnen nur für Informationszwecke zur Verfügung und ersetzt keine professionelle Rechtsberatung. Bitte melden Sie mir alle Fehler, die Sie finden, ebenso weiteres Feedback, damit ich die Datei nachführen kann. Diese Tabellenkalkulation und Risikobeurteilungsmethode wurde für das Schweizer Recht entwickelt, mit Fokus auf dem Schutz von berufsgeheimnisgeschützten Daten. Sie kann für ausländische Gesetze angepasst werden. Wenn Sie dies tun möchten, lassen Sie es mich bitte wissen; es wäre schön, wenn zusätzliche Ausgaben für andere Länder und Rechtsordnungen erstellt und gemeinsam genutzt werden könnten. **Ein wissenschaftlicher Aufsatz, welche die Methode diskutiert, ist in deutscher Sprache veröffentlicht worden** (David Rosenthal, Mit Berufsgeheimnissen in die Cloud: So geht es trotz US CLoud Act, in: Jusletter 10. August 2020; ein Nachdruck davon kann unter www.rosenthal.ch heruntergeladen werden). Ich danke all den Berufskollegen, Statistikern und meinen Klienten, die mir bei der Entwicklung dieses Modells geholfen haben!