Was ist der „CLOUD Act“?

Der CLOUD Act (Clarifying Lawful Overseas Use of Data Act) novellierte das Gesetz zum Datenschutz in der elektronischen Kommunikation (Electronic Communications Privacy Act, ECPA). ECPA bestimmmt, unter welchen Umständen Strafverfolgungsbehörden Zugang zu Informationen erhalten können, die von Technologieunternehmen, einschließlich Cloud-Service-Anbietern, gespeichert werden.[1] Der CLOUD Act wurde am 23. März 2018 verabschiedet.[2]

Der CLOUD Act besteht aus zwei Teilen. Der erste Teil präzisiert, dass Anordnungen, die auf der Grundlage des bestehenden gesetzlichen Rahmens des ECPA erlassen werden, den Zugriff auf Daten unabhängig von deren Speicherort ermöglichen.[3] Der zweite Teil schafft einen neuen Rahmen für zwischenstaatliche Abkommen zur Regelung grenzüberschreitender Ersuchen im Rahmen der Strafverfolgung.[4]

Wann kann Zugang zu Daten von Technologieunternehmen im Rahmen des CLOUD Acts angefragt werden?

Strafverfolgungsbehörden erhalten mittels eines richterlichen Durchsuchungsbeschlusses Zugriff auf die digitalen Inhalte einer Nutzerin bzw. eines Nutzers. Ein richterlicher Durchsuchungsbeschluss darf nur im Rahmen einer strafrechtlichen Ermittlung erteilt werden – und dies auch nur dann, wenn ein unabhängiges Gericht feststellt, dass eine Reihe verfassungsrechtlicher und gesetzlicher Vorgaben erfüllt sind.[5]

Digitale Inhalte können angefragt werden:

- Nur im Rahmen strafrechtlicher Ermittlungen
- Nur nach Einholung eines durch ein unabhängiges Gericht erteilten Durchsuchungsbeschlusses
- Nicht bei Ermittlungen im Zusammenhang mit der nationalen Sicherheit

Der CLOUD Act gestattet keine Sammelabfragen.

- Digitale Inhalte können bei Technologieanbietern nur mit einem richterlichen Durchsuchungsbeschluss angefordert werden, der von einem unabhängigen Gericht erteilt werden muss. Mit einem richterlichen Durchsuchungsbeschluss können nur Daten angefordert werden, die in dem Beschluss selbst genau bezeichnet sind; der Durchsuchungsbeschluss muss von einem unabhängigen Gericht erteilt werden.

AUSKUNFTSERSUCHEN FÜR DIGITALE INHALTE MÜSSEN RECHTLICHEN ANFORDERUNGEN GENÜGEN

Die folgenden Voraussetzungen müssen für die Anfrage nach Zugang zu digitalen Inhalten im Rahmen des CLOUD Act erfüllt sein:

- Die Strafverfolgungsbehörde muss Ermittlungen zu einer Straftat anstellen.
- Die Strafverfolgungsbehörde muss einen richterlichen Durchsuchungsbeschluss beantragen.
- Der Strafverfolgungsbeamte oder die Strafverfolgungsbeamtin muss den Sachverhalt im Antrag auf richterlichen Durchsuchungsbeschluss beeiden.
- Der Antrag auf Erteilung eines richterlichen Durchsuchungsbeschlusses muss eine genaue Beschreibung der angeforderten Informationen enthalten.
- Ein unabhängiges Gericht muss feststellen, dass der Antrag auf Erteilung eines richterlichen Durchsuchungsbeschlusses hinreichende Anhaltspunkte dafür enthält, dass die zu durchsuchenden Informationen Beweise für eine bestimmte Straftat enthalten.

Für Unternehmensdaten gelten zusätzliche Anforderungen:

- Wenn digitale Inhalte einem Unternehmen und nicht einer Einzelperson gehören, hat sich das US-Justizministerium dazu verpflichtet, „Daten direkt von dem Unternehmen und nicht von seinem Cloud-Anbieter anzufordern, sofern die Ermittlungen dadurch nicht beeinträchtigt werden.“[6]
- Mit dieser Verpflichtung wird anerkannt, dass in vielen Fällen das Unternehmen als Kunde von Cloud-Anbietern – und nicht der Cloud-Anbieter selbst – die geeignete Instanz ist, die auf rechtliche Schritte reagieren muss.

Unter welchen Voraussetzungen kann eine Anordnung nach dem CLOUD Act erteilt werden?

Die meisten Datenarten – einschließlich des Inhalts von Mitteilungen – dürfen nach dem CLOUD Act nur dann abgefragt werden, wenn ein unabhängiges Gericht festgestellt hat, dass bestimmte gesetzliche Anforderungen erfüllt sind.[7]

Um Zugriff auf digitale Inhalte zu erhalten, müssen die Strafverfolgungsbehörden einen richterlichen Durchsuchungsbeschluss einholen, der von einem unabhängigen Gericht ausgestellt wird. Dieses Verfahren unterliegt nach US-amerikanischem Recht einer Reihe von verfassungsrechtlichen, gesetzlichen und verfahrensrechtlichen Schutzvorkehrungen.

ES GIBT DREI NOTWENDIGE SCHRITTE:

1. **ANTRAG: Ein Strafverfolgungsbeamte oder eine Strafverfolgungsbeamtin muss bei einem unabhängigen Gericht einen richterlichen Durchsuchungsbeschluss beantragen.** Der Antrag muss Angaben enthalten, aus denen hervorgeht, dass die gesuchten Informationen Beweise für eine Straftat enthalten – und die zu beschaffenden Informationen genau beschreiben. Die Beamtin oder der Beamte, die/der den Antrag auf Erteilung eines richterlichen Durchsuchungsbeschlusses stellt, muss diese Tatsachen beeiden.

2. **GERICHTLICHE GENEHMIGUNG: Ein unabhängiges Gericht muss das Vorliegen eines hinreichenden Verdachts feststellen.** Ein richterlicher Durchsuchungsbeschluss kann nur dann ergehen, wenn die Staatsanwaltschaft ein Gericht davon überzeugt hat, dass hinreichender Verdacht besteht, dass eine bestimmte Straftat stattgefunden hat oder im Begriff ist stattzufinden und dass der zu durchsuchende Ort, z. B. ein E-Mail-Konto, Beweise für diese bestimmte Straftat enthält. Diese Feststellung wird von einem unabhängigen Gericht und nicht von der Strafverfolgungsbehörde selbst getroffen.

3. **ANFECHTBARKEIT: Nach Erteilung einer Anordnung können Technologieunternehmen diese anfechten und Rechtskonflikte geltend machen.** Technologieunternehmen können eine Anordnung vor Gericht anfechten, indem sie bei dem ausstellenden Gericht einen Antrag auf Änderung oder Aufhebung der Anordnung stellen.[8] So sieht der CLOUD Act ausdrücklich vor, dass Anbieter das allgemeine Recht (sog. „Comity-Anfechtungen") geltend machen können, wenn eine Anordnung mit dem Recht eines anderen Landes kollidiert.[9] Die Gerichte bewerten solche Anfechtungen anhand einer Reihe von Faktoren, darunter der Grad der Spezifizität des Ersuchens, die Frage, ob die angeforderten Informationen aus den USA stammen und ob die Informationen auf anderem Wege beschafft werden könnten.[10]

Diese Auflagen führen zu erheblichen Einschränkungen im Hinblick auf Ersuchen zur Herausgabe von digitalen Inhalten. Anbieter, die digitale Inhalte an eine US-Behörde weitergeben, ohne dass hierfür ein Durchsuchungsbefehl vorliegt, der diese Standards erfüllt, riskieren zivil- und strafrechtliche Konsequenzen.[11]

Auskunftsersuchen können auch Daten von Technologieanbietern mit Sitz außerhalb der USA betreffen.

- Der CLOUD Act regelt den Erlass von Anordnungen an breit gefasste Kategorien von Technologieanbietern.[12]
- Diese Technologieanbieter können einer Anordnung nach dem CLOUD Act unterliegen, wenn sie der US-Gerichtsbarkeit unterliegen und technisch in der Lage sind, auf die angeforderten Daten zuzugreifen – unabhängig davon, wo der Anbieter seinen Sitz hat, seine Dienstleistungen erbringt oder seine Daten speichert.[13]
- Viele Unternehmen mit Sitz außerhalb der USA unterliegen der US-Gerichtsbarkeit, z. B. wenn ein Unternehmen Niederlassungen oder Büros in den USA hat oder Verträge mit Kundinnen bzw. Kunden in den USA abschließt.[14]

Was ist ein richterlicher Durchsuchungsbeschluss?

US-Strafverfolgungsbehörden erhalten mittels eines richterlichen Durchsuchungsbeschlusses Zugriff auf digitale Inhalte. Richterliche Beschlüsse unterliegen strengen Auflagen und dürfen nur ausgestellt werden, wenn ein Gericht feststellt, dass eine Strafverfolgungsbeamtin bzw. ein Strafverfolgungsbeamter hinreichende Anhaltspunkte für die Annahme hat, dass die gesuchten Informationen Beweise für eine Straftat enthalten.

Wer erlässt einen richterlichen Durchsuchungsbeschluss? Durchsuchungsbeschlüsse werden von Gerichten erlassen. Dadurch wird sichergestellt, dass eine neutrale und unabhängige Richterin bzw. ein neutraler unabhängiger Richter und nicht nur die Strafverfolgungsbehörde, die den richterlichen Durchsuchungsbeschluss beantragt hat, die beantragte Durchsuchung genehmigt.

Woher stammen die Voraussetzungen für den Erlass eines richterlichen Durchsuchungsbeschlusses? Sowohl die Verfassung der Vereinigten Staaten als auch Gesetze und Verfahrensregeln schreiben den Schutz der Privatsphäre im Rahmen von richterlichen Durchsuchungsbeschlüssen vor. Nach dem vierten Zusatzartikel der US-Verfassung dürfen richterliche Durchsuchungsbeschlüsse nur ausgestellt werden, wenn (1) ein hinreichender Verdacht vorliegt, (2) sie durch einen Eid oder eine eidesstattliche Erklärung gestützt werden und (3) die zu durchsuchenden Orte und zu beschlagnahmenden Gegenstände genau beschrieben werden. Bundesgesetze wie der ECPA beschränken zusätzlich die Situationen, in denen Strafverfolgungsbehörden einen richterlichen Durchsuchungsbeschluss beantragen können. Darüber hinaus enthalten die bundesstaatlichen Strafprozessregeln zusätzliche Sicherheitsvorkehrungen, die einschränken, wie Gerichte Durchsuchungsbeschlüsse erlassen können.

Können richterliche Beschlüsse Sammelauskunftsersuchen bewilligen? Nein. Richterliche Durchsuchungsbeschlüsse werden in konkreten Strafverfahren erteilt, um spezifische Datensätze einzuholen, die im Durchsuchungsbeschluss selbst genau bezeichnet sind. Der vierte Zusatzartikel der US-Verfassung legt fest, dass ein Durchsuchungsbefehl den zu durchsuchenden Ort und die zu verhaftenden Personen oder zu beschlagnahmenden Gegenstände genau beschreiben muss, um sicherzustellen, dass die Durchsuchung sorgfältig auf ihre Rechtfertigungsgründe zugeschnitten ist.

US-GERICHTE: UNABHÄNGIGE ÜBERPRÜFUNG

Die Verfassung der Vereinigten Staaten begründet die Judikative (Gerichte) als einen von drei eigenständigen und unabhängigen Zweigen der staatlichen Gewalt.[15] Die beiden anderen Zweige sind die Exekutive (unter der Leitung der Präsidentin bzw. des Präsidenten) und die Legislative (der Kongress). Im Rahmen dieser Gewaltenteilung erlässt die Justiz weder die Gesetze (das ist die Rolle des Kongresses) noch setzt sie diese durch (das ist die Rolle der Präsidentin bzw. des Präsidenten, der Exekutive und der nachgeordneten Behörden).[16] Diese Struktur gewährleistet, dass die Gerichte als unabhängige Instanzen fungieren, deren Aufgabe es ist, die Gesetze gerecht und unparteiisch auszulegen und anzuwenden, um Streitfälle zu klären. Die Unabhängigkeit der bundesstaatlichen Justiz ist in der US-Verfassung verankert; danach werden Bundesrichterinnen bzw. Bundesrichter etwa auf Lebenszeit ernannt.

In der Praxis bedeutet dies, dass der Antrag einer Strafverfolgungsbehörde (Teil der Exekutive) auf Erteilung eines richterlichen Durchsuchungsbeschlusses zum Erhalt von Informationen im Besitz eines Technologieunternehmens von einer unabhängigen Richterin bzw. einem unabhängigen Richter (Teil der Judikative) geprüft wird.

LEGISLATIVE
Kongress – Erlass von Gesetzen

Der Kongress erlässt Gesetze, in denen die Umstände, unter denen die Strafverfolgungsbehörden einen richterlichen Durchsuchungsbeschluss beantragen können, und die Kriterien für die Ausstellung eines Durchsuchungsbeschlusses festgelegt werden; diese Gesetze ergänzen die verfassungsrechtlichen Anforderungen.

EXEKUTIVE
Präsidentin bzw. Präsident – Durchsetzung von Gesetzen

Die Strafverfolgungsbehörden sind Teil der Exekutive; sie müssen sich an ein Gericht wenden, um einen richterlichen Durchsuchungsbeschluss zu erwirken, und sie müssen die Anforderungen erfüllen, die sowohl durch die (vom Kongress verabschiedeten) Gesetze als auch durch die Verfassung festgelegt sind.

JUDIKATIVE
Gerichte – Auslegung von Gesetzen

Gerichte erlassen Durchsuchungsbeschlüsse; sie tun dies nur, wenn eine Strafverfolgungsbehörde einen Durchsuchungsbeschluss beantragt und die Anforderungen erfüllt, die sowohl durch (vom Kongress verabschiedete) Gesetze als auch durch die Verfassung festgeschrieben sind.

DER CLOUD ACT BESTEHT AUS ZWEI TEILEN

TEIL 1

Klarstellung, dass Anordnungen auf der Grundlage des bestehenden ECPA-Rahmens unabhängig vom Speicherort der Daten sind

TEIL 2

Schaffung eines neuen Rahmens für zwischenstaatliche Vereinbarungen über grenzüberschreitende Strafverfolgungsersuchen

Der CLOUD Act: Eine Präzisierung geltenden US-Rechts

Mit dem CLOUD Act wurde kein neuer rechtlicher Rahmen geschaffen, auf Grundlage dessen Strafverfolgungsbehörden Informationen von Technologieunternehmen einholen können. Stattdessen wurde der durch das Gesetz zum Datenschutz in der elektronischen Kommunikation (ECPA) bereits geltende Rechtsrahmen präzisiert.

Gesetz zum Datenschutz in der elektronischen Kommunikation (Electronic Communications Privacy Act, ECPA): Der 1986 in Kraft getretene ECPA sollte die Privatsphäre im Zusammenhang mit elektronischer Kommunikation wie z. B. E-Mails schützen, indem er u. a. die Umstände beschränkte, unter denen Strafverfolgungsbehörden elektronische Kommunikation von Technologieunternehmen anfordern können.[17] Mit dem ECPA wurde ein rechtlicher Rahmen geschaffen, der jene Voraussetzungen festlegt, die Strafverfolgungsbehörden erfüllen müssen, um sich bei Technologieunternehmen Informationen zu beschaffen.[18]

Gesetz zur Regelung der rechtmäßigen Verwendung von Daten im Ausland (Clarifying Lawful Overseas Use of Data (CLOUD) Act): Mit dem 2018 in Kraft getretenen CLOUD Act wurde der ECPA dahingehend präzisiert, dass der Ort, an dem die Daten gespeichert sind, nicht ausschlaggebend dafür ist, ob ein Gericht eine ECPA-Anordnung erlassen kann.[19] Der CLOUD Act schuf also keine neue Rechtsgrundlage, aufgrund derer Daten von US-Strafverfolgungsbehörden beschafft werden können, sondern stellte klar, wie der Rechtsrahmen des ECPA anzuwenden ist, sollten die gesuchten Daten nicht in den Vereinigten Staaten gespeichert sein.[20] In der Praxis werden Anordnungen, die auf dem CLOUD Act beruhen, nach wie vor auf der Grundlage des seit langem bestehenden Rechtsrahmens des ECPA erlassen und häufig einfach als „ECPA-Anordnungen" oder „ECPA-Anweisungen" bezeichnet. Der CLOUD Act sieht auch ausdrücklich vor, dass die Anbieter die Möglichkeit haben, das allgemeine Recht (sog. „Comity-Anfechtungen") geltend zu machen, wenn eine Anordnung im Widerspruch mit dem Recht eines anderen Landes steht.[21]

Was sind CLOUD-Act-Abkommen?

Der zweite Teil des CLOUD Acts schafft einen Rahmen für neue bilaterale Regierungsabkommen zur Regelung des grenzüberschreitenden Zugriffs auf Daten, die von Technologieanbietern gespeichert werden. Derzeit nutzen die Strafverfolgungsbehörden eines Landes, die Auskunft über in einem anderen Land befindliche Beweismittel einholen wollen, sogenannte Rechtshilfeabkommen (MLAT). Der CLOUD Act schafft einen alternativen Rahmen für solch eine Kooperation, inklusive spezifischer Auflagen, die ein Land erfüllen muss, bevor die Vereinigten Staaten mit diesem Land ein CLOUD-Act-Abkommen eingehen können. Dazu gehört der Nachweis, dass das nationale Recht des Landes einen soliden materiellen und verfahrensrechtlichen Schutz der Privatsphäre und der bürgerlichen Freiheiten bietet.[22] Für den Fall, dass ein US-amerikanischer richterlicher Durchsuchungsbeschluss mit dem Recht eines ausländischen Staates kollidiert, der ein CLOUD-Act-Abkommen eingegangen ist, sieht das Gesetz zudem einen zusätzlichen Mechanismus für Technologieunternehmen vor, den Durchsuchungsbeschluss vor Gericht anzufechten.[23]

Im Oktober 2019 schlossen die Vereinigten Staaten und das Vereinigte Königreich das erste CLOUD-Act-Abkommen.[24] Im selben Monat kündigten die Vereinigten Staaten und Australien Verhandlungen über ein weiteres CLOUD-Act-Abkommen an.[25] Die Vereinigten Staaten und die Europäische Kommission haben ebenfalls formelle Verhandlungen über ein EU-US-Abkommen zur Erleichterung der Erbringung elektronischer Beweismittel bei strafrechtlichen Ermittlungen aufgenommen.[26]

Endnoten

[1] Der CLOUD Act wurde als Teil des Consolidated Appropriations Act 2018, Öffentliches Gesetz Nr. 115–141 (23. März 2018), erlassen. www.congress.gov/115/plaws/publ141/PLAW-115publ141.pdf. *Siehe* Abschnitt V CLOUD Act (zur Änderung des Electronic Communications Privacy Act, US Code Title 18 § 2701 ff.).

[2] *Ebd.*

[3] *Siehe* US Code Title 18 § 2713 (dem Electronic Communications Privacy Act, ECPA, durch Abschnitt 103 des CLOUD Acts hinzugefügt).

[4] *Siehe* US Code Title 18 § 2523.

[5] *Siehe* US Code Title 18 § 2703 (a) (dieser schreibt vor, dass richterliche Durchsuchungsbeschlüsse im Rahmen der strafrechtlichen Verfahren von Bundesgerichten oder Gerichten der Bundestaaten erlassen werden müssen); *Vereinigte Staaten v. Warshak*, 631 F.3d 266 (6th Circuit 2010).

[6] *Siehe* Seeking Enterprise Customer Data Held by Cloud Service Providers, US-Justizministerium, Abteilung für Computerkriminalität und geistiges Eigentum, Strafabteilung (Dezember 2017), www.justice.gov/criminal-ccips/file/1017511/download.

[7] Ohne vorherige gerichtliche Genehmigung kann eine Regierungsbehörde mittels einer Vorladung lediglich eine begrenzte Anzahl von Informationen einholen, nämlich sieben bestimmte, im Gesetz genannte Datenarten, darunter Name, Adresse und Rechnungsdaten einer Anschlussinhaberin bzw. eines Anschlussinhabers. US Code Title 18 § 2703 (c) (2). Eine gerichtliche Anordnung, die auf der Grundlage geringerer Beweise erteilt wird als ein Durchsuchungsbeschluss, kann für die Abfrage von Nicht-Inhaltsdaten, wie z. B. Transaktionsdaten, erwirkt werden; dies erfordert den Nachweis, dass begründete Tatsachen die Annahme rechtfertigen, dass die angeforderten Informationen für eine laufende strafrechtliche Untersuchung relevant und wesentlich sind. US Code Title 18 § 2703 (d).

[8] *Siehe* US Code Title 18 § 2703 Hinweis (2018) (Auslegungsdoktrin).

[9] US Code Title 18 § 2703 Hinweis (2018) (Auslegungsdoktrin).

[10] *Siehe* Dritte zusammenfassende Darstellung des Außenbeziehungsrechts (Restatement (Third) of Foreign Relations Law) § 442. Weitere zu berücksichtigende Faktoren sind (1) die Bedeutung der angeforderten Dokumente bzw. Informationen für die Ermittlungen bzw. das Gerichtsverfahren, (2) das Ausmaß, in dem die Nichtbefolgung des Ersuchens wichtige Interessen der Vereinigten Staaten beeinträchtigen würde, und (3) das Ausmaß, in dem die Befolgung des Ersuchens wichtige Interessen des Staates, in dem sich die Informationen befinden, beeinträchtigen würde.

[11] *Siehe* US Code Title 18 § 2702 (a)–(b) (Verbot für Anbieter elektronischer Kommunikationsdienste („ECS-Anbieter") und Anbieter von Remote-Computing-Diensten („RCS-Anbieter"), digitale Inhalte weiterzugeben, außer unter neun bestimmten Umständen, unter anderem auf richterlichen Durchsuchungsbeschluss, mit Zustimmung der Empfängerin bzw. des Empfängers und soweit dies für die Erbringung der Dienstleistung erforderlich ist).

[12] Der CLOUD Act novelliert den ECPA; Anordnungen im Rahmen dieser Bestimmungen können ECS-Anbieter und RCS-Anbieter betreffen. *Siehe* US Code Title 18 § 2511 (15) (Definition von Anbietern elektronischer Kommunikationsdienste, ECS); US Code Title 18 § 2711 (2) (Definition von Anbietern von Remote-Computing-Diensten, RCS).

[13] *Siehe* US Code Title 18 § 2713 (der besagt, dass sich Anordnungen auf Informationen beziehen können, die sich im „Besitz, Gewahrsam oder unter der Kontrolle" eines Anbieters befinden). *Siehe* US Code 18 § 2713.

[14] Ein Unternehmen unterliegt der Gerichtsbarkeit in den USA, wenn es „Mindestkontakte" mit den Vereinigten Staaten hat, z. B. wenn ein ausländisches Unternehmen das Privileg, in den Vereinigten Staaten Geschäfte zu betreiben, „bewusst in Anspruch nimmt", indem es US-amerikanische Kundinnen bzw. Kunden bedient.

[15] *Siehe* Verfassung der Vereinigten Staaten, Artikel III.

[16] *Siehe* z.B.: Verwaltung der US-Gerichte, Understanding the Federal Courts, www.uscourts.gov/sites/default/files/understanding-federal-courts.pdf.

[17] Öffentliches Gesetz Nr. 99–508 (1986), www.govinfo.gov/content/pkg/STATUTE-100/pdf/STATUTE-100-Pg1848.pdf.

[18] *Siehe* z.B., Bericht des Repräsentantenhauses Nr. 99–647 (1986), www.justice.gov/sites/default/files/jmd/legacy/2013/10/16/houserept-99-647-1986.pdf; Bericht des Senats Nr. 99–541 (1986), www.justice.gov/sites/default/files/jmd/legacy/2014/08/10/senaterept-99-541-1986.pdf.

[19] Öffentliches Gesetz Nr. 115–141 (23. März 2018), www.congress.gov/115/plaws/publ141/PLAW-115publ141.pdf. *Siehe* Abschnitt V CLOUD Act (zur Änderung des Electronic Communications Privacy Act, US Code Title 18 § 2701 ff.).

[20] *Siehe* US Code Title 18 § 2713 (dem Electronic Communications Privacy Act, ECPA, durch den CLOUD Act hinzugefügt).

[21] US Code Title 18 § 2703 Hinweis (2018) (Auslegungsdoktrin).

[22] US Code 18 § 2523 (b) (1).

[23] US Code Title 18 § 2703 (h)(2)(A).

[24] *Siehe: US and UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online*, Justizministerium, 3. Oktober 2019, www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists.

[25] *Siehe: Joint Statement Announcing United States and Australian Negotiation of a CLOUD Act Agreement*, US-Justizministerium, 7. Oktober 2019, www.justice.gov/opa/pr/joint-statement-announcing-united-states-and-australian-negotiation-cloud-act-agreement-us.

[26] *Siehe: Joint US-EU Statement on Electronic Evidence Sharing Negotiations*, Justizministerium, 26. September 2019, www.justice.gov/opa/pr/joint-us-eu-statement-electronic-evidence-sharing-negotiations.