White Paper

Aktuelle Rechtslage zum US-Datentransfer unter besonderer Berücksichtigung des US CLOUD Act

IONOS

Executive Summary

Unter dem CLOUD Act können US-Behörden von Unternehmen selbst dann die Offenlegung der bei ihnen verarbeiteten Daten verlangen, wenn dies gegen die Rechtsordnung im Land der Verarbeitung verstößt. Eine Herausgabe ist nach US-Recht also selbst dann erforderlich, wenn sie gegen europäische Gesetzesvorgaben wie die EU-Datenschutz-Grundverordnung (DSGVO) verstößt. Anders als die DSGVO beschränkt sich der CLOUD Act nicht auf personenbezogene Daten. **So droht neben der ungerechtfertigten Offenlegung personenbezogener Daten beispielsweise auch der Abfluss von Geschäftsgeheimnissen.** Die rechtlichen Implikationen sind jedoch bei Betroffenheit personenbezogener Daten besonders erheblich.

Für betroffene EU-Bürger ist gegen Anfragen nach dem CLOUD Act im Prinzip kein Rechtsschutz möglich. US-Provider gehen daher teilweise selbst gegen Anfragen in Bezug auf die bei ihnen für Kunden verarbeiteten Daten vor. Dennoch kann bereits die Zugriffsmöglichkeit unter dem CLOUD Act bei der Beauftragung von US-Providern zu Datenschutzverstößen unter der DSGVO führen.

> *Solche können seit dem Urteil Schrems II des EuGH auch nicht durch die bloße Vereinbarung von Standarddatenschutzklauseln verhindert werden.*

Die bisher häufigste Rechtsgrundlage der Datenübermittlungen in die USA, der EU-US-Privacy-Shield, wurde durch das Urteil im Juli 2020 unmittelbar für unwirksam erklärt.

Die Vereinbarung von Standarddatenschutzklauseln kann die Sicherheit der Datentransfers erhöhen.

> *Allerdings werden Verantwortliche auch unter Geltung der neuen SCC aus dem Juni 2021 nicht von der Pflicht befreit, im Rahmen eines Data Transfer Risk Assessment selbst zu überprüfen, ob das Datenschutzniveau im Drittland dem in der EU entspricht.*

Bei US-Transfers werden häufig weitere vertragliche, organisatorische und technische Maßnahmen erforderlich, etwa eine ausreichende Verschlüsselung der Daten.

Ein vollständiger Ausschluss des Zugriffs von US-Behörden unter dem CLOUD Act ist daher aktuell kaum möglich.

> *Eine sichere rechtskonforme Nutzung von Cloud-Angeboten erfordert aktuell daher die Einbindung von Anbietern, die nicht dem CLOUD Act unterworfen sind, also insbesondere solchen mit Hauptsitz in der EU.*

Inhalt

1 Einleitung

US-amerikanische Anbieter von elektronischen Kommunikationsdiensten oder Cloud-Services (US-Provider) sind in den meisten Unternehmen aus dem Alltag nicht mehr wegzudenken. Dabei ist die Beauftragung von US-Providern unter Geltung europäischen Rechts durchaus mit rechtlichen Risiken verbunden. Denn während das EU-Recht einen grundrechtsgebundenen Ansatz verfolgt, in dem es vor allem um den Schutz der Betroffenen geht, ist das Datenschutzrecht in den USA im Wirtschaftsrecht angesiedelt und erhält damit dort deutlich weniger Relevanz.

Am 23. März 2018 ist zudem der Clarifying Lawful Overseas Use of Data Act (CLOUD Act[1]) in Kraft getreten. Der CLOUD Act ermöglicht es US-Behörden, Zugriff auf diejenigen Daten zu verlangen, die US-Provider (auch über Tochterunternehmen) im Ausland speichern. Es können also auch Daten betroffen sein, die innerhalb der Europäischen Union (EU) verarbeitet werden oder aus anderen Gründen unter die Regelungen der DSGVO fallen. Der Schutz der Daten vor behördlichem Zugriff kann also mit Geltung des CLOUD Acts nicht mehr dadurch erreicht werden, dass diese außerhalb der USA gespeichert werden. Europäische Unternehmen müssen bei der Beauftragung von US-Providern die neue Rechtslage beachten und bestehende Risiken gegeneinander abwägen.

[1] abrufbar unter https://www.justice.gov/dag/cloudact.

2 Rechtliche Grundlagen der Datenverarbeitung in Deutschland

Rechtsgrundlage für die Verarbeitung personenbezogener Daten ist in Deutschland in erster Linie die DSGVO, ergänzt durch nationale Regelungen wie das Bundesdatenschutzgesetz (BDSG), das Telemediengesetz (TMG) sowie das neue Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien, welches erst am 1. Dezember 2021 in Kraft tritt.

Zudem gibt es weitere Gesetze, die auch im Zusammenhang mit der Verarbeitung nicht-personenbezogener Daten von Bedeutung sein können, etwa das Gesetz gegen den unlauteren Wettbewerb (UWG) oder das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG).

Rechtliche Risiken bestehen im Zusammenhang mit US-Transfers insbesondere durch Verletzungen der Vorschriften aus der DSGVO und dem BDSG. Nach der DSGVO treffen den für die Verarbeitung personenbezogener Daten Verantwortlichen diverse Pflichten. So ist er zum Beispiel für die Information des Betroffenen über die Datenverarbeitung oder die Beantwortung von Betroffenenanfragen verantwortlich.

Werden personenbezogene Daten in einem „Drittland" verarbeitet, also in einem Land, das weder zur EU noch zum Europäischen Wirtschaftsraum gehört, ergeben sich aus Art. 44 ff. DSGVO weitere Vorgaben: Gemäß Art. 46 Abs. 1 DSGVO ist eine Übermittlung personenbezogener Daten in ein Drittland – sofern kein Angemessenheitsbeschluss der EU-Kommission nach Art. 45 Abs. 3 DSVGO vorliegt [2] – nur zulässig, wenn der Verantwortliche oder Auftragsverarbeiter, der die Daten übermittelt, angemessene Garantien vorgesehen hat. Häufig bestehen die vorgesehenen Garantien in Standarddatenschutzklauseln (Standard Contractual Clauses – SCC) gemäß Art. 46 Abs. 2 lit. c) DSGVO. Diese SCC werden von der EU-Kommission erlassen und können entweder eigenständig verwendet oder in einen umfassenden Vertrag integriert werden. Eine Abweichung zu Lasten des Datenschutzes ist nicht zulässig, es können aber weitere Pflichten zum Schutz personenbezogener Daten aufgenommen werden. Da die SCC zum Teil als nicht ausreichend kritisiert werden, fordert der Europäische Datenschutzausschuss (EDSA) [3] weitere Maßnahmen, um den Schutz der personenbezogenen Daten zu gewährleisten. Darunter etwa fallen die Verschlüsselung, Anonymisierung oder Pseudonymisierung der Daten.

Daneben bleiben die allgemeinen datenschutzrechtlichen Pflichten auch bei Drittlandtransfers bestehen. So ist der Verantwortliche insbesondere verpflichtet, Betroffene über den (geplanten) Drittlandtransfer zu informieren und ihm Informationen über die getroffenen geeigneten Garantien zur Verfügung zu stellen.

---

[2] Eine aktuelle Liste ist abrufbar unter: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[3] EDSA - Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, 10. November 2020, S. 28, https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_de.pdf

3 Rechtliche Grundlagen: Der CLOUD Act

3.1 Geschichte des CLOUD Act

Bei dem CLOUD Act handelt es sich um eine Ergänzung des US Stored Communications Act von 1986 (SCA), ein Gesetz, welches US-Provider u. a. verpflichtet, gespeicherte Kommunikationsdaten zu Ermittlungszwecken an US-Behörden offenzulegen. Während der SCA zuvor keine Regelungen darüber enthielt, ob auch Kommunikationsdaten im Ausland von der Offenlegungspflicht umfasst sind, ergänzt der US CLOUD Act den SCA nun dahingehend, dass die Offenlegungspflicht unabhängig vom weltweiten Standort der Daten gilt. Zu differenzieren ist hierbei zum USA Patriot Act, der bereits seit 2001 den Zugriff der US-Behörden auf – in den USA gespeicherte – personenbezogene Daten zu Zwecken der Terrorismusbekämpfung regelt.

Anlass für den Erlass des CLOUD Act war ein Rechtsstreit zwischen Microsoft und der US-Regierung.[4] Microsoft verweigerte die Herausgabe von Kundendaten auf Grundlage des SCA, da diese auf Servern außerhalb der USA gespeichert waren. Noch während des Verfahrens vor dem Supreme Court sorgte die damalige Trump-Regierung jedoch mit Erlass des CLOUD Act für die gesetzlich legitimierte Erweiterung des Zugriffsbereiches des SCA, sodass sich das Verfahren vor dem Supreme Court damit erledigte.

Während bis heute keine Rechtshilfeabkommen zwischen Deutschland oder der EU mit den USA unter dem CLOUD Act geschlossen wurden (ausschließlich mit Großbritannien), gilt seit 2003 lediglich das Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über Rechtshilfe (Mutual Legal Assistance in Criminal Matters Treaty – MLAT[5]), das die Herausgabe von Daten in Strafverfahren regelt. Das MLAT unterscheidet sich vom CLOUD Act maßgeblich darin, dass die US-Regierung im Rahmen des Abkommens eher als Mittelsmann agiert und die Rechtshilfeanträge ausländischer Regierungen prüft, bevor sie an ein US-Gericht übergeben werden. Es gibt somit keinen direkten Weg zwischen den US-Behörden und den Plattformbetreibern, bei denen es zur Anfrage der personenbezogenen Daten kommt.[6] Dieser für die US-Regierung aufwändigere und längere Weg wird durch den CLOUD Act verkürzt. US-Behörden haben nun die Möglichkeit, Anfragen unmittelbar bei dem betreffenden US-Provider zu stellen.

3.2 Inhalte des CLOUD Act

Anders als der Name zunächst vermuten lässt, richtet sich der CLOUD Act nicht nur an Cloud-Anbieter im engeren Sinne. Vielmehr sind alle Anbieter elektronischer Kommunikations- und Remote-Computing-Dienste betroffen (insbesondere Internet-Provider, IT-Dienstleister und Cloud-Anbieter). Auch wenn der CLOUD Act nicht jedes Unternehmen verpflichtet, werden die meisten Unternehmen erfasst, die an internationalen Datenverarbeitungen, etwa als Dienstleister, beteiligt sind. Die Ermittlung, ob ein Unternehmen vom CLOUD Act erfasst ist, ist häufig nicht ohne weiteres

[4] Supreme Court of the United States, United States of America v. Microsoft Corporation, https://www.supremecourt.gov/DocketPDF/17/17-2/41851/20180330172237829_17-2motUnitedStates.pdf.
[5] Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:22003A0719(02)&from=EN.
[6] Thomas Rudl – Nach Microsoft-Urteil: US-Regierung will Zugriff auf im Ausland liegende Daten durch Gesetzesänderungen erzwingen, 27. Juli 2016, https://netzpolitik.org/2016/nach-microsoft-urteil-us-regierung-will-zugriff-auf-im-ausland-liegende-daten-durch-gesetzesaenderungen-erzwingen/

möglich. Diese Anbieter sind im Falle eines Herausgabeverlangens der entsprechend berechtigten US-Behörden verpflichtet, diejenigen Daten herauszugeben, die sie in Besitz, Gewahrsam oder ihrer Kontrolle haben.[7] Ziel des CLOUD Act sind seinem Wortlaut nach gezielte Datenabfragen im Zusammenhang mit einem Strafprozess. Anders als die DSGVO unterscheidet der CLOUD Act nicht nach der Art der Daten – personenbezogene und andere (meist geschäftsbezogene) Daten können gleichermaßen betroffen sein.

Die größte Neuerung unter dem CLOUD Act ist nun, dass nicht mehr nach dem Speicherort der Daten differenziert wird. Vielmehr reicht es aus, dass die Daten durch einen Provider, der seinen Sitz oder seine Niederlassung in den USA hat oder dort einer Geschäftstätigkeit nachgeht, verarbeitet werden. Somit können durch den CLOUD Act auch personenbezogene Daten betroffen sein, die von Verantwortlichen in Europa verarbeitet werden, sofern sie diese Daten an einen US-Provider übermitteln.

Zudem ermöglicht der CLOUD Act den Abschluss von Abkommen zwischen den USA und anderen Ländern. Sofern es ein solches Abkommen gibt, können die Behörden des jeweiligen Landes unmittelbar von US-Providern die Herausgabe von Daten ohne weitere Überprüfung verlangen und umgekehrt. Lediglich die Abkommen mit den Ländern selbst sollen durch die USA alle fünf Jahre im Hinblick auf das dort herrschende Menschenrechtsniveau überprüft werden.

Eine gerichtliche Überprüfung erfolgt im Übrigen nur, wenn die betrof-fenen Unternehmen eine sogenannte „Comity Analysis" beantragen.

Folglich ist jedes Unternehmen, das cloudbasierte Datenverarbeitungen durch US-Provider oder ihre Tochtergesellschaften durchführt, potentiell von Herausgabeverlangen unter dem CLOUD Act betroffen. Unternehmensdaten können also bereits bei Beauftragung europäischer IT-Dienstleister, die ihre Dienste über amerikanische Server oder EU-Server von US-Providern laufen lassen, betroffen sein. Zu ersterem zählen auch webbasierte Services wie Google Drive oder Google Analytics.

4 Welche Risiken entstehen druch den CLOUD Act?

4.1 Zugriff auf europäische Daten

Unter dem CLOUD Act ist es also nicht ausgeschlossen, dass US-Behörden Zugriff auf Daten von Unternehmen in der EU erhalten, die lediglich über die von ihnen eingesetzten EU-Dienstleister einen Bezug zu den Angeboten von US-Providern haben (etwa als Subauftragnehmer).

Auf diese Weise können US-Behörden ohne weitere gerichtliche Überprüfung Zugriff auf sensible Informationen wie Geschäftsgeheimnisse erhalten.

[7] vgl. Title 18 U. S. C. § 2713.

Zudem können auch personenbezogene Daten betroffen sein, die der Regelung durch die DSGVO unterfallen.

Eine Herausgabe dieser personenbezogenen Daten an US-Behörden ist nur auf Grundlage einer tauglichen Rechtsgrundlage, im Regelfall Art. 6 Abs. 1 DSGVO, zulässig. Deren Voraussetzungen sind jedoch im Regelfall nicht erfüllt: Eine Einwilligung des jeweils Betroffenen (etwa Endkunde oder Mitarbeiter) müsste nach Art. 6 Abs. 1 S. 1 lit. a) DSGVO vor der Herausgabe erteilt werden. Diese werden Betroffene jedoch in der Regel verweigern. Sofern es dem Schutz lebenswichtiger Interessen dient, könnte die Datenübermittlung zwar auf Art. 6 Abs. 1 S. 1 lit. d) DSGVO gestützt werden; auch diese Konstellation stellt jedoch eine absolute Ausnahme dar. Insoweit verbleibt eine Rechtfertigung nur auf Grundlage der Interessenabwägung gemäß Art. 6 Abs. 1 S. 1 lit. f) DSGVO. Eine solche Übermittlung wäre gerechtfertigt, wenn das Interesse des Unternehmens an der Übermittlung der personenbezogenen Daten die Interessen der Betroffenen überwiegt. Eine solche Rechtfertigung scheitert im Regelfall jedoch wiederum daran, dass Anfragen einer nicht EU-rechtlich autorisierten Behörde auch kein überwiegendes Interesse begründen können. Dies gilt entsprechend für die Rechtfertigung von Drittlandtransfers aufgrund öffentlicher Interessen unter Art. 49 Abs. 1 lit. d) DSGVO. Für die Offenlegung personenbezogener Daten von EU-Bürgern an US-Behörden liegt daher grundsätzlich keine gesetzliche Rechtsgrundlage vor. Darüber hinaus ist auch die Beachtung der übrigen Vorgaben der DSGVO nicht möglich, da beispielsweise Informationspflichten aufgrund der unzureichenden Information durch die US-Behörden über die Verarbeitung nicht durch den Verantwortlichen erfüllt werden können.[8]

Zwar liegen keine gesicherten Zahlen dazu vor, wie oft US-Behörden tatsächlich Anfragen auf Grundlage des US CLOUD Act stellen und auch eine systematische, groß angelegte bzw. wahllose Erhebung personenbezogener Daten wird unter dem CLOUD Act in der Regel nicht möglich sein[9], sodass die Gefahr des Zugriffes aus vorläufiger Sicht als nicht besonders hoch einzustufen ist. Außerdem ist zu erwarten, dass sich zumindest die großen US-Provider gegen die Offenlegungsanordnungen rechtlich zur Wehr setzen werden.[10]

---

[8] EDSA – 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, S. 5 f., https://edpb.europa.eu/sites/default/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf.
[9] ebd., S. 2
[10] TMicrosoft – Law Enforcement Request Report, https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report (abgerufen am 23. September 2021).

Allerdings reicht schon die bloße Möglichkeit einer (einmaligen) Anfrage aus, um das Risiko einer rechtswidrigen Datenübermittlung und damit gleichermaßen ein Risiko für den Schutz personenbezogener Daten zu begründen.

In jedem Fall verlieren Verantwortliche durch US-Verarbeitungen unter dem CLOUD Act die Kontrolle über ihre Daten.

Dazu kommt, dass die Sensibilität der Daten unter dem CLOUD Act zwar ein Differenzierungskriterium sein kann, grundsätzlich können diese (etwa Gesundheitsdaten) aber gleichermaßen betroffen sein, obgleich sie nach Art. 9 DSGVO einen besonderen Schutz genießen.

4.2 Widerspruch zur DSGVO

Selbst wenn eine Datenherausgabe an US-Behörden im ersten Schritt ausnahmsweise noch nach Art. 6 DSGVO gerechtfertigt sein sollte, so müssten weiterhin die Voraussetzungen für Drittlandtransfers nach den Art. 44 ff. DSGVO vorliegen. Zwar kann die Herausgabe an ausländische Behörden durchaus zulässig sein, allerdings wäre zur Anerkennung der Urteile und Entscheidungen von Gerichten und Behörden in Drittländern wie den USA gemäß Art. 48 DSGVO ein entsprechendes Rechtshilfeabkommen oder vergleichbares Instrument erforderlich. Eine solche Übereinkunft gibt es neben dem MLAT jedoch bis zum heutigen Zeitpunkt nicht. Und so ist eine Herausgabe personenbezogener Daten allein auf Grundlage behördlicher Anforderungen auf Basis des CLOUD Act in der Regel unzulässig.[11] Insofern würde eine Offenlegung an US-Behörden auch auf zweiter Stufe gegen Art. 48 DSGVO verstoßen.

Demgegenüber sind US-Provider nach dem CLOUD Act selbst dann zur Herausgabe von Daten verpflichtet, wenn die Gesetze am Speicherort der Daten dies eigentlich verbieten. Werden Daten beispielsweise auf Servern in Deutschland gespeichert und ist eine Herausgabe aufgrund der geltenden Datenschutzgesetze nicht zulässig, so muss sich der US-Provider entscheiden: Entweder er verweigert die Herausgabe der Daten und riskiert einen Verstoß gegen den CLOUD Act oder er gewährt den Behörden Zugriff und riskiert ein Bußgeld gemäß Art. 83 Abs. 5 DSGVO, das bis zu 20 Mio. Euro bzw. 4 % des jährlichen weltweiten Umsatzes betragen kann.

US-Provider können aufgrund des CLOUD Act also in eine Situation kommen, in der ein rechtskonformes Handeln sowohl unter europäischem als auch unter US-Recht nicht möglich ist.

Eine Rechtfertigung der Herausgabe an die US-Behörden wäre dann allenfalls noch nach Art. 49 Abs. 1 lit. e) DSGVO „zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen“ möglich. Das jedoch auch nur, sofern der Verantwortliche selbst Teil eines Verfahrens ist (Beteiligter), in dem die Herausgabe personenbezogener Daten zur Verfahrensführung notwendig ist.[12]

[11] LfD Niedersachsen – Der CLOUD Act – Zugriff von US-Behörden auf Daten in der EU, 7. September 2020, https://datenschutz.nibis.de/2020/09/07/der-cloud-act-zugriff-von-us-behoerden-auf-daten-in-der-eu/.
[12] Rath/Spies – CLOUD Act: Selbst für die Wolken gibt es Grenzen, CCZ 2018, 229 (230).

4.3 Unzureichender Rechtsschutz

Ein weiteres Risiko unter dem CLOUD Act liegt darin, dass Betroffene in Europa in der Regel nur unzureichenden Rechtsschutz gegen die behördlichen Anfragen erreichen können. So können US-Provider im Falle einer unberechtigten Anordnung auf Grundlage des CLOUD Act Rechtsschutz in Form einer „Comity Analysis“[13] beantragen und sich darauf berufen, dass die Daten weder einen US-Bürger noch einen in der USA ansässigen Nicht-US-Bürger betreffen und zudem das Datenschutzrecht des jeweiligen Speicherortes verletzt wird.

Allerdings kann nur die Verletzung des Rechtes einer „qualifizierten ausländischen Regierung“ geltend gemacht werden, wozu eine Exekutivvereinbarung mit dem jeweiligen Land erforderlich ist,[14] welche aber weder die EU noch Deutschland mit den USA geschlossen haben.

Zwar hatte sich die EU-Kommission zwischendurch zu Verhandlungen grundsätzlich bereit erklärt,[15] allerdings wurde eine im Januar 2020 geschlossene Exekutivvereinbarung Großbritanniens mit den USA durch die EU-Datenschutzbehörden (EDSA) scharf kritisiert. Zur Begründung wurde hier insbesondere angeführt, dass unzureichende rechtliche Mittel gegen entsprechende Anfragen bestünden und fraglich sei, ob die vorgesehenen Schutzbestimmungen im Falle einer Anfrage überhaupt greifen, da mit dem Abkommen immer noch die US-amerikanischen Überwachungsgesetze über dem Datenschutz stehen würden.[16] Insofern scheint der Abschluss einer solchen Exekutivvereinbarung (Stand Oktober 2021) unwahr-scheinlich, zumal nach den Vorgaben des CLOUD Act grundsätzlich nur einzelne Länder zum Abschluss befugt sind,[17] keine internationalen Organisationen wie die EU.

Folglich gibt es kaum effektiven Rechtsschutz gegen Herausgabeverlangen der US-Behörden, den Betroffenen selbst steht ein solches Rechtsmittel von vornherein nicht zu. Hinzu kommt, dass die Durchsuchungsbefehle der US-Behörden häufig mit einer Verschwiegenheitsverpflichtung („gag order“) verbunden sind, sodass Betroffene schlimmstenfalls nicht einmal erfahren, dass ihre personenbezogenen Daten Gegenstand von US-Ermittlungen geworden sind.[18]

[13] Title 18 U. S. C. § 2703 (h) (2) (A).
[14] Title 18 U.S.C. § 2523: „domestic law of the foreign government“
[15] Tobias Haar – Wolkenbruch: US CLOUD Act regelt internationalen Datenzugriff, https://www.heise.de/select/ix/2018/7/1530927567503187.
[16] Vgl. Brief des EDSA an das Europäische Parlament vom 15. Juni 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0054-uk-usagreement.pdf.
[17] Title 18 U.S.C § 2523.
[18] Rath/Spies – CLOUD Act: Selbst für die Wolken gibt es Grenzen, CCZ 2018, 229.

5 Schrems II: Das Urteil zum EU-US-Privacy-Shield

Am 16. Juli 2020 hatte der EuGH mit *Schrems II*[19] sein bislang wichtigstes Urteil zum US-Datentransfer gefällt. Infolge des Urteils ist ein Datentransfer in die USA allein auf Grundlage des EU-US-Privacy-Shields oder der SCC nicht mehr möglich. Der EuGH hatte klargestellt, dass beide Instrumente insbesondere aufgrund des CLOUD Act nicht in der Lage sind, in den USA ein angemessenes Datenschutzniveau herzustellen.

5.1 Unwirksamkeit des EU-US-Privacy-Shields

Grundsätzlich ist die Übermittlung personenbezogener Daten in ein Drittland nur zulässig, wenn dort ein angemessenes Schutzniveau gewahrt wird (vgl. Art. 44 DSGVO). 2016 hatte die EU-Kommission festgestellt, dass es sich bei den USA um ein sicheres Drittland handele, solange die Voraussetzungen des Privacy Shield eingehalten würden (Angemessenheitsbeschluss).[20] Auf Grundlage von Art. 45 DSGVO war damit auch nach Inkrafttreten der DSGVO ein Transfer personenbezogener Daten an einen US-Provider möglich, sofern dieses unter dem Privacy Shield zertifiziert war. Im Juli 2020 hatte der EuGH den Privacy Shield jedoch für unwirksam erklärt, da auch unter seinen Voraussetzungen kein angemessenes Datenschutzniveau bei Datenverarbeitungen in den USA hergestellt werden konnte.[21]

[19] EuGH, Urteil v. 16. Juli 2020, C-311/18 – *Schrems II*.
[20] Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes, https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32016D1250.
[21] Vgl. dazu: *LfD Niedersachsen* – Das Schrems II-Urteil des Europäischen Gerichtshofs und seine Bedeutung für Datentransfers in Drittländer (Stand: Juni 2021), https://lfd.niedersachsen.de/startseite/themen/weitere_themen_von_a_z/internationaler_datenverkehr/das_schrems_ii_urteil_des_eugh_und_seine_bedeutung_fur_datentransfers_in_drittlander/das-schrems-ii-urteil-des-europaischen-gerichtshofs-und-seine-bedeutung-fur-datentransfers-in-drittlander-194085.html.

5.2 Eingeschränkte Gültigkeit der alten Standarddatenschutzklauseln

Neben dem Privacy Shield ging es in dem Urteil auch um die alten Standarddatenschutzklauseln, die die EU-Kommission noch unter Geltung der EU-Datenschutzrichtlinie aus 1995 erlassen hatte. Auch nach dem Urteil des EuGH stellen die SCC grundsätzlich einen zulässigen Mechanismus für datenschutzkonforme Drittlandtransfers dar. Allerdings stellte der EuGH klar, dass die SCC alleine nicht in der Lage sein könnten, bei einem US-Transfer ein sicheres Datenschutzniveau zu gewährleisten. Grund dafür seien insbesondere die behördlichen Zugriffsmöglichkeiten unter dem CLOUD Act bzw. die unzureichenden Möglichkeiten für EU-Bürger, vor US-Gerichten Rechtsschutz gegen Maßnahmen unter dem CLOUD Act zu erlangen. Vielmehr müsse der Datenexporteur (also das EU-Unternehmen) selbst überprüfen, ob weitere Maßnahmen (beispielsweise zusätzliche Vereinbarungen oder technische Schutzmechanismen wie Verschlüsselung) notwendig sind, um ein angemessenes Datenschutzniveau herzustellen. Verantwortliche, die sich aufgrund der Vereinbarung von SCC bisher sicher fühlten, sind nun in der Pflicht, die Rechtmäßigkeit des Datentransfers selbst zu überprüfen – was gerade für kleine Unternehmen oftmals kaum zu bewerkstelligen ist. Diese Wertung lässt sich darüber hinaus auch auf die Verwendung von Binding Corporate Rules (BCR) gemäß Art. 47 DSGVO übertragen.[22]

5.3 Folge des EuGH-Urteils: Haftungsrisiken bei US-Datentransfers

Infolge des obigen EuGH-Urteils ist der Datentransfer in die USA mit erheblichen Unsicherheiten verbunden. EU-Unternehmen, die die Inanspruchnahme von US-Providern bisher auf den Privacy Shield gestützt haben, müssen mit letzteren neue Mechanismen nach Art. 46 und 47 DSGVO vereinbaren oder zu alternativen Providern in Staaten mit angemessenem Datenschutzniveau wechseln. Allerdings sind auch die sonstigen Garantien nach Art. 46 und 47 DSGVO mit Risiken verbunden:

> *Möchte das EU-Unternehmen den US-Transfer auf die SCC oder interne Konzernrichtlinien (Binding Corporate Rules nach Art. 47 DSGVO – BCR) stützen, muss er zunächst das Schutzniveau im Drittland analysieren und darf bei Vorliegen der obigen Garantien erst dann Daten übermitteln, wenn diese Risikobewertung mit positivem Ergebnis abgeschlossen wurde.*[23]

[22] ebd.
[23] EDSA - Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, 10. November 2020, S. 14, https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_de.pdf

6 Sicherheit durch neue Standarddatenschutzklauseln?

6.1 Alte Rechtslage

Die alten SCC wurden noch vor Inkrafttreten der DSGVO erlassen, galten jedoch – wie bereits zuvor geschildert – auch danach zunächst fort. Seit *Schrems II* ist jedoch klar, dass in den USA auch durch die SCC kein angemessenes Niveau zum Schutz personenbezogener Daten erreicht werden konnte. Dies sei nur durch „ergänzende Maßnahmen" ggf. noch erreichbar.[24] So hatte der EDSA Empfehlungen zu ergänzenden Maßnahmen sowie Ergänzungen der SCC formuliert, um den Datentransfer rechtskonform zu gestalten.[25] Zwar sind Statements und Vorgaben des EDSA grundsätzlich nicht verbindlich, allerdings hat sich der Belgische Staatsrat in einem Urteil vom 19. August 2021 im Hinblick auf die Verschlüsselung ausdrücklich auf diese Empfehlungen bezogen und einen US-Transfer, der unter Verschlüsselung der personenbezogenen Daten stattfand, als zulässig bewertet.[26] Auch wenn sich daraus keine unmittelbaren Hinweise auf die gerichtliche Praxis in Deutschland entnehmen lassen, spricht das Urteil dafür, dass die Orientierung an den Empfehlungen des EDSA auch über das Inkrafttreten der SCC hinaus zumindest für eine gewisse Rechtssicherheit sorgen kann. Kann ein Drittlandtransfer nicht vermieden werden, sollte demnach zumindest eine sichere (nicht nur Transport-, sondern auch Ende-zu-Ende-) Verschlüsselung der Daten erfolgen.

Auch wenn einige Unternehmen (zum Beispiel Microsoft[27]) sich durchaus bemühten und entsprechende Ergänzungen in ihre Verträge aufnahmen, blieben diese in der Regel hinter den Anforderungen des EuGH und der Datenschutzbehörden zurück. Zudem wurden viele Unternehmen gar nicht erst tätig, während europäische Unternehmen aufgrund ihrer schwächeren Position in Verhandlungen häufig gar nicht erst in der Lage waren, die notwendigen Änderungen durchzusetzen. Die Unsicherheit wurde durch das Urteil also eher verstärkt als verringert.

[24] *EDPB* – Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, 10. November 2020, S. 2, https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_de.pdf.

[25] ebd.

[26] US-Datentransfer kann mit Verschlüsselung abgesichert werden (Golem), 17. September 2021 https://www.golem.de/news/urteil-zu-schrems-ii-us-datentransfer-kann-mit-verschluesselung-abgesichert-werden-2109-159602.html

[27] *Microsoft* – Im Daten-Dschungel: Wie Microsoft mit dem CLOUD Act umgeht, 11. Februar 2021, https://news.microsoft.com/de-de/im-daten-dschungel-wie-microsoft-mit-dem-cloud-act-umgeht/.

6.2 Neue Rechtslage

Am 27. Juni 2021 sind nun umfassend aktualisierte SCC in Kraft getreten.[28] Mit der Verabschiedung war bei vielen EU-Unternehmen die Hoffnung verbunden, dass eine Verarbeitung personenbezogener Daten durch US-Provider nun wieder ohne größere Hürden möglich sei.

> *Diese Hoffnung wurde indes enttäuscht. Die SCC verpflichten den Datenexporteur (also das EU-Unternehmen) jetzt sogar ausdrücklich, das Datenschutzniveau im Drittland zu überprüfen. Auch die aktualisierte Version alleine ist folglich nicht in der Lage, ein angemessenes Datenschutzniveau herzustellen – vielmehr wurden die Pflichten des Datenexporteurs, die sich bereits infolge von Schrems II ergeben haben, noch einmal ausdrücklich nieder-gelegt und er ist weiterhin verpflichtet, eine Identifizierung und Bewertung aller Risiken vorzunehmen, die mit der Übermittlung verbunden sind (vgl. Klausel 14 der SCC, sog. Data Transfer Risk Assessment).*

Diese Bewertung erfolgt in Zusammenarbeit mit dem Datenimporteur im Drittland (also im Regelfall dem US-Provider) und ist zu dokumentieren. Zur Bestimmung des Datenschutzniveaus durch den Datenexporteur können gem. Klausel 14 und der entsprechenden Fußnote 12 auch einschlägige und dokumentierte praktische Erfahrungen mit früheren Ersuchen von Offenlegungen seitens der Behörde einbezogen werden. Allerdings ist davon auszugehen, dass solche bloßen praktischen Erfahrungen nicht den vom EuGH geforderten Garantien genügen werden.[29]
Die praktischen Erfahrungen stellen vielmehr eine Orientierungshilfe für die EU-Unternehmen dar.

Demgegenüber stehen Informationspflichten des Datenimporteurs, der nun vertraglich verpflichtet wird, dem Datenexporteur mitzuteilen, wenn er das Datenschutzniveau der SCC nach Vertragsschluss nicht mehr einhalten kann. Der Datenexporteur muss dann Abhilfemaßnahmen treffen, also zum Beispiel den Vertrag beenden. Der Datenexporteur bleibt also auch bei Verwendung der neuen SCC für die Risikobewertung verantwortlich.

[28] Abrufbar unter https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en.
[29] *Landes-DSB BW*, Orientierungshilfe: Was jetzt in Sachen internationaler Datentransfer, 01.10.2021, S. 8 f., https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2021/10/OH-int-Datentransfer.pdf

Dennoch sind viele Aspekte der neuen SCC positiv zu bewerten: So wird anders als bisher ein modularer Ansatz verfolgt – es gibt nicht nur eine Version für den Export durch Verantwortliche an Auftragsverarbeiter in Drittländern, die auch den allgemeinen Anforderungen an eine Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 Abs. 3 und 4 DSGVO genügen soll,[30] sondern auch für den umgekehrten Fall, dass der Auftragsverarbeiter in der EU sitzt. Weitere Module betreffen Datenübermittlungen von Auftragsverarbeitern bzw. Verantwortlichen untereinander. Zudem können weitere Parteien der Vereinbarung (nachträglich) beitreten.

Im Falle einer behördlichen Anfrage (zum Beispiel durch das FBI) wird der Datenimporteur zudem verpflichtet, den Datenexporteur zu benachrichtigen und das Offenlegungs-ersuchen bei Zweifeln an dessen Rechtmäßigkeit anzufechten (Klausel 15.1 und 15.2). Insofern werden zumindest einige der Anforderungen der Aufsichtsbehörden umgesetzt, um den US-Transfer rechtssicher zu machen.

Dennoch können Herausgabeverlangen der Behörden nicht vollständig unterbunden werden, da die SCC die Behörden eines Drittlandes nicht binden, sodass US-Transfers auch bei Vereinbarung der neuen SCC rechtswidrig sein können.

Wird ein Transfer auf die SCC gestützt, dürfen bei Neuverträgen ab dem 27. September 2021 nur noch die SCC aus diesem Jahr vereinbart werden. Für Altverträge läuft die Übergangsfrist noch bis zum 27. Dezember 2022, Unternehmen sollten aber zeitnah auf eine Aktualisierung der Vertragsbedingungen drängen.

7 Alternative Cloud-Konstellationen

Ergibt sich aus den vorherigen Erkenntnissen, dass eine Inanspruchnahme von Cloud-Services der US-Provider nach aktueller Rechtslage rechtskonform so gut wie nicht möglich ist, so stellt sich die Frage, ob es alternative Cloud-Konstellationen gibt, die die bestehenden, rechtlichen Hürden überwinden können.

Ein mögliches Modell zur Umgehung der Anfragen von US-Regierungsstellen unter dem CLOUD Act wäre etwa eine Datentreuhand, bei der ein EU-Provider mit alleinigem Zugriff auf die eigenen Server die Datenverarbeitung für den US-Provider übernimmt. Ein entsprechendes Projekt von Microsoft mit der Telekom-Tochter T-Systems (Microsoft Cloud Deutschland) ist vor einigen Jahren jedoch gescheitert.[31] T-Systems hat nun jüngst mit Google eine strategische Partnerschaft vereinbart, bei der T-Systems ein vollständig verschlüsselte Version der Google-Cloud betreibt.[32] Auch mit Microsoft wurde von T-Systems im Hinblick auf die Software Office 365 eine Sonderpartnerschaft dergestalt geschlossen, dass T-System den Betrieb der Software in eigenen Rechenzentren

[30] Vgl. Erwägungsgrund 9 zu den SCC.
[31] Computerwoche, Aus für Microsoft Cloud Deutschland, https://www.computerwoche.de/a/aus-fuer-microsoft-cloud-deutschland,3545727.
[32] Vgl. Michael Kroker – Sisyphusaufgabe, neuer Versuch (Wirtschaftswoche), 9. September 2021, https://www.wiwo.de/technologie/digitale-welt/cloud-partnerschaft-von-deutscher-telekom-und-google-sisyphusaufgabe-neuer-versuch-/27593514.html; Ingo Pakalski – Google und T-Systems planen "souveräne Cloud" (Golem), https://www.golem.de/news/konkurrenz-zu-amazon-und-microsoft-google-und-t-systems-planen-souveraene-cloud-2109-159448.html

übernimmt und die Daten dann verschlüsselt auf Microsoft-Servern abgelegt werden.[33] Ein Datenzugriff durch US-Regierungsstellen auf die deutschen Microsoft-Server wäre dann aufgrund der Verschlüsselung wirkungslos.

Schwachstellen bleiben jedoch die weiterhin möglichen Datenzugriffe der US-Provider im Rahmen bestehender Wartungskonstellationen mit dem deutschen Partner (selbst bei Anwendung des 4-Augen-Prinzips) und möglicher Sicherheitslücken, die von letzterem nur schwer erkennbar sein werden. Zudem bleibt abzuwarten, ob die Datenschutzbehörden einer solchen Treuhandgestaltung offen gegenüberstehen oder diese mit Hinweis auf Restrisiken ebenfalls ablehnen.

Ansonsten gibt es kaum Angebote der bekannten US-Hyperscaler, die in der Lage sind, einen Zugriff unter dem CLOUD Act zu verhindern: Zwar versuchten Microsoft mit der Einführung einer „Datengrenze", durch die Daten ausschließlich in der EU gespeichert und verarbeitet werden sollen,[34] und Google durch den Bau von Rechenzentren in Deutschland Rechtskonformität herzustellen.[35] Allerdings ändert dies nichts daran, dass es sich hierbei um US-Unternehmen handelt, die auch bei Verarbeitung in der EU dem CLOUD Act unterliegen.[36]

Teilweise wird als Alternative auf das europäische Cloud-Projekt Gaia-X[37] verwiesen. Gaia-X Use Cases werden jedoch gerade als Proof-of-Concept erarbeitet. Im praktischen Alltag von Unternehmen spielen Sie derzeit noch keine tragende Rolle. Es ist aber davon auszugehen, dass sich das zukünftig deutlich ändert. Eine abschließende Prüfung auf Einhaltung datenschutzrechtlicher Anforderungen ist zum jetzigen Zeitpunkt noch nicht möglich.[38]

Auch das sog. „Confidential Computing" (oder „Zero-Knowledge-Computing"), bei dem Daten nicht nur bei der Speicherung und Übertragung verschlüsselt werden, sondern auch während des Verarbeitungsvorganges[39], befindet sich noch in der Entwicklung.[40]

---

[33] T-Systems – EU-Datenschutz für Microsoft 365, https://www.t-systems.com/de/de/newsroom/news/hoechster-eu-datenschutz-fuer-microsoft365-447402.
[34] Cloud Act: Microsoft will Cloud wieder DSGVO-kompatibel machen, 07. Mai 2021, https://www.onetoone.de/artikel/db/369156grollmann.html; Microsoft erweitert Datenschutz für Cloud-Dienste in der EU (Handelsblatt), 06. Mai 2021, https://www.handelsblatt.com/technik/it-internet/software-microsoft-erweitert-datenschutz-fuer-cloud-dienste-in-der-eu/27165260.html?ticket=ST-111412-k61iUWxyvYrdpbM4RTkm-ap6.
[35] Google wird Eigentümer des neuen Rechenzentrums in Hanau, 02. September 2021, https://www.op-online.de/region/hanau/hanau-google-wird-eigentuemer-des-neuen-rechenzentrums-im-technologiepark-wolfgang-90955343.html.
[36] Zeit Online – Microsoft bietet Datenverarbeitung in Europa an, https://www.zeit.de/news/2021-05/06/microsoft-bietet-datenverarbeitung-in-europa-an.
[37] Mehr Informationen zu Gaia-X finden sich unter: https://www.bmwi.de/Redaktion/DE/Dossier/gaia-x.html
[38] Dazu: Wie Gaia-X europäische Daten vor dem Zugriff von US-Behörden schützen will (Handelsblatt), 25. April 2021 https://www.handelsblatt.com/politik/deutschland/cloud-projekt-wie-gaia-x-europaeische-daten-vor-dem-zugriff-von-us-behoerden-schuetzen-will/27126688.html; Dietmar Neuerer – Streit über Cloud-Nutzung in den USA – Wirtschaft sendet Hilferuf an die Bundesregierung (Handelsblatt), 3. Mai 2021 https://www.handelsblatt.com/politik/deutschland/brief-an-die-bundesregierung-streit-ueber-cloud-nutzung-in-den-usa-wirtschaft-sendet-hilferuf-an-die-bundesregierung/27151300.html?ticket=ST-72913-ELaVFdPcSMxvBmTdnozH-ap6.
[39] Confidential Computing: Was hat das mit der Sealed Cloud zu tun?, 21. Februar 2021, https://www.idgard.de/privacyblog/confidential-computing-und-sealed-cloud.
[40] ebd.

8 Fazit und Handlungsempfehlungen

Auch bei Abschluss der aktuellen Version der SCC wird der US-behördliche Zugriff nicht ausgeschlossen und die Verantwortung für die Rechtmäßigkeit des Datentransfers verbleibt bei den EU-Unternehmen. Eine Rechtskonformität kann damit nur sichergestellt werden, wenn der beauftragte Provider nicht dem CLOUD Act unterworfen ist, auch wenn die betreffenden Server innerhalb der EU liegen. Damit scheiden grundsätzlich alle US-Provider und ihre Tochterunternehmen aus. **Die Datenschutzaufsicht in Baden-Württemberg hat im Oktober 2021 eine Checkliste für Unternehmen bereitgestellt, die die einzelnen Prüfungsschritte bei der Umsetzung der datenschutzrechtlichen Anforderungen beschreibt.**[41] **Dort wird konkret empfohlen, „nur Dienste zu nutzen, die keine Daten in ein Drittland übertragen". Auch andere deutsche Datenschutzbehörden teilen diese Ansicht und hatten bereits im Juni 2021 angefangen, Fragebögen zu einigen standardmäßig mit einem Drittlandtransfer verbundenen Verarbeitungssituationen zu versenden.**[42] Zudem liegen zwischenzeitlich die ersten behördlichen Untersagungsverfügungen einer EU-Aufsichtsbehörde wegen unzulässigen US-Datentransfers trotz Vorliegen der SCC vor.[43] Insoweit ist anzuraten, intern genau zu prüfen, ob Dienstleister eingebunden werden, die dem US CLOUD Act unterliegen.

Disclaimer

Alle Informationen in diesem White Paper dienen allein der allgemeinen Information. Sie stellen keinesfalls eine Rechtsberatung im Einzelfall dar, können und sollen diese auch nicht ersetzen.

[41] *Landes-DSB BW*, Orientierungshilfe: Was jetzt in Sachen internationaler Datenverkehr, 01.10.2021, S. 12 f., https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2021/10/OH-int-Datentransfer.pdf
[42] Pressemitteilung der Berliner Beauftragten für Datenschutz und Informationsfreiheit vom 01.06.2021, https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2021/20210601-PM-Schrems_II_Pruefung.pdf.
[43] Europäischer Datenschutzausschuss, Census 2021: Portuguese DPA (CNPD) suspended data flows to the USA, https://edpb.europa.eu/news/national-news/2021/census-2021-portuguese-dpa-cnpd-suspended-data-flows-usa_en

Über IONOS

IONOS ist mit mehr als acht Millionen Kundenverträgen der führende europäische Anbieter von Cloud-Infrastruktur, Cloud-Services und Hosting-Dienstleistungen.

Das Produktportfolio bietet alles, was Unternehmen benötigen, um in der Cloud erfolgreich zu sein: von Domains über klassische Websites und Do-It-Yourself-Lösungen, Online-Marketing-Tools bis hin zu vollwertigen Servern und einer IaaS-Lösung. Das Angebot richtet sich an Freiberufler, Gewerbetreibende und Konsumenten sowie an Unternehmenskunden mit komplexen IT-Anforderungen.

IONOS Cloud ist die europäische Cloud-Alternative von IONOS. Unser Produktportfolio umfasst mit der Cloud Compute Engine eine IaaS Compute Engine mit eigenem Code Stack für Virtualisierung, Managed Kubernetes für Container-Anwendungen, eine Private Cloud powered by VMware sowie S3 Object Storage. Mit unserem Angebot bieten wir etablierten mittelständischen und großen Unternehmen, regulierten Industrien, der Digitalwirtschaft und dem öffentlichen Sektor alle notwendigen Dienste und Services um in und mit der Cloud erfolgreich zu sein.

IONOS entstand 2018 aus dem Zusammenschluss von 1&1 Internet und dem Berliner IaaS-Anbieter ProfitBricks. IONOS ist Teil der börsennotierten United Internet AG (ISIN DE0005089031). Zur IONOS Markenfamilie gehören STRATO, Arsys, Fasthosts, home.pl, InterNetX, SEDO, United Domains und World4You.

Weitere Informationen unter cloud.ionos.de

Impressum

IONOS SE
Berlin Office
Revaler Straße 30
10245 Berlin, Germany

IONOS Cloud Kontakt

Telefon +49 30 57700 840
Telefax +49 30 57700 8598
E-Mail produkt@cloud.ionos.de
Website https://cloud.ionos.de

Vorstand

Hüseyin Dogan, Dr. Martin Endreß, Claudia Frese, Hans-Henning Kettler, Arthur Mai, Britta Schmitt, Achim Weiß

Aufsichtsratsvorsitzender

Markus Kadelke

Handelsregister

IONOS SE: Amtsgericht Montabaur / HRB 24498

Umsatzsteuer-IdentNummer

IONOS SE: DE815563912

Copyright

IONOS