VISCHER

US CLOUD Act:
Warum er Cloud-Projekte nicht verhindern sollte

David Rosenthal
21. Oktober 2020

Keine gute Presse für den US CLOUD Act …

Firmen gehen beim Cloud-Computing unkalkulierbare Risiken ein

Der Zugriff der US-Behörden auf Daten aus
verunsichert Firmen, die Cloud-Computing-
amerikanischen Anbietern einsetzen. Poter
mit dem neuen Datenschutzgesetz der EU.
segmentierten Vorgehen und einer Risikoab

Giorgio V. Müller
17.05.2019, 07.00 Uhr

Hören

Sensible Personendaten bei Behörden

Datenschützer warnen vor Microsoft-Produkt

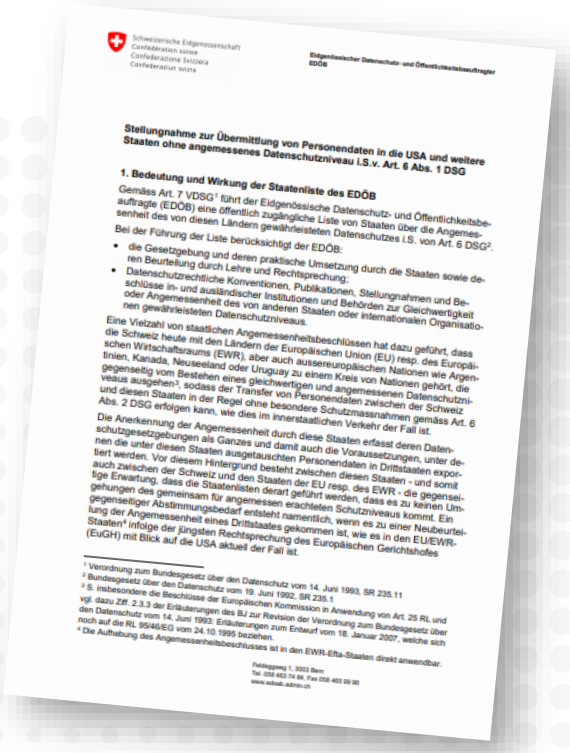
Vertrauliche Angaben über die Schweizer Bevölkerung werden mit den Office-Programmen von Microsoft bearbeitet. Dabei besteht die Gefahr, dass sich US-Behörden Zugriff verschaffen, befürchten die kantonalen Datenschützer.

Quellen: NZZ (oben), Tagesanzeiger (rechts, vom 25.5.2020, https://bit.ly/37ab2Lk)

Und dann kam noch "Schrems II"

b) Bei der Prüfung der datenschutzrechtlichen Risiken ist insbesondere relevant, ob die Daten an ein Unternehmen des nicht gelisteten Staates geliefert werden, das besonderen Zugriffen der dortigen Behörden unterworfen ist[17]. Weiter ist zu prüfen, ob die ausländische Empfängerpartei berechtigt und in der Lage ist, die zur Durchsetzung der schweizerischen Datenschutzgrundsätze nötige Mitwirkung zu leisten. Muss dies verneint werden, laufen die in den Standardvertragsklauseln vorgesehenen Mitwirkungspflichten ins Leere.

c) Der schweizerische Datenexporteur muss in solchen Fällen technische Massnahmen prüfen, die den Behördenzugriff auf die übermittelten Personendaten im Zielland faktisch verhindern. Bei der Datenhaltung im Sinne eines reinen Cloud-Betriebs durch Dienstleister in einem nicht gelisteten Staat wäre z.B. eine Verschlüsselung denkbar, welche nach den Prinzipien BYOK (bring your own key) und BYOE (bring your own encryption) umgesetzt ist, so dass im Zielland keine Klardaten vorliegen und der Dienstleister keine Möglichkeit hat, die Daten selber aufzuschlüsseln. Bei über die reine Datenhaltung hinausgehenden Dienstleistungen im Zielland gestaltet sich der Einsatz solcher technischen Massnahmen indessen als anspruchsvoll. Soweit solche Massnahmen nicht möglich sind, empfiehlt der EDÖB auf die Übermittlung von Personendaten in den nicht gelisteten Staat gestützt auf vertragliche Garantien zu verzichten.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

Stellungnahme zur Übermittlung von Personendaten in die USA und weitere Staaten ohne angemessenes Datenschutzniveau i.S.v. Art. 6 Abs. 1 DSG

1. Bedeutung und Wirkung der Staatenliste des EDÖB

Gemäss Art. 7 VDSG[1] führt der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) eine öffentlich zugängliche Liste von Staaten über die Angemessenheit des von diesen Ländern gewährleisteten Datenschutzes i.S. von Art. 6 DSG[2].

Bei der Führung der Liste berücksichtigt der EDÖB:

- die Gesetzgebung und deren praktische Umsetzung durch die Staaten sowie deren Beurteilung durch Lehre und Rechtsprechung;
- Datenschutzrechtliche Konventionen, Publikationen, Stellungnahmen und Beschlüsse in- und ausländischer Institutionen und Behörden zur Gleichwertigkeit oder Angemessenheit des von anderen Staaten oder internationalen Organisationen gewährleisteten Datenschutzniveaus.

Eine Vielzahl von staatlichen Angemessenheitsbeschlüssen hat dazu geführt, dass die Schweiz heute mit den Ländern der Europäischen Union (EU) resp. des Europäischen Wirtschaftsraums (EWR), aber auch aussereuropäischen Nationen wie Argentinien, Kanada, Neuseeland oder Uruguay zu einem Kreis von Nationen gehört, die gegenseitig vom Bestehen eines gleichwertigen und angemessenen Datenschutzniveaus ausgehen[3], sodass der Transfer von Personendaten zwischen der Schweiz und diesen Staaten in der Regel ohne besondere Schutzmassnahmen gemäss Art. 6 Abs. 2 DSG erfolgen kann, wie dies im innerstaatlichen Verkehr der Fall ist.

Die Anerkennung der Angemessenheit durch diese Staaten erfasst deren Datenschutzgesetzgebungen als Ganzes und damit auch die Voraussetzungen, unter denen die unter diesen Staaten ausgetauschten Personendaten in Drittstaaten exportiert werden. Vor diesem Hintergrund besteht zwischen diesen Staaten - und somit auch zwischen der Schweiz und den Staaten der EU resp. des EWR - die gegenseitige Erwartung, dass die Staatenlisten derart geführt werden, dass es zu keinen Umgehungen des gemeinsam für angemessen erachteten Schutzniveaus kommt. Ein gegenseitiger Abstimmungsbedarf entsteht namentlich, wenn es zu einer Neubeurteilung der Angemessenheit eines Drittstaates gekommen ist, wie es in den EU/EWR-Staaten[4] infolge der jüngsten Rechtsprechung des Europäischen Gerichtshofes (EuGH) mit Blick auf die USA aktuell der Fall ist.

[1] Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993, SR 235.11
[2] Bundesgesetz über den Datenschutz vom 19. Juni 1992, SR 235.1
[3] S. insbesondere die Beschlüsse der Europäischen Kommission in Anwendung von Art. 25 RL und vgl. dazu Ziff. 2.3.3 der Erläuterungen des BJ zur Revision der Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993: Erläuterungen zum Entwurf vom 18. Januar 2007, welche sich noch auf die RL 95/46/EG vom 24.10.1995 beziehen.
[4] Die Aufhebung des Angemessenheitsbeschlusses ist in den EWR-Efta-Staaten direkt anwendbar.

Feldeggweg 1, 3003 Bern
Tel. 058 462 74 84, Fax 058 465 99 96
www.edoeb.admin.ch

Quelle: Eidg. Datenschutz- und Öffentlichkeitsbeauftragter, EDÖB, vom 8. September 2020 (https://bit.ly/3k7rulb)

Das Problem mit der Cloud

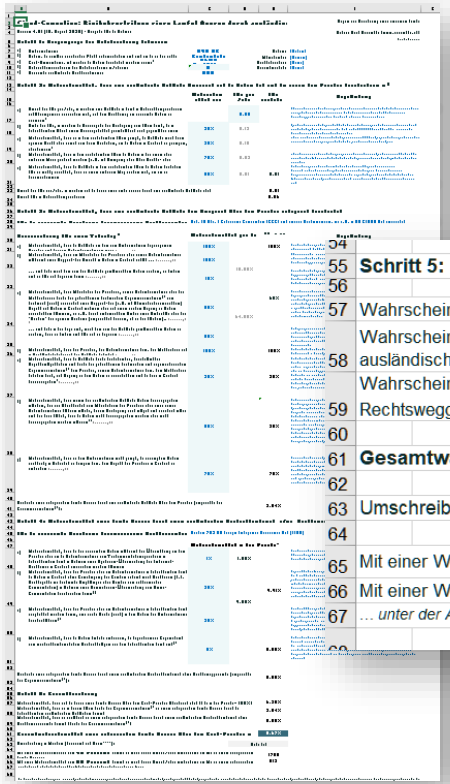
In "Schrems II" ging es dem EuGH zusätzlich um das Problem des nachrichtendienstlichen Zugriffs von US-Behörden auf ausländische E-Mails und Internetübertragungen *ohne* gerichtliche Überprüfung

- Nebst Data Governance, drei **Herausforderungen**
  - Datensicherheit
  - Business Continuity
  - Lawful Access – Schutz vor ausländischen Behörden
- Die ersten zwei können mit technischen und organisatorischen **Massnahmen** gelöst werden, die dritte **nur beschränkt**
  - Befiehlt eine ausländische Behörde einem Provider im Ausland (z.B. Microsoft Corp. oder Microsoft Ireland Operations Ltd.) die Offenlegung von Kundendaten rechtsgültig, muss er dem folgen
  - US CLOUD Act erlaubt US-Behörden in Strafuntersuchungen US-Provider auch dann zur Herausgabe von Daten zu zwingen, wenn diese im Ausland lagern (die Schweiz hat eine analoge Regelung)

Die Lösung?

- Das sagen die **Datenschutzbehörden**
  - Lasst einfach keine Zugriffe aus den USA mehr zu
  - Verschlüsselt die Daten so, dass Provider sie nie lesen kann
- Selbst bei einem **Schweizer RZ** ist beides oft **unrealistisch**
  - Der Provider muss bei vielen Dienst die Daten lesen können
  - Er will seinen Support von ausserhalb erbringen können
- Rechtlich geht es primär um das **Amts- und Berufsgeheimnis**
  - Falls es zur Offenlegung kommt, war sie vorsätzlich verursacht?
  - Vorsatz: Entscheider hält Offenbarung für möglich und findet sich mit einer etwaigen Offenbarung ab ("dann passiert es halt")
- **Wichtig:** Es gibt **nie Null-Risiko** – auch nicht im Datenschutz

Wird am besten in einem interdisziplinären Workshop gemacht



Benötigter Input: Bisherige Anfragen von Behörden, getroffene technische und organisatorische Massnahmen

54		
55	**Schritt 5: Gesamtbeurteilung**	
56		
57	Wahrscheinlichkeit, dass sich die Frage eines Lawful Access über den Cloud-Provider überhaupt stellt (1 Fall in der Periode = 100%)	6.25%
58	Wahrscheinlichkeit, dass es in diesen Fällen trotz der Gegenmassnahmen[14)] zu einem erfolgreichen Lawful Access durch die betreffenden ausländischen Behörden kommt	2.84%
59	Wahrscheinlichkeit, dass es zusätzlich zu einem erfolgreichen Lawful Access durch einen ausländischen Nachrichtendienst ohne Rechtsweggarantie kommt (trotz der Gegenmassnahmen[14)])	0.50%
60		
61	**Gesamtwahrscheinlichkeit eines erfolgreichen Lawful Access über den Cloud-Provider in der Betrachtungsperiode:*** **	0.67%
62		
63	Umschreibung in Worten (basierend auf Hillson****):	Sehr tief
64		
65	Mit einer Wahrscheinlichkeit von **90 Prozent** kommt es nach dieser Anzahl Jahre mindestens ein Mal zu einem erfolgreichen Lawful Access:	1'705
66	Mit einer Wahrscheinlichkeit von **50 Prozent** kommt es nach dieser Anzahl Jahre mindestens ein Mal zu einem erfolgreichen Lawful Access:	513
67	*… unter der Annahme, dass die Wahrscheinlichkeit sich über Zeit weder erhöht noch reduziert (wie bei einem Münzwurf)*	

Excel: https://www.rosenthal.ch/downloads/Rosenthal_Cloud_Lawful_Access_Risk_Assessment.xlsx
Siehe auch den dazugehörigen Beitrag (https://bit.ly/2HaEet5) und Anhang (https://bit.ly/2H8MyZY)

Wie vorgehen?

- **Datensicherheit** und **BCM** konzipieren und festlegen
- **Vertrag** bzw. Vertragsergänzungen mit Provider aushandeln
- **Dokumentation** des Vorhabens und der Risikobeurteilung
  - Beschreibung des Vorhabens (welche Daten wo, wann, wie, etc.)
  - Beurteilung der klassischen Datensicherheits- und BCM-Risiken
  - Beurteilung des Lawful Access-Risikos (Excel)
  - Beurteilung der rechtlichen Vorgaben (Rechtsgrundlage, etc.)
- Staatliche Organe: **Datenschutzbehörde** involvieren
  - Behörde prüft, ob "Hausaufgaben" gemacht → Dokumentation
- **Management-Entscheid** bezüglich Restrisiko

Wie bei jedem Outsourcing-Projekt

Gilt leider auch für Microsoft …

Im neuen DSG: "Datenschutz-Folgenabschätzung"

Haltung und Know-how sehr unterschiedlich je nach Kanton

Normalerweise nicht das Problem

VISCHER

Anmeldung zu Updates unseres **Data & Privacy Blogs** auf www.vischer.com

Vielen Dank für die Aufmerksamkeit!

Fragen: drosenthal@vischer.com

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

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

www.vischer.com

https://bit.ly/3dFX7zL