

## US CLOUD Act: Das Ende des Datenschutzes gegenüber Behörden der USA

Seit rund zwei Jahren liest man immer wieder vom "CLOUD Act". Im Factsheet wird erläutert, um was es geht und in welcher Weise Schweizer Unternehmen betroffen sein können.

### I. Grundsätzliches

#### Kontext und Inhalt des CLOUD Acts

Am 22. März 2018 beschloss der Kongress der Vereinigten Staaten von Amerika (USA) ein Gesetz mit dem Titel "Clarifying Lawful Overseas Use of Data Act" (US CLOUD Act). Das Gesetz hat teilweise auch extraterritoriale Wirkung.

Kernstück des Gesetzes ist die Verpflichtung von Unternehmen in den USA und mit US-Bezug, amerikanischen Sicherheits- und Strafverfolgungsbehörden auch dann Zugriff auf Daten von Nutzern zu geben, wenn diese Daten nicht in den USA gespeichert sind. Hintergrund dieser Regelung war ein amerikanischer Gerichtsfall, in welchem sich Microsoft gegenüber den US-Behörden gegen die Herausgabe von Nutzer-Daten wehrte, welche auf einem Server in Irland gespeichert wurden.

Der CLOUD Act findet Anwendung auf Internet-Unternehmen und IT-Dienstleister, welche Kommunikationsdienstleistungen (electronic communications services) oder Online-Dienstleistungen (remote computing services) anbieten. Der Anwendungsbereich ist gemäss bestehender Praxis in den USA sehr weit und umfasst unter anderem E-Mail-Dienste, Instant-Messaging, Internet-Telefonie, Datenspeicherung und -sicherung, Web-Shops, Hosting sowie Cloud-Anwendungen im engeren Sinn.

Dem Gesetz unterstehen Internet-Unternehmen und IT-Dienstleister mit Sitz in den USA oder mit einem US-Bezug. Ein solcher Bezug zu den USA ist sicher bei Tochter-

gesellschaften von US-Unternehmen anzunehmen. Der Begriff des US-Bezugs ist aber sehr weit und könnte auch Auftragsverarbeiter von US-Unternehmen oder IT-Dienstleister, die in den USA Werbung für ihre Dienstleistungen machen, umfassen. Unklar ist, ob eine Tochtergesellschaft in den USA genügt, damit das Mutterhaus in der Schweiz in den Anwendungsbereich des CLOUD Acts fällt.

#### Praxisbeispiel 1: MailChimp

MailChimp ist ein Cloud-basierter Service zum Management von Newsletter, der von zahlreichen Schweizer Unternehmen für das E-Mail-Marketing eingesetzt wird. Betreiber der Plattform ist ein Unternehmen mit Sitz in den USA. Die von Schweizer Kunden in MailChimp verwalteten Adressen, unterstehen somit dem CLOUD Act.

#### Praxisbeispiel 2: WeTransfer

WeTransfer ist ein Dienst für den Datenaustausch (engl. "file transfer"). Mit Hilfe dieses Dienstes können grosse Dateien versendet werden. Dabei werden die Dateien zunächst in eine Cloud hochgeladen. Der Download-Link kann anschliessend mit anderen Personen per E-Mail geteilt werden. Die Daten werden dabei auf dem Filesharing-Server für einen bestimmten Zeitraum gespeichert. Anschliessend löscht der Anbieter die Dateien wieder aus der Cloud.

Zwar hat WeTransfer seinen Sitz in den Niederlanden, nutzt aber Speicherorte in den USA. Die von Schweizer Kunden mit WeTransfer übertragenen Daten, unterstehen somit dem CLOUD Act.

### **Möglichkeit vertraglicher Erweiterungen**

Der CLOUD Act sieht weiter vor, dass die USA mit ausländischen Staaten bilaterale Regierungsvereinbarungen treffen, die ausländischen Ermittlungsbehörden den Zugriff auf Daten erlauben, die von US-Firmen gespeichert werden. Im Gegenzug sollen die US-Ermittler ebenfalls Zugriff auf Daten haben, die in dem entsprechenden Land gespeichert sind.

Staaten, die mit den USA ein solches Abkommen schliessen, können den Status eines "Qualifying Foreign Governments" erlangen, was sich prozessrechtlich auf IT-Dienstleister in diesem Staat auswirkt. Zur Erlangung dieses Status ist allerdings neben dem Vertragsabschluss die Zustimmung des US Generalanwalts und der Verzicht des US Kongresses auf ein Veto notwendig.

### **Vorerst keine Vereinbarung mit der Schweiz**

Die Schweiz hat bislang mit den USA keine solche Regierungsvereinbarung abgeschlossen. Gemäss Aussagen von Bundesrätin Karin Keller-Sutter während der Frühjahressession 2019 des Schweizer Parlaments wird der Abschluss eines solchen Vertrags im Zusammenhang mit der Umsetzung eines parlamentarischen Vorstosses "geprüft".

Eine solche Regierungsvereinbarung würde ausschliesslich den Schweizer (Strafverfolgungs-)Behörden nützen und würde für die Schweizer Bürgerinnen und Bürger gegenüber den Schweizer Behörden zu einer Schlechterstellung bezüglich des Datenschutzes führen.

### **Bilaterales Abkommen UK – USA**

Am 3. Oktober 2019 haben das Vereinigte Königreich (Grossbritannien; UK) und die USA hinsichtlich des CLOUD Acts eine bilaterale Regierungsvereinbarung abgeschlossen. Grossbritannien musste dazu ein besonderes Gesetz erlassen (UK Crime Overseas Production Orders Act 2019).

Mithin können US-Behörden (einschliesslich des Justizministeriums) mittels Durchsuchungsbefehl direkt bei britischen IT-Unternehmen (Personen-)Daten anfordern, wenn dies zur Prävention, Ermittlung und Strafverfolgung bei schweren Delikten (Strafandrohung über 3 Jahre) erforderlich ist – wobei ein Verdacht genügt. Umgekehrt gilt dies auch für britische Behörden, einschliesslich der Behörde zur Korruptionsbekämpfung (Serious Fraud Office, SFO). Wegen des Brexit fällt ab Ende 2020 der Schutz des europäischen Rechts dahin.

## **II. Folgen für den Datenschutz**

### **Umgehung des Rechtshilfeverfahrens**

Einzige Voraussetzung, dass eine US-Behörde im Anwendungsbereich des CLOUD Acts auf Daten zugreifen darf, ist das Vorliegen eines Durchsuchungs- oder Beschlagnahmefehls. Solche Anordnungen können in den USA neben Gerichten auch zahlreiche Verwaltungsbehörden im Rahmen von Voruntersuchungen oder Verwaltungsstrafverfahren erlassen. Der Durchsuchungs- oder Beschlagnahmefehl kann mit einer Strafandrohung für den Widersetzungsfall verbunden sein. Eine gerichtliche Überprüfung in den USA ist weitestgehend ausgeschlossen, insbesondere so lange als der Sitzstaat des ausländischen Unternehmens keine anerkannte Regierungsvereinbarung mit den USA hat. Das übliche Rechtshilfeverfahren, das dem betroffenen Unternehmen die Anrufung eines Gerichts in seinem Sitzstaat ermöglicht, wird mit dem CLOUD Act umgangen.

Ausserhalb der USA wird die US-Behörde den Zugriff auf die Daten nicht physisch erzwingen können. Mögliche Strafandrohungen und andere Sanktionen können allerdings ein Unternehmen ausserhalb der USA zur Herausgabe der Daten zwingen.

Am Verfahren auf Zugriff zu den Daten sind nur die US-Behörde und das IT-Unternehmen beteiligt. Die in ihren Persön-

lichkeitsrechten betroffenen Personen und Dritte, denen das Recht an den Daten zusteht, erfahren möglicherweise gar nichts vom Zugriff auf die Daten. Somit werden wesentliche grundrechtliche bzw. verfassungsrechtliche Grundsätze des europäischen und schweizerischen Datenschutzrechts verletzt.

### **Keine Ausnahme beim Swiss-US Privacy Shield**

Mit dem Swiss-US-Privacy Shield, einem durch Regierungsvereinbarung geschaffenen Zertifizierungsmechanismus für US-Unternehmen, gelten für die schweizerischen Exporte von Personendaten in die USA die gleichen Standards wie für diejenigen aus der EU; die Übertragung von Personendaten an Unternehmen, die am Privacy Shield teilnehmen, gelten nach überwiegender schweizerischer Rechtsauffassung als Übertragung in einen Staat mit angemessenem Datenschutzniveau.

Der CLOUD Act findet allerdings auch auf US-Unternehmen Anwendung, die nach dem Privacy Shield zertifiziert sind. *Das Privacy Shield bietet somit weder einen erhöhten Schutz vor Zugriffen auf Daten noch bessere verfahrensrechtliche Rahmenbedingungen.*

### **Widerspruch zu EU-Recht und Schweizer Recht**

Der CLOUD Act steht im Widerspruch zu der für den gesamten EU-Raum (bis Ende 2020 zudem auch noch für Grossbritannien) geltenden EU-Datenschutzgrundverordnung (DSGVO): Art. 48 DSGVO lässt die Herausgabe von Personendaten an eine Behörde eines Drittstaats (d.h. eines Staates, der nicht zur EU gehört) nur im Rahmen eines Rechtshilfeverfahrens zu, das sich auf ein Rechtshilfeabkommen stützt. Eine Verletzung von Art. 48 DSGVO kann mit einer Busse bis zu 20 Mio. Euro oder 4 Prozent des weltweit erzielten Jahresumsatzes des fehlbaren Unternehmens sanktioniert werden.

Art. 271 des schweizerischen Strafgesetzbuchs stellt Handlungen für einen fremden Staat unter Strafe. Die Herausgabe von Daten an eine ausländische Behörde ausserhalb der gesetzlichen und völkerrechtlichen Rechtshilfeverfahren erfüllt diesen Tatbestand. Die Datenherausgabe kann zudem in bestimmten Fällen auch eine strafbare Verletzung des Geschäfts- oder Berufsgeheimnisses darstellen.

## **III. Betroffenheit von Schweizer Unternehmen**

### **Schweizer Unternehmen als Dateninhaber**

Schweizer Unternehmen können vom CLOUD Act betroffen sein, weil sie Dienstleistungen von Service Providern nutzen, die dem US-Gesetz unterstehen. Betroffen sein können insbesondere auch Personendaten der Kunden des Schweizer Unternehmens. *Zusicherungen von IT-Dienstleistern in der Schweiz und im EU-Raum, sie würden nicht dem CLOUD Act unterstehen, sind mit Vorsicht zu geniessen.* Die bestehenden Unsicherheiten hinsichtlich des Vollzugs des CLOUD Acts und das Fehlen einer Regierungsvereinbarung für die Schweiz gebieten bei Unternehmen, die heikle Personendaten von Kunden oder Geschäftsgeheimnisse von Drittunternehmen bearbeiten, eine sorgfältige Risikoabwägung bezüglich des CLOUD Acts.

#### **Praxistip:**

#### **Zur Vermeidung von Konflikten wegen des CLOUD Acts:**

- Möglichst nur Dienstleistungen von IT-Anbietern nutzen, die sowohl den Sitz wie alle Server in der Schweiz oder der EU haben und keinen oder einen möglichst geringen US-Bezug aufweisen.
- Insbesondere MailChimp und WeTransfer meiden.
- Wenn Kundendaten mit Diensten eines Anbieters verarbeitet werden, der dem CLOUD Act untersteht, muss dies in der Datenschutzerklärung erwähnt werden.

## Schweizer Unternehmen als Service Provider

Schweizer Unternehmen können vom CLOUD Act betroffen sein, wenn sie entsprechende IT-Dienstleistungen erbringen und einen US-Bezug aufweisen. Sie können in eine unangenehme Konfliktsituation geraten, wenn einerseits eine US-Behörde unter Strafandrohung die Herausgabe von Daten verlangt, andererseits aber das schweizerische Strafrecht – wenn das Unternehmen der DSGVO untersteht, zusätzlich auch Art. 48 DSGVO – diese Datenherausgabe unter Strafandrohung verbieten. Das Unternehmen steht dann praktisch vor der Wahl, die eine oder andere Strafe in Kauf nehmen zu müssen. Diese Situation wird zumindest so lange bestehen, als für die Schweiz keine Regierungsvereinbarung besteht.

In Fällen von *Begehren von US-Behörden auf Datenherausgabe* muss die Person, deren Personendaten betroffen sind, zwingend informiert werden. Wenn die Daten im Auftrag eines anderen Unternehmens bearbeitet werden, muss sichergestellt werden, dass dieses die betroffene Person informiert. Der Konflikt kann allenfalls dadurch gelöst werden, dass die betroffene Person der Herausgabe der Daten zustimmt. Zu prüfen wäre wohl im konkreten Einzelfall, ob nicht doch eine Möglichkeit besteht, die Herausgabe der Daten durch einen Beschluss einer schweizerischen Justizbehörde – zumindest vorläufig – auch gegenüber dem US-Recht wirksam zu verhindern; am einfachsten ginge dies mit einem Gesuch um vorsorgliche Massnahme der betroffenen Person beim zuständigen Zivilgericht.

Zur Vermeidung der Konfliktsituation kann – soweit es sich nicht um besonders schützenswerte Daten handelt – im Dienstleistungsauftrag mit Einzelpersonen vereinbart werden, dass diese präventiv der Datenherausgabe an eine US-Behörde auf der Grundlage eines Durchsuchungs- oder Beschlagnahmungsbefehls und gestützt auf den US CLOUD Act zustimmen.

### Checkliste:

#### Vorgehen bei einem Herausgabebegehren einer US Behörde

Im Falle eines Begehrens einer US-Behörde auf Datenherausgabe gestützt auf den CLOUD Act:

- den Kunden, dessen Daten betroffen sind, informieren und sicherstellen, dass Drittpersonen, deren Personendaten betroffen sind, informiert werden;
- den Kunden bzw. die betroffenen Personen auf die zivilrechtlichen und zivilprozessrechtlichen Möglichkeiten nach schweizerischem Recht hinweisen;
- mit dem Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) Kontakt aufnehmen;
- Rechtsberatung oder Rechtsbeistand beziehen.

### Rechtlicher Hinweis:

Recht ist keine exakte Wissenschaft und stetigem Wandel unterworfen. Der Inhalt des Factsheets wurde mit grosser Sorgfalt erarbeitet, trotzdem muss jede Haftung für den Inhalt abgelehnt werden.

Bitte beachten Sie den Aktualitätsstand des Factsheets.

