VISCHER

Amts- und Berufsgeheimnis in der Cloud.

Digitale Kommunikation als Strafbarkeitsrisiko?

David Rosenthal, Partner, VISCHER AG
20. September 2024

Emotional, geprägt von Mythen und Legenden …

Beispiel Datenschutzbeauftragte Kanton Zürich

Risiken und Regeln

Die Cloud ist im Verwaltungsalltag angeko
Viele An
weitere
nung. D
ken der A
anderes

Spezialfall CLOUD Act

Der CLOUD Act ist ein Gesetz der USA. Es ermöglicht bestimmten US-Behörden, amerikanische Unternehmen zu verpflichten, Daten ihrer Kundinnen und Kunden herauszugeben, auch wenn diese Daten nicht in Datenzentren in den USA gespeichert sind. Der CLOUD Act ist ein Gesetz mit extraterritorialer Wirkung. Dieses Verfahren und dieser Zugriff auf Daten sind mit dem Datenschutzrecht und dem übergeordneten schweizerischen Recht nicht vereinbar. Es verstösst gegen den «ordre public» der Schweiz.

dsb datenschutzbeauftragte des kantons zürich

Besondere datenschutzrechtliche Aspekte der Cloud Nutzung – unter Berücksichtigung des «CLOUD Act»

WICHTIG: Dieser Leitfaden ist Teil der datenschutzrechtlichen Ausführungen zur Auslagerung. Er gilt nur unter Berücksichtigung aller Anforderungen, konkretisiert in den Leitfäden Bearbeiten im Auftrag und Verschlüsselung der Daten im Rahmen der Auslagerung. In jedem Fall ist eine Risikobeurteilung vorzunehmen.

		Personendaten / Besondere Personendaten	
		Amtsgeheimnis	Beispielsweise Steuergeheimnis Sozialhilfegeheimnis Berufsgeheimnis
Besondere Voraussetzungen			
		✓	✓
CH Cloud, EU Cloud (DSGVO)		✓	✓
		✓	✗
Standardvertragsklauseln		✗	
		✓	✓
Standardvertragsklauseln mit zusätzlichen Massnahmen		✓[1]	✗
		✗	
Standardvertragsklauseln mit zusätzlichen Massnahmen		✓	✓

[1] Der Auftragnehmer verpflichtet sich, den Schlüssel nur auf explizite Anfrage und nach explizitter Einwilligung des Auftraggebers einzusetzen.

[2] Besondere Personendaten können bei Anwendbarkeit des CLOUD Acts nicht mit einer vertraglichen Absicherung ausgelagert werden. Die Risikobeurteilung und Festlegung von angemessenen organisatorischen und technischen Massnahmen (§ 7 IDG) ergibt, dass in dieser Konstellation eine Verschlüsselung mit Schlüsselmanagement beim öffentlichen Orga n erforderlich ist.

Quellen: datenschutz.ch & DSB ZH TB 2022

Vorgaben Datenschutz

- Öffentlich-rechtliche Organe brauchen eine **Rechtsgrundlage**
- Cloud-Nutzung in der Regel "nur" eine **Auftragsbearbeitung**
  - Keine Einwilligung der betroffenen Personen erforderlich
  - Vorgaben punkto Datensicherheit, Vertrag und Datenexporte
  - Grundsatz der Verhältnismässigkeit: Welche Alternativen gibt es?
  - Betrieb muss weiterhin Kontrolle haben: Ist ein Exit möglich?
  - Keine nicht tragbaren Risiken eingehen: DSFA gemacht?
  - Pflicht zur Transparenz, Informationspflicht
- Betrifft nicht nur **Dritte**, sondern auch **Mitarbeitende**
  - Microsoft will z.B. Mitarbeiterdaten für eigene Zwecke bearbeiten
  - Tools erlauben dem Betrieb die Überwachung von Mitarbeitenden

In der Praxis gut lösbar

Vorgaben Amts- und Berufsgeheimnis

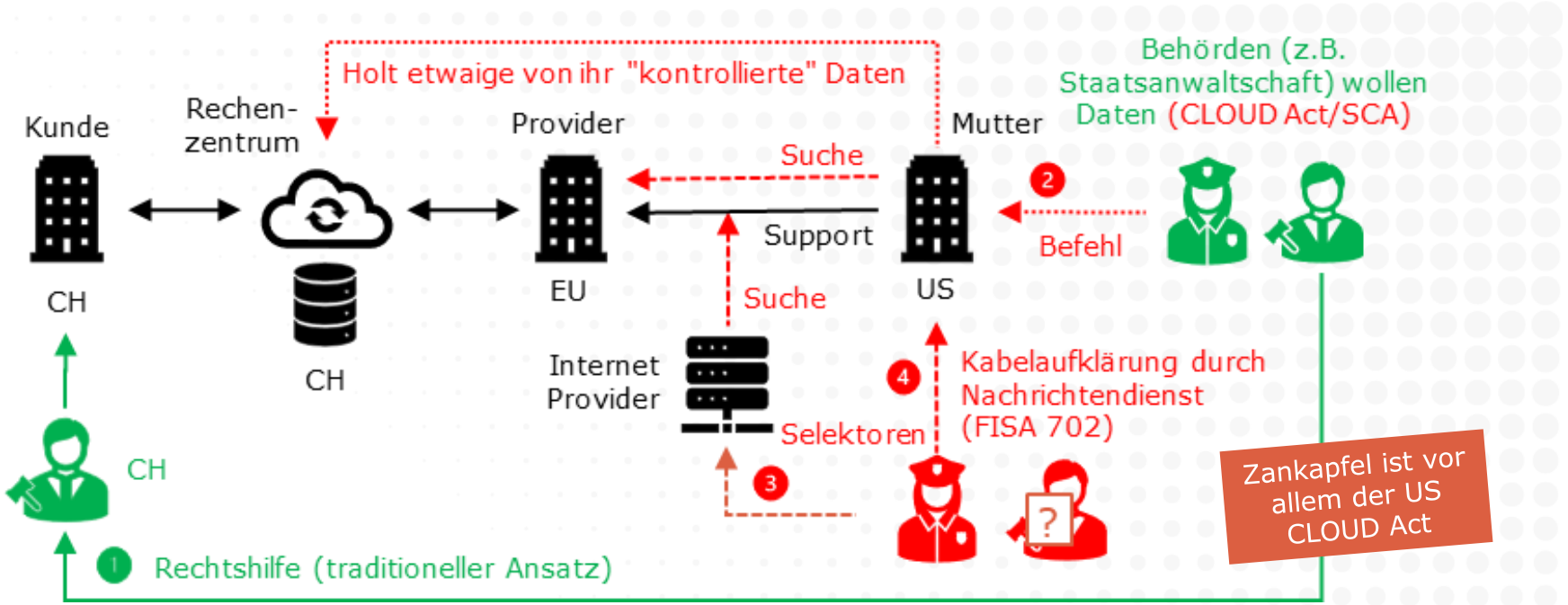
- **Offenbarung** gegenüber Provider vs. ausländischer Behörde
- Fünf **Bedingungen** für den Beizug eines Cloud-Providers
  - Datensicherheit und Verwendungskontrolle sind angemessen
  - Beizug geschäftlich begründet
  - Beizug widerspricht nicht der Erwartung der geschützten Person
  - Beizug verletzt keine gesetzliche oder vertragliche Pflicht
  - Subordinationsverhältnis des Cloud-Providers (BGE 145 II 229)
- **Ergebnis:** Auslagerung ist i.d.R. erlaubt, sofern kein Grund zur Annahme, dass es zum Lawful Access im Ausland kommt
  - Eigennutzung durch Provider ausschliessen; Waiver nicht nötig
  - Strafbarkeit der Hilfsperson im Ausland ist keine Voraussetzung

Art. 320 Abs. 1 StGB seit 2023: "Wer ein Geheimnis offenbart, das ihm in seiner Eigenschaft als Mitglied einer Behörde oder als Beamter anvertraut worden ist oder das er in seiner amtlichen oder dienstlichen Stellung oder als Hilfsperson eines Beamten oder einer Behörde wahrgenommen hat, …"

Vgl. Cloud-Bericht der Bundeskanzlei und mein Aufsatz zum Thema https://bit.ly/2HaEet5 (zur Herleitung)

In der Praxis gut lösbar

Ausländischer Lawful Access?



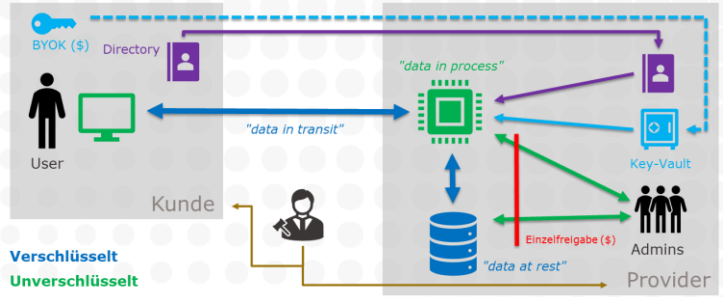
Ausländischer Lawful Access?

BJ/Bundesrat: US Lawful Access-Recht ist nicht ordre public widrig
https://vischerlnk.com/4dXs2WD

	Stored Communications Act (SCA) & US CLOUD Act (letzterer bezüglich der Territorialität)	Abschnitt 702 FISA (innerhalb der USA) EO 12333/EO 14086 (ausserhalb der USA)
Zweck	Aufklärung/Verfolgung von "schweren Straftaten"	Schutz der nationalen Sicherheit, Untersuchung von Verbrechen (FBI)
Art des Lawful Access	Einmaliger gezielter Zugriff auf spezifische Kundendaten bei einem US-Provider	Kontinuierliche Suche in Kontobeständen der US-Provider nach IDs von Zielpersonen (Zufallstreffer)
Vom Lawful Access betroffen	Verdächtiger einer Straftat, an einer solchen Straftat beteiligte Personen	Zielpersonen der US-Nachrichtendienste (ca. 200k) + Personen, die mit ihnen kommunizieren
Vereinbarkeit mit europäischem Recht	✓ Art. 18(1) Übereinkommen über Computerkriminalität	✗ EuGH 16.7.2020 C-311/18 "Schrems II" ✓ Angemessenheitsbeschluss der Europäischen Kommission und des Bundesrates wg. EO 14086
Vergleichbare Regelung Schweiz	Art. 265 StPO (Territorialität: z.B. BGE 143 IV 270)	Art. 39 ff. NDG ("Kabelaufklärung")
Zu prüfen nach Art. 16 DSG	Nein	Seit 15. September 2024: Nein
Zu prüfen bei Berufs-/Amtsgeheimnis	Ja	Ja
Bewertungsmethode	"Cloud-Computing: Risikobeurteilung eines Lawful Access durch ausländische Behörden" (aka "Methode Rosenthal")	"EU SCC Transfer Impact Assessment (TIA)" (auch im linken Formular enthalten)

Dann verschlüsseln wir doch einfach alles!

- Wird von einzelnen (realitätsfremden) **Datenschutzbehörden** noch verlangt
  - Für die meisten Anwendungen untauglicher Ansatz, weil der "Computer in der Cloud" mit den Daten ja im Klartext arbeiten soll …
- Wesentlich ist, dass die **Kontrolle** über den Schlüssel grundsätzlich beim Kunden bleibt
  - Der Kunde definiert über sein Benutzerverzeichnis, wer für welche Daten den Schlüssel erhält
  - Der Schlüssel lagert jedoch im Rechenzentrum des Providers
  - Zugriffe durch Providerpersonal wird vertraglich und technisch eingeschränkt, können aber i.d.R. nicht ausgeschlossen werden



Setup von M365

Welche besonderen Massnahmen treffen?

- Verschlüsselung von Daten (MPIP*, CMK, nicht BYOK, DKE/E2E)
- Europäische Gegenpartei (z.B. Microsoft Ireland Operations)
- Datenhaltung (und ggf. Bearbeitung) in der Schweiz
- Manuelle Provider-Zugriffe einschränken ("Customer Lockbox")
- Vertraulichkeitsverpflichtung, Defend-your-data-Klausel
- Schutzmassnahmen für Personendaten gelten für alle Inhalte
- Einschränkung der Bearbeitung für eigene Providerzwecke, inklusive Abuse Monitoring (z.B. bei KI-Services)
- Nutzungsrichtlinien (Umgang mit Amts-/Berufsgeheimnissen)

Massnahmen gegen Lawful Access aus dem Ausland (US CLOUD Act)

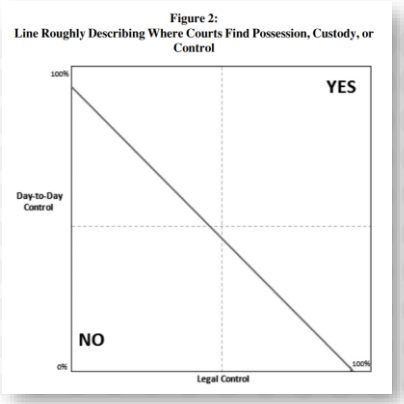
… nebst den üblichen Massnahmen zur Informationssicherheit

* Beim Verkehr von Strafverfolgungsbehörden mit Parteien und deren Vertretern ggf. ein Problem wg. Des Trackings und der technischen Voraussetzungen

Wie wirken die Massnahmen (USA)?

- Zugriff durch **Abhören**?
  - Wir verschlüsseln Daten "in-transit"
- Zugriff durch **Herausgabebefehl**?
  - Fehlende Zuständigkeit über europäische Tochtergesellschaften
  - Fehlende Kundenbeziehung des US-Providers
  - Grundsatz "possession, custody, control"
  - Grundsatz der "International Comity"
- Es braucht kein Executive Agreement!
  - Cloud-Gutachten **Schefer/Glass** fehlerhaft

Dazu: https://www.rosenthal.ch/downloads/Rosenthal_Cloud-Gutachten-Replik.pdf



Quelle: 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, January 23, 2020 (https://bit.ly/3i2xfC9).

Technical ability exists where the third-party grants the subpoenaed party access to the data, there is an underlying agreement that restricts use but not access, there is a mechanism for accessing the data, and there is a historical pattern of regularly accessing the data during normal daily operations (SEC v. Strauss, 2009 WL 3459204, at *8 (S.D.N.Y. Oct. 28, 2009).

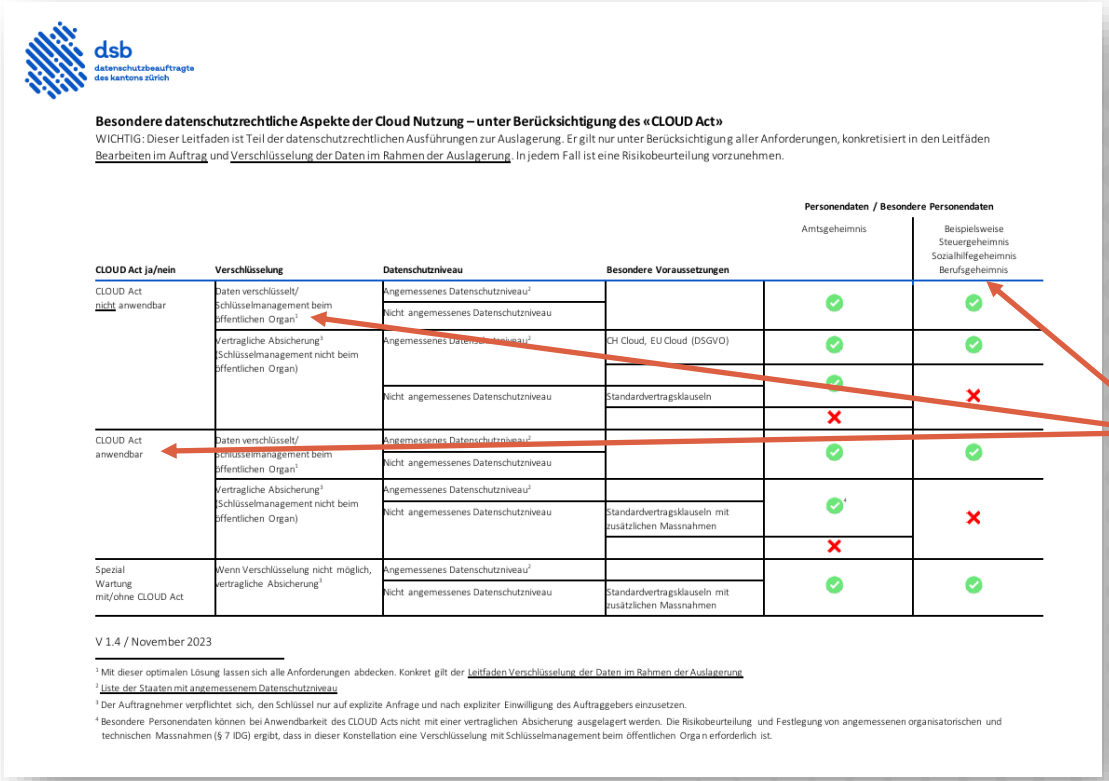
Technical ability does not exist where the entities do not make their information routinely accessible to one another, only provide as much access as necessary to assist with a specific task, do not have software designed to permit access, and have never provided documents to each other before (Nortel Networks, 2004 WL 2149111, at *3).

Beurteilung mit "Methode Rosenthal"

Input: Bisherige Erfahrungen mit Anfragen ausländischer Behörden, technische und organisatorische Massnahmen

55			
56	**Schritt 5: Gesamtbeurteilung**		
57			
58	Wahrscheinlichkeit, dass sich die Frage eines Lawful Access über den Cloud-Provider überhaupt stellt (1 Fall in der Periode = 100%)		6.25%
59	Wahrscheinlichkeit, dass es in diesen Fällen trotz der Gegenmassnahmen[14)] zu einem erfolgreichen Lawful Access durch die betreffenden ausländischen Behörden kommt		2.84%
60	Wahrscheinlichkeit, dass es zusätzlich zu einem erfolgreichen Lawful Access durch einen ausländischen Nachrichtendienst ohne Rechtsweggarantie kommt (trotz der Gegenmassnahmen[14)])		0.40%
61			
62	**Gesamtwahrscheinlichkeit eines erfolgreichen Lawful Access über den Cloud-Provider in der Betrachtungsperiode:***		0.58%
63			
64	Umschreibung in Worten (basierend auf Hillson****):	Sehr tief	
65			
66	Soviele Jahre braucht es, damit es mit einer Wahrscheinlichkeit von **90 Prozent** mindestens ein Mal zu einem Lawful Access kommt:		1'988
67	Soviele Jahre braucht es, damit es mit einer Wahrscheinlichkeit von **50 Prozent** mindestens ein Mal zu einem Lawful Access kommt:		598
68	*… unter der Annahme, dass die Wahrscheinlichkeit sich über Zeit weder erhöht noch reduziert (wie bei einem Münzwurf)*		

Excel: https://vischerlnk.com/flara; FAQ: https://vischerlnk.com/flarafaq
Vgl. auch den Beitrag unter https://bit.ly/2HaEet5 und Anhang unter https://bit.ly/2H8MyZY.



dsb
datenschutzbeauftragte
des kantons zürich

Besondere datenschutzrechtliche Aspekte der Cloud Nutzung – unter Berücksichtigung des «CLOUD Act»

WICHTIG: Dieser Leitfaden ist Teil der datenschutzrechtlichen Ausführungen zur Auslagerung. Er gilt nur unter Berücksichtigung aller Anforderungen, konkretisiert in den Leitfäden Bearbeiten im Auftrag und Verschlüsselung der Daten im Rahmen der Auslagerung. In jedem Fall ist eine Risikobeurteilung vorzunehmen.

				Personendaten / Besondere Personendaten	
				Amtsgeheimnis	Beispielsweise Steuergeheimnis Sozialhilfegeheimnis Berufsgeheimnis
CLOUD Act ja/nein	**Verschlüsselung**	**Datenschutzniveau**	**Besondere Voraussetzungen**		
CLOUD Act nicht anwendbar	Daten verschlüsselt/ Schlüsselmanagement beim öffentlichen Organ[1]	Angemessenes Datenschutzniveau[2]		✓	✓
		Nicht angemessenes Datenschutzniveau			
	Vertragliche Absicherung[3] (Schlüsselmanagement nicht beim öffentlichen Organ)	Angemessenes Datenschutzniveau[2]	CH Cloud, EU Cloud (DSGVO)	✓	✓
		Nicht angemessenes Datenschutzniveau	Standardvertragsklauseln	✓	✗
				✗	
CLOUD Act anwendbar	Daten verschlüsselt/ Schlüsselmanagement beim öffentlichen Organ[1]	Angemessenes Datenschutzniveau[2]			
		Nicht angemessenes Datenschutzniveau		✓	✓
	Vertragliche Absicherung[3] (Schlüsselmanagement nicht beim öffentlichen Organ)	Angemessenes Datenschutzniveau[2]			
		Nicht angemessenes Datenschutzniveau	Standardvertragsklauseln mit zusätzlichen Massnahmen	✓[4]	✗
				✗	
Spezial Wartung mit/ohne CLOUD Act	Wenn Verschlüsselung nicht möglich, vertragliche Absicherung[3]	Angemessenes Datenschutzniveau[2]			
		Nicht angemessenes Datenschutzniveau	Standardvertragsklauseln mit zusätzlichen Massnahmen	✓	✓

V 1.4 / November 2023

[1] Mit dieser optimalen Lösung lassen sich alle Anforderungen abdecken. Konkret gilt der Leitfaden Verschlüsselung der Daten im Rahmen der Auslagerung

[2] Liste der Staaten mit angemessenem Datenschutzniveau

[3] Der Auftragnehmer verpflichtet sich, den Schlüssel nur auf explizite Anfrage und nach expliziter Einwilligung des Auftraggebers einzusetzen.

[4] Besondere Personendaten können bei Anwendbarkeit des CLOUD Acts nicht mit einer vertraglichen Absicherung ausgelagert werden. Die Risikobeurteilung und Festlegung von angemessenen organisatorischen und technischen Massnahmen (§ 7 IDG) ergibt, dass in dieser Konstellation eine Verschlüsselung mit Schlüsselmanagement beim öffentlichen Orga n erforderlich ist.

Solche Unterscheidungen sind rechtlich und praktisch unbegründet …

- "Besonderes" Amtsgeheimnis?
- Schlüssel*management* entscheidend und nicht wer den Schlüssel hat?
- CLOUD Act anders behandeln?

Quelle: datenschutz.ch (DSB ZH)

Ein (total) verunglückter Regelungsversuch …

C. Digitaler Arbeitsplatz

Informationsbearbeitung durch Dritte im Rahmen des digitalen Arbeitsplatzes

§ 17. [1] Das öffentliche Organ kann die Bearbeitung von Informationen in Anwendungen des digitalen Arbeitsplatzes an Anbieterinnen von cloudbasierten Informatikdienstleistungen übertragen, wenn sich deren Rechenzentren in der Schweiz oder in der Europäischen Union befinden, und wenn:

a. das öffentliche Organ besondere Personendaten sowie vertrauliche oder der Geheimhaltung unterliegende Informationen auch gegenüber der Cloud-Anbieterin wirksam verschlüsselt, so dass die Cloud-Anbieterin darauf nicht ohne Mitwirkung des öffentlichen Organs zugreifen kann und

b. das öffentliche Organ die sonstigen Informationen durch alle zumutbaren organisatorischen, technischen und vertraglichen Massnahmen schützt und das verbleibende Risiko einer Bekanntgabe insbesondere angesichts der Bedeutung der Informationen, des Zwecks und der Art und Weise ihrer Bearbeitung sowie der Grundrechte der betroffenen Personen vertretbar ist.

[2] Im Übrigen gelten die Bestimmungen des Gesetzes über die Information und den Datenschutz.

Mit dem Erfordernis einer End-to-End-Verschlüsselung ist der Beizug eines IT-Dienstleisters für ganz viele Anwendungen ausgeschlossen – auch bei Schweizer Anbietern

Warum soll bei an sich erlaubtem Auslandsbezug nur die EU zulässig sein?

Was ist "Cloud"? Wir sprechen hier von einer ganz normalen IT-Auslagerung – warum soll da alles anderes sein? Speziell ist nur der Auslandsbezug!

Vorentwurf Gesetz über digitale Basisdienste, Kanton Zürich

Zum risikobasierten Ansatz und der Beurteilung mit "Methode Rosenthal"

Staatsanwaltschaft des Kantons Basel-Stadt

- Die Bedenken bezüglich einer strafrechtlichen Verantwortlichkeit beschränkt sich mit Blick auf das geplante Outsourcing in die Microsoft Cloud, gemäss Ihren Angaben, auf die Frage des "Lawful Access" ausländischer Behörden auf die geheimnisgeschützten Daten. Im Vordergrund steht dabei die Gefahr eines Zugriffs US-amerikanischer Behörden auf Grundlage des US Cloud Acts. Dieser Einschätzung kann aus Sicht der Staatsanwaltschaft zugestimmt werden.

- Die Berechnung des Risikos eines ausländischen "Lawful Access" erscheint nach Ansicht der Staatsanwaltschaft grundsätzlich ein geeignetes Kriterium, um die Vertretbarkeit der Auslagerung auch vor einem strafrechtlichen Hintergrund zu beurteilen. Eine Überprüfung des Ergebnisses im konkreten Fall ist der Staatsanwaltschaft indes nicht möglich, da dieses letztlich von den Einschätzungen der einzelnen Berechnungsfaktoren abhängt. Diese können von aussen nicht überprüft werden.

Schefer/Glass: Alternativlos

Bundeskanzlei: "Gute Praxis"

Kanton Zürich: "Standard"

In der Praxis breit benutzt

Auszug aus: Schreiben der Staatsanwaltschaft Basel-Stadt nach einem Workshop zur Berechnung des Risikos eines ausländischen Behördenzugriffs im Kontext eines Cloud-Projekts des Basler USB/UKBB

Was konkret tun?

ANWALTSPRAXIS / PRATIQUE DU BARREAU

M365 IN DER ANWALTSKANZLEI: SO GEHT ES

DAVID ROSENTHAL
lic. iur., Partner bei VISCHER, Lehrbeauftragter ETH Zürich und Universität Basel

Stichworte: Cloud, Berufsgeheimnis, Datenschutz, Outsourcing, Risikomanagement

Wenn Schweizer Anwaltskanzleien M365 – das Office-Cloud-Angebot von Microsoft – für sich nutzen wollten, fehlte es lange Zeit an den erforderlichen Verträgen. Diese sind nun verfügbar. Worauf aus Sicht des Berufsgeheimnisses und Datenschutzes beim Einsatz zu achten ist, beschreiben wir in diesem Beitrag.

M365 ist die Abkürzung für «Microsoft 365», eine Sammlung von Office-Anwendungen, Cloud-Diensten und weiteren Funktionen, die von Microsoft angeboten werden. M365 kann komplett online eingesetzt werden, aber am gebräuchlichsten ist ein Mix: Der Mailserver (*Exchange Online*), die Speicherlaufwerke (*SharePoint Online, OneDrive*) und Kommunikation und Kollaboration (*Teams, Forms, Power-Automate*) werden in der Cloud betrieben, die eigentlichen Office-Anwendungen (*wie Word, Excel und PowerPoint*) laufen lokal installiert, auch wenn ein Zugriff via Internet möglich wäre. Eine Telefonzentrale kann mit *Teams* ebenfalls abgelöst werden, allerdings gilt die Sprachqualität nicht als überragend. Andere Anwendungen (z. B. *Yammer* oder *Viva*) werden hierzulande meistens nicht benutzt.

Lokal betrieben wird auch das Herzstück jeder Installation, das *Active Directory*: Es ist die Datenbank der Benutzer und der Zugriffsberechtigungen. Eine Kopie davon wird in die Cloud repliziert (als *Azure Active Directory*), damit die Microsoft-Server den Zugriff auf die Anwendungen und die Schlüssel für die Verschlüsselung steuern können, aber die Kontrolle darüber bleibt beim Kunden. Das ist ein wichtiges Sicherheitselement.

I. Die richtigen Verträge

Nicht nur die Dienstleistungen eines grossen Cloud-Anbieters wie Microsoft ändern sich ständig, auch seine Verträge. Im Auftrag des SAV haben wir vor einiger Zeit begonnen, die vertraglichen Absicherungen zum Schutz des Berufs- und Amtsgeheimnisses, die wir für den Finanzsektor und die öffentliche Hand verhandeln konnten, auch für die Anwaltschaft zugänglich zu machen.[1] Ein Rahmenvertrag schied als Möglichkeit aus. Darum musste Microsoft davon überzeugt werden, ihre Standardverträge für KMU und speziell Berufsgeheimnisträger entsprechend anzupassen, weil eine individuelle Verhandlung von Vertragsklauseln in diesem Segment kaum möglich ist; vertrieben wird die Software über Vertriebspartner. Die letzte solche Anpassung erfolgte – mit einem Jahr Verzögerung – im April 2023, sodass jetzt ein Set an Vertragszusätzen vorliegt, das eine aus Sicht des Datenschutzes und Berufsgeheimnisses zufriedenstellende Absicherung bietet, übrigens nicht nur für Anwaltskanzleien, sondern zum Beispiel auch für Arztpraxen.

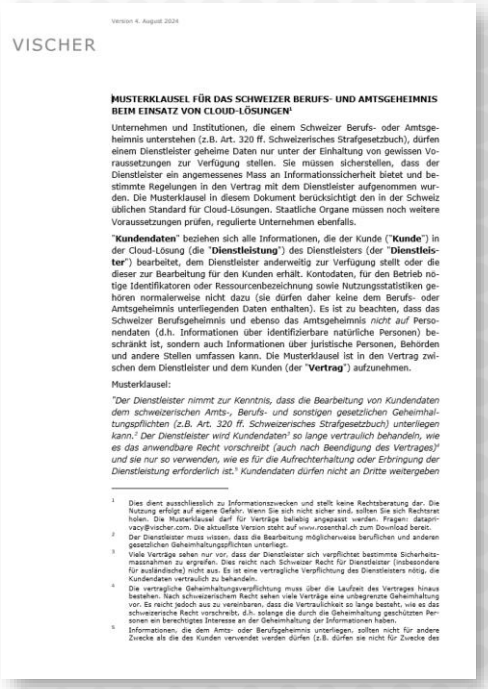
Konkret sollte eine Anwaltskanzlei folgenden Vertrag mit folgenden Vertragszusätzen abschliessen, wenn sie M365 einsetzen will (*wir empfehlen jeweils die englischen Fassungen, da die deutschen Fassungen teilweise Übersetzungsfehler aufweisen*):

- **Microsoft Customer Agreement (MCA)**[2] Dies ist der Hauptvertrag, der die allgemeinen Geschäftsbedingungen für die Nutzung der Cloud-Dienste von Microsoft festlegt. Er enthält u. a. die Regelung zur Haftung und die Geheimhaltungspflicht. Aber: Dieser Vertrag wird nicht mit Microsoft Schweiz, sondern Microsoft Ireland Operations Ltd. abgeschlossen und untersteht irischem Recht und dem Gerichtsstand Irland. Das ist bei Microsoft der Standard.
- **Data Protection Addendum (DPA),** vom Januar 2023 oder später.[3] Das ist ein Zusatz zum MCA, der die spezifischen Datenschutzbestimmungen enthält. Er beschreibt unter anderem die Rolle von Microsoft als Auftragsverarbeiter, die technischen und organisatorischen Massnahmen zum Schutz der Daten, die Unterauftragsverar-

1 Vgl. den früheren Bericht: DAVID ROSENTHAL, Microsoft-Cloud für Schweizer Anwälte, in: Anwaltsrevue 10/2020 (https://anwaltsrevue.recht.ch/de/artikel/02anr/02anr/microsoft-cloud-fur-schweizer-anwalte, https://www.rosenthal.ch/downloads/Rosenthal-Anwalte-Cloud.pdf).
2 https://www.microsoft.com/licensing/docs/customeragreement.
3 https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA.

1. Zuverlässigen Cloud-Provider ermitteln
2. Informationssicherheit prüfen (lassen)
3. Verträge mit Zusätzen zum Schutz des Amts- und Berufsgeheimnisses abschliessen
4. Schutzmassnahmen treffen bzw. aktivieren
5. Risikobeurteilung ("FLARA") vornehmen
6. Nutzungsregeln erlassen
7. Im Auge behalten

vischerlnk.com/4ck2J0L



Version 4. August 2024

VISCHER

MUSTERKLAUSEL FÜR DAS SCHWEIZER BERUFS- UND AMTSGEHEIMNIS BEIM EINSATZ VON CLOUD-LÖSUNGEN[1]

Unternehmen und Institutionen, die einem Schweizer Berufs- oder Amtsgeheimnis unterstehen (z.B. Art. 320 ff. Schweizerisches Strafgesetzbuch), dürfen einem Dienstleister geheime Daten nur unter der Einhaltung von gewissen Voraussetzungen zur Verfügung stellen. Sie müssen sicherstellen, dass der Dienstleister ein angemessenes Mass an Informationssicherheit bietet und bestimmte Regelungen in den Vertrag mit dem Dienstleister aufgenommen wurden. Die Musterklausel in diesem Dokument berücksichtigt den in der Schweiz üblichen Standard für Cloud-Lösungen. Staatliche Organe müssen noch weitere Voraussetzungen prüfen, regulierte Unternehmen ebenfalls.

"**Kundendaten**" beziehen sich alle Informationen, die der Kunde ("**Kunde**") in der Cloud-Lösung (die "**Dienstleistung**") des Dienstleisters (der "**Dienstleister**") bearbeitet, dem Dienstleister anderweitig zur Verfügung stellt oder die dieser zur Bearbeitung für den Kunden erhält. Kontodaten, für den Betrieb nötige Identifikatoren oder Ressourcenbezeichnung sowie Nutzungsstatistiken gehören normalerweise nicht dazu (sie dürfen daher keine dem Berufs- oder Amtsgeheimnis unterliegenden Daten enthalten). Es ist zu beachten, dass das Schweizer Berufsgeheimnis und ebenso das Amtsgeheimnis *nicht auf* Personendaten (d.h. Informationen über identifizierbare natürliche Personen) beschränkt ist, sondern auch Informationen über juristische Personen, Behörden und andere Stellen umfassen kann. Die Musterklausel ist in den Vertrag zwischen dem Dienstleister und dem Kunden (der "**Vertrag**") aufzunehmen.

Musterklausel:

"Der Dienstleister nimmt zur Kenntnis, dass die Bearbeitung von Kundendaten dem schweizerischen Amts-, Berufs- und sonstigen gesetzlichen Geheimhaltungspflichten (z.B. Art. 320 ff. Schweizerisches Strafgesetzbuch) unterliegen kann.[2] Der Dienstleister wird Kundendaten[3] so lange vertraulich behandeln, wie es das anwendbare Recht vorschreibt (auch nach Beendigung des Vertrages)[4] und sie nur so verwenden, wie es für die Aufrechterhaltung oder Erbringung der Dienstleistung erforderlich ist.[5] Kundendaten dürfen nicht an Dritte weitergeben

1 Dies dient ausschliesslich zu Informationszwecken und stellt keine Rechtsberatung dar. Die Nutzung erfolgt auf eigene Gefahr. Wenn Sie sich nicht sicher sind, sollten Sie sich Rechtsrat holen. Die Musterklausel darf für Verträge beliebig angepasst werden. Fragen: dataprivacy@vischer.com. Die aktuellste Version steht auf www.rosenthal.ch zum Download bereit.
2 Der Dienstleister muss wissen, dass die Bearbeitung möglicherweise beruflichen und anderen gesetzlichen Geheimhaltungspflichten unterliegt.
3 Viele Verträge sehen nur vor, dass der Dienstleister sich verpflichtet bestimmte Sicherheitsmassnahmen zu ergreifen. Dies reicht nach Schweizer Recht für Dienstleister (insbesondere für ausländische) nicht aus. Es ist eine vertragliche Verpflichtung des Dienstleisters nötig, die Kundendaten vertraulich zu behandeln.
4 Die vertragliche Geheimhaltungsverpflichtung muss über die Laufzeit des Vertrages hinaus bestehen. Nach schweizerischem Recht sehen viele Verträge eine unbegrenzte Geheimhaltung vor. Es reicht jedoch aus zu vereinbaren, dass die Vertraulichkeit so lange besteht, wie es das schweizerische Recht vorschreibt, d.h. solange die durch die Geheimhaltung geschützten Personen ein berechtigtes Interesse an der Geheimhaltung der Informationen haben.
5 Informationen, die dem Amts- oder Berufsgeheimnis unterliegen, sollten nicht für andere Zwecke als die des Kunden verwendet werden dürfen (z.B. dürfen sie nicht für Zwecke des

vischerlnk.com/3Xfz16e

VISCHER

Danke für Ihre Aufmerksamkeit!

Fragen: david.rosenthal@vischer.com

Zürich
Schützengasse 1
Postfach
8021 Zürich, Schweiz
T +41 58 211 34 00

www.vischer.com

Basel
Aeschenvorstadt 4
Postfach
4010 Basel, Schweiz
T +41 58 211 33 00

Genf
Rue du Cloître 2-4
Postfach
1211 Genf 3, Schweiz
T +41 58 211 35 00

Weitere Infos und Tools:
www.rosenthal.ch