Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD

Bundesamt für Justiz BJ

17. September 2021

Bericht zum US CLOUD Act

BJ-D-443E3401/32

Bericht zum US Cloud Act

Inhaltsverzeichnis

Bericht zum US Cloud Act

1 Auftrag

Im März 2018 haben die USA den sogenannten ***C**larifying **L**awful **O**verseas **U**se of **D**ata Act* (nachfolgend *CLOUD Act)*[1] verabschiedet. Er soll den US-Strafverfolgungsbehörden im Bereich der Verhütung, Ermittlung, Aufklärung oder Verfolgung schwerer Straftaten (*serious crimes*) den Zugriff auf Daten ermöglichen, die von Anbietern von Kommunikationsdiensten (*Communication Service Providers*, CSP) mit Sitz in den USA gespeichert worden sind. Dies unabhängig davon, ob die entsprechenden Daten in den USA oder, etwa über Tochtergesellschaften, im Ausland gespeichert sind, was dem US-Gesetz einen extraterritorialen Anwendungsbereich verleiht.[2] Der *CLOUD Act* erlaubt zudem unter bestimmten Bedingungen den Abschluss bilateraler Vollzugsvereinbarungen (*Executive Agreements*) zwischen den USA und anderen Staaten. Damit wird Reziprozität hergestellt: Die Strafverfolgungsbehörden des Partnerstaates können mit ihren Ersuchen ebenfalls direkt an US-CSP gelangen, ohne um Rechtshilfe ersuchen zu müssen. Der Partnerstaat toleriert dafür einen entsprechenden Zugriff der US-Strafverfolgungsbehörden auf Daten, die bei CSP auf seinem Territorium gespeichert sind. Vor allem dieser Aspekt hat zur Frage geführt, inwieweit der Abschluss einer solchen Vereinbarung mit den USA für die Schweiz opportun wäre.

Das Bundesamt für Justiz (BJ) ist die schweizerische Zentralstelle im Bereich der Rechtshilfe in Strafsachen.[3] In dieser Funktion führt es die Aufsicht über die Anwendung des Rechtshilfegesetzes und ist daneben verantwortlich für die Weiterentwicklung der Rechtsgrundlagen in diesem Bereich. Vor diesem Hintergrund – und aufgrund der Interventionen diverser Akteure aus Privatwirtschaft, Verbänden, Verwaltung und Strafverfolgung beim BJ – hat dieses den vorliegenden Bericht erarbeitet. Dieser soll eine Grundlage für die weiterführende Diskussion mit öffentlichen und privaten Stakeholdern in der Schweiz bilden. Zu diesem Zweck beleuchtet er insbesondere grundsätzliche juristische Fragen, die sich im Zusammenhang mit dem *CLOUD Act* und seiner Vereinbarkeit mit dem Schweizer Recht stellen.

2 Einleitung

Als Folge der Globalisierung spielt auch die zwischenstaatliche Zusammenarbeit in Strafsachen eine immer wichtigere Rolle. Die fortschreitende Digitalisierung sämtlicher Lebensbereiche und im vorliegenden Kontext insbesondere die Erhebung und Übergabe elektronischer Beweismittel stellt diese Zusammenarbeit dabei vor Herausforderungen verschiedenster Art:

- Daten sind *flüchtig* – die herkömmliche Strafrechtshilfe ist oft zu langsam, um diese über Landesgrenzen hinweg rechtzeitig sicherzustellen;
- Daten sind *nicht territorial geprägt* – soll wirklich der *Lageort* für strafbehördliche Zugriffsrechte auf Daten relevant sein, oder nicht eher die Frage, wer und von wo aus sich *Zugriff* auf die Daten verschaffen kann? Noch komplexer wird es bei *blockchain*, wo die Daten physisch nicht mehr an einem eindeutig bestimmbaren Ort liegen;
- Daten sind *verschlüsselt* – wie können sie von Strafverfolgungsbehörden, gerade im internationalen Verkehr, wirksam entschlüsselt werden? Gibt es zwischenstaatliche oder globale Regeln?

Es ist offensichtlich: Die zwischenstaatliche Erhebung elektronischer Beweismittel stellt Grundpfeiler der transnationalen Strafverfolgung in Frage. Das Prinzip der Territorialität im

[1] Vollständiger Wortlaut abrufbar unter: https://www.congress.gov/bill/115th-congress/senate-bill/2383/text.

[2] Bereits an dieser Stelle ist darauf hinzuweisen, dass der CLOUD Act nur in *Strafverfahren* zur Anwendung kommt. Im Strafverfahren kommt dem Territorialitätsprinzip aus verschiedenen Gründen eine besondere Bedeutung zu. Dazu unten 2. sowie insb. 5.1. Es wird im weiteren Verlauf daher von der *Territorialität insbesondere mit Blick auf das Strafverfahrensrecht* die Rede sein.

[3] Vgl. Art. 17 Rechtshilfegesetz (IRSG, SR **351.1**) sowie Art. 3 Rechtshilfeverordnung (IRSV, SR **351.11**).

bisherigen Sinne gerät ins Wanken. Die Verfahren der traditionellen souveränitätsorientierten Strafrechtshilfe sind zu langsam. Man setzt auf direktere Zusammenarbeitsformen, mitunter auf direkte Beteiligung Privater an Strafverfahren im Ausland. Dies ist teilweise aus der Not geboren: Rechtshilfebehörden in Staaten, in denen viele CSP ihren Sitz haben, stossen an die Kapazitätsgrenzen.

Entsprechende Anpassungen im Rechtshilferecht werden zurzeit in verschiedenen Foren, in der EU, aber auch im Europarat und auf UNO-Ebene diskutiert.

Die EU möchte mit einem Vorschlag betreffend Herausgabe- und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen vom April 2018 (E-Evidence-Verordnung)[4] eine erleichterte Zusammenarbeit zwischen ihren Mitgliedstaaten einführen und auf diese Weise die Zusammenarbeit beschleunigen. Im Europarat ist das Komitee für die Cybercrime-Konvention (Budapest-Konvention)[5], das TC-Y, zurzeit an der Erarbeitung eines Zweiten Protokolls zu dieser Konvention, welches die zwischenstaatliche Zusammenarbeit für mittels Computersystemen begangene Straftaten sowie für den Bereich der elektronischen Beweismittel allgemein regeln soll. Auf UNO-Ebene laufen Vorbereitungen zu einem multilateralen Instrument zur Bekämpfung der Cyberkriminalität.

Während in diesen Foren multilaterale Instrumente diskutiert werden, die auf die Zusammenarbeit zwischen Staaten setzen, haben die USA im März 2018 mit dem *CLOUD Act* auf nationaler Ebene ein Gesetz mit extraterritorialem Anwendungsbereich geschaffen. Das Gesetz soll einerseits den direkten Zugriff der US-Strafverfolgungsbehörden auf Daten von CSP mit Sitz in den USA ermöglichen – unabhängig davon, ob diese Daten in den USA oder im Ausland gespeichert sind – ohne für die im Ausland gespeicherten Daten den Weg über die zwischenstaatliche Rechtshilfe beanspruchen zu müssen. Über bilaterale *Executive Agreements*, die durch den *CLOUD Act* möglich werden, sollen die Strafverfolgungsbehörden der entsprechenden ausländischen Staaten andererseits ohne die Notwendigkeit von Rechtshilfeersuchen ebenfalls Zugang zu den entsprechenden Daten der CSP mit Sitz in den USA erhalten können, indem sie die betreffenden CSP direkt zu deren Herausgabe auffordern. Die ausländischen Staaten können dabei aber keinen Zwang anwenden. Das *Executive Agreement* erlaubt es den CSP, Daten an einen anderen Staat herauszugeben, sie sind jedoch nicht dazu verpflichtet.

Die Schweiz hat mit den USA einen Rechtshilfevertrag abgeschlossen, den Staatsvertrag vom 23. Mai 1973[6] über gegenseitige Rechtshilfe in Strafsachen (nachfolgend RVUS). Die schweizerischen Behörden erhalten die von einem US-CSP gespeicherten Daten folglich über die internationale Rechtshilfe in Strafsachen. Dieser Weg ist jedoch langwierig, denn das U.S. Department of Justice (DOJ) muss ein entsprechendes Ersuchen prüfen und es der Vollzugsbehörde übermitteln, die dem Ersuchen in der Regel erst nach einem Gerichtsverfahren entsprechen kann und die Beweise schliesslich übermittelt. Erfahrungsgemäss erhalten schweizerische Strafverfolgungsbehörden die ersuchten elektronischen Beweismittel nicht immer – und vor allem nicht immer rechtzeitig. Gleichzeitig hat das DOJ bereits 2016 Weisungen zu den elektronischen Beweismitteln erlassen und fordert die ausländischen Behörden auf, sich direkt an die CSP zu wenden, wenn sie lediglich Abonnentendaten (*basic subscriber information*: Name und Adresse, Art und Dauer des in Anspruch genommenen Dienstes, Zahlungsinstrumente inkl. Kreditkarten- und Kontonummern; im Folgenden Bestandsdaten)

[4] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen, COM/2018/225 final – 2018/0108 (COD) vom 17. April 2018.

[5] Übereinkommen des Europarates über die Cyberkriminalität, SEV 185, SR **0.311.43**.

[6] SR **0.351.933.6**

erhalten wollen.[7] In der Praxis geben gewisse CSP derartige Daten schon heute heraus, während andere die Herausgabe verweigern und auf den offiziellen Weg verweisen.

Auch wenn die Schweiz mit den USA ein *Executive Agreement* abschlösse, bliebe dieser Umstand so bestehen. Weiterhin könnte nur auf dem Rechtshilfeweg um Durchführung von Zwangsmassnahmen ersucht und dieser Zwang gewissermassen über den anderen Staat ausgeübt werden. Die schweizerischen Strafverfolgungsbehörden könnten sich nach Abschluss eines *Executive Agreements* zwar direkt an einen CSP wenden – nunmehr auch für Daten, die über Abonnenteninformationen hinausgehen – dürften aber keine Zwangsmassnahmen anordnen. Würde sich ein CSP weigern, Daten herauszugeben, müsste die Schweiz den Rechtshilfeweg beschreiten, um die Daten zwangsweise erheben zu lassen. Würde ein CSP jedoch kooperieren, verliefe die Zusammenarbeit schneller. Die Rechtshilfe mit den USA könnte damit überdies generell entlastet werden und die involvierten Behörden könnten sich auf Fälle konzentrieren, in denen die Zusammenarbeit verweigert wurde oder die nicht in den Geltungsbereich des *CLOUD Acts* fallen. Es gilt die Vermutung, dass sich diejenigen CSP, die schon heute bei der Herausgabe von Bestanddaten kooperieren, gestützt auf ein *Executive Agreement* aufgrund der klaren Rechtslage weiterhin kooperativ zeigen würden. Weitere CSP würden evtl. zu einer solchen Zusammenarbeit motiviert.

3 Der *CLOUD Act*

3.1 Ausgangslage

Der *CLOUD Act* ist ein US-amerikanisches Bundesgesetz, welches das Gesetz über gespeicherte Nachrichten, den *Stored Communications Act* (SCA) ergänzt und im März 2018 im Zusammenhang mit einem Gerichtsverfahren in Sachen Microsoft erlassen wurde. Konkret ging es damals darum, dass Microsoft 2013 gestützt auf den SCA von einem US-Richter aufgefordert worden war, in einem Strafverfahren E-Mails und Informationen zu einem von Microsoft gehosteten Account herauszugeben. Microsoft gab die Informationen heraus, die sich auf einem Server in den USA befanden, nicht hingegen die E-Mails, die auf einem Server in Irland gespeichert waren. Dies mit dem Argument, ein amerikanisches Unternehmen könne aufgrund einer derartigen Anordnung nicht zur Herausgabe von auf einem Server im Ausland gespeicherten Daten verpflichtet werden. Das amerikanische Gericht sei nicht zuständig; der SCA habe keine extraterritoriale Wirkung.

Microsoft verlor den Fall in erster Instanz, gewann aber vor dem Berufungsgericht, woraufhin das DOJ die Angelegenheit an den Supreme Court weiterzog. Noch vor dessen Urteil verabschiedete der Kongress den *CLOUD Act*, der den SCA änderte und dem Gesetz die heutige extraterritoriale Wirkung verleiht.

3.2 Inhalt

3.2.1 Wesentlicher materieller Inhalt

Der *CLOUD Act* verpflichtet die CSP mit Sitz in den USA, welche ausserhalb der USA Datenspeicherzentren führen, die Daten, die sich auf ihren Servern befinden, aufzubewahren und den zuständigen US-Strafverfolgungsbehörden auf Ersuchen herauszugeben. Dies unabhängig davon, ob die Daten in den USA oder im Ausland gespeichert sind.[8] Betroffen sind Gesellschaften nach amerikanischem Recht, d. h. Gesellschaften, die der US-Gerichtsbarkeit unterstehen.[9] Verlangt wird in diesem Zusammenhang ein Mindestbezug zu den USA (*mi-*

[7] Für über Abonnentendaten hinausgehende Ersuchen muss lex lata auf jeden Fall der Rechtshilfeweg beschritten werden.

[8] *CLOUD Act,* §2713. Siehe ebenfalls BISMUTH, S. 683.

[9] DOJ, «Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act», S. 6 f.

nimum contacts), wobei die entsprechende Interpretation und Qualifikation in der Kompetenz der US-Gerichte liegt. Auch Unternehmen mit Holdinggesellschaften, Tochtergesellschaften oder Zweigniederlassungen in den USA können betroffen sein, unter Umständen sogar ausländische Cloud-Anbieter, die in den USA Werbung für ihre Dienstleistung machen. Lediglich denjenigen ausländischen CSP, die keinen solchen Mindestbezug zu den USA haben, werden keine neuen Pflichten auferlegt.

Aus dem *CLOUD Act* selber ergibt sich keine Mindestdauer für die Aufbewahrung von Daten. Im Zusammenhang mit anderen Bestimmungen des US-Rechts, etwa dem SCA, scheint sich aber – mindestens in gewissen Fällen – eine Pflicht zur Aufbewahrung von Daten während 180 Tagen zu ergeben.

Der CSP kann gemäss *CLOUD Act* eine strafbehördliche Anordnung zur Herausgabe von Daten vor einem US-Gericht anfechten (Antrag auf Aufhebung oder Änderung), wenn es sich bei der betroffenen Person nicht um eine sogenannte *US person*[10] handelt und wenn die Bekanntgabe der Daten gegen das Recht eines Staates, welcher ein *Executive Agreement (vgl. unten, 3.2.2.)* mit den USA abgeschlossen hat (*qualifying foreign government*; im Folgenden QFG) zu verstossen droht. Das Gericht berücksichtigt für seinen Entscheid betreffend Aufhebung oder Abänderung der angefochtenen Herausgabeanordnung die Interessen der USA und des QFG, die Beziehung der betroffenen Person zu den USA und zum Staat, der um die Herausgabe der Daten ersucht hat, die Wahrscheinlichkeit einer Strafe und das allfällige Strafmass, die Bedeutung der angeforderten Daten für die Untersuchung und die Interessen der ersuchenden Behörde sowie die Wahrscheinlichkeit, mittels weniger einschneidender Möglichkeiten rechtzeitig und effektiv zu den entsprechenden Daten zu gelangen.[11] Falls das Gericht es als notwendig erachtet, kann die sofortige Herausgabe der Daten angeordnet werden, noch bevor der Entscheid zum Aufhebungs- oder Abänderungsantrag gefällt wurde.[12]

Weder der ausländische Staat noch die betroffene Person selber kann sich dem Ersuchen der US-Behörden widersetzen, sondern ausschliesslich der CSP.

3.2.2 Möglichkeit des Abschlusses von *Executive Agreements* mit anderen Staaten auf der Grundlage des *CLOUD Acts*

3.2.2.1 Allgemeines

Der zweite Teil des *CLOUD Acts* ermöglicht es den USA, unter gewissen Voraussetzungen mit anderen Staaten *Executive Agreements* abzuschliessen, auf deren Grundlage die zuständigen Behörden beider Staaten die CSP mit Sitz im jeweils anderen Staat direkt um Informationen oder auf ihren Servern gespeicherte Daten ersuchen können. Gestützt auf entsprechende *Executive Agreements* können die CSP die ihnen vom anderen Staat direkt zugeschickte internationale Herausgabeanordnung (*international production order*, im Folgenden Herausgabeanordnung) direkt beantworten. Die CSP können aber vom ausländischen Staat wie erwähnt nicht zur Herausgabe der Daten gezwungen werden. Eine Herausgabeanordnung ersetzt also die Rechtshilfe nicht – dies gilt zumindest dann, wenn der CSP nicht freiwillig kooperiert.

[10] *CLOUD Act*, § 2713 (h) (2) (A)

[11] *CLOUD Act,* § 2713 (h) (3) (A)-(H)

[12] *CLOUD Act,* § 2713 (h) (4)

3.2.2.2 Materielle Voraussetzungen

Gemäss *CLOUD Act* muss der Staat, der mit den USA ein *Executive Agreement* aushandeln will, gewisse Mindestvoraussetzungen erfüllen:[13]

Seine nationale Gesetzgebung muss mit Bezug auf den Schutz der Privatsphäre und der bürgerlichen Freiheiten im Hinblick auf die Sammlung von Daten und seine Aktivitäten, die Gegenstand des *Executive Agreements* sind, «robuste» materielle und verfahrensmässige Garantien bieten, die mit denjenigen in den USA vergleichbar sind. Er muss namentlich über angemessene Gesetzesbestimmungen im Bereich der Cyberkriminalität und der elektronischen Beweismittel verfügen. Dies kann unter anderem dadurch nachgewiesen werden, dass er Vertragspartei der Budapest-Konvention ist.

Allgemein muss der betreffende Staat die Rechtsstaatlichkeit sowie den Grundsatz der Nichtdiskriminierung achten und sich an die geltenden internationalen Verpflichtungen im Bereich der Menschenrechte halten, darunter den Schutz vor willkürlichen und rechtswidrigen Eingriffen in das Privatleben, das Recht auf ein faires Verfahren, auf Meinungsäusserungs-, Vereinigungs- und Versammlungsfreiheit, das Verbot von willkürlichen Festnahmen und Inhaftierungen sowie von Folter und grausamer, unmenschlicher oder erniedrigender Behandlung oder Strafe.

Die Regierungsstellen, die auf der Grundlage des *Executive Agreements* um Daten ersuchen dürfen, müssen ein rechtlich klar definiertes Mandat haben und insbesondere im Bereich der Erhebung, Speicherung, Verwendung und Bekanntgabe der Daten über klare gesetzliche Vorgaben und Verfahren verfügen. Es müssen ausreichende Mechanismen bestehen, mit denen die Transparenz hinsichtlich der Erhebung und Verwendung elektronischer Daten durch die fremde Regierung nachgewiesen werden kann.

Der betroffene Staat muss sodann nachweisen, dass er bestrebt ist, den weltweiten freien Datenverkehr sowie den offenen, freien und vernetzten Charakter des Internets zu fördern und zu schützen.[14] Und schliesslich muss er reziproke Rechte für den Zugriff auf die Daten gewährleisten, das heisst, den CSP mit Sitz in seinem Hoheitsgebiet erlauben, Ersuchen der US-Strafverfolgungsbehörden direkt nachzukommen.

Eine auf das *Executive Agreement* gestützte Herausgabeanordnung darf nicht direkt auf derartige *US persons* abzielen. Der betroffene Staat muss daher geeignete Massnahmen ergriffen haben, um dies zu vermeiden. Der *CLOUD Act* enthält sodann eine ganze Liste mit weiteren Voraussetzungen, die eine Herausgabeanordnung erfüllen muss.[15]

3.2.2.3 Formelle Voraussetzungen

In den USA ist die Exekutive für den Abschluss der *Executive Agreements* zuständig. Der US Attorney General entscheidet zusammen mit dem Aussenminister, ob der andere Staat die Voraussetzungen für den Abschluss erfüllt, und übermittelt die schriftliche Bestätigung dem

[13] *CLOUD Act,* § 2523 (b)

[14] *CLOUD Act*, §2523 (b) (1) (B) (vi)

[15] *CLOUD Act,* § 2523 (b) (2) und (3)

US-Kongress.[16] Das derart zertifizierte *Executive Agreement* kann von amerikanischer Seite in Kraft treten, falls der Kongress nicht innert 180 Tagen Widerspruch erhebt.[17]

Die Vereinbarung wird jeweils für eine bestimmte Zeit abgeschlossen. Der Staat, der mit den USA eine derartige Vereinbarung abschliesst, muss sich dabei einer periodischen Evaluation durch die USA unterziehen.[18]

3.2.3 Inhalt des Executive Agreements

Ein erster Teil des *Executive Agreements* müsste allgemeine Bestimmungen wie Definitionen, anwendbares Recht, Form und Inhalt der Ersuchen, zuständige Behörden und Bestimmungen zum Datenschutz enthalten.

Eine der wichtigsten Definitionen ist diejenige von *serious crime* (schwere Straftaten). Gemäss *CLOUD Act* müssen sich die auf der Grundlage eines *Executive Agreements* gestellten Ersuchen auf die Verfolgung schwerer Straftaten beschränken. Darunter sind neben Terrorismus, der im *CLOUD Act* explizit erwähnt wird, etwa Mord oder Kindesentführung zu verstehen. Es muss auch bestimmt werden, welche Daten unter das *Executive Agreement* fallen können, nämlich ob ausschliesslich Daten, die bereits gespeichert worden sind, betroffen sind, oder ob auch in Echtzeit abgefangene Daten in Frage kommen. Der Begriff des CSP und was ein solcher genau umfasst, muss schliesslich ebenfalls definiert werden.

In der Schweiz sind der Zusammenarbeit im Rechtshilferecht verschiedene Grenzen gesetzt. Insoweit als der *CLOUD Act* eine Form der internationalen Zusammenarbeit in Strafsachen ermöglicht, wäre zu prüfen, in welchem Umfang bei einer allfälligen Aushandlung eines *Executive Agreements* die gemäss schweizerischem Recht wesentlichen Prinzipien für die Zusammenarbeit in den Text einfliessen. Allfällige spezifische Ausschlussgründe müssten explizit in ein solches *Executive Agreement* hineinverhandelt werden.

Ein allfälliges *Executive Agreement* muss sodann auch technische Bestimmungen über die Übermittlung von Informationen und die Speicherung von Daten enthalten. Es muss geregelt werden, dass die Übermittlung von Daten und Informationen über einen sicheren Kanal erfolgt. Auch die Anforderungen bezüglich der Speicherung von Daten in einem gesicherten System und dem Zugang zu diesen Daten im ersuchenden Staat müssen festgelegt werden.

In formeller Hinsicht muss das *Executive Agreement* Bestimmungen zu den einzuhaltenden Verfahren, unter anderem zur Frage von Beschwerden oder Aufhebungsanträgen im Zusammenhang mit Herausgabeanordnungen enthalten.

3.2.4 Voraussetzungen für Herausgabeanordnungen gestützt auf ein *Executive Agreement*

Gemäss *CLOUD Act* müssen Herausgabeanordnungen, die sich auf ein *Executive Agreement* stützen, verschiedene Mindestvoraussetzungen erfüllen.[19]

Bei der Person, deren Daten von der ausländischen Herausgabeanordnung betroffen sind, darf es sich nicht um eine *US person* handeln, d. h. sie darf weder Staatsangehörige der

[16] *CLOUD Act,* §2523 (b)

[17] *CLOUD Act*, §2523(d) (2)

[18] *CLOUD Act,* §2523(b) (4) (J)

[19] *CLOUD Act*, § 2523 (b) (3)

USA sein noch dort ihren Wohnsitz, oder im Fall einer Gesellschaft, ihren Sitz dort haben.[20] Im umgekehrten Fall dürften die US-Strafverfolgungsbehörden nicht die Herausgabe von Daten von Personen mit schweizerischer Staatsangehörigkeit, mit Wohnsitz in der Schweiz oder einer Gesellschaft mit Sitz in der Schweiz verlangen. Der ausländische Staat darf somit unter dem *Executive Agreement* weder Anordnungen zustellen, welche direkt *US persons* zum Ziel haben, noch solche, die zwar eine *non US person* betreffen, die aber zum Ziel haben, Informationen über eine *US person* zu erhalten, und umgekehrt.[21] Wie Tochtergesellschaften von Schweizer Unternehmen, die nach US-Recht gegründet wurden, in diesem Zusammenhang behandelt würden, scheint nicht klar. Wenn es um Personen geht, die vom Anwendungsbereich des *Executive Agreements* ausgeschlossen sind, muss auf dem Weg der Rechtshilfe um die entsprechenden Daten ersucht werden.

Die Herausgabeanordnung muss sich auf ein *serious crime* beziehen – ein Begriff, der im *Executive Agreement* zu definieren wäre (vgl. Ziff. 5.3). Sie muss zudem namentlich im Einklang mit dem Recht des anordnenden Staates sein, eine Person, eine Adresse, einen persönlichen Gegenstand oder ein anderes Identifizierungsmerkmal angeben und durch nachvollziehbare und glaubwürdige Fakten gerechtfertigt sein (keine sog. *Fishing expeditions*), von einem Gericht oder einer anderen unabhängigen Behörde überprüft werden können und, im Fall von Abhörungsanordnungen, zeitlich befristet und verhältnismässig sein.[22]

In der Anordnung muss nicht nachgewiesen werden, dass eine *probable cause* vorliegt,[23] was die Zusammenarbeit gerade im Verhältnis mit den USA erleichtert und zu einer starken Entlastung der schweizerischen Strafverfolgungsbehörde führen würde.

4 Rechtsvergleich

4.1 *Executive Agreement* zwischen den USA und dem Vereinigten Königreich

Das Vereinigte Königreich (UK) ist der erste und bisher einzige Staat, mit dem die USA ein *Executive Agreement* gestützt auf den *CLOUD Act* ausgehandelt haben. Der genaue Wortlaut des Instruments, das am 3. Oktober 2019 unterzeichnet wurde, aber nach wie vor nicht in Kraft ist, ist online abrufbar.[24] Als erstes derartiges Instrument ist es von besonderer Bedeutung, da es die wesentlichen Grundzüge auch künftiger *Executive Agreements* festlegen dürfte.

Es handelt sich um eine relativ kurze Vereinbarung, die in verschiedenen Punkten auf andere Instrumente verweist, namentlich die Budapest-Konvention, das Abkommen zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über den Schutz personenbezogener Daten[25] sowie den Vertrag über die Rechtshilfe in Strafsachen zwischen den USA und UK. Seine Struktur ist derjenigen eines Rechtshilfevertrags in Strafsachen ähnlich. Es enthält Definitionen, Zweck, Grenzen, Bestimmungen zum Datenschutz usw.

Die Definitionen der für das *Executive Agreement* wichtigen Begriffe umfassen insbesondere diejenigen der zuständigen Behörde, des CSP, der Daten sowie des *serious crime* (Art.

---

[20] Gemäss *CLOUD Act*, § 2523 (a) (2) "incorporated in the United States".

[21] *CLOUD Act,* § 2523 (b) (3) (A) und (B)

[22] *CLOUD Act,* § 2523 (b) (3) (D)

[23] DOJ, «Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act», S. 8.

[24] Abrufbar unter: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf. Gemäss Auskunft der britischen Botschaft in Bern ist ein Inkrafttreten des Abkommens evtl. Ende Sommer 2021 zu erwarten.

[25] Abkommen zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über den Schutz personenbezogener Daten bei der Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten, ABl. L 336 vom 10. Dezember 2016, S. 3.

1). Die Anordnungen zur Offenlegung oder Herausgabe ausserhalb des eigenen Staates gespeicherter Daten (nachfolgend Anordnung) müssen dem nationalen Recht der anordnenden Vertragspartei entsprechen (Art. 5 Abs. 1). Das nationale Recht der Vertragspartei, in der sich der CSP befindet, muss demgegenüber nicht zwingend eingehalten werden. Die Anordnung muss vor eine Justizbehörde oder unabhängige Behörde der anordnenden Vertragspartei gebracht werden können, damit diese deren Vereinbarkeit mit ihrem nationalen Recht überprüfen kann (Art. 5 Abs. 2). Das bedeutet, dass ein Provider mit Sitz in den USA, der eine Anordnung von UK erhält, den Fall an die britischen Behörden ziehen kann. Für kleinere CSP kann es jedoch schwierig sein, in einem anderen Staat, insbesondere in den USA, zu klagen. Das *Executive Agreement* sieht eine Art Zentralbehörde vor, welche die Vereinbarkeit der Anordnung mit dessen Text überprüfen muss, bevor sie an den CSP gesandt wird (Art. 5 Abs. 6). Demnach muss eine Behörde, die Informationen von einem CSP erhalten will, zuerst diese Zentralbehörde konsultieren.

Wenn ein CSP der Ansicht ist, dass die erhaltene Anordnung nicht dem *Executive Agreement* entspricht, so muss er dies zuerst bei den zuständigen Behörden des Staates geltend machen, der die Anordnung übermittelt hat, d. h. des Staates, in dem er gerade nicht seinen Sitz hat. Wenn er mit seiner Einrede nicht durchdringt, kann sich der CSP auch an die zuständigen Behörden in seinem Sitzstaat wenden (Art. 5 Abs. 11). Beide Behörden suchen nach einer einvernehmlichen Lösung. Sollte die Behörde des Sitzstaats zum Schluss gelangen, dass die Anordnung nicht dem Abkommen entspricht, kann sie die Behörde des anderen Staates darüber informieren, und das Abkommen ist auf die Anordnung nicht anwendbar (Art. 5 Abs. 12). Es scheint damit ein Verfahren vorgesehen zu sein, wonach die Zentralbehörde des Sitzstaates in letzter Instanz darüber entscheiden kann, ob eine Anordnung dem *Executive Agreement* entspricht.

Die gestützt auf das *Executive Agreement* erhaltenen Daten dürfen nicht ohne Zustimmung des Staates, in dem der CSP seinen Sitz hat, an einen Drittstaat weitergegeben werden (Art. 8 Abs. 2). Wird um Informationen zu einer Person ersucht, die sich ausserhalb des Territoriums der anordnenden Vertragspartei befindet und kein Staatsbürger der selbigen ist, muss der Drittstaat, dessen Angehöriger diese Person ist, darüber in Kenntnis gesetzt werden.[26]

Wenn die erhobenen Daten Fälle betreffen, die in den USA zur Verhängung der Todesstrafe oder in UK zur Verletzung der Meinungsäusserungsfreiheit gemäss amerikanischem Verständnis führen könnten, muss die Zentralbehörde des anderen Staates einbezogen werden und der Verwendung der Daten zustimmen (Art. 8 Abs. 4). Ohne Zustimmung des anderen Staates dürfen die gestützt auf den *CLOUD Act* in UK beschafften Daten nicht verwendet werden, um in den USA die Todesstrafe auszusprechen, und dürfen die in den USA beschafften Daten nicht verwendet werden, um in UK eine Strafe in Verbindung mit der Verletzung der Meinungsäusserungsfreiheit zu verhängen[27] – es bestehen also entsprechende Vetorechte.[28]

In Bezug auf den persönlichen Geltungsbereich des *Executive Agreements* besteht eine Asymmetrie zwischen den USA und UK. Britische Anordnungen dürfen sich nicht auf *US persons* beziehen. Das umfasst sowohl Personen mit Wohnsitz/Sitz in den USA, unabhängig

[26] DASKAL, SWIRE, «The UK-US *CLOUD Act* Agreement is Finally Here, Containing New Safeguards». Art. 5 des Abkommens.

[27] CHRISTAKIS, «21 Thoughts and Questions about the UK-US *CLOUD Act* Agreement», pt. 15–16; Explanatory Memorandum to the Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America in Access to Electronic Data for the Purpose of Countering Serious Crime, pt. 19–20.

[28] DASKAL, SWIRE, «The UK-US *CLOUD Act* Agreement is Finally Here, Containing New Safeguards».

von ihrer Staatsangehörigkeit, als auch amerikanische Staatsangehörige mit Wohnsitz im Ausland. Amerikanische Anordnungen hingegen dürfen sich grundsätzlich auf britische Staatsangehörige beziehen. Bloss Personen, die sich *auf britischem Territorium* befinden, sind vom Geltungsbereich des Abkommens ausgenommen – unabhängig von deren Staatsangehörigkeit. Dahinter scheinen Grundsätze des EU-Rechts (Unionsbürgerschaft) zu stehen.[29]

Die CSP werden auch durch das *Executive Agreement* nicht verpflichtet, den Ersuchen der Behörden des anderen Staates zu entsprechen. Wenn ein CSP die Auskunft verweigert, kommt das Gesetz des ersuchenden Staates zur Anwendung.[30] Wenn eine Zwangsmassnahme erforderlich ist, ist grundsätzlich internationale Rechtshilfe in Strafsachen zu beantragen. In Bezug auf die Verschlüsselung ist das Instrument neutral. Es verpflichtet die Provider nicht zur Entschlüsselung.[31]

Die Einhaltung des *Executive Agreements* wird von den Parteien ein Jahr nach Inkrafttreten und daraufhin in regelmässigen Abständen überprüft (Art. 12 Abs. 1). Jede Partei muss der anderen überdies jährlich einen Bericht zu dessen Anwendung unterbreiten (Art. 12 Abs. 4). Es soll während fünf Jahren in Kraft sein und kann dann aufgehoben oder auf unbestimmte Zeit verlängert werden.

4.2 EU-E-Evidence vs. *US CLOUD Act*: Kollision oder Verhandlung?

4.2.1 E-Evidence-Gesetzgebung der EU

Auf EU-Ebene laufen aktuell ebenfalls Bestrebungen zur Verbesserung des grenzüberschreitenden Zugangs zu elektronischen Beweismitteln (sog. E-Evidence). Es soll innerhalb der EU ein Rechtsrahmen geschaffen werden, der die Sicherung von und den Zugang zu elektronischen Beweismitteln in grenzüberschreitenden Fällen für die Polizei und die Justizbehörden erleichtern und beschleunigen soll. Die Idee für eine E-Evidence-Gesetzgebung ist zurückzuführen auf die Terroranschläge in Brüssel im März 2016 und der daraus entstandenen Forderung in der EU, neue Wege zu finden, um elektronische Beweismittel schneller und wirksamer zu sichern und verstärkter mit Drittländern und im europäischen Hoheitsgebiet tätigen Dienstleistungserbringern zusammenzuarbeiten.[32]

Im April 2018 legte die Kommission zwei Gesetzgebungsvorschläge zur E-Evidence vor: einen Vorschlag für eine Verordnung über Europäische Herausgabe- und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen[33] und einen Vorschlag für eine Richtlinie zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren.[34]

Der Verordnungsvorschlag führt für die betroffenen Behörden verbindliche Europäische Herausgabeanordnungen (EPOC) und Europäische Sicherungsanordnungen (EPOC-PR) ein.

---

[29] Abrufbar unter: https://www.hrw.org/news/2019/10/29/groups-urge-congress-oppose-us-uk-cloud-act-agreement.

[30] Explanatory Memorandum to the Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America in Access to Electronic Data for the Purpose of Countering Serious Crime, pt. 18.

[31] CHRISTAKIS, «21 Thoughts and Questions about the UK-US *CLOUD Act* Agreement», pt. 14; DASKAL, SWIRE, «The UK-US *CLOUD Act* Agreement is Finally Here, Containing New Safeguards».

[32] Gemeinsame Erklärung der EU-Minister für Justiz und Inneres und der Vertreter der EU Organe zu den Terroranschlägen vom 22. März 2016 in Brüssel vom 24. März 2016, abrufbar unter: https://www.consilium.europa.eu/de/press/press-releases/2016/03/24/statement-on-terrorist-attacks-in-brussels-on-22-march/.

[33] Vorschlag der Europäischen Kommission für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen vom 17. April 2018, COM(2018)225 final.

[34] Vorschlag der Europäischen Kommission für eine Richtlinie des Europäischen Parlaments und des Rates zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren vom 17. April 2018, COM(2018)226 final.

Diese Instrumente sollen parallel zu den derzeit bestehenden Rechtsinstrumenten bestehen, welche der Erleichterung von Beweiserhebungen im Hoheitsgebiet eines anderen Mitgliedstaats dienen, wie z. B. der Richtlinie 2014/41/EU über die Europäische Ermittlungsanordnung in Strafsachen («EEA-Richtlinie»)[35].

Die Europäische Herausgabeanordnung soll den Behörden ermöglichen, mit einer richterlichen Anordnung digitale Daten anzufordern, die von einem CSP in einem anderen EU-Staat gespeichert wurden und als Beweismittel in strafrechtlichen Ermittlungen oder Strafverfahren erforderlich sind. Diese Idee baut im Wesentlichen darauf auf, dass jeder CSP, der in der EU Dienstleistungen erbringen will, dort einen Vertreter (sog. *legal representative*) bestimmen muss, der Zugang zu den Daten des gesamten Unternehmens hat. Die vorgeschlagene Richtlinie sieht einheitliche Regeln für die Bestellung von solchen Vertretern vor. Die Behörden (Polizei oder Staatsanwaltschaft eines EU-Mitgliedstaates) können für die Zustellung und Ausführung von Anordnungen direkt auf diesen Vertreter zugreifen, und zwar unabhängig davon, wo in der EU dieser Vertreter seinen Sitz hat. Der Kontakt erfolgt auch hier nicht mehr zwischen den Behörden eines Staates, sondern zwischen einer Behörde und einem Unternehmen, also einer privaten Stelle.[36] Die betroffenen Unternehmen müssen die Daten innerhalb von wenigen Stunden bis Tagen (10 Tage, in dringenden Fällen innerhalb von 6 Stunden) herausgeben.

Die Europäische Sicherungsanordnung richtet sich – wie die Europäische Herausgabeanordnung – an den Vertreter eines CSP, der sich ausserhalb des Rechtssystems des Anordnungsmitgliedstaates befindet. Mit der Sicherungsanordnung können die CSP verpflichtet werden, Daten mit Blick auf ein späteres Herausgabeersuchen zu sichern.[37]

Aktuell befindet sich das Geschäft im sog. Trilog, d. h. dem politischen Bereinigungsprozess zwischen der EU-Kommission, dem Rat der EU und dem Europäischen Parlament.

4.2.2 Gespräche zwischen der EU und den USA

Die EU-Kommission beantragte im Februar 2019 ein Verhandlungsmandat zur Aufnahme von Gesprächen mit den USA über ein Abkommen zwischen der Europäischen Union und den USA über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln für die justizielle Zusammenarbeit in Strafsachen.[38] Im Juni 2019 ermächtigte der Rat der Europäischen Union die Kommission zur Aufnahme entsprechender Verhandlungen im Namen der EU.[39]

Grund für die Aufnahme von Gesprächen mit der USA ist primär die E-Evidence-Gesetzgebung der EU. Obwohl die Vorschläge zu E-Evidence CSP betreffen, die Dienstleistungen auf dem EU-Markt erbringen, besteht die Gefahr, dass die darin vorgesehenen Verpflichtungen mit Rechtsvorschriften von Drittstaaten kollidieren. Die Entwürfe zur E-Evidence-Gesetzgebung der EU enthalten zwar kollisionsrechtliche Bestimmungen. Da aber die in strafrechtlichen Verfahren im EU-Raum relevantesten CSP ihren Sitz in den USA haben und somit der Hoheitsgewalt der USA unterstehen, sollte ein Abkommen zwischen der EU und den USA all-

[35] Richtlinie 2014/41/EU des Europäischen Parlaments und des Rates vom 3. April 2014 über die Europäische Ermittlungsanordnung in Strafsachen, ABl. L 130 vom 1.5.2014, S. 1.

[36] TSILIKIS, S. 169 f. und 172 f.

[37] Zum Ganzen siehe Ausführungen im Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen, Erwägung 47.

[38] Empfehlung der Europäischen Kommission für einen Beschluss des Rates über die Ermächtigung zur Aufnahme von Verhandlungen über ein Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln für die justizielle Zusammenarbeit in Strafsachen vom 5. Februar 2019, COM(2019) 70 final.

[39] Abrufbar unter: https://www.consilium.europa.eu/de/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-E-Evidence-in-criminal-matters/.

fällige Kollisionen von Verpflichtungen im Verhältnis zwischen beiden Systemen vermeiden. Ziel der EU ist es, mit einem völkerrechtlichen Abkommen Rechtskollisionen insbesondere in Bezug auf Inhaltsdaten zu vermeiden und den Zugang zu elektronischen Beweismitteln zu beschleunigen. Da das geltende amerikanische Recht US-CSP die Beantwortung von Ersuchen ausländischer Strafverfolgungsbehörden hinsichtlich Inhaltsdaten untersagt und Strafverfolgungs- und Justizbehörden aus der EU derzeit Schwierigkeiten haben, entsprechende Daten mithilfe von Rechtshilfeersuchen zu beschaffen, soll ein Abkommen einen effizienteren Rechtsrahmen für diese Behörden schaffen und eine direkte Zusammenarbeit mit CSP ermöglichen. Ein Abkommen zwischen der EU und den USA würde aus EU-Sicht also primär das Ziel und die Wirksamkeit der Vorschläge zu E-Evidence ergänzen, insbesondere in Bezug auf Inhaltsdaten, die sich im Besitz eines US-CSP in den USA befinden. Mit Bezug auf Nichtinhaltsdaten fordern die amerikanischen Behörden die Strafverfolgungs- und Justizbehörden der EU wegen der steigenden Zahl der Rechtshilfeersuchen wie erwähnt bereits heute auf, diese Daten direkt bei den US-CSP anzufordern (vgl. Einleitung). In dieser Hinsicht erlaubt das US-Recht CSP mit Sitz in den USA, solche Ersuchen direkt zu beantworten, verpflichtet sie jedoch nicht dazu. Ein Abkommen zwischen der EU und den USA soll daher auch beim Zugang zu Nichtinhaltsdaten, die sich im Besitz eines US-CSP befinden, mehr Rechtssicherheit schaffen.[40]

Bei den Verhandlungen zwischen der EU und den USA handelt es sich gemäss informellen Informationen damit um keine eigentlichen «CLOUD-Act»-Verhandlungen. Ziel ist es vielmehr, eine Brücke zwischen dem amerikanischen *CLOUD Act* und der E-Evidence-Gesetzgebung zu bauen. Während in diesem Prozess die EU versucht, ihr E-Evidence-System durchzusetzen, möchten die USA dem System des *CLOUD Acts* zum Durchbruch verhelfen. Da die beiden Systeme genau umgekehrte Ansätze gewählt haben (USA: extraterritoriale Wirkung; EU: Verpflichtung des CSP bzw. des Vertreters zur «territorialen» Anwesenheit), sind sie nicht ohne Weiteres kompatibel. Ziel ist es jedoch, dass auf beiden Seiten des Atlantiks Behörden direkt an CSP gelangen können, unabhängig davon, auf welchem Kontinent sie den Firmensitz haben. Durch das Abkommen sollen die rechtlichen Aspekte des Zugangs zu Inhalts- und Nichtinhaltsdaten, die sich im Besitz von CSP in der EU und in den USA befinden, denselben Vorschriften unterliegen.

Bisher haben gemäss informellen Informationen vier Verhandlungsrunden stattgefunden. Ein wesentlicher Teil der Gespräche betraf den Datenschutz. In diesem Punkt hat die Kommission erklärt, dass das Rahmenabkommen zwischen der EU und den USA zum Datenschutz ergänzt werden muss.[41] Zu zahlreichen Punkten bestehen noch grosse Differenzen. Allerdings dürfte es für die Kommission nicht einfach sein, in den Verhandlungen substanziell weiterzukommen, solange die Trilogverhandlungen zum E-Evidence-Paket vom nicht abgeschlossen sind. Denn ihre Verhandlungsposition hängt wesentlich vom Ergebnis dieses Verfahrens ab.[42] Die Form des Abkommens ist noch offen. Es wird sich zudem in den bestehenden Rechtsrahmen einfügen müssen,[43] und das Verhältnis zwischen den verschiedenen Rechtsquellen wird noch zu klären sein.

---

[40] Empfehlung für einen Beschluss des Rates über die Ermächtigung zur Aufnahme von Verhandlungen über ein Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln für die justizielle Zusammenarbeit in Strafsachen vom 5.2.2019, COM(2019) 70 final.

[41] Abkommen zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über den Schutz personenbezogener Daten bei der Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten (ABl. L 336, 10.12.2016, S. 3–13).

[42] Report of the Commission services on the second round of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, 6 November 2019, abrufbar unter: https://www.statewatch.org/news/2019/nov/eu-council-usa-E-Evidence-13713-19.pdf.

[43] Siehe z. B. Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über Rechtshilfe sowie die Budapest-Konvention und die bilateralen Übereinkommen mit den Mitgliedstaaten.

Die Verhandlungen mit den USA werden zudem beeinflusst von den parallel dazu laufenden Verhandlungen im Europarat über ein Zweites Zusatzprotokoll zur Budapest-Konvention, die ähnliche Fragen zum Gegenstand haben und ähnliche Schwierigkeiten mit sich bringen, da die EU in den Verhandlungen zu diesem Protokoll einen grossen Einfluss hat (siehe Ziff. 4.3). Die Inhalte dieses Protokolls können damit direkte Auswirkungen auf die Verhandlungen zwischen der EU und den USA haben.[44]

Ist das Abkommen einmal ausgehandelt, muss das Europäische Parlament dem Wortlaut des Abkommens noch zustimmen und der Rat einen Beschluss zum Abschluss des Abkommens fassen.

4.3 Das Zweite Zusatzprotokoll zum Europarats-Übereinkommen über die Cyberkriminalität (Budapest-Konvention)[45]

Dem gleichen Grundziel wie die bereits erwähnten Instrumente und Vorhaben dient das Zweite Zusatzprotokoll zur Budapest-Konvention, das zurzeit im Europarat ausgearbeitet wird: Auch dieses Instrument soll dazu dienen, Strafverfolgungsbehörden den Zugang zu elektronischen Beweismitteln zu erleichtern. Es soll die künftige Zusammenarbeit zwischen den Vertragsstaaten – darunter auch die USA, in denen viele der am meisten genutzten CSP ihren Sitz haben – bei der Verfolgung von *cyber-enabled criminality* effizienter gestalten und beschleunigen. Es soll insbesondere dazu dienen, Strafverfolgungsbehörden den Zugang zu elektronischen Beweismitteln zu erleichtern, vor allem wenn sich diese im Ausland befinden. Die Zusammenarbeit mit ausländischen Providern soll erleichtert werden.

Entsprechend enthält das Protokoll unter anderem Bestimmungen, welche die Vertragsparteien verpflichten sollen, in ihrem nationalen Recht Regelungen für die direkte Zusammenarbeit mit CSP auf dem Gebiet einer anderen Vertragspartei zu schaffen. Dabei geht es um Zugriff auf Informationen zu Domain-Namen oder Nutzerdaten, Verfahren zur beschleunigten Herausgabe von Nutzerinformationen und Verbindungsdaten sowie die beschleunigte Herausgabe gespeicherter Daten in Notfällen. Weitere Bestimmungen enthalten die Voraussetzungen für die Zusammenarbeit sowie Bestimmungen bezüglich Ausschlussgründen, insb. Datenschutz.

Die mit dem Zweiten Zusatzprotokoll verfolgten Ziele, die auf einen gewissen Abbau und eine «Auslagerung» rechtsstaatlicher und verfahrensmässiger Garantien zugunsten einer rascheren Kooperation ausgerichtet sind, stehen allerdings im Widerspruch zum Anspruch, dass das Übereinkommen von möglichst vielen Staaten weltweit ratifiziert werden soll. Der Europarat hat die Schwelle für einen Beitritt von Drittstaaten zur Budapest-Konvention erheblich gesenkt. So werden auch Staaten zum Beitritt eingeladen, die teilweise nicht willens oder in der Lage sind, grundlegende Menschenrechte und Verfahrensgarantien sicherzustellen.

Konkret besteht mit diesem Protokoll die Gefahr, dass im Rahmen der Strafverfolgung eine erleichterte Zusammenarbeit mit Staaten geschaffen wird, ohne dass gleichzeitig ein genügender verfahrensrechtlicher Schutz und genügende Garantien im Bereich der Menschenrechte gewährleistet sind. Die zuweilen zitierte «*community of trust among the States Parties*» ist nur schwerlich denkbar in einem stetig erweiterten Kreis von Vertragsstaaten, von denen nicht alle die aus schweizerischer Sicht grundlegenden Verfahrensgarantien und elementaren Grundrechte einhalten können oder wollen.

---

[44] Factsheet der Europäischen Kommission vom 5. Februar 209, Fragen und Antworten: Mandat für das Zweite Zusatzprotokoll zum Budapester Übereinkommen, abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/de/MEMO_19_865 (Stand 1.7.2020).

[45] Übereinkommen des Europarates über die Cyberkriminalität (Budapest-Konvention), SEV 185, SR **0.311.43**; https://www.coe.int/de/web/conventions/full-list/-/conventions/treaty/185.

Die Arbeiten des Europarates hätten im Dezember 2020 abgeschlossen werden sollen, was angesichts der teilweise erheblichen Differenzen zwischen den Delegationen (z. T. grundsätzlich divergierende Betrachtungsweisen der US-Delegation und von Australien, Kanada, Japan einerseits sowie der EU andererseits) jedoch nicht möglich war. Es ist fraglich, ob die Schweiz angesichts des beschriebenen Dilemmas zwischen Universalisierung des Protokolls und Vereinfachung der Zusammenarbeit einerseits und Aspekten des Rechtsschutzes andererseits eine rasche Unterzeichnung des Protokolls anstreben wird. Ein behutsames Vorgehen mit regelmässiger Analyse der kurz- und mittelfristigen Auswirkungen und Erfahrungen mit dem neuen Protokoll erscheint zum heutigen Zeitpunkt angezeigt.

Ergänzend ist darauf hinzuweisen, dass auch auf globaler Ebene im UNO-Rahmen Vorarbeiten hin zu einer globalen Cyber-Crime-Konvention unternommen werden. Das anhand der Budapest-Konvention erörterte Spannungsfeld zeigt sich hier natürlich umso akzentuierter. Die Arbeiten sind allerdings zurzeit noch zu wenig weit gediehen, weshalb im vorliegenden Bericht nicht weiter darauf eingegangen wird.

5 Rechtliche Fragen

5.1 Territorialität und Souveränität

Das Territorialitätsprinzip ist ein zentraler Pfeiler des Völkerrechts, gerade auch mit Blick auf Abgrenzungsfragen im Bereich der strafrechtlichen Zuständigkeit. Es weist eine enge Verbindung zur staatlichen Souveränität auf. Staatssouveränität beinhaltet positiv betrachtet die Kompetenz der Staaten, sich rechtlich und strukturell selbst zu organisieren und internationale Verträge abzuschliessen, und negativ betrachtet das Verbot, sich in interne Angelegenheiten anderer Staaten einzumischen (Interventionsverbot[46]). Aus dem Territorialitätsprinzip und den durch das Gebot der staatlichen Nichteinmischung gesetzten Grenzen leitet sich das Verbot für die Staaten ab, durch ihre Rechtsetzung oder tatsächliche Handlungen die Souveränität und die territoriale Integrität anderer Staaten zu verletzen.

Im *Lotus-Entscheid*[47] von 1927, dem ein Frankreich und die Türkei betreffender Zwischenfall auf hoher See zugrunde lag, hielt der Ständige Internationale Gerichtshof (StIGH) fest, dass das Territorialitätsprinzip über das eigene Hoheitsgebiet hinausgehende Rechtsanwendungen zumindest dann nicht ausschliesst, wenn sie völkerrechtlich nicht explizit verboten sind. In einem Entscheid von 1992 nahm auch das Bundesgericht darauf Bezug: «[D]ie extraterritoriale Anwendung des eigenen Rechts [wird] auch im Völkerrecht und im internationalen Strafrecht nicht a priori als unzulässig betrachtet [...]. Vielmehr darf sich die interne Gesetzgebung nach vorherrschender Lehre und Praxis auch auf extraterritoriale Sachverhalte beziehen, wenn eine eindeutige Binnenbeziehung dieser Sachverhalte zum inländischen Recht besteht»[48].

Der internationale Handel, die globale Mobilität und namentlich auch die moderne Kommunikation mit weltweit verfügbaren, jederzeit abrufbaren Daten stellen das Territorialitätsprinzip vielleicht nicht grundsätzlich in Frage. Sie vervielfachen aber die Berührungspunkte und das Kollisionspotenzial zwischen den verschiedenen staatlichen Rechtsordnungen. Umso wichtiger sind klare Abgrenzungen zwischen völkerrechtlich zulässigen, über das eigene Territorium hinauswirkenden Rechtsanwendungen und verbotener extraterritorialer Kompetenzüberschreitung. Völkerrechtlich anerkannte Anknüpfungspunkte sind namentlich die territoriale Anknüpfung (z. B. Aufenthalt oder Wohnsitz einer Person, Sitz oder Niederlassung eines

[46] Art. 2 Abs. 7 UNO-Charta, SR **0.120**.

[47] Publications de la Cour Permanente de Justice Internationale (CPJI), Recueil des Arrêts, Série A – No. 10, S. 18 f., Arrêt No. 9: Affaire du «Lotus» du 7 septembre 1927.

[48] BGE 118 Ia 137 E. 2b S. 142.

Unternehmens, Ausführungsort einer Tätigkeit) oder die persönliche Anknüpfung (z. B. Staatsangehörigkeit einer handelnden oder von einer Handlung betroffenen Person). In Einzelfällen, etwa zur Wahrung der eigenen Sicherheit bei Angriffen oder akuten Bedrohungen sowie zur Wahrung allgemein anerkannter, fundamentaler Interessen der internationalen Gemeinschaft wie beispielsweise zur Bekämpfung schwerster Verbrechen im Rahmen des Universalitätsprinzips, kann auch eine Anknüpfung an ein bestimmtes materielles Verhalten ausreichen.

Auch das Strafrecht knüpft an diesen völkerrechtlichen Grundsätzen an.[49] Als letztes und schärfstes Mittel, das einer demokratischen Ordnung zur Verteidigung ihrer Werte zur Verfügung steht,[50] ist der Bezug zu Souveränität und Territorialität im Strafrecht jedoch besonders eng. Im Unterschied beispielsweise zu einem Zivilverfahren kann im Strafverfahren nie von der Mitwirkung der Parteien – insbesondere nicht der beschuldigten Person – ausgegangen werden. Vielmehr kann diese den Grundsatz, dass sie sich nicht selbst beschuldigen muss,[51] für sich in Anspruch nehmen. Beweiserhebung im inquisitorischen Strafprozessrecht kontinentaleuropäischer Staaten ist daher grundsätzlich eine staatliche Aufgabe. Der *Staat* ermittelt – so zumindest die Fiktion – die Wahrheit.[52] Strafrechtliche Beweiserhebung ist daher mit direkten Zugriffsmöglichkeiten für die Strafverfolgungsbehörden verbunden. Aufgrund der zentralen Rolle staatlicher Organe bei strafrechtlicher Beweiserhebung ist zu ihrer Vornahme grundsätzlich der Staat zuständig, *auf dessen Territorium die Beweismittel liegen*. Die Belegenheit einer Sache spielt im Rahmen von Strafverfahren daher eine zentrale Rolle: Zuständig für die Erhebung von Sachbeweisen ist grundsätzlich die Strafverfolgungsbehörde am Lageort. Dieses Prinzip wurde bisher im Grund auch auf Daten übertragen – diese sind ebenfalls am «Lageort» zu erheben.

Der *CLOUD Act* hält sich nur beschränkt an diese Prinzipien. Sein Geltungsbereich ist in räumlicher, zeitlicher und inhaltlicher Hinsicht sehr weit gefasst (siehe Ziff. 3.2). Unter das Gesetz fallen alle CSP mit Sitz in den USA. Damit findet das Gesetz auf Daten Anwendung, die von ausländischen CSP ausserhalb der USA gespeichert oder kontrolliert werden, wenn diese CSP in den USA Geschäftsniederlassungen betreiben. Allenfalls könnte es auch schon genügen, wenn nicht-US-CSP aus dem Ausland auf den US-Markt ausgerichtete Dienstleistungen anbieten.[53] Einerseits können US-Strafverfolgungsbehörden somit gestützt auf den *CLOUD Act* Daten erheben, die nicht in den USA liegen. Andererseits können sich die amerikanischen Behörden an Unternehmen wenden, die ihren Sitz nicht in den USA haben und insofern nicht zwingend ihrer Gerichtsbarkeit unterstehen. Insbesondere diese zweite Tatsache kann hinsichtlich der Territorialität als problematisch erachtet werden. Gemäss dem *CLOUD Act* können sich die amerikanischen Behörden direkt an eine Privatperson (den CSP) im Hoheitsgebiet des anderen Staates wenden, ohne dass der Staat darüber informiert wird. Zudem stehen dem ausländischen CSP als Rechtsmittel nur Verfahren in den USA zu Verfügung, dessen Recht er nicht unbedingt kennt, sodass er benachteiligt sein könnte.

Dadurch wird das völkerrechtliche Territorialitätsprinzip zwar nicht grundsätzlich in Frage gestellt, doch der Geltungsbereich des *CLOUD Acts* kann zu extraterritorialen *strafrechtlichen*

---

[49] Vgl. dazu die strafrechtliche Zuständigkeit begründenden Prinzipien der Territorialität, der Personalität sowie des Weltrechtsprinzips.

[50] Vgl. m.w.H. FRANZ RIKLIN, Schweizerisches Strafrecht, Allgemeiner Teil I, Verbrechenslehre, Zürich 2007, §4 N 7.

[51] Vgl. Art. 6 Abs. 1 EMRK sowie Art. 113 Abs. 1, Art. 140, Art. 158 Abs. 1 Bst. b, Art. 262 Abs. 2 und Art. 265 Abs. 2 Bst. a StPO.

[52] Vgl. Art. 2 bzw. Art. 6 StPO.

[53] Vgl. dazu den Bericht zuhanden der französischen Nationalversammlung «Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extraterritoriale» vom 26. Juni 2019, Ziff. 1.2.4.2.1, S. 29 f.; abrufbar unter: https://www.dalloz-actualite.fr/sites/dalloz-actualite.fr/files/resources/2019/06/rapport_gauvain.pdf.

Kompetenzkonflikten führen. Die Frage der «Tolerierung» eines solchen extraterritorialen Zugriffs auf Daten müsste in einem allfälligen *Executive Agreement* geregelt werden.

5.2 Rechtsnatur der *Executive Agreements*

Der *CLOUD Act* sieht vor, dass die USA mit anderen Staaten *Executive Agreements* abschliessen können (vgl. dazu. 3.2.2). Gestützt auf solche Vereinbarungen sollen sich Strafverfolgungsbehörden aus Staaten mit (aus US-Sicht) rechtsstaatlich-demokratischer Grundordnung sowie mit den USA vergleichbaren Datenschutzstandards und Verfahrensgarantien direkt an die CSP in den USA wenden können, um Daten zur strafrechtlichen Verfolgung von *serious crimes* zu erhalten. Gleichzeitig tolerieren diese Partnerstaaten den Zugriff der US-Strafverfolgungsbehörden auf Daten bei CSP in ihrem Territorium. Die Datenherausgabe erfolgt in einem solchen Fall ohne Rechtshilfeverfahren direkt zwischen dem CSP und dem jeweils «ersuchenden» Staat.

Der *CLOUD Act per se* (also auch ohne zusätzliches *Executive Agreement*) bietet den US-Strafverfolgungsbehörden, wie dargelegt wurde, die Möglichkeit, in einem US-Strafverfahren Zugang zu den Daten zu erhalten, die im Besitz eines US-CSP irgendwo auf der Welt gespeichert sind. Vor diesem Hintergrund ist die Möglichkeit, mit anderen Staaten unter gewissen Voraussetzungen *Executive Agreements* abzuschliessen, ein wichtiges Element zur Förderung der Akzeptanz des *CLOUD Acts*. Die USA verlassen sich dabei auf die Attraktivität ihres CSP-Standorts und bieten ihren Partnern Reziprozität an, um so den Mangel des *CLOUD Acts* mit Blick auf den Respekt des völkerrechtlichen Territorialitätsprinzips zu heilen. Auch der Mangel hinsichtlich Rechtsschutz wird adressiert: Wenn in den USA ein Verfahren gegen einen ausländischen Staatsangehörigen eröffnet wird, können die amerikanischen Behörden gestützt auf den *CLOUD Act* grundsätzlich um die Herausgabe von dessen Daten ersuchen. Es besteht jedoch eine Ausnahme betreffend die Bekanntgabe der Daten eines ausländischen Staatsangehörigen, mit dessen Heimatstaat die USA ein *Executive Agreement* abgeschlossen haben. Liegt ein solches vor, können die CSP gemäss dem *CLOUD Act* einen Aufhebungs- oder Änderungsantrag stellen, wenn ihr Kunde nicht eine *US person* ist und wenn die Datenbekanntgabe das Recht des QFG verletzen könnte. Ein *Executive Agreement* könnte folglich für Schweizer Staatsangehörige und Personen, die der schweizerischen Gerichtsbarkeit unterstehen, einen gewissen Schutz bieten. Wenn die Gefahr besteht, dass die Bekanntgabe gegen schweizerisches Recht verstösst, könnten die CSP in den USA eine Klage einreichen, um die Rechte der betroffenen Personen zu schützen. Demnach würde ein *Executive Agreement* einen gewissen Schutz vor einem unbefugten Zugriff der US-Strafverfolgungsbehörden auf (Personen-)Daten in der Schweiz bieten. Wie dieser Schutz ausgestaltet sein müsste, damit er übergeordnetem Schweizer Recht zu genügen vermöchte, wird unten bei 5.5 und 5.6 erörtert.

In formeller Hinsicht bemerkenswert ist, dass der *CLOUD Act* als US-Bundesgesetz selbst bereits die Voraussetzungen für einen Abschluss, den materiellen Geltungsbereich sowie wesentliche Inhalte der *Executive Agreements* beschreibt. Dennoch handelt es sich bei den *Executive Agreements* formal betrachtet um bilaterale Staatsverträge, die unter die Wiener Vertragsrechtskonvention (WVK)[54] fallen. Auf diese Verträge und ihre Auslegung finden somit die allgemeinen völkerrechtlichen Regeln und die daraus entwickelte Praxis Anwendung und nicht etwa amerikanisches Recht oder die amerikanische Rechtsprechung. Die Anwendung amerikanischen Rechts wäre nur möglich, wenn ein *Executive Agreement* direkt auf amerika-

[54] Wiener Übereinkommen über das Recht der Verträge vom 23. Mai 1969, SR **0.111**.

nisches Recht verweisen würde. Die zwischen den USA und dem Vereinigten Königreich abgeschlossene Vereinbarung tut das nicht.[55] Sie enthält eigenständige Pflichten und Rechte, die nicht aus nationalem Recht abgeleitet sind. Die Bestimmungen des *CLOUD Acts*, die sich mit den *Executive Agreements* befassen, sind aus einer völkerrechtlichen Perspektive daher eher «Handlungsanweisungen» des US-Gesetzgebers an die eigene Regierung.

Staatsverträge bedürfen in der Schweiz der Zustimmung der Bundesversammlung. Der Bundesrat unterzeichnet sie und unterbreitet sie der Bundesversammlung zur Genehmigung. Nach einem positiven Beschluss ratifiziert er sie (Art. 184 Abs. 2 der Bundesverfassung [nachfolgend BV][56]). Ausnahmsweise darf der Bundesrat Staatsverträge allein abschliessen. Das ist der Fall, wenn sich seine Zuständigkeit aus einem Gesetz oder völkerrechtlichen Vertrag ergibt (Art. 166 Abs. 2 BV). In diesen Fällen wird ihm von der Bundesversammlung die Vertragsschliessungskompetenz mittels Delegation eingeräumt. Ausserdem kann der Bundesrat Staatsverträge selbständig abschliessen, wenn es sich um Verträge von beschränkter Tragweite handelt (so Art. 7*a* Abs. 2 des Regierungs- und Verwaltungsorganisationsgesetzes [RVOG][57]).

Ein *Executive Agreement*, wie es im *CLOUD Act* geregelt ist, wäre kein Vertrag von beschränkter Tragweite. Eine solche Vereinbarung, die es schweizerischen und amerikanischen Behörden ermöglichen würde, Daten direkt bei den CSP einzuholen, würde die datenschutzrechtlichen und verfahrensrechtlichen Garantien der betroffenen natürlichen oder juristischen Personen wesentlich berühren. Zudem enthält die schweizerische Gesetzgebung im Bereich des Datenschutzes zwar eine Delegationsnorm zugunsten des Bundesrates (Art. 67 nDSG), ein *Executive Agreement* wie dasjenige gestützt auf den *CLOUD Act* liesse sich aber nicht darunter subsumieren. Es ist damit davon auszugehen, dass gemäss Artikel 184 Absatz 2 BV die Genehmigung der Bundesversammlung nötig wäre.

Der Abschluss eines *Executive Agreements* hätte erhebliche Auswirkungen auf die Kantone und die Gemeinden. Zum einen sind Daten betroffen, die in den Geltungsbereich des kantonalen Datenschutzrechts fallen. Zum anderen geht es um strafrechtliche Verfahren, die mehrheitlich in die Zuständigkeit der Kantone fallen. Auch wenn der Bund gestützt auf seine umfassende Kompetenz in auswärtigen Angelegenheiten (Art. 54 Abs. 1 BV) Staatsverträge auch in Bereichen abschliessen kann, die in die Kompetenz der Kantone fallen, muss er diese zwingend einbeziehen, wenn er aussenpolitische Entscheide fällen will, «die ihre Zuständigkeiten oder ihre wesentlichen Interessen betreffen» (Art. 55 Abs. 1 BV). Dann muss der Bundesrat die Kantone rechtzeitig und umfassend informieren und ihre Stellungnahmen einholen (Art. 55 Abs. 2 BV). Ein solcher Fall wäre beim Abschluss eines *Executive Agreements* voraussichtlich gegeben.

5.3 Der Begriff «serious crime» (schwere Straftat)

Die *Executive Agreements* können als Grundlage für die Beschaffung von Informationen zum Zweck der Verhütung, Ermittlung, Aufklärung oder Verfolgung von *serious crimes* dienen.[58] Welche Delikte im Sinne des *Executive Agreements* solche *serious crimes* darstellen, kann etwa mittels Deliktskatalog oder Nennung einer Mindeststrafandrohung im *Executive Agreement* verdeutlicht werden.

---

[55] Agreement between the United Kingdom and the USA on Access to Electronic Data for the Purpose of Countering Serious Crime vom 3. Oktober 2019, Fn. 21.

[56] SR **101**

[57] SR **172.010**

[58] DOJ, «Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act», S. 5.

Die erstgenannte Variante (Deliktskatalog) birgt dabei den Nachteil, dass sie statisch ist. Es ist eine stete Aktualisierung vorzunehmen und im Falle von Gesetzesanpassungen könnten Widersprüche entstehen.

Die zweite Variante (Nennung einer Mindeststrafandrohung) ist dynamisch, beinhaltet jedoch einen potenziell weiter gefassten Geltungsbereich (z. B. alle Verbrechen und Vergehen). Dabei zeigt sich die Herausforderung, dass die Straftaten in den verschiedenen Staaten nicht unbedingt gleich qualifiziert werden. Während eine Handlung im einen Staat mit einer hohen Strafe bedroht ist, wird sie vielleicht im anderen Staat milder oder gar nicht bestraft. Es stellt sich also die Frage, ob in beiden Staaten das Kriterium der *serious crimes* erfüllt sein müsste und man also an einer entsprechend «qualifizierten» beidseitigen Strafbarkeit anknüpft – oder ob man den Zugriff auf Daten bei einem CSP selbst dann tolerieren würde, wenn die Tat im eigenen Staat nicht entsprechend strafbar wäre.

Angesichts des nach wie vor ausgesprochen grossen Engagements der USA im Kampf gegen den Terrorismus ist absehbar, dass die umfassende Abdeckung der Zusammenarbeit bei «Terrorismus» auf jeden Fall ein US-Ziel für ein allfälliges *Executive Agreement* wäre. Dies ist vor dem Hintergrund der möglicherweise engeren Definition der terroristischen Organisation im revidierten Artikel 260ter StGB[59] nicht unproblematisch. Besonders deutliche und politisch heikle unterschiedliche Bewertungen lägen voraussichtlich im Bereich der *fiskalischen Delinquenz* vor. Der generelle Ausschluss der *Steuerhinterziehung* (vgl. Art. 3 Abs. 3 IRSG) ist kaum mit den Interessen der USA vereinbar. Dies dürfte ausserdem für den Bereich der *Ehrverletzungsdelikte* gelten. In den USA gilt eine sehr weitgehende Redefreiheit (*freedom of speech*), die grundsätzlich auch Hassrede (*hate speech*) umfasst, soweit darin nicht ein unmittelbarer Aufruf zu Gewalt gesehen wird. Viele solcher Reden wären in der Schweiz längst strafbar, insbesondere unter dem Tatbestand der Rassendiskriminierung (Art. 261bis StGB).

Es zeichnet sich damit ab, dass es herausfordernd wäre, zwischen der Schweiz und den USA einen gemeinsamen Standard für den Begriff der *«serious crimes»* zu finden.

5.4 Die Erhebung elektronischer Daten

Das Ziel des *CLOUD Acts* bzw. eines *Executive Agreements* ist es, elektronische Daten grenzüberschreitend erhebbar zu machen. Eine wichtige Frage ist daher, bei wem welche Daten wie erhoben werden können. So kann beurteilt werden, ob die Erhebungsmodalitäten kompatibel sind oder gegebenenfalls angepasst werden müssen.

In den USA wie in der Schweiz richtet sich die Gesetzgebung an Fernmeldedienstanbieter und damit zusammenhängende Dienstleistungserbringer.

5.4.1 Adressaten

Die US-Gesetzgebung unterscheidet zwischen Anbietern von elektronischen Kommunikationsdiensten (*electronic communication services*) und jenen von Ferncomputerdiensten (*remote computing services*). Ein elektronischer Kommunikationsdienst ist jedes Dienstleistungsangebot, das dem Benutzer erlaubt, drahtgebundene oder elektronische Mitteilungen (*wire or electronic communications*) zu senden oder zu empfangen.[60] «Drahtgebunden» sind

[59] Vgl. BBl **2020** 7891.

[60] «[A]ny service which provides to users thereof the ability to send or receive wire or electronic communications» (18 USC § 2510(15)).

Mitteilungen mittels der menschlichen Stimme.[61] Elektronische Mitteilungen beinhalten vereinfacht gesagt den Transfer von Daten unter Ausschluss von Mitteilungen mittels menschlicher Stimme.[62] Ferncomputerdienste umfassen die öffentliche Bereitstellung von Speicherkapazität oder Prozessorleistung über einen elektronischen Kommunikationsdienst.[63]

In der Schweiz wird vereinfacht gesagt unterschieden zwischen Anbietern von Fernmeldediensten («FDA») und abgeleiteten Kommunikationsdiensten. Fernmeldedienste beinhalten die «fernmeldetechnische Übertragung von Informationen für Dritte»,[64] während sich die abgeleiteten Kommunikationsdienste «auf Fernmeldedienste stützen und eine Einweg- oder Mehrwegkommunikation ermöglichen».[65] Nach der Botschaft des Bundesrates meint die Einwegkommunikation z. B. das Hochladen bzw. Online-Bearbeiten von Dokumenten (z. B. Google Docs oder Microsoft Office online). Abgeleitete Kommunikationsdienste sind demnach u. a. Webhosting-Angebote, Plattformen für den Dokumentenaustausch und nicht zuletzt Cloud-Dienste.[66] Die Mehrwegkommunikation bezieht sich auf die Interaktion zwischen Nutzern, wie sie z. B. E-Mail, eine Chatfunktion oder eine Voice-Over-IP-Anwendung wie Skype ermöglicht.[67]

Die Ausgangslage in beiden Rechtsordnungen (USA und Schweiz) zeigt sich vor diesem Hintergrund zwar nicht als «identisch», doch immerhin auch nicht so unterschiedlich, dass eine Einigung auf eine gemeinsame Definition der Adressaten in einem *Executive Agreement* als unmöglich erschiene.

5.4.2 Datenart

Bei der Datenart bestehen ebenfalls Parallelen. Grundsätzlich wird auf beiden Seiten des Atlantiks zwischen Bestands-, Rand- und Inhaltsdaten unterschieden. Bestandsdaten (*basic subscriber information*[68]) im Sinne des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs BÜPF geben Auskunft über den Kunden und das Vertragsverhältnis mit dem Provider.[69] Randdaten im Sinne des BÜPF oder Metadaten (*transactional data*) beschreiben vereinfacht gesagt insbesondere, wer wann mit wem wie kommuniziert

---

[61] «‹[W]ire communication› means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce» (18 USC § 2510(1)). «‹[A]ural transfer› means a transfer containing the human voice at any point between and including the point of origin and the point of reception» (18 USC § 2510(18)).

[62] «‹[E]lectronic communication› means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include— (A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device (as defined in section 3117 of this title); or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds» (18 USC § 2510(12)).

[63] «[T]he term ‹remote computing service› means the provision to the public of computer storage or processing services by means of an electronic communications system» (18 USC § 2711(2)).

[64] Art. 3 Bst. b Fernmeldegesetz (FMG, SR **784.10**).

[65] Art. 2 Bst. c Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF, SR **780.1**).

[66] So ausdrücklich die Botschaft, BBl **2013** 2708.

[67] BBl **2013** 2708; anzumerken ist, dass derzeit eine Revision des FMG läuft, welche auch eine Revision des Art. 2 BÜPF enthält, mit dem Ziel, dieses System anzupassen und insb. die Pflichten der Anbieterinnen abgeleiteter Kommunikationsdienste genauer zu definieren.

[68] Dazu gehören insbesondere Name, Adresse, Art und Dauer des in Anspruch genommenen Dienstes, Zahlungsinstrumente inkl. Kreditkarten- und Kontonummern: 18 USC § 2703(c)(2).

[69] Vgl. die Definition in Art. 18 Abs. 3 der Budapest-Konvention: «[A]lle in Form von Computerdaten oder in anderer Form enthaltenen Informationen, die bei einem Diensteanbieter über Teilnehmer seiner Dienste vorliegen, mit Ausnahme von Verkehrsdaten oder inhaltsbezogenen Daten, und durch die Folgendes festgestellt werden kann:

a. die Art des genutzten Kommunikationsdienstes, die dafür getroffenen technischen Massnahmen und die Dauer des Dienstes;

b. die Identität des Teilnehmers, seine Post- oder Hausanschrift, Telefon- und sonstige Zugangsnummer sowie Angaben über Rechnungsstellung und Zahlung, die auf der Grundlage des Vertrags oder der Vereinbarung in Bezug auf den Dienst zur Verfügung stehen;

c. andere Informationen über den Ort, an dem sich die Kommunikationsanlage befindet, die auf der Grundlage des Vertrags oder der Vereinbarung in Bezug auf den Dienst vorliegen.»

hat.[70] Inhalt (*content*) schliesslich bezeichnet die Substanz der eigentlichen Nachricht in Wort oder Schrift. Je näher der staatliche Eingriff an den Kern der Kommunikation, d. h. an den Inhalt kommt, desto intrusiver und daher rechtfertigungsbedürftiger ist er. In den USA und in der Schweiz können Bestandsdaten ohne gerichtliche Genehmigung erhoben werden. Die Erhebung von Rand- und Inhaltsdaten benötigt in beiden Ländern eine gerichtliche Genehmigung. In der Schweiz stellt die Erhebung von Rand- oder Inhaltsdaten eine Zwangsmassnahme dar, die Erhebung von Bestandsdaten jedoch nicht.

5.4.3 Erhebungsmodalitäten

So weit ist die Lage in den beiden Ländern ähnlich. Einen wichtigen Unterschied gibt es bei den Modalitäten der Datenerhebung. In der Schweiz erfolgt diese über den Dienst für die Überwachung des Post- und Fernmeldeverkehrs (Dienst ÜPF).[71] Dieser hat die Funktion einer Drehscheibe zwischen den Behörden und CSP: Die Überwachungsanordnungen sowie die resultierenden Daten werden – gegebenenfalls mit Ermächtigung des Zwangsmassnahmengerichts – über diese Drehscheibe ausgetauscht.

Der *CLOUD Act* hingegen basiert auf der Prämisse, dass die CSP direkt aufgefordert werden und verpflichtet sind, die Daten herauszugegeben. Ein solcher Direktzugriff auf die CSP würde aber die folgenden Problempunkte aufwerfen:

- Es wäre systemwidrig, den US-Behörden den Direktzugriff auf CSP zu ermöglichen, während die Schweizer Behörden den Dienst ÜPF zwischenschalten müssen. Es stellt sich die Frage der Gleichbehandlung. Und ein wichtiger Aspekt hierzu ist die Kostenfrage: Die Schweizer Behörden zahlen für die Nutzung des Dienstes ÜPF hohe Gebühren, die beim Direktzugriff nicht – oder nicht so – anfallen würden.
- Dies würde ferner zu einer Erhebung auf zwei Gleisen führen: Die CSP, die unter dem BÜPF Abläufe und Protokolle für die Abfrage durch den Dienst ÜPF eingerichtet haben, müssten parallel dazu US-Behörden auf anderem Weg bedienen.
- Ob die Echtzeit-Überwachung so überhaupt möglich wäre, ist fraglich: Die Überwachung wird i. d. R. durch den CSP auf Anordnung der Strafverfolgungsbehörde und Verfügung des Dienstes ÜPF vorgenommen, manchmal muss sie aber nur vom Anbieter ermöglicht und geduldet werden. Dem Vernehmen nach bedingt die Überwachung umfangreiche technische Vorbereitungen, die von Fall zu Fall stark variieren. Es ist deshalb zweifelhaft, ob dies im bilateralen Verhältnis zwischen einer US-Behörde und einem Schweizer CSP bewerkstelligt werden könnte.
- Die Verfügungen des Dienstes ÜPF sind Verfügungen i. S. v. Artikel 5 des Bundesgesetzes vom 20. Dezember 1968 über das Verwaltungsverfahren (nachfolgend VwVG)[72]. Der betroffene CSP kann dagegen (insbesondere gegen Verfügungen, mit denen eine Überwachung zur Umsetzung einer Überwachungsanordnung angeordnet wird, die von einer Strafverfolgungsbehörde erlassen/übermittelt wurde) in eingeschränktem Rahmen Rechtsmittel ergreifen. Dies könnte *de facto* noch stärker eingeschränkt oder gar ausser Kraft gesetzt werden, wenn der Dienst ÜPF keine Rolle mehr spielt bzw. diese Verfügungen nicht mehr übermittelt.

Denkbar wäre es, den US-Behörden den Zugang ebenfalls über den Dienst ÜPF zu gewähren. Dies würde allerdings eine massive Aufgabenausweitung für den Dienst ÜPF bedeuten. Ausserdem «passt» der *CLOUD Act* nach seinem Wortlaut nicht auf diese Lösung, da er

[70] Vgl. die Definition in Art. 8 Bst. b BÜPF: «Daten, aus denen hervorgeht, mit wem, wann, wie lange und von wo aus die überwachte Person Verbindung hat oder gehabt hat, sowie die technischen Merkmale der entsprechenden Verbindung».

[71] «Dienst für die Überwachung des Post- und Fernmeldeverkehrs gemäss Artikel 269 der Strafprozessordnung (StPO)», vgl. Art. 3 BÜPF.

[72] SR **172.021**

von der Prämisse ausgeht, dass die Daten direkt beim CSP erhoben werden (allerdings könnten evtl. im *Executive Agreement* die nötigen Anpassungen vereinbart werden).

Die Vorteile einer Lösung via Dienst ÜPF lägen aber auf der Hand: Was die Datenerhebung betrifft, wäre insoweit Gleichbehandlung zwischen US- und den schweizerischen Behörden erstellt (u. a. müssten die US-Behörden mit denselben Gebühren belastet werden). Ausserdem hätten die US-Behörden einen *single point of contact*, einen einzigen Ansprechpartner, was im internationalen Verkehr ohnehin von Vorteil ist. Noch weitergedacht, könnte der Dienst ÜPF so die Rolle einer Zentralbehörde für die US-Datenerhebung einnehmen. Damit könnten Bedenken begegnet werden, die im Wegfallen der Aufsichtsfunktion des BJ begründet liegen: Beim direkten Zugriff, wie er im *CLOUD Act* vorgesehen ist, ist nicht klar, wer die in der Rechtshilfe geltenden Ausschlussgründe prüft, wer die Einhaltung des Spezialitätsgrundsatzes überwacht etc. Wie aber der schweizseitige Rechtsschutz funktionieren könnte, ist – wie unten aufgezeigt wird – ebenso noch zu definieren (siehe Ziff. 5.6)

5.5 Schutz der Grundrechte, insbesondere der Daten und des Privatlebens

5.5.1 Die EU-Ebene: Verhältnis zwischen dem *CLOUD Act* und der EU-Datenschutz-Grundverordnung DSGVO

5.5.1.1 Vereinbarkeit des *CLOUD Acts mit der DSGVO*

Die Vereinbarkeit des *CLOUD Acts* und eines allfälligen, gestützt auf dessen Grundsätze abgeschlossenen *Executive Agreements* mit dem Recht der EU, namentlich deren Datenschutz-Grundverordnung[73] (DSGVO), die seit 2018 in Kraft ist, ist auch für die Schweiz von Bedeutung. Die DSGVO ist für die Schweiz als Nicht-Mitgliedstaat der EU zwar nicht unmittelbar anwendbar, da es sich nicht um eine Weiterentwicklung des Schengen-Acquis handelt. Ihre Bestimmungen gelten aber für Unternehmen in der Schweiz, die gemäss Artikel 3 DSGVO in den Geltungsbereich der Verordnung fallen. Dies ist vorliegend namentlich dann der Fall, wenn der seine Dienstleistungen erbringende CSP innerhalb der EU niedergelassen ist oder, bei fehlender Niederlassung, wenn eine Datenbearbeitung im Zusammenhang damit steht, betroffenen Personen in der EU Dienstleistungen anzubieten oder deren Verhalten zu beobachten, soweit dies in der EU erfolgt.

Um mit der EU und ihren Mitgliedstaaten ungehindert Personendaten austauschen zu können, muss die Schweiz von der Europäischen Kommission weiterhin als Drittstaat mit einem angemessenen Datenschutzniveau gemäss Artikel 45 DSGVO anerkannt bleiben. Die Beibehaltung des *Angemessenheitsbeschlusses* setzt voraus, dass das schweizerische Recht den datenschutzrechtlichen Anforderungen der Verordnung gleichwertig ist. Die Beurteilung der Kompatibilität des *CLOUD Acts* und des allfälligen Abschlusses eines darauf gründenden *Executive Agreements* mit der DSGVO hat entsprechend Folgen im Hinblick auf den für die Schweiz notwendigen Angemessenheitsbeschluss der EU. Dafür spricht auch, dass die Europäische Kommission in ihrer Beurteilung der Angemessenheit des UK-Datenschutzniveaus mit Blick auf die DSGVO das UK-US-*CLOUD Act* Agreement auf dessen Vereinbarkeit mit dem EU-Datenschutzrecht hin überprüfte.[74] Nicht geprüft wird im vorliegenden Kontext demgegenüber die Situation mit Blick auf die Richtlinie (EU) 2016/680[75] zum Datenschutz in

[73] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG; ABl. L 119/2016 v. 4. Mai 2016.

[74] Durchführungsbeschluss der Kommission vom 28. Juni 2021 gemäss der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zur Angemessenheit des Schutzes personenbezogener Daten durch das Vereinigte Königreich: C(2021) 4800 final, Ziff. 153 - 156.

[75] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung

Strafsachen. Sie ist zwar Schengen-relevant und damit von der Schweiz anzuwenden, hier aber insofern nicht von Bedeutung, als der *CLOUD Act* Datenbekanntgaben von privaten CSP *an* Strafverfolgungsbehörden und nicht Datenbekanntgaben *durch* (Strafverfolgungs-)Behörden regelt, welche die (ausschliesslichen) Adressaten der Richtlinie sind. Das UK-US-*CLOUD Act* Agreement scheint schliesslich auch keine Bedeutung für die Beurteilung der Angemessenheit des UK-Datenschutzniveaus mit Blick auf die Richtlinie (EU) 2016/680 durch die Europäische Kommission gehabt zu haben.[76]

Die Prüfung der massgebenden Rechtsgrundlagen ergibt zusammengefasst, dass Datenbearbeitungen gestützt auf Anordnungen einer US-Strafverfolgungsbehörde im Rahmen des *CLOUD Acts* im Hinblick auf die *Rechtmässigkeit* als problematisch zu beurteilen sind. Dies gilt sowohl für die Aufbewahrung von Personendaten als auch für deren Offenlegung.

Zwar anerkennt neben dem Europäischen Datenschutzausschuss (EDSA) und dem Europäischen Datenschutzbeauftragten (EDSB) auch die Europäische Kommission im Grundsatz, dass gestützt auf die einschlägigen Artikel 6 und insbesondere Artikel 49 DSGVO in ganz bestimmten Ausnahmesituationen eine Datenbearbeitung bzw. die Bekanntgabe von Daten an einen Drittstaat auch dann gerechtfertigt sein kann, wenn dieser Staat weder über einen Angemessenheitsbeschluss der Europäischen Kommission noch über spezifische Garantien (Art. 46 DSGVO) mit Bezug auf den Schutz der Daten verfügt. Dies wäre namentlich der Fall, wenn der CSP die Personendaten *zum Schutz der lebenswichtigen Interessen der betroffenen Person selbst* bekannt geben würde (Art. 6 Abs. 1 Bst. d i. V. m. Art. 49 Abs. 1 Bst. f DSGVO). Nicht ausgeschlossen ist des Weiteren, dass sich eine solche Datenbekanntgabe durch ein in der EU und den Mitgliedstaaten anerkanntes öffentliches Interesse rechtfertigen liesse, sofern beispielsweise konkrete Anzeichen für einen schweren Straftatbestand oder einen terroristischen Anschlag in der EU bestehen würden (Art. 49 Abs. 1 Bst. d DSGVO). Jedoch dürfte dieser Ausnahmetatbestand in der Praxis nur sehr schwer zu erfüllen sein, da die DSGVO solche Bekanntgaben aufgrund der besonderen Risiken für die Rechte und Freiheiten der betroffenen Personen nur unter sehr strikt auszulegenden Voraussetzungen und in absoluten Ausnahmefällen erlaubt.

Auch im Hinblick auf weitere Kernelemente der DSGVO könnten sich Datenbearbeitungen gestützt auf den *CLOUD Act* als heikel erweisen:

Unter dem Gesichtspunkt der Transparenz könnte es problematisch sein, dass die US-Strafverfolgungsbehörden in gewissen Fällen nicht verpflichtet sind, die betroffenen Personen über die Bekanntgabe der Daten zu benachrichtigen und mittels gerichtlicher Verfügung auch den CSP verpflichten können, die betroffene Person nicht über die Bekanntgabe ihrer Daten zu informieren.[77] Nach europäischem Rechtsverständnis wird die Information der betroffenen Person über jeden behördlichen Zugang zu ihren Daten auch im Bereich der Strafverfolgung

---

von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates; ABl L119/89 v. 4.5.2016.

[76] Durchführungsbeschluss der Kommission vom 28. Juni 2021 gemäss der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates zur Angemessenheit des Schutzes personenbezogener Daten durch das Vereinigte Königreich: C(2021) 4801 final. Um der Stellungnahme 15/2021 des Europäischen Datenschutzausschusses zum Angemessenheitsbeschluss von UK nach der Richtlinie (EU) 2016/680 Rechnung zu tragen, welcher insbesondere die im UK-US CLOUD Act Agreement vorgesehenen Abhörungsanordnungen äusserst kritisch beurteilt, hat die Europäische Kommission ihren Beschluss ergänzt. Im Rahmen der Überwachung der künftigen datenschutzrelevanten Entwicklungen im Vereinigten Königreich wird sie besondere Aufmerksamkeit auf den Abschluss von internationalen Abkommen legen, welche Auswirkungen auf das gegenwärtige Datenschutzniveau haben (Rz. 165 des Beschlusses). Selbst wenn jedoch die Richtlinie (EU) 2016/680 in der EU so ausgelegt wird, dass sie zusätzlich zu Datenbekanntgaben auch Datenbearbeitungen durch Strafverfolgungsbehörden umfasst, gilt in der Schweiz ein engeres Verständnis des Geltungsbereichs dieser Richtlinie, welchen wir vorliegend nicht tangiert sehen.

[77] *CLOUD Act,* § 2703 (b) (1) und § 2705 (b).

und -vollstreckung als unverzichtbar erachtet.[78] Gemäss EuGH muss die betroffene Person spätestens dann über die Weitergabe ihrer Personendaten an ausländische Strafverfolgungsbehörden informiert werden, wenn dies die entsprechenden Ermittlungen nicht mehr beeinträchtigen kann.[79]

Mit Bezug auf die Verhältnismässigkeit kommen der EDSA und der EDSB zum Schluss, dass im *CLOUD Act* diesem Grundsatz im Allgemeinen Rechnung getragen wird.[80] So kann eine US-Strafverfolgungsbehörde die Offenlegung von Personendaten nur verlangen, wenn ein Gericht die Herausgabe zuvor genehmigt und die Behörde durch eidesstattliche Erklärung dargelegt hat, dass ein hinreichender Verdacht besteht, dass ein bestimmtes Verbrechen stattgefunden hat oder stattfindet und die herausverlangten Informationen Beweise für dieses bestimmte Verbrechen enthalten.[81] Die Herausgabeanordnung muss die geforderten Personendaten zudem genau beschreiben, da sogenannte *Fishing expeditions*, um zu sehen, ob Beweise vorhanden sind, nicht zulässig sind.[82] Die europäischen Datenschutzbehörden stellen aber auch fest, dass im Falle anderer Formen von Anfragen keine entsprechenden richterlichen Kontrollen verlangt werden.[83] Hier müsste im Einzelfall geprüft werden, ob eine Datenbearbeitung verhältnismässig wäre oder nicht.

Im Gegensatz zur DSGVO, welche die Personendaten aller natürlichen Personen gleichermassen schützt, ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsortes, unterscheidet der *CLOUD Act* zwischen Daten von «US-Personen» und von anderen Personen. Namentlich kann im Falle des Vorliegens eines *Executive Agreements* ein CSP nur dann die gerichtliche Kontrolle einer Anordnung einer US-Strafverfolgungsbehörde im Falle kollidierender rechtlicher Verpflichtungen verlangen, wenn es sich nicht um Personendaten von US-Personen handelt.[84] Gemäss EDSB ist hingegen jegliche Ungleichbehandlung aus datenschutzrechtlicher Sicht aufgrund der Staatsangehörigkeit oder der Ansässigkeit der betroffenen Person mit der DSGVO unvereinbar.[85]

Der *CLOUD Act* sieht keine datenschutzrechtlichen Garantien für die betroffenen Personen vor, etwa in Form eines Zugangs- oder Auskunftsrechts hinsichtlich ihrer Daten. Vielmehr erlaubt er, in gewissen Fällen ganz von einer Information der betroffenen Personen über eine Datenbekanntgabe an eine US-Strafverfolgungsbehörde abzusehen.[86] Dies widerspricht grundsätzlich Artikel 8 Absatz 2 der europäischen Grundrechtscharta[87], wo in Bezug auf die Bearbeitung von Personendaten explizit das Recht auf Auskunft und das Recht auf Berichtigung garantiert wird.

Der *CLOUD Act* sieht keine Möglichkeit für die von einer Herausgabeanordnung betroffene Person vor, sich gegen die Bekanntgabe ihrer Personendaten zur Wehr zu setzen. Eine begrenzte Abwehrmöglichkeit ist in Fällen einer Rechtskollision nur für den CSP vorgesehen, und nur unter der Voraussetzung, dass ein *Executive Agreement* zwischen der USA und

---

78 Siehe unter anderem EuGH, Gutachten 1/15 EU-Kanada PNR-Abkommen, ECLI:EU:C:2017:592, Rn. 220 und Stellungnahme 23/2018 des EDSA, S. 19.

79 EuGH, Gutachten 1/15 EU-Kanada PNR-Abkommen, ECLI:EU:C:2017:592, Rn. 220.

80 EDSA/EDSB, Initial legal assessment, S. 2.

81 DOJ, "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the *CLOUD Act*", S. 8.

82 Idem, S. 8.

83 EDSA/EDSB, Initial legal assessment, S. 2.

84 *CLOUD Act* § 2703.

85 Stellungnahme 2/2019 des EDSB, Ziff. 50.

86 *CLOUD Act* § 2703 (b) (1) und § 2705 (b).

87 Charta der Grundrechte der Europäischen Union, ABl. 2000/C 364/01 vom 18.12.2000.

dem entsprechenden Staat abgeschlossen wurde.[88] Der betroffenen Person steht gegen eine solche Anordnung hingegen weder eine Beschwerde an eine unabhängige Aufsichtsbehörde zur Verfügung, noch ein gerichtlicher Rechtsbehelf gegen die Bekanntgabe. Das Fehlen eines Rechts auf einen wirksamen gerichtlichen Rechtsbehelf steht im Widerspruch zu dem in Artikel 47 der europäischen Grundrechtscharta garantierten Recht auf wirksamen gerichtlichen Rechtsschutz. Ausserdem betont der EuGH die Wichtigkeit, dass eine betroffene Person einen administrativen Rechtsbehelf bei einer unabhängigen Kontrollstelle einlegen kann.[89]

Als wesentliche Garantie des Datenschutzes schreibt Artikel 8 Absatz 3 der europäischen Grundrechtscharta die Kontrolle durch eine unabhängige Stelle vor. Der EDSB betont in dieser Hinsicht, dass auch die zuständigen Behörden des Staates, in deren Regelungshoheit sich die angefragten Personendaten befinden, in die Verfahren um Bekanntgabe elektronischer Beweismittel mit einbezogen werden sollen, damit ein wirksamer Schutz der Grundrechte garantiert werden kann.[90] Entsprechend sollten auch die zuständigen Datenschutzbehörden bei direkten Anordnungen an die Dienstleister benachrichtigt werden, um eine Kontrolle zu ermöglichen.[91] Dass CSP Personendaten an eine US-Strafverfolgungsbehörde bekannt geben, ohne die eigenen zuständigen Behörden zu benachrichtigen, könnte sich vor diesem Hintergrund als problematisch erweisen.

5.5.1.2 Fazit: Risiko des Abschlusses eines *Executive Agreements* mit den USA im Hinblick auf den Angemessenheitsbeschluss der Schweiz

Der in Ziff. 5.5.1.1 erwähnte *Angemessenheitsbeschluss* wird von der Kommission regelmässig, nämlich mindestens alle vier Jahre, überprüft (Art. 97 DSGVO). Zu den wesentlichen Aspekten, die bei der Überprüfung berücksichtigt werden, gehören die Datenschutzvorschriften, die Vorschriften betreffend die Weiterübermittlung personenbezogener Daten an ein anderes Drittland sowie der Abschluss internationaler Übereinkommen in Bezug auf den Schutz von Personendaten. Der EuGH hat im Urteil *Schrems II* im Zusammenhang mit dem Zugriff von Behörden auf Personendaten, welche im Empfängerstaat zu Zwecken der nationalen Sicherheit weitergegeben wurden, präzisiert, dass die Kommission bei ihrem Entscheid das im Empfängerstaat geltende innerstaatliche Recht berücksichtigen muss. Das entscheidende Kriterium für die Angemessenheit ist, ob die Regelung, die den Zugriff der Behörden im Empfängerstaat zum Zweck der nationalen Sicherheit erlaubt, auch klare Bestimmungen zur Beschränkung des Zugriffs enthält, also klar festhält, unter welchen Voraussetzungen und Umständen dieser Zugriff erlaubt ist. Er muss auf das absolut Nötigste beschränkt sein.[92] Darüber hinaus muss die einschlägige Regelung im Empfängerstaat wirksame und durchsetzbare Rechte zum Schutz der betroffenen Person vor allfälligen Missbräuchen vorsehen.[93]

Der Schweiz wurde im Jahr 2000 von der EU attestiert, dass sie über ein angemessenes Datenschutzniveau verfügt. Dieser Angemessenheitsbeschluss gilt vorerst auch unter der seit dem 25. Mai 2018 anwendbaren DSGVO weiter. Im Frühjahr 2019 hat die Europäische Kommission mit der erneuten Evaluierung der Schweiz begonnen. Dabei führt sie die Überprüfung auf der Grundlage des geltenden schweizerischen Rechts durch, hat sich aber bereit gezeigt, die anlässlich der Revision des Datenschutzgesetzes (DSG) einzuführenden Stärkungen

[88] Siehe hierzu vorne Ziffer 3.2.2.

[89] Entscheid des EuGH, *Maximilian Schrems vs. Data Protection Commissioner*, C-362-14, Rn. 56 – 58.

[90] Stellungnahme 2/2019 des EDSB, Ziff. 28. Im Kontext mit den Europäischen Herausgabe- und Sicherungsanordnungen für Elektronische Beweismittel in Strafsachen, siehe auch Stellungnahme 23/2018 des EDSA, S. 16.

[91] Siehe Stellungnahme 23/2018 des EDSA, S. 8.

[92] EuGH, *Schrems II,* E. 175-176.

[93] EuGH, *Schrems II,* E. 177-178.

des Datenschutzes zu berücksichtigen, sofern die Totalrevision des DSG (nDSG) zeitnah abgeschlossen wird. Da das nDSG am 25. September 2020 von den Eidgenössischen Räten genehmigt wurde (vgl. unten 5.5.2.1.) und das Inkrafttreten des neuen Gesetzes sowie der dazugehörigen Verordnungen für die zweite Hälfte 2022 geplant ist, sollte dies gegeben sein.

In ihrem Beschluss über die Angemessenheit des UK Datenschutzniveaus gemäss DSGVO – welcher von der Europäischen Kommission zusammen mit dem Beschluss über die Angemessenheit von UK nach der Richtlinie (EU) 2016/680 am 28. Juni 2021 verabschiedet wurde – beurteilte die Kommission auch das UK-US *CLOUD Act* Agreement.[94] Dies zeigt, dass auch der Inhalt eines *Executive Agreements* zwischen der Schweiz und den USA im Hinblick auf eine erneute Beurteilung der Angemessenheit des schweizerischen Datenschutzniveaus berücksichtigt würde.

Im Beschluss mit Blick auf UK hält die Europäische Kommission fest, dass beim Inkrafttreten des UK-US *CLOUD Act* Agreements Daten, welche aus der EU an CSP in UK übertragen werden, Gegenstand von Herausgabeanordnungen von US-Strafverfolgungsbehörden sein könnten. Eine Bewertung der Bedingungen und Garantien, unter denen solche Herausgabeanordnungen ausgeführt werden, ist deshalb im Hinblick auf die Entscheidung der Angemessenheit des UK Datenschutzniveaus relevant. Zwar beurteilt die Kommission das Abkommen im Hinblick auf die Anforderungen der DSGVO nicht per se als unangemessen. Einerseits hebt die Europäische Kommission hervor, dass sie selbst über ein Mandat der Mitgliedstaaten verfügt, in diesem Bereich Verhandlungen mit den USA zu führen und deshalb kein «*double standard*» hinsichtlich eines entsprechenden Abkommens zwischen UK und USA geschaffen werden dürfe. Andererseits bewertet die Kommission insbesondere die im Abkommen festgelegten strengen Anforderungen an Herausgabeanordnungen und an Echtzeit-Überwachungen als positiv, sowie dass darin durch einen Verweis auf das Rahmenabkommen zwischen der EU und den USA[95] alle in jenem festgelegten Garantien und Rechte sinngemäss Anwendung finden.[96] Die Kommission hält zudem fest, dass die britischen Behörden ihr gegenüber bestätigten, dass das Abkommen erst in Kraft treten soll, wenn die Einhaltung dieser Datenschutzstandards für alle im Rahmen dieses Abkommens übermittelten Daten sichergestellt sei.

Wesentlich skeptischer zeigen sich in diesem Hinblick der EDSA[97] und das Europäische Parlament[98]. Diese bezweifeln insbesondere, ob mit einem blossen Verweis auf das EU-US Rahmenabkommen die darin garantierten datenschutzrechtlichen Ansprüche durch betroffene Personen nach britischem Recht wirksam und einklagbar wären sowie ob die darin vorgesehenen Schutzmassnahmen auf alle Herausgabeanordnungen der US-Strafverfolgungsbehörden Anwendung fänden – oder ob nicht doch amerikanisches Recht vorgehe. Die Kommission hält diesen Befürchtungen entgegen, dass der Angemessenheitsbeschluss eine kontinuierliche Überwachung der relevanten Entwicklungen in diesem Bezug vorsehe. Die Kommission werde dabei ein besonderes Augenmerk auf die Anwendung und die Umsetzung der Garantien des Rahmenabkommens im Rahmen von entsprechenden Datenübermittlungen richten und die notwendigen Konsequenzen ziehen, sofern es Anzeichen dafür gebe, dass

---

94 Rz. 153 – 156 des Angemessenheitsbeschlusses von UK nach der DSGVO.

95 Siehe FN 41

96 Artikel 9 Absatz 1 des UK-US CLOUD Act Agreements hält entsprechend fest, dass ein diesem Rahmenabkommen gleichwertiger Schutz «auf alle Personendaten Anwendung findet, welche bei der Ausführung von Anordnungen, die gestützt auf das Abkommen ergehen, erhoben werden. »

97 Stellungnahme des EDSA 14/2021 vom 13. April 2021 zum Entwurf des Durchführungsbeschlusses der Europäischen Kommission gemäss der Verordnung (EU) 2016/679 über die Angemessenheit des Schutzes personenbezogener Daten im Vereinigten Königreich, Rz. 88 ff.

98 Entschliessung des Europäischen Parlaments vom 21. Mai 2021 zu der Angemessenheit des Schutzes personenbezogener Daten durch das Vereinigte Königreich (2021/2594(RSP)), Ziff. 25.

ein gleichwertiges Schutzniveau nicht mehr gewährleistet sei. Als wesentliche Massnahme in dieser Hinsicht betont die Europäische Kommission auch die in Artikel 4 des Angemessenheitsbeschlusses festgelegte *«sunset clause»*, gemäss welcher die Geltungsdauer des Angemessenheitsbeschlusses des UK Datenschutzniveaus nach vier Jahren automatisch endet, sofern keine zusätzliche Vereinbarung getroffen wird.

Selbst wenn nach Ansicht der Europäischen Kommission das UK-US-*CLOUD Act* Agreement mit den europäischen Datenschutzstandards vereinbar ist, ist die Ausgangslage mit Blick auf die Schweiz eine andere. So setzt UK, mit Ausnahme des Bereiches der Einwanderungskontrolle,[99] im Unterschied zur Schweiz die DSGVO zumindest momentan noch vollständig um. Zudem stellen der Verweis auf das Rahmenabkommen zwischen der EU und den USA sowie die entsprechende Versicherung der britischen Behörden, das Abkommen nur bei Gewährleistung der entsprechenden Garantien in Kraft treten zu lassen, nach Ansicht der Kommission sicher, dass die Personendaten, welche gestützt auf das UK-US *CLOUD Act* Abkommen übermittelt würden, weiterhin dem Schutz eines EU-Rechtsinstrumentes unterstehen.

In diesem Hinblick scheinen die Möglichkeiten für die Schweiz eingeschränkter. Aufgrund des engen und aus datenschutzrechtlicher Sicht problematischen Rahmens des *CLOUD Acts* ist nicht davon auszugehen, dass die Schweiz mit dem Abschluss eines *Executive Agreements* den oben beschriebenen datenschutzrechtlichen Anforderungen genügen könnte. So verfolgt auch die Kommission mit ihren eigenen Verhandlungen mit den USA das Ziel eines *umfassenden Abkommens*, das den Austausch elektronischer Beweismittel regelt und damit weitergeht als ein *Executive Agreement*, wie es im *CLOUD Act* vorgesehen ist. Ein umfassender Rechtsschutz, wie er vom europäischen Datenschutzrecht verlangt und nach Ansicht der Kommission im Fall von UK gewährleistet ist, könnte für die Schweiz deshalb wohl nur durch den Abschluss eines *umfassenden* Abkommens mit den USA erreicht werden. Dieses müsste den Austausch elektronischer Beweismittel regeln und *gleichzeitig* ein hohes, den europäischen und nationalen Standards entsprechendes Datenschutzniveau vorsehen. Schliesslich müsste im Einklang mit den Forderungen des EDSA sichergestellt werden, dass ein solches Abkommen im Fall des Datenaustauschs zwischen CSP und Strafverfolgungsbehörden *dem US-Recht vorginge*.

Überdies ist anzunehmen, dass die Europäische Kommission den zum UK-US *CLOUD Act* Agreement geäusserten Bedenken des EDSA und des Europäischen Parlaments im Hinblick auf künftige Angemessenheitsbeschlüsse mehr Gewicht einräumen wird als im Fall von UK. Hier schien der Zeitdruck ein wesentlicher Faktor zu sein, nach Ende der Übergangsfrist eine Rechtsgrundlage für Datentransfers aus der EU nach UK zu haben. Dieser Faktor scheint die Kommission dazu bewogen zu haben, trotz dem Widerstand des Parlaments und des EDSA nicht von ihrem Vorhaben abzuweichen, die Angemessenheitsbeschlüsse mit Blick auf UK bis Ende Juni 2021 zu verabschieden. Wie bereits erwähnt, wurden die Beschlüsse am 28. Juni verabschiedet und sind auf 2025 befristet.

In ihren Angemessenheitsbeschlüssen mit Blick auf UK betont die Europäische Kommission, dass sie sich bei ihren Beurteilungen wesentlich vom Urteil des EuGH zur Rechtssache *Schrems II* vom 16. Juli 2020 leiten lasse. Dies spricht ebenfalls für ein bedachtsames Vorgehen der Schweiz, hat der Gerichtshof darin doch befunden, dass die Europäische Kommission beim Entscheid über die Angemessenheit der Bekanntgabe von Daten an die USA im

[99] Aufgrund des Urteils des UK *Court of Appeal* vom 26. Mai 2021, mit welchem die in UK vorgesehenen Ausnahmeregelungen von datenschutzrechtlichen Ansprüchen im Bereich der Einwanderungskontrolle als mit der DSGVO unvereinbar beurteilt werden, schliesst die Europäische Kommission diesen Bereich vom Angemessenheitsbeschluss nach der DSGVO vorläufig aus. Sobald feststeht, ob und wie UK diese Mängel beheben wird, wird die Kommission einen Wiedereinbezug prüfen und den Beschluss gegebenenfalls entsprechend anpassen (Rz. 6 des Angemessenheitsbeschlusses von UK nach der DSGVO).

Rahmen des *Privacy-Shield-Abkommens* nicht berücksichtigt hat, dass die Bestimmungen zu den staatlichen Überwachungsprogrammen im amerikanischen Recht keine hinreichenden Garantien zur Erfüllung der Anforderungen der DSGVO bezüglich Datenschutz und keinen genügenden Rechtsschutz für die betroffenen «nicht US Personen» bieten.[100] Daraus kann geschlossen werden, dass die Europäische Kommission im Rahmen künftiger Angemessenheitsbeschlüsse bei der Beurteilung der Garantien, die völkerrechtliche Verträge zur Behebung solcher grösserer Datenschutzlücken bieten, noch strenger sein wird. Überdies zeigen die derzeit vorgenommenen Angleichungen von weiteren Rechtsakten auf dem Gebiet der Strafverfolgung und -vollstreckung an die Richtlinie (EU) 2016/680,[101] dass die EU künftig die Voraussetzungen für den Datenaustausch in diesen Bereichen noch strenger handhaben wird.

5.5.2 Rechtmässigkeit der Bearbeitung und Bekanntgabe von Daten gestützt auf eine Herausgabeanordnung auf der Grundlage des *CLOUD Acts* nach Schweizer Recht

5.5.2.1 Der vorliegend relevante datenschutzrechtliche Rahmen in der Schweiz

Auf Bundesebene ist der Datenschutz gegenwärtig primär im Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG)[102] geregelt. Gegenstand des DSG ist die Bearbeitung von Daten durch Bundesorgane wie auch durch Privatpersonen. Zahlreiche bereichsspezifische Datenschutznormen regeln zudem in Spezialgesetzen die Bearbeitung von Daten durch Bundesorgane. Für die Bearbeitung von Daten durch Bundesorgane und Private finden zudem die Verordnung vom 14. Juni 1993[103] zum Bundesgesetz über den Datenschutz (VDSG) sowie die Verordnung vom 28. September 2007[104] über die Datenschutzzertifizierungen Anwendung. Die Bearbeitung von Daten durch kantonale oder kommunale Organe wird in den kantonalen Datenschutzgesetzen geregelt.

Am 25. September 2020 hat das Parlament die Totalrevision des DSG verabschiedet (nDSG).[105] Zurzeit läuft die Vernehmlassung zur revidierten VDSG. Das Inkrafttreten der revidierten Datenschutzgesetzgebung ist nach derzeitigem Stand für die zweite Hälfte 2022 geplant. Mit der Totalrevision des Datenschutzrechts wird der schweizerische Datenschutz im Einklang mit dem europäischen Datenschutzniveau wesentlich gestärkt.

Für die Frage der Vereinbarkeit der Bearbeitung von Daten gestützt auf Herausgabeanordnung mit dem schweizerischen Datenschutzrecht sind das geltende DSG, die VDSG sowie die relevanten Bestimmungen des totalrevidierten DSG (inkl. VDSG) massgebend. Im vorliegenden Zusammenhang nicht speziell berücksichtigt werden müssen demgegenüber aufgrund seines Geltungsbereichs das Bundesgesetz vom 28. September 2018[106] über den Datenschutz in Anwendung des Schengen-Besitzstands in Strafsachen (SDSG) wie auch die von der Schweiz unterzeichnete, revidierte Datenschutzkonvention 108+ des Europarates. Letztere ist inhaltlich der Richtlinie (EU) 2016/680 und der DSGVO sehr ähnlich; die darin enthaltenen Grundsätze wurden im Rahmen der DSG-Revision berücksichtigt.

---

[100] EuGH, *Schrems II*, E. 175-178.

[101] Siehe «Communication from the Commission to the European Parliament and the Council; Way forward on aligning the former third pillar acquis with data protection rules», einsehbar auf https://ec.europa.eu/info/sites/info/files/1_en_act_part1_v7.pdf (Stand 07.06.2021).

[102] SR **235.1**

[103] SR **235.11**

[104] SR **235.13**

[105] BBl **2020** 7639

[106] SR **235.3**

5.5.2.2 Problematische Aspekte im Hinblick auf die Grundsätze des schweizerischen Datenschutzrechts

Das schweizerische Datenschutzrecht geht von einem anderen Ansatz aus als das Verständnis der DSGVO, wonach die Bearbeitung von Daten durch Privatpersonen grundsätzlich widerrechtlich ist, ausser sie lasse sich auf einen Rechtfertigungsgrund stützen. Datenbearbeitungen durch Private sind in der Schweiz grundsätzlich erlaubt, soweit sie nicht persönlichkeitsverletzend sind. Eine Persönlichkeitsverletzung liegt insbesondere vor, wenn eine Datenbearbeitung gegen die allgemeinen Grundsätze in Artikel 4 DSG/Artikel 6 nDSG (insb. Rechtmässigkeit, Bearbeitung nach Treu und Glauben, Verhältnismässigkeit, Zweckgebundenheit und Erkennbarkeit der Datenbearbeitung für die betroffene Person) verstösst oder die Anforderungen an die Datenrichtigkeit (Art. 5 DSG/Art. 6 Abs. 5 nDSG) und an die Datensicherheit (Art. 7 DSG/Art. 8 nDSG) nicht erfüllt (Art. 12 Abs. 2 Bst. a DSG bzw. Art. 30 Abs. 2 Bst. a nDSG).[107] Diese Grundsätze finden sich generell unverändert im revidierten Recht wieder. Kumulativ zu den datenschutzrechtlichen Grundsätzen müssen Datenbekanntgaben ins Ausland zudem die Anforderungen von Artikel 6 DSG erfüllen[108], welche grundsätzlich auch im revidierten Recht übernommen wurden (Art. 16 f. nDSG).

Im Hinblick auf die datenschutzrechtlichen Grundsätze scheinen Datenbearbeitungen gestützt auf den *CLOUD Act* in verschiedener Hinsicht als problematisch. So verlangt der Grundsatz von Treu und Glauben, dass die allgemeinen Regeln mit Bezug auf die Datenbearbeitung angewendet werden. Dies gilt auch dann, wenn Vorschriften und Garantien mit Bezug auf den Datenschutz unvollständig oder nicht konkret sind. Davon betroffen ist insbesondere die Frage der Transparenz einer Datenbearbeitung. Vor diesem Hintergrund könnten Datenbearbeitungen, welche gestützt auf Herausgabeanordnungen vorgenommen werden, in verschiedener Hinsicht problematisch sein. Die Bekanntgabe von Daten, die nicht gestützt auf ein Rechtshilfeersuchen erfolgt, kann als Verstoss gegen Treu und Glauben angesehen werden. Das Gleiche lässt sich auch in Bezug auf Datenbearbeitungen sagen, die heimlich erfolgen oder mit denen die betroffene Person nicht rechnen muss.[109] Als problematisch könnte sich zudem die Bestimmung im *CLOUD Act* erweisen, welche die Information der betroffenen Person vor dem vorstehenden Zugriff der Behörden auf die Daten gänzlich untersagt.

Gemäss dem Grundsatz der Verhältnismässigkeit dürfen nur Daten bearbeitet werden, die für den Zweck der Bearbeitung geeignet und notwendig sind. Zwischen dem Zweck und den verwendeten Mitteln muss ein angemessenes Verhältnis bestehen, und die Rechte der betroffenen Personen sind soweit wie möglich zu wahren.[110] Der Grundsatz gilt auch für Privatpersonen, die Daten bearbeiten. Dabei ist immer die Interessenlage des Datenbearbeiters und jene der betroffenen Person zu berücksichtigen. Insofern, als der *CLOUD Act* im Rahmen von Herausgabeanordnungen eine gerichtliche Überprüfung vorsieht (vgl. Ziff. 3.2.1), kann prinzipiell davon ausgegangen werden, dass dem Grundsatz der Verhältnismässigkeit Rechnung getragen wird. Der Umstand, dass bei anderen Formen von Anfragen keine derartige Kontrolle verlangt wird, könnte sich mit Bezug auf die Verhältnismässigkeit hingegen als problematisch erweisen. Zudem ist unter dem Aspekt der Notwendigkeit zu prüfen, ob der Weg über die klassische Rechtshilfe nicht zum gleichen Ziel führen würde und damit als «mildere»

[107] BRUNO BAERISWYL in: BAERISWYL BRUNO (Hrsg.), Stämpflis Handkommentar zum Datenschutzgesetz (SHK DSG), Bern 2015, Vorbemerkungen zu Art. 4 – 11*a,* Rz. 3.

[108] MAURER-LAMBROU/STEINER in BSK DSG und BGÖ, Art. 6 DSG, Rz. 11a.

[109] Botschaft DSG, BBl **1988** II 413 (449).

[110] Botschaft DSG, BBl **1988** II 413 (450).

Massnahme, die einen weniger einschneidenden Eingriff in die Persönlichkeitsrechte der betroffenen Person bedeuten würde, zu bevorzugen wäre.

Jede Datenbearbeitung darf nur zu einem bestimmten Zweck erfolgen, der für die betroffene Person zudem erkennbar sein muss. Wenn Private Personendaten bearbeiten, ergibt sich der Zweck dieser Datenbearbeitung primär aus den Angaben, welche der betroffenen Person bei der Erhebung ihrer Daten mitgeteilt werden oder die aus den Umständen ersichtlich sind. Es muss für die betroffene Person nachvollziehbar sein, was mit ihren Daten geschieht. Eine Weiterbearbeitung der Personendaten zu einem anderen Zweck, welcher für sie berechtigterweise als unerwartet und nicht erkennbar angesehen werden kann, würde ihr Recht auf Privatsphäre und auf informationelle Selbstbestimmung verletzen, sofern diese Zweckänderung beispielsweise nicht durch ihre Einwilligung gerechtfertigt wäre. Werden Personendaten gestützt auf Sicherungs- und Herausgabeanordnungen nach dem *CLOUD Act* aufbewahrt oder an US-Strafverfolgungsbehörden bekannt gegeben, stellt dies eine Zweckänderung im Hinblick auf den ursprünglich durch die CSP im Rahmen ihrer vertraglichen Dienstleistung bearbeiteten Personendaten dar. Das Gesetz verlangt in diesem Fall einen entsprechenden Rechtfertigungsgrund für die Zweckänderung und eine Information der betroffenen Personen.

Der Grundsatz der Erkennbarkeit verlangt, dass für die betroffene Person die Beschaffung ihrer Personendaten und insbesondere der Zweck ihrer Bearbeitung erkennbar sein müssen. Dieser Grundsatz ist die Voraussetzung für das Recht auf informationelle Selbstbestimmung und für die Wahrnehmung der datenschutzrechtlichen Ansprüche. Für die Verantwortlichen ergibt sich aus diesem Grundsatz eine Informationspflicht gegenüber der betroffenen Person, sofern für sie eine Datenbearbeitung nicht offensichtlich erkennbar ist.[111] Auch unter diesem Aspekt erweisen sich Datenbearbeitungen, die gestützt auf Herausgabeanordnungen durch US-Behörden vorgenommen werden, als problematisch, da sie gestützt auf ausländisches Recht erfolgen. Zudem müsste auch geprüft werden, ob der Umstand, dass eine US-Strafverfolgungsbehörde einem CSP mittels gerichtlicher Verfügung untersagen kann, die betroffene Person über die Bekanntgabe ihrer Daten zu informieren, mit dem Grundsatz der Transparenz vereinbar wäre oder sich gegebenenfalls rechtfertigen liesse. Eine Information muss aber spätestens dann erfolgen, sobald dies allfällige Ermittlungen nicht mehr beeinträchtigen kann.

5.5.2.3 Rechtfertigungsgründe für private Personen bei Verletzungen der Persönlichkeit gemäss Artikel 13 DSG/Artikel 27 nDSG

Mögliche Rechtfertigungsgründe, damit eine Datenbearbeitung nicht als widerrechtliche Persönlichkeitsverletzung gilt, sind die Einwilligung der betroffenen Person, ein überwiegendes privates oder öffentliches Interesse oder eine durch Gesetz gerechtfertigte Datenbearbeitung. Gemäss Rechtsprechung des Bundesgerichts lässt sich eine Verletzung der datenschutzrechtlichen Grundsätze von Artikel 4, Artikel 5 Absatz 1 und Artikel 7 Abs. 1 DSG (bzw. Art. 6 und 8 nDSG) dabei aber nur mit grosser Zurückhaltung rechtfertigen.[112]

Eine Persönlichkeitsverletzung kann dadurch gerechtfertigt sein, dass die betroffene Person in die Datenbearbeitung einwilligt. Damit die Einwilligung rechtsgültig ist, muss die betroffene Person angemessen über die Datenbearbeitung informiert worden sein. Aufgrund der Informationen muss es ihr möglich sein abzuschätzen, welche Risiken für ihre Persönlichkeitsrechte bestehen. Eine angemessene Information sollte deshalb besonders auch die spezifi-

[111] BAERISWYL, SHK DSG, Art. 4, Rz. 47 - 50.

[112] BGE 136 II 508, Erw. 5.2.4.

sche Risikosituation der Bekanntgabe ins Ausland umfassen und das Fehlen angemessener Datenschutzbestimmungen thematisieren. Die Einwilligung muss zudem freiwillig sein, d.h. dass die betroffene Person muss sich ohne Druck für oder gegen die Datenbearbeitung entscheiden können.[113] In der Literatur wird vertreten, dass eine Einwilligung zudem nur dann freiwillig sein kann, wenn der Person eine mit nicht unzumutbaren Nachteilen behaftete Handlungsalternative zur Verfügung steht.[114]

Im vorliegenden Kontext ist als problematisch anzusehen, dass bei Datenbearbeitungen gestützt auf Herausgabeanordnungen der Konnex zu der vom CSP für den Kunden zu erbringenden Dienstleistung und der dafür notwendigen Datenbearbeitung fehlt. Der Kunde müsste also diesem für die Dienstleistungserbringung nicht notwendigen Zweck zustimmen, um die Dienstleistung beanspruchen zu können. Wird ein Vertrag von der Einwilligung in eine Datenbearbeitung abhängig gemacht, die für die Vertragserfüllung nicht nötig ist, so wird im EU Recht grundsätzlich davon ausgegangen, dass die Einwilligung nicht freiwillig erfolgt. Bei Datenbearbeitungen im Rahmen der Strafverfolgung und -vollstreckung kann zudem grundsätzlich davon ausgegangen werden kann, dass der betroffenen Person keine echte Wahlfreiheit zukommt. Dies deutet zumindest darauf hin, dass damit die Anforderungen an die rechtsgültige Einwilligung im Zusammenhang mit dem *CLOUD Act* nicht gegeben sein dürften, und ein CSP könnte sich nicht auf die Einwilligung der betroffenen Person als Rechtfertigungsgrund für Datenbearbeitungen und -bekanntgaben gestützt auf Herausgabeanordnungen berufen.

Auch private Verantwortliche können sich auf ein überwiegendes privates oder öffentliches Interesse berufen, um eine persönlichkeitsverletzende Datenbearbeitung zu rechtfertigen. Massgebend ist jedoch, dass im Rahmen einer Interessenabwägung die betroffenen Interessen gegeneinander abgewogen werden und im Ergebnis das private oder öffentliche Interesse höher zu gewichten ist als das Interesse der von der Persönlichkeitsverletzung betroffenen Person. Eine – nicht abschliessende – Aufzählung von möglichen überwiegenden Interessen des Verantwortlichen findet sich in Artikel 13 Absatz 2 DSG respektive in Artikel 31 Absatz 2 nDSG.

Das *Eigeninteresse* des Verantwortlichen kann – neben allfälligen Interessen von Drittpersonen oder ausnahmsweise auch dem Interesse der betroffenen Person selbst – eine Datenbearbeitung rechtfertigen.[115] Im Kontext von Datenbearbeitungen gestützt auf Herausgabeanordnungen wäre eine Rechtfertigung im Eigeninteresse des CSP zu prüfen, falls er bei einer Nichtbefolgung der Anordnung mit Sanktionen nach US-Recht zu rechnen hätte. So hat die Europäische Kommission in ihrem Amicus-Curiae-Schreiben zum Microsoft-Fall vor dem Obersten Gerichtshof der USA für diesen Fall ein berechtigtes Interesse des CSP als möglich erachtet. Aber auch im nationalen Kontext dürfte eine Aufbewahrung oder Bekanntgabe von Daten nur dann als rechtmässig erachtet werden, wenn die Interessen der in ihrem Persönlichkeitsrecht verletzten betroffenen Person nicht überwiegen. Es ist jedoch nicht davon auszugehen, dass bei einer Interessenabwägung ein allfälliges Interesse des CSP, nicht sanktioniert zu werden, die Interessen der in ihrem Persönlichkeitsrecht verletzten Person überwiegen würde. So ist grundsätzlich anerkannt, dass das Interesse einer Person am Schutz ihrer Persönlichkeit und am Schutz der Privatsphäre und der informationellen Selbstbestimmung

[113] BAERISWYL, SHK DSG, art. 4, Rz. 65.

[114] Siehe RAMPINI in BSK DSG, Art. 13, Rz. 6.

[115] WERMELINGER, A., «Art. 13», in Baeriswyl, B. (Hrsg.), *Datenschutzgesetz – Stämpflis Handkommentar*, Bern: Stämpfli 2015, Rz. 11.

bereits *an sich* ein gewichtiges Interesse darstellt.[116] Bei der Interessenabwägung dürfte sodann auch hier wesentlich ins Gewicht fallen, dass die USA grundsätzlich weniger starke datenschutz- und verfahrensrechtliche Garantien gewähren.

Als Beispiele für *öffentliche* Interessen, die vom privaten Verantwortlichen geltend gemacht werden können, werden in der Literatur die Sicherheit oder der Kampf gegen Geldwäscherei genannt.[117] Mit überwiegendem öffentlichen Interesse ist dabei das öffentliche Interesse aus Sicht der Schweiz gemeint. Dieses beschränkt sich nicht auf rein inländische Interessen, sondern kann auch in der Unterstützung von Anliegen eines ausländischen Staats (beispielsweise bei der Bekämpfung der Geldwäscherei) liegen oder wenn ein Anliegen eines ausländischen Staates eine Reflexwirkung auf die Schweiz zeitigt und damit indirekt auch im öffentlichen Interesse der Schweiz liegt.[118] Ein ausländisches Anliegen beispielsweise im Bereich der Terrorismusbekämpfung könnte demnach ein berechtigtes öffentliches Interesse aus Sicht der Schweiz darstellen.[119] Hier scheint die Schweiz weniger restriktiv zu sein als die EU mit der DSGVO, nach welcher ein öffentliches Interesse nur dann vorliegen kann, wenn dieses im Unionsrecht oder im Recht eines Mitgliedstaates anerkannt ist.

Sofern das konkret mit einer Herausgabeanordnung verfolgte schwere Verbrechen (*serious crimes*) als im öffentlichen Interesse liegend anerkannt würde und die Bekanntgabe dafür unerlässlich wäre, könnte sich ein CSP, der in dieser Hinsicht Personendaten bearbeitet, auf diesen Rechtfertigungsgrund berufen. Allerdings muss dieses öffentliche Interesse das Interesse der in ihrer Persönlichkeit verletzten betroffenen Person überwiegen. Da Datenbearbeitungen gestützt auf Anordnungen von US-Strafverfolgungsbehörden jedoch grundsätzlich als nicht vereinbar mit den hier geltenden datenschutzrechtlichen Grundsätzen anzusehen sind, hat der Schutz der Persönlichkeitsrechte und der Privatsphäre sowie der informationellen Selbstbestimmung der betroffenen Person bei der Beurteilung wesentlich ins Gewicht zu fallen. Es wären damit hohe Hürden an die Verhältnismässigkeit solcher Datenbearbeitungen zu stellen.

Die Datenbearbeitung kann schliesslich auch durch Gesetz gerechtfertigt sein, wobei als Rechtfertigungsgrund für eine allfällige Persönlichkeitsverletzung nur eine *Rechtsgrundlage im schweizerischen Recht* in Frage kommt. Da im vorliegenden Kontext ein US-Rechtsakt, nämlich der *CLOUD Act*, als Rechtsgrundlage für die Anordnungen dient, könnte sich ein CSP nicht auf den Rechtfertigungsgrund der gesetzlichen Grundlage gemäss Artikel 13 Absatz 1 DSG respektive Artikel 31 Absatz 1 nDSG berufen. Dies würde sich voraussichtlich erst durch den Abschluss eines umfassenden Staatsvertrages mit den USA im Bereich des Datenaustauschs inkl. entsprechender Schutzstandards ändern, welcher den Anforderungen an grenzüberschreitende Datenbekanntgaben (Art. 6 Abs. 2 Bst. a DSG bzw. Art. 16 Abs. 2 Bst. a nDSG) genügt. Ein blosses *Executive Agreement* gemäss *Cloud Act* vermöchte diese Anforderungen kaum zu erfüllen.

5.5.2.4 Vereinbarkeit mit den Anforderungen an grenzüberschreitende Datenbekanntgaben (Art. 6 DSG/Art. 16 und 17 nDSG)

Weil Personendaten durch die Bekanntgabe ins Ausland nicht mehr dem Schutz der schweizerischen Datenschutzgesetzgebung unterstehen, sondern einer ausländischen Rechtsordnung unterstellt werden, erhöht sich das Risiko von Persönlichkeitsverletzungen. Art. 6

---

[116] ROSENTHAL, JÖHRI, Art. 13, Rz. 14 verweisen diesbezüglich auf die bundesgerichtliche Rechtsprechung in BGE **97** II 106 f.

[117] MAURER-LAMBROU, STEINER, «Art. 6 DSG», Rz. 32.

[118] ROSENTHAL, JÖHRI, Art. 6, Rz. 60. Ebenso BAERISWYL, B., BLONSKI, D., «Art. 6», in Baeriswyl, B. (Hrsg.), *Datenschutzgesetz – Stämpfli Handkommentar*, Bern: Stämpfli 2015, Rz. 30.

[119] Siehe z. B. ROSENTHAL, JÖHRI, Art. 6, Rz. 61.

DSG stellt Anforderungen an solche Datenbekanntgaben, durch welche die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde. Letztere ist von Gesetzes wegen grundsätzlich dann anzunehmen, wenn der betreffende Staat nicht über eine Gesetzgebung verfügt, die einen angemessenen Datenschutz gewährleistet, also einen dem schweizerischen Recht vergleichbaren Schutz gewährleistet. Bei den USA ist dies nicht der Fall. So wird das Datenschutzniveau der USA vom EDÖB inzwischen *in keinem Bereich mehr als angemessen* angesehen.

Da bereits festgestellt wurde, dass Datenbearbeitungen gestützt auf Herausgabeanordnungen im Hinblick auf die datenschutzrechtlichen Grundsätze generell als problematisch anzusehen sind und von deren Rechtswidrigkeit gemäss schweizerischem Datenschutzrecht auszugehen ist, erübrigen sich mit Bezug auf die Vereinbarkeit mit den Anforderungen an grenzüberschreitende Datenbekanntgaben detaillierte Ausführungen.

Zusammenfassend kann aber Folgendes festgehalten werden: Auch bei Fehlen eines angemessenen Schutzes im Ausland können Datenbekanntgaben ausnahmsweise zulässig sein, nämlich dann, wenn rechtlich bindende und durchsetzbare Instrumente geeignete Garantien für einen angemessenen Schutz der Daten im Ausland vorsehen, wenn die betroffene Person in die Bekanntgabe einwilligt, wenn die Datenbekanntgabe unerlässlich ist zur Wahrung eines überwiegenden öffentlichen Interesses oder zur Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht oder erforderlich zum Schutz des Lebens oder der körperlichen Integrität der betroffenen Person oder eines Dritten.

Konkret wäre im Einzelfall denkbar, dass CSP Personendaten an US-Strafverfolgungsbehörden bekannt geben, sofern dies zum Schutz der lebenswichtigen Interessen der betroffenen Person selbst, oder im Rahmen konkreter laufender Strafverfahren für die Durchsetzung von Rechtsansprüchen unerlässlich ist. Ausserdem könnten sich CSP auch auf ausländische Sicherheitsinteressen berufen, um ein öffentliches Interesse aus Sicht der Schweiz geltend zu machen. In jedem Fall aber müssen die betroffenen Interessen vorsichtig gegeneinander abgewogen werden. Da prinzipiell von einer schwerwiegenden Gefährdung der Persönlichkeitsrechte der betroffenen Personen auszugehen ist, deren Personendaten an US-Strafverfolgungsbehörden gestützt auf Herausgabeanordnungen bekannt gegeben werden, sollten diese Ausnahmefälle generell aber nur mit Zurückhaltung als Rechtfertigungsgründe für solche Datenbekanntgaben angenommen werden.

5.5.2.5 Weitere aus datenschutz- und grundrechtlicher Sicht problematische Aspekte

Daneben lassen sich auch weitere aus datenschutz- und grundrechtlicher Sicht problematische Aspekte im Zusammenhang mit solchen Datenbearbeitungen aufführen. Mit Blick auf den Schutz der Privatsphäre (Art. 13 BV) sind solche Datenbearbeitungen in verschiedener Hinsicht als heikel anzusehen. Artikel 8 der Europäischen Menschenrechtskonvention (nachfolgend EMRK)[120] anerkennt das Grundrecht auf Achtung des Privatlebens. Gemäss der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (nachfolgend EGMR) muss jeder Eingriff in das Privatleben gesetzlich vorgesehen sein, einen rechtmässigen Zweck verfolgen und sich auf das in einer demokratischen Gesellschaft Erforderliche beschränken.[121] In Bezug auf das Recht auf Datenschutz wendet der Gerichtshof den Ansatz der «unbedingten Erforderlichkeit» an.[122] Sowohl der EGMR (in Anwendung der EMRK)

[120] SR **0.101**

[121] Zum Beispiel EGMR, *Liberty und andere gegen Vereinigtes Königreich*, Urteil vom 1. Juli 2008, Beschwerde 58243/00, ECLI:CE:ECHR:2008:0701JUD005824300.

[122] EGMR, *Szabó und Vissy gegen Ungarn*, Urteil vom 12. Januar 2016, Beschwerde 37138/14, ECLI:CE:ECHR:2016:0112JUD003713814, S. 33; EuGH, *Digital Rights Ireland und Seitlinger u. a.*

als auch der EuGH (in Anwendung der Europäischen Charta) haben zahlreiche Garantien zur Kontrolle der elektronischen Kommunikation durch die Regierungen geschaffen.[123]

Auch in diesem Zusammenhang erscheinen im Wesentlichen die gleichen Aspekte des *CLOUD Act* als besonders heikel, die bereits unter Ziffer 5.5.1.1 im Zusammenhang mit der Vereinbarkeit mit der DSGVO erwähnt wurden.[124] Es handelt sich dabei um die im *CLOUD Act* vorgesehene unterschiedliche Regelung betreffend Inhalts- und Nichtinhaltsdaten und von Daten von US-Personen und anderen Personen, die fehlende Unterscheidung zwischen Verantwortlichem und Auftragsbearbeiter, die Überwachung von Kommunikationsinhalten in Echtzeit, fehlende Rechte der betroffenen Person namentlich bezüglich Auskunft und Information sowie fehlende administrative und gerichtliche Rechtsbehelfe für die betroffene Person. Der fehlende Anspruch auf gerichtliche Beurteilung ist neben seiner Problematik aufgrund der datenschutzrechtlichen Vorgaben insbesondere auch unvereinbar mit der in Artikel 29*a* BV statuierten Rechtsweggarantie, wonach jede Person bei Rechtsstreitigkeiten Anspruch auf Beurteilung durch eine richterliche Behörde (in der Schweiz) hat.[125]

5.5.2.6 Schlussfolgerung zur Datenschutzkompatibilität eines *Executive Agreements*

Insgesamt sind Datenbekanntgaben und -bearbeitungen gestützt auf Herausgabeanordnungen nicht nur im Hinblick auf die Vereinbarkeit mit der DSGVO, sondern auch mit derjenigen mit dem schweizerischen Datenschutzrecht sowie allgemein aus grundrechtlicher Sicht als grundsätzlich problematisch anzusehen. Eine wichtige Voraussetzung für die Anerkennung der Angemessenheit des schweizerischen Datenschutzniveaus durch die Europäische Kommission ist schliesslich die Ratifizierung des Änderungsprotokolls zur Datenschutzkonvention des Europarates[126] *(«Datenschutzkonvention 108+»*). Da die Umsetzung der konventionsrechtlich vorgeschriebenen datenschutzrechtlichen Garantien für eine Ratifizierung der Datenschutzkonvention 108+ vorausgesetzt wird (Art. 4 Abs. 2 Datenschutzkonvention 108+), ist ein Abschluss eines *Executive Agreements* auch vor diesem Hintergrund als heikel einzustufen.

Mangels angemessenen Datenschutzes in den USA ist davon auszugehen, dass Datenbekanntgaben an US-Strafverfolgungsbehörden einen schwerwiegenden Eingriff in die Persönlichkeitsrechte der betroffenen Personen darstellen würden. Vorbehaltlich einer eingehenderen Prüfung kann angenommen werden, dass deren allfällige Einwilligung vermutlich keinen gültigen Rechtfertigungsgrund darstellen würde. Denkbar wäre zwar, dass ein CSP eine solche Datenbekanntgabe mit den Sicherheitsinteressen der USA rechtfertigen könnte. Ein denkbarer Rechtfertigungsgrund wäre auch, dass die Bekanntgabe im Interesse der betroffenen Person selbst (d. h. zum Schutz ihrer eigenen lebenswichtigen Interessen oder zur Durchsetzung von Rechtsansprüchen in einem konkreten Strafverfahren) erfolgen würde. Aber selbst hier müsste bei der Interessenabwägung wesentlich ins Gewicht fallen, dass die Datenbekanntgabe die Persönlichkeit der betroffenen Person schwerwiegend gefährden würde.

Namentlich im Hinblick auf die datenschutzrechtlichen Grundsätze der Transparenz und Verhältnismässigkeit sind Datenbearbeitungen gestützt auf Herausgabeanordnungen als problematisch anzusehen. Selbst wenn auch hier im Einzelfall nicht auszuschliessen wäre, dass

---

[123] EGMR, *Roman Zakharov gegen Russland*, Urteil vom 4. Dezember 2015, Beschwerde 47143/06, E-CLI:CE:ECHR:2015:1204JUD004714306.

[124] Siehe zum Folgenden namentlich das Dokument «Évaluation du CCBE de la loi CLOUD Act des États-Unis», vom 28.02.2019, Conseil des Barreaux Européens, abrufbar unter: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/FR_SVL_20190228_CCBE-Assessment-of-the-U-S-CLOUD-Act.pdf.

[125] Vgl. dazu die weiteren Ausführungen unten bei 5.6.1.

[126] SR **0.235.1**

sich CSP auf ein schützenswertes öffentliches Interesse oder auf die Interessen der betroffenen Person selbst berufen könnten, sollte entsprechend der bundesgerichtlichen Rechtsprechung und der Haltung der europäischen Datenschutzbehörden eine Verletzung der datenschutzrechtlichen Grundsätze, die als schwerwiegender Eingriff in die Persönlichkeitsrechte der betroffenen Person anzusehen ist, nur mit grosser Zurückhaltung gerechtfertigt werden können.

Auch in Bezug auf weitere, aus datenschutz- und grundrechtlicher Sicht wichtige Kernanliegen erweisen sich Datenbearbeitungen gestützt auf Herausgabeanordnungen als bedenklich. Wesentlich ins Gewicht fallen hier insbesondere die unter dem *CLOUD Act* fehlenden Zugangs-, Berichtigungs- und Löschrechte der betroffenen Personen mit Bezug auf ihre Daten, aber auch das Fehlen von Rechtsschutzmöglichkeiten sowie von verfahrensrechtlichen Garantien. Insbesondere mit Blick auf die Rechtsweggarantie (Artikel 29a BV) erscheint ein *Executive Agreement* nach schweizerischem Recht problematisch.

5.5.3 Welcher Datenschutz müsste in einem *Executive Agreement* mit den USA aufgenommen werden?

Ein allfälliges *Executive Agreement* wäre ein völkerrechtlicher Vertrag zwischen der Schweiz und den USA. Der Vertrag sollte mithin hinreichende Garantien enthalten, damit auch für die an die US-Strafverfolgungsbehörden bekanntzugebenden Personendaten ein dem hiesigen Recht entsprechender Datenschutz- und Grundrechtsschutzstandard sichergestellt wird. Mangels entsprechender Garantien im *CLOUD Act* müssten die wesentlichsten Grundsätze und Garantien sowie die Rechte der betroffenen Personen im Abkommen selbst geregelt werden.

Es ist allerdings fraglich, ob der vom *CLOUD Act* vorgegebene Rahmen für *Executive Agreements* solche umfassenden datenschutzrechtlichen Garantien überhaupt zulässt, vor allem, weil dieses Gesetz selbst aus datenschutzrechtlicher Sicht als problematisch anzusehen ist. Erwähnenswert ist dabei insbesondere, dass eine betroffene Person selbst bei Vorliegen eines *Executive Agreements* nicht die Möglichkeit hätte, sich gegen die Bekanntgabe ihrer Personendaten zu wehren, da der *CLOUD Act* einen Abwehrmechanismus lediglich für die CSP vorsieht, und auch dies nur in einem sehr begrenzten Rahmen. Die laufenden Verhandlungen zwischen der EU und den USA (siehe Ziff. 4.2.2) zeigen denn auch die Absicht der EU, den Datenaustausch von elektronischen Beweismitteln in Strafsachen in einem umfassenden Rahmenabkommen zu regeln, welches substantiell wesentlich über ein *Executive Agreement* hinausgeht.

Der Beschluss der Europäischen Kommission vom 28. Juni 2021 über die Angemessenheit des UK Datenschutzniveaus nach der DSGVO zeigt, dass der Abschluss eines *Executive Agreements* mit den USA Folgen für die künftige Beurteilung der Angemessenheit des schweizerischen Datenschutzes haben wird. Der Entscheid des EU-Parlaments vom 21. Mai 2021, den von der Kommission vorgelegten Adäquanzentscheid des UK zurückzuweisen – u. a. mit Verweis auf «onward transfers of data to other countries and bulk access to data by law enforcement»[127] – verdeutlicht die Begründetheit dieser Annahme.

Im Unterschied zur UK, welche im Gegensatz zur Schweiz die DSGVO mit Ausnahme des Bereichs der Einwanderungskontrolle vollständig umsetzt und im UK-US *CLOUD Act* Agreement einen Verweis auf die im EU-US Rahmenabkommen gewährleisteten Rechte und Garantien durchzusetzen verspricht, muss davon ausgegangen werden, dass ein *Executive*

[127] Vgl. Pressemitteilung des EU-Parlaments vom 21.5.2021, einsehbar über: https://www.europarl.europa.eu/news/en/press-room/20210517IPR04124/data-protection-meps-urge-the-commission-to-amend-uk-adequacy-decisions (Stand 26.5.2021).

Agreement, welches die Schweiz im engen Rahmen des *CLOUD Acts* mit den USA abschlösse, nicht den Anforderungen der EU an ein angemessenes Datenschutzniveau genügen dürfte. In dieser Hinsicht sowie im Einklang mit den Verhandlungen zwischen der EU und den USA sollte vielmehr ein umfassendes Abkommen anvisiert werden, welches die Datenbearbeitungen und -bekanntgaben von elektronischen Beweismitteln in Strafsachen durch CSP an die US- und die schweizerischen Strafverfolgungsbehörden abschliessend regelt und ein hohes Schutzniveau für die in diesem Rahmen bearbeiteten Personendaten und die Grundrechte und -freiheiten der betroffenen Personen garantiert. Vor diesem Hintergrund liegt es im Interesse der Schweiz, die Verhandlungsergebnisse in Bezug auf das Übereinkommen zwischen der EU und den USA abzuwarten.

Zudem sollten auch die gegenwärtigen Entwicklungen auf europäischer Ebene im Zusammenhang mit dem Datenschutz weiterverfolgt werden. In seinem Urteil vom 16. Juli 2020 in der Rechtssache «Schrems II» hält der EuGH fest, dass die Bestimmungen zu den staatlichen Überwachungsprogrammen im amerikanischen Recht keine hinreichenden Garantien zur Erfüllung der Anforderungen der DSGVO an den Datenschutz und keinen genügenden Rechtsschutz für die betroffenen nichtamerikanischen Personen bieten.[128] Die Europäische Kommission stützt sich in ihren Beschlüssen über die Angemessenheit des Datenschutzniveaus von UK wesentlich auf diesen Entscheid ab. Deshalb dürfte er auch einen wesentlichen Einfluss auf die Beurteilung eines allfälligen *Agreements* mit den USA im Hinblick auf die Angemessenheit des schweizerischen Datenschutzniveaus haben. Auch die von der Europäischen Kommission durchgeführte Anpassung von EU-Rechtsakten, welche Datenbearbeitungen im Bereich der Strafverfolgung und -vollstreckung regeln, an die Richtlinie (EU) 2016/680 lässt vermuten, dass künftig Datenbekanntgaben aus der EU an Drittstaaten in diesem Zusammenhang noch strenger beurteilt werden.[129]

5.6 Vereinbarkeit mit dem schweizerischen Rechtshilferecht

Die internationale Rechtshilfe in Strafsachen (akzessorische Rechtshilfe) zwischen der Schweiz und den USA wird hauptsächlich im Staatsvertrag vom 25. Mai 1973[130] zwischen der Schweizerischen Eidgenossenschaft und den Vereinigten Staaten von Amerika über gegenseitige Rechtshilfe in Strafsachen (nachfolgend RVUS) und im Bundesgesetz vom 3. Oktober 1975[131] zu diesem Gesetz (nachfolgend BG-RVUS) geregelt. Weder im RVUS noch im BG-RVUS geregelte Aspekte werden durch das Rechtshilfegesetz (IRSG)[132] und dessen Verordnung (IRSV)[133] abgedeckt. Subsidiär gilt die Strafprozessordnung (StPO)[134] für Massnahmen, die nicht direkt im IRSG geregelt sind. Für die Schweizer CSP gilt zudem das BÜPF.

Nachfolgend wird die Vereinbarkeit eines allfälligen *Executive Agreements* und des *CLOUD Acts* mit diesen rechtlichen Grundlagen geprüft. Dabei ist klar, dass sämtliche Bestrebungen im Bereich «E-Evidence» am hergebrachten rechtshilferechtlichen Rahmen rütteln. Das ist mit Blick auf die Regelungsmaterie wohl unerlässlich und durchaus so gewollt. Im vorliegenden Abschnitt wird dieser im Raum stehende «Paradigmenwechsel» weg von einer klassischen Rechtshilfe und hin zu einer direkteren Form der Zusammenarbeit dennoch aus der

[128] EuGH, *Schrems II,* E. 175-178.

[129] Mitteilung der Kommission an das Europäische Parlament und den Rat – Weiteres Vorgehen hinsichtlich der Angleichung des früheren Bestitzstands des dritten Pfeilers an die Datenschutzvorschriften, einsehbar auf https://eur-lex.europa.eu/resource.html?uri=cellar:c835f51d-b6d5-11ea-bb7a-01aa75ed71a1.0023.02/DOC_1&format=PDF (Stand 1.7.2020).

[130] SR **0.351.933.6**

[131] SR **351.93**

[132] SR **351.1**

[133] SR **351.11**

[134] SR **312.0**

Warte der Grundsätze und Prinzipien des Schweizer Rechtshilferechts beleuchtet. Ziel ist, vor dem Hintergrund dieser Prinzipien Möglichkeiten und Schranken aufzuzeigen.

5.6.1 Gründe für die Ablehnung eines Rechtshilfeersuchens und Rechtsweggarantie

Im schweizerischen Rechtshilfeverfahren sind gewisse zwingende Ablehnungsgründe für ausländische Rechtshilfeersuchen vorgesehen. Diese sind bei Beweiserhebungsmassnahmen in der Schweiz von Amtes wegen zu prüfen und können von betroffenen Personen im hiesigen Verfahren vor schweizerischen Behörden und Gerichten geltend gemacht werden. Die Ablehnungsgründe finden sich hauptsächlich in den Artikeln 2 und 3 IRSG.[135] Für Fälle von Straftaten mit politischem, militärischem, fiskalischem[136], währungs-, handels- oder wirtschaftspolitischem Charakter wird keine Rechtshilfe geleistet, ebenso wie in Fällen, in denen das ausländische Verfahren elementare Grundsätze verletzt oder generell schwere Mängel aufweist. Dies ist etwa dann der Fall, wenn das ausländische Verfahren den Verfahrensgrundsätzen der EMRK zuwiderläuft, das Verfahren durchgeführt wird, um die verfolgte Person wegen ihrer politischen Anschauungen, ihrer Zugehörigkeit zu einer bestimmten sozialen Gruppe oder aus Gründen der Rasse, der Religion oder der Volkszugehörigkeit zu bestrafen oder dazu führen könnte, dass ihre Situation aus einem dieser Gründe erschwert wird.

Hintergrund für diese Ablehnungsgründe ist letztlich Artikel 5 BV, der eine umfassende Bindung staatlichen Handelns an das Recht – inklusive Völkerrecht – statuiert. Mit einem *Executive Agreement* würden nun die (digitalen) Informationen und Beweismittel nicht mehr in einem schweizerischen Verwaltungsverfahren von einer schweizerischen Behörde erhoben, sondern der in der Schweiz domizilierte CSP würde direkt am US-Strafverfahren mitwirken. Mit der Herausgabe von Daten Dritter (seiner Kunden) zugunsten eines ausländischen Strafverfahrens, in welchem diese als Beweismittel verwendet werden können, nähme der CSP voraussichtlich eine hoheitliche Aufgabe wahr. Das *Executive Agreement* würde diese nach schweizerischem Recht staatliche Aufgabe an einen Privaten – eben den CSP – delegieren. Daher bliebe der CSP an die Grundrechte gebunden. Folglich dürfte ein *Executive Agreement* nicht hinter den aus Grundrechtssicht gebotenen Schutz – also wohl den heutigen Schutzstand im geltenden Rechtshilferecht – zurückfallen.

Es müssten daher aus schweizerischer Sicht Wege gefunden werden, diese Ausschlussgründe auch im neuen, direkten Verfahren unter dem *CLOUD Act* effizient sicherzustellen. Es geht dabei letztlich um die Sicherung des *«ordre public»*.[137] Das trifft namentlich auf die politischen und fiskalischen Straftaten zu. Entsprechende Ausschlussgründe müssten voraussichtlich auch in einem allfälligen *Executive Agreement* zwischen der Schweiz und den USA enthalten sein. Ebenfalls muss die Schweiz auf jeden Fall die EMRK-Mindestgarantien beachten. Auch diese müssten daher umfassend in einem *Executive Agreement* verankert werden.

Es stellt sich die Frage, in welchem Verfahren die Einhaltung solcher Ausschlussgründe sichergestellt werden könnte. Grundsätzlich ist unter dem *CLOUD Act* gar kein schweizerisches Verfahren und keine Involvierung schweizerischer Behörden mehr angedacht. Einzig der CSP könnte im US-Verfahren und vor einem US-Gericht geltend machen, die Verwendung der Daten verstosse gegen den in der Schweiz geltenden *«ordre public»*. Eine so weitgehende Unterwerfung unter fremdes Recht und fremde Gerichte ist die Schweiz bislang noch nicht eingegangen. Es ist – insbesondere mit Blick auf die verfassungsmässig garantierte Rechtsweggarantie in Artikel 29*a* BV – höchst fraglich, ob ein derartiges Verfahren

[135] Sie werden in dieser Form jeweils auch in die modernen bilateralen Rechtshilfeverträge der Schweiz aufgenommen. Im älteren RVUS werden diese unter die generell gehaltene Ausschlussklausel der «ähnlichen wesentlichen Interessen» gemäss Art. 3 Abs. 1 Bst. a subsumiert.

[136] Mit Ausnahme von Abgabebetrug, wo Rechtshilfe geleistet werden kann, vgl. Art. 3 Abs. 3 IRSG.

[137] ZIMMERMANN, Rz. 612.

in einem allfälligen *Executive Agreement* verfassungskonform umsetzbar wäre. Vielmehr ist davon auszugehen, dass – wie es bereits beim Datenschutz angeklungen ist – ein weiterer Rahmen erforderlich wäre, als ihn ein *Executive Agreement* unter dem *CLOUD Act* vorsieht.

5.6.2 Grundsatz der beidseitigen Strafbarkeit

Nach dem Grundsatz der beidseitigen Strafbarkeit kann eine Zwangsmassnahme auf Ersuchen eines anderen Staates nur dann vollstreckt werden, wenn die betreffende Tat sowohl im ersuchenden Staat als auch im ersuchten Staat strafbar ist. Die Zusammenarbeit nach dem *CLOUD Act* beinhaltet allerdings keine Zwangsmassnahmen. Der Begriff des *serious crime* soll die Zusammenarbeit nach dem *CLOUD Act* auf die «wichtigsten» Straftaten beschränken. Im *Executive Agreement* zwischen dem UK und den USA wird der Begriff *serious crime* anhand der drohenden Freiheitsstrafe definiert. Das *Agreement* zwischen UK und den USA geht dabei jedoch nicht vom Erfordernis der beidseitigen Strafbarkeit aus. Dieser Punkt ist verschiedentlich kritisiert worden.[138] Im Ergebnis bedeutet das, dass eine Straftat, die in den USA mit mindestens drei Jahren Freiheitsstrafe bestraft wird, Anlass zu einer Herausgabeanordnung an einen CSP in UK geben kann und dieser der Anordnung nachkommen muss, unabhängig davon, ob die Straftat in UK strafbar ist oder nicht. Namentlich mit Blick auf Steuerdelikte könnte dieser Punkt für die Schweiz mit Blick auf ein allfälliges *Executive Agreement* besonders problematisch sein.

Mit Blick auf das im Rechtshilferecht bekannte Erfordernis der beidseitigen Strafbarkeit stellt sich für die Schweiz im Zusammenhang mit dem *CLOUD Act* somit die Frage, ob eine entsprechende Zusammenarbeit trotz fehlender Strafbarkeit in der Schweiz denkbar wäre. Wird diese Frage verneint, müsste der im *Executive Agreement* zu definierende Begriff des *serious crime* um eine Dimension der beidseitigen Strafbarkeit erweitert werden. Erneut stellt sich allerdings die Frage, wie diese ohne schweizerisches Verfahren überprüft und bei Bedarf durchgesetzt werden könnte. Ob es genügt, wenn der CSP – nicht einmal der Betroffene selbst – im US-Strafverfahren geltend machen kann, das entsprechende Steuerdelikt sei in der Schweiz nicht rechtshilfefähig, ist eine Frage der politischen Bewertung.

5.6.3 Anspruch auf rechtliches Gehör

Mit Blick auf das rechtliche Gehör wird erneut die Bundesverfassung relevant. Der in Artikel 29 Absatz 2 BV verankerte Anspruch auf rechtliches Gehör garantiert, dass die einzelne Person sich äussern kann, bevor ein Entscheid zu ihrem Nachteil gefällt wird, dass sie Zugang zu den Akten erhält, Beweismittel zum Sachverhalt, die einen Einfluss auf den Entscheid haben könnten, einreichen oder beantragen kann sowie an der Beweiserhebung mitwirken, die Beweise zur Kenntnis nehmen und dazu Stellung nehmen kann.

Im Bereich der zwischenstaatlichen Zusammenarbeit in Strafsachen sind diese Anforderungen in Artikel 29 ff. VwVG und einigen Sonderbestimmungen des IRSG und des BG-RVUS konkretisiert.

Im heutigen Rechtshilfeverfahren mit den USA umfasst der Anspruch auf rechtliches Gehör zusammengefasst den Anspruch auf einen Rechtsbeistand (Art. 21 IRSG), auf Akteneinsicht (Art. 26 und 27 VwVG durch Verweis von Art. 9 BG-RVUS) und Mitwirkung bei der Ausführung des Ersuchens (Art. 12 Abs. 2 und Art. 18 Abs. 1 RVUS), den Anspruch jeder persönlich und direkt von einer Rechtshilfemassnahme betroffenen Person, die ein schutzwürdiges Interesse an deren Aufhebung oder Änderung hat, auf eine begründete Verfügung im Hinblick auf

[138] Z. B. von Human Rights Watch, abrufbar im Internet unter: https://www.hrw.org/news/2019/10/29/groups-urge-congress-oppose-us-uk-cloud-act-agreement.

die Geltendmachung ihres Beschwerderechts (Art. 17 f. BG-RVUS) sowie den Anspruch auf eine Rechtsmittelbelehrung (Art. 22 IRSG).

Grundsätzlich würde es der *CLOUD Act* der zuständigen Behörde in der Schweiz (die im *Executive Agreement* bestimmt würde) ermöglichen, die CSP mit Sitz in den USA direkt um Informationen und Daten zu ersuchen, die auf ihren Servern gespeichert sind, und die amerikanischen Behörden könnten die CSP mit Sitz in der Schweiz direkt um auf ihren Servern gespeicherte Daten ersuchen. Dieses System hätte zur Folge, dass weder die (natürlichen und juristischen) Personen, um deren Daten ersucht wird, noch eine andere Behörde (z. B. das BJ als Aufsichtsbehörde oder Zentralstelle) über eine Bekanntgabe von Daten oder Informationen informiert würden. Sie könnten nicht aktiv verlangen, über die Bekanntgabe ihrer Daten informiert zu werden[139] und könnten zu einer entsprechenden Datenbekanntgabe auch nicht Stellung nehmen. Folglich könnte der Anspruch einer direkt von der Bekanntgabe betroffenen Person oder Behörde auf rechtliches Gehör nicht gewährleistet werden.

Da der *CLOUD Act* grundsätzlich nicht vorsieht, dass die betroffene Person/Behörde Anspruch auf rechtliches Gehör hat, stellt sich die Frage, ob dieser Anspruch der betroffenen Personen/Stellen in einem *Executive Agreement* vorgesehen werden könnte. Selbst wenn dies bejaht würde, würde sich erneut die Frage stellen, wie dieser Anspruch ohne schweizerisches Verfahren sichergestellt werden könnte. Auch mit Blick auf Artikel 29 Absatz 2 BV wäre ein *Executive Agreement* kaum verfassungsmässig umsetzbar. Der vertragliche Rahmen müsste ausgedehnt werden.

5.6.4 Aufsichts- und Kontrollbehörde

In erster Linie ist das BJ zuständig für die Ausführung der Abkommen und der Gesetze im Bereich der zwischenstaatlichen Zusammenarbeit in Strafsachen (Art. 17 Abs. 2 IRSG und Art. 7 Abs. 6*a* der Organisationsverordnung vom 17. November 1999[140] für das Eidgenössische Justiz- und Polizeidepartement, nachfolgend OV-EJPD). Im Rahmen der internationalen Rechtshilfe in Strafsachen mit den USA erfüllt es die Funktion der Zentralstelle nach Artikel 28 Absatz 1 RVUS sowie die Funktion der Aufsichtsbehörde, die ihm aufgrund seiner Legitimation zur Beschwerde gegen Verfügungen der ausführenden Behörde des Kantons oder des Bundes zukommt (Art. 19 Abs. 1 erster Satz BG-RVUS). Es ist ausserdem berechtigt, beim Bundesgericht gegen Verfügungen des Bundesstrafgerichts Beschwerde zu erheben (Art. 19 Abs. 1 erster Satz BG-RVUS).

Zusätzlich zur Möglichkeit, Beschwerde zu erheben, nimmt das BJ seine Aufsichtspflicht während des gesamten Rechtshilfeverfahrens in der Schweiz wahr. Dies namentlich dann, wenn es bei Erhalt eines Rechtshilfeersuchens prüft, ob die Voraussetzungen für ein Eintreten auf das Ersuchen erfüllt sind, wenn es die Verfügungen der ausführenden Behörden (namentlich kantonale Staatsanwaltschaften und Bundesanwaltschaft) auf die korrekte Anwendung des Rechtshilferechts prüft und wenn es die Informationen und Beweismittel mit dem Hinweis übermittelt, wie sie die ersuchende Behörde gemäss dem Grundsatz der Spezialität verwenden darf (Art. 5 RVUS). Das BJ überwacht ausserdem die ausgehenden Rechtshilfeersuchen (Art. 30 IRSG).

Grundsätzlich könnten die zuständigen Schweizer Behörden gemäss dem *CLOUD Act* die US-CSP direkt um Daten ersuchen und umgekehrt. So werden die Schweizer CSP Heraus-

[139] Gemäss Art. 3 Abs. 1 Bst. a Ziff. 3 Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (BGÖ, SR **152.3**) sind die Verfahren der internationalen Rechts- und Amtshilfe auch vom Anwendungsbereich dieses Gesetzes ausgenommen. Die Zugangsrechte zu den Daten richteten sich daher voraussichtlich bloss nach den in einem *Executive Agreement* vorgesehenen Regeln.

[140] SR **172.213.1**

gabeanordnungen der USA erhalten, von denen das BJ voraussichtlich keine Kenntnis erlangt und bei denen es folglich seine Aufsichtspflicht nicht wahrnehmen kann. Demgegenüber wird die Behörde, die im *Executive Agreement* dafür zuständig erklärt wird, in der Schweiz Herausgabeanordnungen anzuordnen, gleichzeitig ausführende Behörde sein und allein die Achtung des Rechts garantieren müssen.

Der *CLOUD Act* versieht die CSP hinsichtlich der eingehenden Ersuchen folglich mit einer Schlüsselrolle. Denn sie allein würden Kenntnis vom Ersuchen der USA erhalten und hätten die Kontrolle über das darauf folgende Verfahren.[141] Den kleineren Dienstanbietern könnte es an Fachwissen und Ressourcen für diese Rolle mangeln.[142] Bei ausgehenden Ersuchen fiele diese Rolle den ausführenden Behörden zu.

Obwohl eine Herausgabeanordnung grundsätzlich einer gewissen Kontrolle unterliegen dürfte,[143] sieht der *CLOUD Act* scheinbar nicht vor, dass eine eigentliche Aufsichtsbehörde eingerichtet wird. Da einer der Zwecke des *CLOUD Act* darin zu bestehen scheint, dass Informationen und Daten unmittelbar und rasch ausgetauscht werden können, würde ein Aufsichtssystem den Austausch auch verlangsamen. Doch wie im Abkommen zwischen dem UK und den USA scheint es nicht ausgeschlossen zu sein, einen eingeschränkten Kontrollmechanismus einzuführen (vgl. oben, 4.1.), wenn er im *Executive Agreement* vorgesehen ist.

Es stellt sich somit die Frage, ob – entgegen dem eigentlichen Konzept gemäss *CLOUD Act* – in einem *Executive Agreement* eine Aufsichts- oder Kontrollbehörde für ein- und ausgehende Ersuchen eingerichtet werden könnte. Eine solche wäre voraussichtlich unabdingbar, um die Verfassungsmässigkeit der Zusammenarbeit zu gewährleisten (vgl. dazu unten, 5.6.8.). Zu definieren wäre, welche Stelle diese Aufsicht wahrnähme sowie welche Rolle und welche konkreten Kontrollmöglichkeiten sie hätte.

5.6.5 Grundsatz der Spezialität

Im Bereich der Rechtshilfe hat der Grundsatz der Spezialität zur Folge, dass der ersuchende Staat Schriftstücke, Informationen und Auskünfte nicht zur Verfolgung von Straftaten verwenden werden darf, für welche die Schweiz die Zusammenarbeit ausgeschlossen hat. Das betrifft politische, militärische, fiskalische,[144] währungs-, handels- und wirtschaftspolitische Delikte oder Fälle, in denen die Gewährung der Zusammenarbeit die Souveränität, die Sicherheit, die öffentliche Ordnung oder andere wesentliche Interessen des ersuchten Staates beeinträchtigen würde.[145] Der Grundsatz der Spezialität schützt sowohl die schweizerische Souveränität als auch die von den Rechtshilfehandlungen betroffene Person. Er gilt für den ersuchenden Staat sowie für jeden Drittstaat, der über ihn Kenntnis von den Auskünften und Informationen erlangen könnte.

Der Grundsatz der Spezialität gilt grundsätzlich auch im Verkehr mit den USA.[146] Obwohl die Regierungsbehörden, die mittels *Executive Agreement* ermächtigt würden, im Sinne des Abkommens um Daten zu ersuchen, über einen rechtlich eindeutig definierten Auftrag und na-

---

[141] Siehe in diesem Sinn BISMUTH, S. 685.

[142] BISMUTH, S. 685.

[143] *CLOUD Act*, § 2523 (b) (3) (D) (v).

[144] Rechtshilfe ist bei Abgabebetrug möglich, vgl. Art. 3 Abs. 3 IRSG.

[145] Vgl. Art. 2 des Europäischen Übereinkommens vom 20. April 1959 über die Rechtshilfe in Strafsachen (EUeR, SR **0.351.1**) sowie Art. 1*a* und 3 IRSG.

[146] Vgl. Art. 5 Abs. 1 RVUS sowie Art. 67 IRSG. Zu den Einschränkungen, vgl. ZIMMERMANN, Rz. 734 mit weiteren Hinweisen.

mentlich in Bezug auf die Verwendung der Daten über klare Verfahren verfügen müssen,[147] scheint der *CLOUD Act* keine Bestimmung des Typs «Grundsatz der Spezialität» zu enthalten, zumindest nicht eine klare und wirksame Regelung zur erlaubten bzw. untersagten Verwendung der erhaltenen Daten.

In das Abkommen zwischen dem UK und den USA wurde eine Möglichkeit aufgenommen, die bereits im *CLOUD Act* vorgesehen ist: Die gestützt auf das Abkommen erhaltenen Daten dürfen nicht ohne Zustimmung des Staates, in dem der CSP seinen Sitz hat, an einen Drittstaat weitergegeben werden (Art. 8 Abs. 2). Gemäss dem Abkommen muss der Drittstaat zudem informiert werden, wenn die Person, um deren Informationen ersucht wird, sich nicht im UK befindet oder keine *US person* ist.[148] Wenn die Daten Straftaten betreffen, die in den USA zur Todesstrafe oder im UK zur Verletzung der Meinungsäusserungsfreiheit nach US-Verständnis führen könnten, muss die Zentralbehörde des anderen Staates benachrichtigt werden und zustimmen (Art. 8 Abs. 4). Die gestützt auf den *CLOUD Act* erhaltenen Daten dürfen, wie in Ziffer 4.1 erwähnt, nicht ohne vorgängige Einwilligung des anderen Staates zur Verhängung der Todesstrafe in den USA oder zur Verletzung der Meinungsäusserungsfreiheit im UK verwendet werden. Das UK hat folglich ein Vetorecht hinsichtlich der Verwendung von Beweismitteln in Verfahren, in denen die Todesstrafe beantragt wurde.

Grundsätzlich verlöre die Schweiz mit einem *Executive Agreement* weitgehend die Kontrolle über die Verwendung der bekannt gegebenen Daten. Dies umso mehr, wenn darin nicht eine schlagkräftige Aufsichtsbehörde (im weiteren Sinn) eingesetzt würde. Es erscheint überdies fraglich, ob der Grundsatz der Spezialität im bisherigen Sinne (also inkl. beispielsweise des Ausschlusses für fiskalische Delikte) in einem *Executive Agreement* verankert werden könnte. Vor allem aber stellt sich die Frage, wie dessen Anwendung – ausschliesslich noch in einem US-Verfahren und nur durch den betroffenen CSP als Partei – in einem mit dem geltenden höherrangingen Schweizer Recht vereinbaren Umfang durchgesetzt werden könnte.

5.6.6 Begrenzung der Zusammenarbeit aus «politischen» Gründen

Es ist bereits angeklungen, dass die Schweiz die Rechtshilfe auch dann verweigern kann, wenn diese die Hoheitsrechte, die Sicherheit, die öffentliche Ordnung oder andere wesentliche Interessen der Schweiz zu verletzen droht.[149] Dies geschieht i. d. R. auf entsprechende Rüge der betroffenen Partei. Die Rechtshilfe kann auch an Bedingungen geknüpft werden, wenn solche Interessen betroffen sind.[150] Die Entscheidkompetenz liegt in diesen Fällen beim EJPD, welches die anderen Departemente in seinen Entscheid einbezieht. Der Entscheid des EJPD unterliegt der Beschwerde an den Bundesrat. Eine solche «Souveränitätsschutz-Klausel» wäre kaum mit dem *CLOUD Act* vereinbar.

5.6.7 Vereinbarkeit mit der Strafprozessordnung und dem Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs

Bei der Ausarbeitung eines bilateralen Abkommens wäre auch darauf zu achten, dass die darin enthaltenen Bestimmungen vereinbar sind mit den einschlägigen Normen der StPO[151], den übrigen anwendbaren Erlassen im Bereich des Strafprozesses sowie des

147 *CLOUD Act*, § 2523 (b) (1) (B) (iv)

148 Art. 5 des Abkommens. Siehe ebenfalls DASKAL, SWIRE, «The UK-US *CLOUD Act* Agreement is Finally Here, Containing New Safeguards»; Drittstaat ist in diesem Kontext der Staat, dessen Staatsangehörigkeit die betroffene Person hat.

149 Art. 1a IRSG; vgl. auch Art. 3 Abs. 1 Bst. a RVUS.

150 ZIMMERMANN, Rz. 714.

151 Die wichtigsten Voraussetzungen der StPO für die Überwachung des Fernmeldeverkehrs lauten wie folgt: Anordnung der Überwachung durch die Staatsanwaltschaft (Art. 269 Abs. 1 Einleitungssatz, Art. 273 Abs. 1 StPO); dringender Verdacht der Begehung einer Straftat gemäss dem Katalog nach Art. 269 Abs. 2 StPO für die Überwachung des Inhalts des Fernmeldeverkehrs (Art. 269 Abs. 1 Bst. a StPO) oder eines Verbrechens, Vergehens oder einer Übertretung nach Art. 179^{septies} StGB für die Überwachung der Randdaten (Art. 273

BÜPF[152]. Auf jeden Fall müsste darauf geachtet werden, dass die ausländischen Strafverfolgungsbehörden nicht umfassendere Kompetenzen und Möglichkeiten erhalten als die nationalen Behörden. Das bedeutet zum Beispiel, dass die US-Strafverfolgungsbehörden nicht weiter gefasste (grenzüberschreitende) Herausgabeanordnungen erlassen dürfen als die schweizerischen Strafverfolgungsbehörden gegenüber den CSP in der Schweiz oder dass der Rechtsschutz bei amerikanischen Herausgabeanordnungen nicht stärker eingeschränkt sein darf als bei nationalen Massnahmen.[153]

Diese Vorgabe führt mit Blick auf das System des *CLOUD Act* zu Schwierigkeiten. Die Anforderungen der StPO und des BÜPF müssten in den amerikanischen Strafverfahren angewendet werden, auch was die Zufallsfunde (Art. 243 und Art. 278 StPO), das Verbot der Verwertung von Beweismitteln usw. betrifft, da es ja keine schweizerischen Verfahren mehr gäbe.

Vor diesem Hintergrund wäre das Verfahren nach *CLOUD Act* auch in einem allfälligen *Executive Agreement* kaum in einer Art und Weise regelbar, wie es den genannten gesetzlichen Grundlagen in der Schweiz entspricht. Wenn eine schweizerische Behörde eine Aufsichtsfunktion als Zentralbehörde für die Beschaffung von Daten durch die USA wahrnähme, könnte zwar eine vorgängige Überprüfung wahrgenommen und beim Versand der Daten etwa auf den Grundsatz der Spezialität hingewiesen werden. Selbst auf diesem Weg wäre die Einhaltung der Anforderungen an die nationalen Verfahren jedoch nicht gewährleistet. U.a. ist kaum denkbar, dass auf diesem Weg ein umfassendes Beschwerderecht eingerichtet werden könnte.

Es ist in diesem Zusammenhang zu prüfen, ob die wesentlichen geltenden Bestimmungen im Bereich der grenzüberschreitenden Übergabe von «E-Evidence» nicht eher in einem nationalen Gesetz geregelt werden sollten. Dieses Regime könnte dann als Grundlage für eine unbestimmte Anzahl künftiger bilateraler Abkommen dienen. Entsprechend sind z. B. UK und Australien vorgegangen. Selbst auf diesem Weg, wo zunächst auf gesetzgeberischem Weg grundlegende «Systemkompatibilität» hergestellt würde, wären anschliessend im Rahmen eines *Executive Agreements* noch weitere rechtliche Fragen zu klären. Zunächst müsste die konkrete Interaktion der Rechtssysteme definiert werden, und daneben wäre eine Reihe von technischen Aspekten zu regeln, z. B. die Frage, wie es sich mit der Aufbewahrungsfrist für die Randdaten verhält bzw. ob diese auch für die US-CSP gilt. Das Schweizer Recht sieht eine Aufbewahrungsfrist sowie eine Dauer für die rückwirkende Überwachung vor. Das scheint in den USA nicht grundsätzlich der Fall zu sein. Was also gälte im bilateralen Verhältnis?

Abs. 1 StPO); die Schwere der Straftat rechtfertigt die Überwachung (Achtung des Grundsatzes der Verhältnismässigkeit: Art. 269 Abs. 1 Bst. b. StPO); Achtung des Grundsatzes der Subsidiarität (Art. 269 Abs. 1 Bst. c StPO); Genehmigung durch das Zwangsmassnahmengericht (Art. 272 Abs. 1 und 273 Abs. 2 StPO); Umgang mit nicht benötigten Ergebnissen (Art. 276 StPO); Verwertbarkeit von Ergebnissen aus nicht genehmigten Überwachungen (Art. 277 StPO); Regelung der Zufallsfunde (Art. 278 StPO); Mitteilung der Überwachung (Art. 279 Abs. 1 und 2 StPO); Beschwerde (Art. 279 Abs. 3 StPO).

[152] Die wichtigsten Voraussetzungen des BÜPF für die Überwachung des Fernmeldeverkehrs lauten wie folgt: Der Dienst ÜPF ist sozusagen die Schnittstelle zwischen den Strafverfolgungsbehörden und den Anbietern (Überwachungsanordnung wird nicht direkt von der Strafverfolgungsbehörde an den Anbieter übermittelt, sondern an den Dienst ÜPF, der in der Folge eine entsprechende Verfügung [Art. 5 VwVG] an den betreffenden Dienstanbieter übermittelt; die vom Anbieter gelieferten Daten werden nicht direkt an die zuständige Strafverfolgungsbehörde übermittelt, sondern an den Dienst ÜPF, der sie danach der zuständigen Strafverfolgungsbehörde zur Verfügung stellt); spezifische Pflichten der verschiedenen Kategorien von Anbietern, die im Gesetz und den entsprechenden Verordnungen genannt werden, mehr oder weniger umfangreiche Pflichten je nach Art des Anbieters; Entschädigung des Anbieters für jede Überwachung, wird vom Dienst ÜPF entrichtet und durch einen Teil der Gebühr finanziert, die von der Strafverfolgungsbehörde an den Dienst ÜPF bezahlt wird; Beschwerde des Anbieters gegen die Verwaltungsverfügung des Dienstes ÜPF (es können keine Rügen im Zusammenhang mit dem Strafverfahren geltend gemacht werden).

[153] Vgl. z.B. Art. 274 sowie 279 StPO.

5.6.8 Welche «rechtshilferechtlichen» Inhalte müssten in ein *Executive Agreement* aufgenommen werden?

Auch beim und nach dem Abschluss eines *Executive Agreements* bliebe die Schweiz an ihre grund- und menschenrechtlichen Verpflichtungen gebunden. Es müssten daher aus rechtlicher Sicht zwingend Wege gefunden werden, wie die verfassungsmässigen Garantien des *rechtlichen Gehörs* (Art. 29 Abs. 2 BV) und der *Rechtsweggarantie* (Art. 29*a* BV) gewahrt blieben. Auch die verfahrensmässigen *Mindestgarantien gemäss EMRK* sowie der schweizerische *«ordre public»* (u. a. mit Blick auf den Ausschluss der Rechtshilfe im Bereich von politischen oder fiskalischen Delikten) müssten garantiert werden können. Ebenfalls wäre sicherzustellen, dass ein allfälliges *Executive Agreement* die US-Strafverfolgungsbehörden gegenüber den schweizerischen Strafverfolgungsbehörden nicht ungebührlich privilegiert, was die Erhebung von Daten in der Schweiz anbelangt (vgl. dazu 5.4.3.). Es ist kaum vorstellbar, wie die diesbezüglichen Vorgaben des *schweizerischen Strafprozessrechts* allesamt in einem *Executive Agreement* verankert werden sollten. Es scheint daher unabdingbar, dass die Schweiz zunächst ihre eigenen Standards im Bereich der grenzüberschreitenden Herausgabe von «E-Evidence-System» definiert, bevor sie mittels Staatsverträgen Brücken zu den Systemen von Partnerstaaten baut. Dies würde es ausserdem ermöglichen, ein solches System eigenständig und unter Berücksichtigung des Schweizer Rechts zu gestalten, wobei die schweizerische Souveränität auch mit Blick auf eine direktere Zusammenarbeit im Bereich von «E-Evidence» in hinreichendem Masse gewahrt und wichtige schweizerische Werte geschützt blieben.

6 Datensicherheit und Entschlüsselung

6.1 Gesicherte Übermittlung

Eine Übertragung von Daten von einem Schweizer CSP an eine US-Strafverfolgungsbehörde müsste in einer mit dem Schweizer Recht konformen Art geschehen. Es wäre im Einzelfall zu prüfen, wie die Personendaten von einem CSP an eine Behörde ins Ausland übertragen werden. Bei E-Mail-basierten Systemen (oder anderen Systemen mit Zwischenservern) erscheint eine Transport- und Inhaltsverschlüsselung notwendig, um den Datenschutz während der gesamten Übermittlung zu gewährleisten. Bei einer Upload-Plattform (oder einem ähnlichen System ohne Weiterleitung der Daten an andere Systeme) erscheint die Transportverschlüsselung als ausreichend, falls die Plattform von der Behörde selbst betrieben wird. Ist der Betrieb der Upload-Plattform an Dritte ausgelagert, erscheint auch eine Inhaltsverschlüsselung erneut als notwendig.

Werden besonders schützenswerte Personendaten übertragen – was im Rahmen von Strafverfahren der Regelfall sein dürfte – so sieht der Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes des EDÖB vor, dass die Personendaten stets inhaltsverschlüsselt sein müssen[154].

Es müssten in einem *Executive Agreement* demnach auch Regelungen gefunden werden, die diese schweizerischen Standards für die Übermittlung der Daten an eine US-Strafverfolgungsbehörde respektieren. Die Ergebnisse der Verhandlungen zwischen der EU und den USA im Bereich Datenschutz dürften für die Schweiz diesbezüglich nützlich sein.

[154] EDÖB, Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes, August 2015, S. 20, abrufbar unter: https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/datenschutz/leitfaeden/technische-und-organisatorische-massnahmen-des-datenschutzes.html.

6.2 Neutral encryption

Von der Frage der rechtskonformen, sicheren Übermittlung der Daten von einem Schweizer CSP an die US-Strafverfolgungsbehörden oder umgekehrt zu unterschieden ist die Frage der verschlüsselten Aufbewahrung der Daten *beim CSP*.

Die CSP können eine Vielzahl von Dienstleistungen anbieten, die dem Bedürfnis nach Datensicherheit von (Kunden-)Daten gerecht werden. Dazu gehören Verschlüsselungen. Der *CLOUD Act* sieht keine Pflicht zur Offenlegung von Verschlüsselungen vor. Er enthält insbesondere keine Bestimmung für die Entschlüsselung von Daten, welche die CSP im Namen ihrer Benutzer oder Kunden besitzen.[155] Die CSP können somit nicht zur Entschlüsselung von Daten gezwungen werden, die vom Kunden verschlüsselt wurden.[156]

Zwar verpflichten beispielsweise die FINMA oder das BAG in spezialrechtlichen Bestimmungen (z. B. Art. 12 Abs. 5 der Verordnung vom 22. März 2017 über das elektronische Patientendossier [EPDV])[157] zur Speicherung von Kundendaten im Inland und nach schweizerischem Recht. Selbst wenn Betroffene – in diesem Falle also Finanz- bzw. Gesundheitsdienstleister – dieser Verpflichtung nachkommen und besonders schützenswerte Personendaten bei schweizerischen Datencentern hinterlegen, besteht in gewissen Situationen im Anwendungsbereich des *CLOUD Act* das Risiko eines möglichen Zugriffs auf Daten durch die US-Behörden. Bei der Auslagerung von Daten können gesetzliche und/oder vertragliche Geheimnispflichten es erfordern, dass Daten verschlüsselt gespeichert werden. Bei der Verschlüsselung bestehen verschiedene technische Vorgehensweisen, welche sich u. a. dadurch unterscheiden, ob nach *CLOUD Act* eine technische Zugriffsmöglichkeit auf die Daten besteht oder nicht.

Zu unterscheiden ist zunächst zwischen kundenseitiger Verschlüsselung und serverseitiger Verschlüsselung. Werden die Daten bereits auf dem Rechner des Kunden bzw. Datenherrn verschlüsselt und anschliessend verschlüsselt an den CSP übermittelt (kundenseitige Verschlüsselung), verbleibt der kryptographische Schlüssel beim Kunden. Dem CSP ist es nicht möglich, die Daten zu entschlüsseln. Folglich sind diese – ohne Mitwirkung des Kunden bzw. Datenherrn – weitgehend gegen einen Zugriff der US-Behörden unter dem *CLOUD Act* geschützt. Anders ist die Lage bei der serverseitigen Verschlüsselung. Bei dieser muss zwischen drei verschiedenen Varianten unterschieden werden. Zuerst gibt es die Möglichkeit, den Schlüssel durch den CSP verwalten zu lassen, d. h. der Schlüssel ist ebenfalls in der Cloud hinterlegt und der CSP hat legalen Zugriff darauf. Bei dieser Variante kann der CSP den US-Behörden den Zugriff auf verschlüsselte Daten grundsätzlich ermöglichen. Der Schutz der Kundendaten hängt vom Kooperationswillen des CSP ab, denn wie einleitend festgehalten wurde, besteht gemäss *CLOUD Act* keine Verpflichtung des CSP zur Entschlüsselung von Kundendaten. In einer zweiten Variante verwaltet der Kunde den Schlüssel zwar selbst («*Bring Your Own Key*, BYOK», manchmal auch «*Bring Your Own Encryption*, BYOE»). Dieser muss aber allenfalls in der Cloud hinterlegt und gespeichert sein. Mit der Hinterlegung des Schlüssels auf der Cloud greift der *CLOUD Act*, d. h. die Daten können vom CSP entschlüsselt und somit herausgegeben werden. Ob der CSP das darf, hängt zunächst von seinen Nutzungsbedingungen und in zweiter Linie wohl vom erzeugten Druck seitens der US-Behörden ab. In einer dritten Variante der serverseitigen Verschlüsselung wird der

[155] «The terms of the agreement shall not create any obligation that providers be capable of decrypting data or limitation that prevents providers from decrypting data», *CLOUD Act*, § 2523(b)(3). Siehe ebenfalls DOJ, «Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the *CLOUD Act*», S. 6; ZAGARIS, «U.S. and UK Sign Cross-Border Data Access Agreement for Cross-Border Enforcement and Warn Facebook on Proposed Encryption», S. 360.

[156] Gemäss Schweizer Recht können CSP nur gezwungen werden, Daten zu entschlüsseln, die sie selbst verschlüsselt haben (Art. 26 Abs. 2 Bst. c BÜPF).

[157] SR **816.11**

kryptographische Schlüssel durch den Kunden einzig auf seiner eigenen Hardware gesichert. Bei dieser Variante besteht der gleiche Schutz wie bei der kundenseitigen Verschlüsselung. Der CSP kann die Daten nicht ohne Mitwirken des Kunden bzw. Datenherrn entschlüsseln.

Vor dem Hintergrund dieser Darstellung wird Folgendes deutlich: Zwar besteht für die CSP gemäss *CLOUD Act* keine Verpflichtung zur Entschlüsselung von Daten, welche sie im Namen ihrer Benutzer oder Kunden besitzen[158]. Ungeachtet dieser (Nicht-)Regelung muss man sich aber bewusst sein, dass je nach technischer Möglichkeit und oder vertraglicher Abrede ein Zugriff seitens der US-Behörden auf solche Daten nicht ausgeschlossen werden kann.

7 Schlussfolgerung

Eine der derzeit grössten Herausforderungen im Bereich der zwischenstaatlichen Zusammenarbeit in Strafsachen betrifft die Sicherung und Herausgabe elektronischer Beweismittel. Es steht fest, dass in diesem Bereich neue und innovative Ansätze erforderlich sind, da ansonsten die grenzüberschreitende Strafverfolgung stark erschwert wird. Der vorliegende Bericht beleuchtet verschiedene internationale Initiativen zum erleichterten Zugang zu elektronischen Beweismitteln: Der Europarat verabschiedet ein Zweites Zusatzprotokoll zur Budapest-Konvention, die EU eine *«E-Evidence*-Gesetzgebung», in der Europäische Sicherungs- und Herausgabeanordnungen vorgesehen sind, und die UNO hat die Vorarbeiten zu einem multilateralen Übereinkommen zur Cyberkriminalität aufgenommen. Gleichzeitig sind auch auf Ebene einzelner Staaten Entwicklungen zu beobachten. Die wichtigste nationale Initiative stellt die Verabschiedung des *CLOUD Act* durch die USA dar. Dieses US-Bundesgesetz hat für die US-Strafverfolgungsbehörden und CSP extraterritoriale Wirkungen. Es erlaubt es den US-Strafverfolgungsbehörden, Zugang zu den Daten zu erhalten, die von CSP mit Sitz in den USA aufbewahrt werden – unabhängig davon, wo auf der Welt die Daten gespeichert sind. Das Gesetz bezweckt ausserdem eine «Internationalisierung» des amerikanischen Systems, da die US-Behörden die Möglichkeit erhalten, *Executive Agreements* abzuschliessen, mit denen System und Geltungsbereich des *CLOUD Act* auf andere Staaten ausgedehnt werden sollen. Da die bedeutsamsten CSP ihren Sitz in den USA haben, ist die Zusammenarbeit mit diesem Staat bezüglich der elektronischen Beweismittel namentlich für die Schweiz von besonderer Bedeutung. Aus diesem Grund stellt sich die Frage eines allfälligen Abschlusses eines *Executive Agreement* mit den USA. Der vorliegende Bericht bettet diese Frage in den grösseren Zusammenhang des «Paradigmenwechsels im Bereich der Strafrechtshilfe» ein und geht den dabei auftauchenden rechtlichen Fragen nach. Er prüft die Vereinbarkeit des *CLOUD Act* mit dem Schweizer Recht insbesondere auf zwei Ebenen: Hinsichtlich des Datenschutzrechts sowie der Prinzipien des Rechts der zwischenstaatlichen Zusammenarbeit in Strafsachen. Dabei gelangt das BJ zu folgenden Schlüssen:

- Datenschutzrecht: Die vom *CLOUD Act* erfassten Daten sind Personendaten im Sinne des Datenschutzrechts. Vor diesem Hintergrund ist es von besonderer Bedeutung, dass ein allfälliges *Executive Agreement* mit dem für die Schweiz relevanten Datenschutzrecht vereinbar ist. Das Datenschutzrecht der EU ist in der Schweiz zwar nicht direkt anwendbar, es wird im vorliegenden Bericht jedoch eingehend beleuchtet, da die Schweiz auch weiterhin von der EU als *Drittstaat mit angemessenem Datenschutzniveau (Angemessenheitsbeschluss)* anerkannt werden muss, damit sie mit den EU-Mitgliedstaaten Personendaten austauschen und am freien Datenverkehr mit der EU teilhaben kann – und damit uneingeschränkten Zugang zum *«digitalen Binnenmarkt»* der EU behält. Das EU-Datenschutzrecht hat folglich einen grossen Einfluss auf die Schweiz. Das schweizerische Datenschutzrecht wurde zudem soeben totalrevidiert. Im vorliegenden Bericht wird die Vereinbarkeit des *CLOUD Acts* mit dem

[158] DASKAL, SWIRE, «The UK-US *CLOUD Act* Agreement is Finally Here, Containing New Safeguards».

geltenden und dem künftigen Datenschutzrecht analysiert. Das Ergebnis dieser Analyse legt den Schluss nahe, dass eine Herausgabe von Daten gestützt auf eine Herausgabeanordnung auf der Grundlage des *CLOUD Acts* nur in spezifischen Ausnahmefällen mit dem schweizerischen und europäischen Datenschutzrecht vereinbar ist.

- Rechtshilferecht: Der *CLOUD Act* ermöglicht die Übermittlung elektronischer Daten von einem CSP im Ausland an eine US-Strafverfolgungsbehörde, welche die erhaltenen Daten und Informationen in der Folge in einem US-Strafverfahren als Beweismittel verwenden darf. Diese direkte Zusammenarbeit würde den herkömmlichen Rechtshilfeweg mindestens teilweise ersetzen. Der Abschluss eines *Executive Agreements* würde damit zu einem *Paradigmenwechsel* im Bereich der internationalen Strafrechtskooperation führen: Erstmals würde ein schweizerischer Privater direkt an einem ausländischen Strafverfahren mitwirken, ohne dass dafür ein schweizerisches Verfahren oder wenigstens eine Bewilligung im Einzelfall vorliegt. Diese neue Form der Zusammenarbeit hätte Auswirkungen auf verschiedene Garantien und Prinzipien, welche im Recht der internationalen Rechtshilfe in Strafsachen gelten. Insbesondere betroffen wären die verfassungsmässigen Garantien des rechtlichen Gehörs und des Zugangs zu einem Gericht in der Schweiz, da die von der Datenherausgabe betroffene Person (Datenherr/in) keine Kenntnis von der Bekanntgabe mehr erlangen würde und dagegen folglich auch keine Beschwerde erheben könnte. Auch könnte das BJ seine Rolle als Aufsichtsbehörde im Rechtshilfeverfahren und damit als Garant der Einhaltung der einschlägigen schweizerischen Rechtsprinzipien nicht mehr wahrnehmen. Die Herausgabe wäre einzig abhängig vom Kooperationswillen des CSP. So würden die Rechte der von einem Rechtshilfeersuchen betroffenen Personen geschwächt, aber auch die Möglichkeiten staatlicher Kontrolle – und damit letztlich die schweizerische Souveränität über das Verfahren. Auch mit Blick auf die Vereinbarkeit mit den Prinzipien des Rechtshilferechts wirft der *CLOUD Act* also grosse Fragen auf und scheint schwer mit dem übergeordneten schweizerischen Recht vereinbar zu sein.

8 Weiteres Vorgehen

Der vorliegende Bericht soll eine *Grundlage zur Diskussion* mit Partnerdiensten inner- und ausserhalb der Bundesverwaltung sowie mit Stakeholdern aus Verbänden, der Privatwirtschaft sowie weiteren interessierten Kreisen bilden. Gestützt auf die Ergebnisse aus dieser Diskussion wird das BJ zu gegebener Zeit Antrag an das GS EJPD bezüglich weiterem Vorgehen in Sachen US *CLOUD Act* im Speziellen und «E-Evidence» generell stellen.

9 Bibliographie

BAERISWYL, B., «Vorbemerkungen zu Art. 4–11*a*» in Baeriswyl, B. (Hrsg.), *Datenschutzgesetz – Stämpflis Handkommentar*, Bern: Stämpfli 2015.

BAERISWYL, B., «Art. 4», in Baeriswyl, B. (Hrsg.), *Datenschutzgesetz – Stämpflis Handkommentar*, Bern: Stämpfli 2015.

BAERISWYL, B., «Art. 10*a*», in Baeriswyl, B. (Hrsg.), *Datenschutzgesetz – Stämpflis Handkommentar*, Bern: Stämpfli 2015.

BAERISWYL, B., BLONSKI, D., «Art. 6», in Baeriswyl, B. (Hrsg.), *Datenschutzgesetz – Stämpflis Handkommentar*, Bern: Stämpfli 2015.

BILGIC, S., «Something Old, Something New, and Something Moot: The Privacy Crisis Under the *CLOUD Act*», 32:1 2018 *Harvard Journal of Law and Technology*, S. 321.

BISMUTH, R., «Le *Cloud Act* face au projet européen *E-Evidence:* confrontation ou coopération?», in *Revue critique de droit international* privé, 2019:3, S. 681.

CHRISTAKIS, T., «21 Thoughts and Questions about the UK-US *CLOUD Act* Agreement: (and an Explanation of How it Works – with Charts)», *European Law Blog*, 17.10.2019, abrufbar unter: https://europeanlawblog.eu/2019/10/17/21-thoughts-and-questions-about-the-uk-us-cloud-act-agreement-and-an-explanation-of-how-it-works-with-charts/.

DASKAL, J., «Unpacking the *CLOUD Act*», 2018:4 *eucrim*, S. 220.

DASKAL, J., «*Microsoft Ireland*, the *CLOUD Act*, and International Lawmaking 2.0», 2018:71 *Stanford Law Review Online* S. 9, abrufbar unter: Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0 | Stanford Law Review.

DASKAL, J., SWIRE, P., «The UK-*US CLOUD Act* Agreement is Finally Here, Containing New Safeguards», *Just Security*, 08.10.2019, abrufbar unter: https://www.justsecurity.org/66507/the-uk-us-cloud-act-agreement-is-finally-here-containing-new-safeguards/.

DASKAL, J., SWIRE, P., CHRISTAKIS, T., «The globalization of criminal evidence», 16.10.2018, abrufbar unter: https://iapp.org/news/a/the-globalization-of-criminal-evidence/.

LUTZ T., EGLI L., «Braucht die Schweiz ein CLOUD Act Executive Agreement?», Schweizerische Juristen-Zeitung SJZ 2021, S. 119.

MAURER-LAMBROU, U., STEINER, A., «Art. 6 DSG», in Maurer-Lambrou, U., Blechta, G.P. (Hrsg.), *Basler Kommentar: Datenschutzgesetz – Öffentlichkeitsgesetz*, Basel: Helbing Lichtenhahn 2014.

MAURER-LAMBROU, U., STEINER, A., «Art. 4 DSG», in Maurer-Lambrou, U., Blechta, G.P. (Hrsg.), *Basler Kommentar: Datenschutzgesetz – Öffentlichkeitsgesetz*, Basel: Helbing Lichtenhahn 2014.

PLENACOSTE, F., DAOUD, E., «*CLOUD Act*: Des inquiétudes légitimes», 2018:12 *Droit de la propriété intellectuelle et du numérique,* S. 680.

RAMPINI, C., «ART. 13 DSG», in Maurer-Lambrou, U., Blechta, G.P. (Hrsg.), *Basler Kommentar: Datenschutzgesetz – Öffentlichkeitsgesetz*, Basel: Helbing Lichtenhahn 2014.

ROSENTHAL, D., JÖHRI, Y., *Handkommentar zum Datenschutzgesetz*, Zürich: Schulthess 2008.

ROSENTHAL, D., «Mit Berufsgeheimnissen in die Cloud: So geht es trotz US *CLOUD Act*», *Jusletter*, 10. August 2020.

TSILIKIS, D., «Auf der grenzüberschreitenden Suche nach E-Evidence im Strafverfahren: die Unionsrechtsperspektive im digitalen Zeitalter», in Meier, J., Zurkinden, N., Staffler, L. (Hrsg.), *Recht und Innovation – Innovation durch Recht, im Recht und als Herausforderung für das Recht*, Zürich: Dike 2020, S. 163.

ZAGARIS, B., «U.S. and UK Sign Cross-Border Data Access Agreement for Cross-Border Enforcement and Warn Facebook on Proposed Encryption», 35:10 2019 *International Enforcement Law Reporter,* S. 357.

ZERDICK, T., «Art. 48 – Nach dem Unionsrecht nicht zulässige Übermittlung oder Offenlegung» in Ehmann, E., Selmayr, M. (Hrsg.), *Datenschutz-Grundverordnung – Kommentar*, 2. Aufl., Beck: München 2018.

ZIMMERMANN, R., *La coopération judiciaire internationale en matière pénale*, 5. Aufl., Bern: Stämpfli 2019.

EDPB/CEPD, «Initial legal assessment of the impact of the US *CLOUD Act* on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence», 10. Juli 2019, abrufbar unter: https://edpb.europa.eu/sites/edpb/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf (EDPB/CEPD, Initial legal assessment).

US DOJ, «Promoting Public Safety, Privacy, and the Rule of Law around the World: The Purpose and Impact of the *CLOUD Act*», White Paper, 2019, abrufbar unter: https://www.justice.gov/dag/page/file/1153436/download.

10 Abkürzungen

Abs.	Absatz
Art.	Artikel
BBl	Bundesblatt
BG	Bundesgesetz
BG-RVUS	Bundesgesetz zum Staatsvertrag mit den USA über gegenseitige Rechtshilfe in Strafsachen
BJ	Bundesamt für Justiz
BSK	Basler Kommentar
Bst.	Buchstabe(n)
Budapest-Konvention	Übereinkommen des Europarates über die Cyberkriminalität (Cybercrime-Konvention)
BÜPF	Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft
CLOUD Act	Clarifying Lawful Overseas Use of Data Act (USA)
CSP	Communication Service Provider
Datenschutzkonvention 108+	Änderungsprotokoll zur Datenschutzkonvention des Europarates
Dienst ÜPF	Dienst Überwachung Post- und Fernmeldeverkehr
DOJ	U.S. Department of Justice
DSG	Bundesgesetz über den Datenschutz
DSGVO	Datenschutz-Grundverordnung der EU
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDSA	Europäischer Datenschutzausschuss
EDSB	Europäischer Datenschutzbeauftragter
EEA-Richtlinie	Richtlinie 2014/41/EU über die Europäische Ermittlungsanordnung in Strafsachen
E-Evidence	Bestrebungen der EU zur Verbesserung des grenzüberschreitenden Zugangs zu elektronischen Beweismitteln
EGMR	Europäischer Gerichtshof für Menschenrechte
EMRK	Europäische Menschenrechtskonvention
EPOC	Europäische Herausgabeanordnung
EPOC-PR	Europäische Sicherungsanordnung
Erw.	Erwägung
EUeR	Europäisches Übereinkommen über die Rechtshilfe in Strafsachen
EuGH	Gerichtshof der EU (Europäischer Gerichtshof)
FDA	Anbieter von Fernmeldediensten
FINMA	Eidgenössische Finanzmarktaufsicht
FMG	Fernmeldegesetz
GS EJPD	Generalsekretariat des Eidgenössischen Justiz- und Polizeidepartements
IRSG	Bundesgesetz über internationale Rechtshilfe in Strafsachen (Rechtshilfegesetz)
IRSV	Verordnung über internationale Rechtshilfe in Strafsachen (Rechtshilfeverordnung
nDSG	Total revidiertes Datenschutzgesetz vom 25.09.2020
OV-EJPD	Organisationsverordnung für das Eidgenössische Justiz- und Polizeidepartement
QFG	Qualifying foreign government (Staat, der ein Executive Agreement mit den USA abgeschlossen hat)
RVUS	Staatsvertrag Schweiz-USA über gegenseitige Rechtshilfe in Strafsachen
SCA	Stored Communications Act (USA)
SDSG	Bundesgesetz über den Datenschutz in Anwendung des Schengen-Besitzstands in Strafsachen
SEV	Sammlung der Europaratsverträge
SHK	Stämpflis Handkommentar
SR	Systematische Sammlung des Bundesrechts
StIGH	Ständiger Internationaler Gerichtshof (bis 1946)

StGB	Schweizerisches Strafgesetzbuch
StPO	Schweizerische Strafprozessordnung
T-CY	Komitee des Europarates für die Cybercrime-Konvention
UK	Vereinigtes Königreich
VDSG	Verordnung zum Bundesgesetz über den Datenschutz
VwVG	Bundesgesetz über das Verwaltungsverfahren
WVK	Wiener Vertragsrechtskonvention
Ziff.	Ziffer