Evangelische Kirche in Deutschland

DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Gemeinsame Stellungnahme der Konferenz der Beauftragten für den Datenschutz in der EKD zur Datenübermittlung in die USA

15. Oktober 2021

Herausgegeben vom Beauftragten für den Datenschutz der Evangelischen Kirche in Deutschland (BfD EKD)

Lange Laube 20
30159 Hannover

T. +49(511) 768128-0
F. +49(511) 768128-20

info@datenschutz.ekd.de
https://datenschutz.ekd.de

Einleitende Hinweise

In Ergänzung zur Gemeinsamen Stellungnahme der Konferenz der Beauftragten für den Datenschutz in der EKD zum „Schrems II“-Urteil des EuGH vom 16. Juli 2020 werden in dieser Stellungnahme die Entwicklung sowie die rechtlichen Grundlagen bei der Übermittlung personenbezogener Daten in die USA erläutert. Im Rahmen der rechtlichen Grundlagen werden insbesondere die Entwicklungen in Bezug auf das Safe Habor-Abkommen sowie das EU-US Privacy Shield dargestellt und auf die neu beschlossenen Standarddatenschutzklauseln der Europäischen Kommission eingegangen. Da der EuGH in seinem „Schrems II“-Urteil festgestellt hat, dass in den USA verschiedene Sicherheitsgesetze gelten, die einem mit dem in der EU vergleichbaren Datenschutzniveau entgegenstehen, erfolgt abschließend ein Überblick über das in der Datenschutz-Grundverordnung geregelte Marktortprinzip sowie über den sogenannten CLOUD Act.

Entwicklung

26.07.2000	Das Safe Harbor-Abkommen tritt in Kraft (gemäß Richtlinie 95/46/EG).
06.10.2015	Der EuGH erklärt das Safe Harbor-Abkommen in erster Schrems-Entscheidung für ungültig.
01.08.2016	Das EU-US Privacy Shield-Abkommen als Nachfolgeregelung tritt in Kraft.
24.05.2018	Das novellierte DSG-EKD tritt in Kraft, welches mit der seit 2016 in Kraft getretenen Europäischen Datenschutz-Grundverordnung (DSGVO) in Einklang gebracht worden war.
25.05.2018	Die bereits im Mai 2016 in Kraft getretene Europäische Datenschutz-Grundverordnung (DSGVO) ist jetzt unmittelbar in den Mitgliedstaaten der EU anwendbar.

25.05.2018	Der Europäische Datenschutzausschuss veröffentlicht die Leitlinien 02/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679 (DSGVO) bei Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen.
16.07.2020	Der EuGH kippt das EU-US Privacy Shield-Abkommen.
24.07.2020	Veröffentlichung der Gemeinsamen Stellungnahme der Konferenz der Beauftragten für den Datenschutz in der EKD zum „Schrems II"-Urteil des EuGH vom 16. Juli 2020
12.08.2020	Pressemitteilung: Gespräche zu „neuem" EU-US Privacy Shield-Abkommen eingeleitet
12.08.2020	Fragen und Antworten (FAQ) des BfD EKD zum „Schrems II"-Urteil des EuGH vom 16. Juli 2020
10.11.2020	EDSA veröffentlicht erforderliche Maßnahmen beim Transfer personenbezogener Daten in Drittländer
	Entwurf neuer Standarddatenschutzklauseln
15.01.2021	Pressemitteilung des Bundesbeauftragten zu neuen Standarddatenschutzklauseln
04.06.2021	Die Europäische Kommission veröffentlicht neue Standarddatenschutzklauseln.

Rechtliche Grundlagen

Die rechtliche Grundlage für die Übermittlung personenbezogener Daten in Drittstaaten findet sich in § 10 DSG-EKD.

Die Übermittlung ist nach **§ 10 Abs. 1 DSG-EKD** über die weiteren Voraussetzungen der Datenverarbeitung nur dann zulässig, wenn

1. die EU-Kommission ein angemessenes Datenschutzniveau entsprechend den Bestimmungen des Artikel 45 Absatz 2 Datenschutz-Grundverordnung festgestellt hat,
2. als geeignete Garantien Standarddatenschutzklauseln verwendet werden, die von der Kommission gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 Datenschutz-Grundverordnung erlassen oder genehmigt worden sind.

Falls diese Voraussetzungen nicht vorliegen ist die Übermittlung nach **§ 10 Abs. 2 DSG-EKD** zulässig, wenn

1. die betroffene Person in die vorgeschlagene Datenübermittlung ausdrücklich eingewilligt hat, nachdem sie über die für sie bestehenden möglichen Risiken aufgeklärt worden ist;
2. die Übermittlung für die Erfüllung eines Vertrages oder Rechtsverhältnisses zwischen der betroffenen Person und der verantwortlichen Stelle oder zur Durchführung von vertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich ist;
3. die Übermittlung zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person von der verantwortlichen Stelle mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrages erforderlich ist;
4. die Übermittlung aus wichtigen Gründen des kirchlichen Interesses notwendig ist;
5. die Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist oder
6. die Übermittlung zum Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen erforderlich ist, sofern die betroffene Person aus physischen oder rechtlichen Gründen außer Stande ist, ihre Einwilligung zu geben.

Safe Harbor-Abkommen und EU-US Privacy Shield-Abkommen

Das EU-US Privacy Shield-Abkommen, das bislang gemäß § 10 Abs. 1 Nr. 1 DSG-EKD als Rechtsgrundlage für die Übermittlung von personenbezogenen Daten in die USA herangezogen werden konnte, ist der Nachfolger des **Safe Harbor-Abkommens** aus dem Jahr 2000. Das Safe Harbor-Abkommen wurde im Oktober 2015 vom EuGH in der ersten Schrems-Entscheidung für ungültig erklärt. Bereits im Jahr 2013 hielt die EU-Kommission fest, dass die Datenschutzerfordernisse durch das Safe Harbor-Abkommen nicht den europäischen Standards entsprechen. Auch die Datenschutzbehörden kritisierten das Abkommen, da im Rahmen des Patriot Acts US-Sicherheitsbehörden unter Umständen auch ohne Benachrichtigung der Dateninhaber Zugriff auf die in den Vereinigten Staaten gespeicherten Daten gewährt werden müsse.

Am 06. Oktober 2015 erklärte der EuGH das Abkommen dann in seiner **ersten Schrems-Entscheidung** (Az.: C-362/14) für ungültig. Das Safe Harbor-Abkommen laufe ins Leere, da die US-amerikanischen Unternehmen, die sich dem unterworfen hätten, jederzeit und ohne Einschränkung verpflichtet seien, die Schutzregeln unangewendet zu lassen und personenbezogene Daten an die US-amerikanischen Sicherheitsbehörden herauszugeben, „ohne dass es in den Vereinigten Staaten Regeln gibt, die dazu dienen, etwaige Eingriffe zu begrenzen, noch, dass es einen wirksamen gerichtlichen Rechtsschutz gegen solche Eingriffe gibt.“ (Pressemitteilung des EuGH Nr. 117/15 zum Urteil). Damit waren für das Gericht der Wesensgehalt der Grundrechte auf Achtung des Privatlebens und des wirksamen gerichtlichen Rechtsschutzes verletzt.

Nach mehrmonatigen Verhandlungen wurde das Nachfolgeabkommen **EU-US Privacy Shield** am 12. Juli 2016 von der Europäischen Kommission angenommen. Die Regelungen zum EU-US Privacy Shield-Abkommen sahen z. B. klarere gesetzliche Grundlagen für einen Datenzugriff durch US-Behörden, ausdrückliche Anforderungen an Zweckbindung, Erforderlichkeit und Verhältnismäßigkeit solcher Zugriffe und geeignete Maßnahmen gegen Missbrauch und unbefugte Zugriffe vor. Die US-Behörden sind für ihren Umgang mit personenbezogenen Daten von US-Bürgern verantwortlich und werden durch eine unabhängige Beschwerdestelle ("Ombudsperson") überwacht. Bei dieser und bei Behörden und Gerichten sollten sich in Zukunft auch EU-Bürger über den Umgang mit ihren personenbezogenen Daten beschweren können.

Dennoch war das Abkommen von Anfang an erheblicher Kritik ausgesetzt. Insbesondere wurde bemängelt, dass die Überwachungsgesetze in den USA nicht oder nur unwesentlich geändert wurden. Auch blieben Massenüberwachungsmaßnahmen durch die amerikanische Regierung weiterhin zulässig. Sie unterlägen insbesondere keiner Verhältnismäßigkeitsprüfung, was gegen europäisches Recht verstoße. Außerdem könnten die betroffenen Personen ihre Rechte weiterhin nicht wirksam verfolgen, weil sie von der Überwachung gar nicht erführen. Deshalb helfe ihnen auch der Ombudsmann nicht, der zudem nicht über die hierzu notwendigen Befugnisse verfüge. Auch die nötige Unabhängigkeit fehle ihm als Beamter des amerikanischen Außenministeriums.

Am 16. Juli 2020 erklärte der EuGH dann auch das EU-US Privacy Shield-Abkommen in seiner **„Schrems II“-Entscheidung** für ungültig. Die Gesetze, auf deren Grundlage amerikanische Sicherheitsbehörden auf die in die USA übermittelten personenbezogenen Daten zugreifen können (Section 702 FISA/E.O. 12333), würden Art. 7 und Art. 8 der EU-Grundrechtecharta unverhältnismäßig beschränken und verstießen gegen Art. 52 (1) S. 2 der EU-Grundrechtecharta. So werde der Zugriff auf die personenbezogenen Daten von Nicht-US-Amerikanern nicht beschränkt. Es bestehe kein Rechtsschutz gegen die Zugriffe durch die amerikanischen Sicherheitsbehörden, der den Anforderungen des Art. 47 der EU-Grundrechtecharta genügt. Gegen Zugriffe auf der Basis der E.O. 12333 bestehe keinerlei Rechtsschutz. Der Ombudsmann könne diesen Umstand nicht ausgleichen, da er nicht unabhängig und nicht ermächtigt ist, gegenüber den US-amerikanischen Nachrichtendiensten verbindliche Entscheidungen zu treffen. Gespräche über eine Nachfolgevereinbarung wurden im August 2020 bereits eingeleitet.

Standarddatenschutzklauseln

Standarddatenschutzklauseln, die von der Europäischen Kommission erlassen wurden, können ohne weitere Genehmigung durch die Aufsichtsbehörden gemäß § 10 Abs. 1 Nr. 2 DSG-EKD als **Grundlage für Übermittlungen personenbezogener Daten** in Drittländer und an internationale Organisationen genutzt werden, wenn sie im Wesentlichen unverändert in die zugrundeliegenden Verträge übernommen werden.

Feststellungen des EuGH

Im Zusammenhang mit dem „Schrems II"-Urteil hat der EuGH ausdrücklich festgestellt, dass die bestehenden Standarddatenschutzklauseln aufrechterhalten bleiben. Es gilt im Hinblick auf den Schutz vor Zugriffen durch Sicherheitsbehörden von Drittstaaten wie den USA der gleiche Standard wie bei Angemessenheitsentscheidungen. Dabei ist jedoch zu beachten, dass nach den Ausführungen des EuGH die Standarddatenschutzklauseln aufgrund ihres Vertragscharakters naturgemäß keine drittstaatlichen Behörden binden könnten und dennoch das verbürgte Datenschutzniveau zu gewährleisten sei. Nach rechtlicher Würdigung des EuGH bestehe keine Verpflichtung der EU-Kommission beim Erlass von Standarddatenschutzklauseln das Datenschutzniveau von Drittstaaten zu überprüfen. Der EuGH betont vielmehr die **Verantwortung des Datenexporteurs**, für jede Datenübermittlung das Schutzniveau im Drittland zu prüfen und geeignete Garantien für den Schutz der in ein Drittland übermittelten Daten vorzusehen. Dabei kann es erforderlich sein, über die Standarddatenschutzklauseln hinaus ergänzende Garantien durch zusätzliche Maßnahmen vorzusehen. Denkbar sind rechtliche, technische oder organisatorische Maßnahmen. Die tatsächliche Wirksamkeit solcher Maßnahmen darf jedoch nicht durch die Rechtsordnung des Drittlandes beeinträchtigt werden. Der Datenexporteur ist verpflichtet die Datenübermittlung auszusetzen oder zu beenden, wenn der Schutz der übermittelten Daten auch durch zusätzliche Maßnahmen nicht hinreichend sichergestellt werden kann.

Bei der Prüfung und **Bewertung der Standarddatenschutzklauseln als geeignete Garantien** müssen daher mindestens folgende Umstände berücksichtigt werden:

- die Regelungen der geeigneten Garantien selbst, also z.B. die Standarddatenschutzklauseln;
- alle relevanten Aspekte des Rechts des betreffenden Drittstaates im Hinblick auf den Zugriff auf die dorthin übermittelten personenbezogenen Daten durch Sicherheitsbehörden;
- die jeweiligen konkreten Umstände der Datenübermittlung inklusive ggf. vom Datenexporteur zu ergreifende zusätzliche Garantien.

Auch wenn das Urteil unmittelbar nur auf Standarddatenschutzklauseln bezogen ist, gelten die dort konkretisierten Anforderungen des EuGH entsprechend auch bei der **Nutzung von verbindlichen internen Datenschutzvorschriften** (Binding Corporate Rules, BCR). Auch hier hat der Verantwortliche zu prüfen, ob im Drittland ein gleichwertiges Schutzniveau vorherrscht oder ob gegebenenfalls zusätzliche Maßnahmen ergriffen werden können, um das angemessene Schutzniveau zu erreichen.

Empfehlungen des Europäischen Datenschutzausschusses

Im November 2020 hat der Europäische Datenschutzausschuss (EDSA) Empfehlungen zu Maßnahmen verabschiedet, die ergänzend herangezogen werden können, um die Einhaltung des europäischen Schutzniveaus für personenbezogene Daten bei **Drittstaatentransfers** – unter anderem auf Basis der Standarddatenschutzklauseln – zu gewährleisten.

Die Veröffentlichungen des Europäischen Datenschutzausschusses (EDSA) – zu finden unter https://edpb.europa.eu/ – sind:

- „Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten“ und
- „Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien bei Überwachungsmaßnahmen.

Der EDSA beschreibt **sechs Stufen**, die bei einer Datenübermittlung berücksichtigt werden müssen, wenn die Rechtmäßigkeit von Datenübermittlungen in Drittländer bewertet wird. Der Ausschuss hält hierbei ausdrücklich fest, dass die Ergebnisse dieser Bewertung und die ggf. getroffenen Maßnahmen zu dokumentieren sind, um dies gegenüber den Aufsichtsbehörden in Erfüllung der Rechenschaftspflicht nachweisen zu können.

Stufe 1: Dokumentation aller Übermittlungen personenbezogener Daten in Drittländer

Stufe 2 und 3: Auswahl eines Transferinstruments sowie Prüfung der Wirksamkeit

Stufe 4: Auswahl und verbindliche Vereinbarung zusätzlicher Schutzmaßnahmen

Stufe 5: Formale Bestätigung der Prozessschritte (soweit erforderlich)

Stufe 6: Regelmäßige Überprüfung der getroffenen Maßnahmen

Neue Standarddatenschutzklauseln der Europäischen Kommission

Die Europäische Kommission hat nach dem „Schrems II“-Urteil des EuGH neue Standarddatenschutzklauseln veröffentlicht. Zwar hat der EuGH in seinem Urteil ausdrücklich festgestellt, dass die Standarddatenschutzklauseln weiterhin gültig bleiben. Der EuGH hat aber bemängelt, dass in einigen Drittländern kein Datenschutzniveau besteht, das mit dem in der Europäischen Union vergleichbar ist. In diesen Fällen könne ein gleichwertiges Datenschutzniveau nur durch zusätzliche Maßnahmen hergestellt werden. Eine Überarbeitung der bereits bestehenden Standarddatenschutzklauseln ist damit erforderlich geworden.

Nach intensiven Verhandlungen hat die Europäische Kommission am 4. Juni 2021 neue Standarddatenschutzklauseln zur Übermittlung von personenbezogenen Daten aus der EU in Drittländer beschlossen und veröffentlicht. Wie auch die bisher geltenden Standarddatenschutzklauseln dürfen auch die neuen Standarddatenschutzklauseln grundsätzlich nicht verändert werden. Sie sind vorrangig vor anderen Vereinbarungen, die zwischen den Parteien getroffen wurden, zu berücksichtigen.

Unterschiede ergeben sich jedoch in Bezug auf den Aufbau und den Inhalt der neuen Standarddatenschutzklauseln. Die neuen Standarddatenschutzklauseln sind in vier Module aufgebaut. Es ist jeweils im Einzelfall zu prüfen, welches Modul im konkreten Fall einschlägig ist. Im Rahmen der Module werden folgende Konstellationen bei der Übermittlung von personenbezogenen Daten in ein Drittland unterschieden:

1. Übermittlung von personenbezogenen Daten von einem Verantwortlichen an einen anderen Verantwortlichen
2. Übermittlung von personenbezogenen Daten von einem Verantwortlichen an einen Auftragsverarbeiter
3. Übermittlung von personenbezogenen Daten von einem Auftragsverarbeiter an einen anderen Auftragsverarbeiter
4. Übermittlung von personenbezogenen Daten von einem Auftragsverarbeiter an einen Verantwortlichen.

Bei der Verwendung der neuen Standarddatenschutzklauseln ist darauf zu achten, dass die auf den Einzelfall zugeschnittenen Klauseln verwendet werden.

Inhaltlich soll mithilfe der neuen Standarddatenschutzklauseln bei der Übermittlung von personenbezogenen Daten in ein Drittland ein Schutzniveau hergestellt werden, dass dem in der EU bestehenden Schutzniveau gleichwertig ist. Dazu sind in den neuen Standarddatenschutzklauseln Garantien vorgesehen, die die Einhaltung der Klauseln durch den Datenimporteur sicherstellen und die Rechte der Betroffenen stärken sollen. Insbesondere treffen den Datenimporteur verschiedene Informationspflichten gegenüber dem Datenexporteur und der betroffenen Person. Der Datenimporteur muss aktiv prüfen, ob mithilfe der bestehenden Standarddatenschutzklauseln ein gleichwertiges Datenschutzniveau erreicht werden kann oder ob zusätzliche – technische und organisatorische – Maßnahmen erforderlich sind.

Weitere Änderungen ergeben sich auch im Hinblick auf die Verarbeitung von personenbezogenen Daten im Auftrag. In Fällen, in denen sich der Auftragsverarbeiter in einem Drittland befindet, ist neben der Verwendung der Standarddatenschutzklauseln für die Übermittlung von personenbezogenen Daten in Drittländer kein zusätzlicher Auftragsverarbeitungsvertrag zu schließen. In Art. 1 Absatz 2 des Durchführungsbeschlusses 2021/914 ist ausdrücklich festgelegt, dass in den Standarddatenschutzklauseln auch die Rechte und Pflichten der Verantwortlichen und der Auftragsverarbeiter in Bezug auf die in Art. 28 Abs. 3 und 4 DSGVO genannten Fragen im Hinblick auf die Übermittlung personenbezogener Daten von einem Verantwortlichen an einen Auftragsverarbeiter festgelegt sind. Dies gilt auch in Fällen, in denen personenbezogene Daten von einem Auftragsverarbeiter an einen Unterauftragsverarbeiter übermittelt werden.

Um die dauerhafte Einhaltung der Klauseln sicherstellen zu können, ist in den neuen Standarddatenschutzklauseln geregelt, dass die Parteien eine sogenannte Datentransfer-Folgenabschätzung (DTFA) durchführen müssen. Dabei müssen die Parteien insbesondere die Umstände der Übermittlung, die geltenden Gesetze und Rechtsvorschriften des jeweiligen Drittlandes berücksichtigen sowie die Klauseln durch weitere vertragliche, technische und organisatorische Garantien ergänzen.

Einwilligung

Eine Übermittlung von personenbezogenen Daten in die USA kann auch auf der Grundlage von § 10 Abs. 2 DSG-EKD zulässig sein. In dem „Schrems II“-Urteil hat der EuGH ausdrücklich den Datentransfer

auf der Grundlage einer Einwilligung als Möglichkeit der Übermittlung genannt. In der DSGVO ist die Einwilligung in Art. 49 jedoch im Gegensatz zu § 10 Abs. 2 Nr. 1 DSG-EKD als **Ausnahmetatbestand** überschrieben. Die Anforderungen an die Aufklärung über die bestehenden möglichen Risiken sind in beiden Gesetzen als hoch einzustufen.

Zwischenfazit

Wo immer ein Datentransfer in die USA auf Grundlage von § 10 Abs. 1 DSG-EKD geschieht, muss sichergestellt sein, dass ein gleichwertiges Schutzniveau gewährleistet wird. Eine Übermittlung auf der Grundlage der neuen Standarddatenschutzklauseln ist möglich, jedoch sind diese an den Einzelfall anzupassen und durch weitere vertragliche, technische und organisatorische Maßnahmen zu ergänzen. Geeignete Maßnahmen wären beispielsweise die Pseudonymisierung oder die Verschlüsselung. Diese werden vom EDSA ausdrücklich als mögliche Maßnahmen beschrieben, sofern der Datenimporteur (und entsprechend auch die ausländische Behörde) keine Möglichkeit hat, die Daten auf einzelne Personen zurück zu führen. Die Übermittlung von Klardaten dürfte dagegen problematisch sein.

Im Übrigen ist eine Datenübermittlung nur auf der Grundlage von § 10 Abs. 2 Nr. 1 bis 6 DSG-EKD möglich. Bezüglich der Einwilligung nach § 10 Abs. 2 Nr. 1 DSG-EKD ist zu beachten, dass diese im Beschäftigtendatenschutz nur schwer umzusetzen ist. Auch bei einer Übermittlung, die eine Vielzahl von Personen betrifft, wäre die Widerrufbarkeit der Einwilligung ein hoher Unsicherheitsfaktor. Die Einwilligung kommt also möglicherweise nur für einzelne Datenübermittlungen in Betracht, die eine überschaubare Anzahl von externen Personen betreffen (z.B. Veranstaltungen mit Externen). Zu beachten sind jedoch die hohen Anforderungen an die Informiertheit über mögliche Risiken.

Das Marktortprinzip der Datenschutz-Grundverordnung

In einigen Fällen unterliegen auch außereuropäische Unternehmen den Bestimmungen der DSGVO. Hintergrund ist das sogenannte Marktortprinzip, das erstmalig in die DSGVO mitaufgenommen wurde. Fraglich ist, wie sich diese Regelung auf den Datentransfer in die USA und die dort geltenden Gesetze auswirkt.

Das Marktortprinzip ist in **Art. 3 Abs. 2 DSGVO** geregelt und schließt unter bestimmten Voraussetzungen Unternehmen, die nicht in der EU niedergelassen sind, aber personenbezogene Daten von Betroffenen verarbeiten, die sich in der EU befinden, in den Anwendungsbereich der DSGVO mit ein.

Gemäß Art. 3 Abs. 2 lit. a) DSGVO findet die DSGVO auf außereuropäische Unternehmen Anwendung, wenn die Datenverarbeitung im Zusammenhang damit steht, den betroffenen Personen in der EU **Waren oder Dienstleistungen** anzubieten. Das Unternehmen muss dies offensichtlich beabsichtigen. Irrelevant ist, ob entgeltliche oder unentgeltliche Angebote vorliegen.

Nach Art. 3 Abs. 2 lit. b) DSGVO findet die DSGVO auch auf außereuropäische Unternehmen Anwendung, wenn die Datenverarbeitung im Zusammenhang damit steht, das **Verhalten** von betroffenen Personen

zu **beobachten**, soweit dieses Verhalten in der EU erfolgt. Dazu kann beispielsweise der Einsatz von Tracking-Cookies oder Browser Fingerprints gehören.

Erfüllt ein nicht in der EU niedergelassenes Unternehmen die Voraussetzungen von Art. 3 Abs. 2 DSGVO, so muss es die **DSGVO vollumfänglich beachten**. Das Unternehmen ist dann verpflichtet, einen in einem betroffenen Mitgliedsstaat niedergelassenen Vertreter zu benennen. Dadurch soll den betroffenen Personen ermöglicht werden, die Betroffenenrechte auszuüben. Auch soll den Aufsichtsbehörden ermöglicht werden, ihre Aufsichtsmaßnahmen effektiv durchzusetzen. Die Pflicht entfällt nur in Fällen, in denen die Datenverarbeitung lediglich gelegentlich erfolgt, sie keine umfangreiche Verarbeitung sensibler personenbezogener Daten einschließt oder sie zu keinem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Ein US-amerikanisches Unternehmen, das aufgrund des Marktortprinzips der DSGVO unterfällt, hat die europäischen Datenschutzbestimmungen vollumfänglich zu beachten.

CLOUD Act

Unterliegt ein US-Unternehmen den Vorschriften der DSGVO, so ist zu fragen, ob dies Auswirkungen auf die geltenden US-Sicherheitsgesetze, insbesondere auf den CLOUD Act (Clarifying Lawful Overseas Use of Data Act), hat.

Der EuGH hat im „Schrems II"-Urteil festgestellt, dass in den USA kein gleichwertiges Schutzniveau für die personenbezogenen Daten der betroffenen Personen besteht. Dies führt der EuGH insbesondere darauf zurück, dass in den USA verschiedene Sicherheitsgesetze gelten, die es den US-amerikanischen Behörden ermöglichen, auf personenbezogene Daten von Nicht-US-amerikanischen Bürgern zuzugreifen, die an US-amerikanische Unternehmen übermittelt wurden. Dazu gehört beispielsweise auch der sog. CLOUD Act.

Der **CLOUD Act** wurde im März 2018 vom US-Kongress verabschiedet. Er ergänzt den Stored Communication Act (SCA), der den US-Behörden einen direkten Zugriff auf Daten aufgrund eines Rechtsaktes (z.B. einer Verwaltungsanordnung) gewährt.

Hintergrund des CLOUD Acts ist der sog. **Microsoft-Irland-Fall**. Microsoft wehrte sich dabei gegen eine Anordnung einer US-amerikanischen Behörde, die die Herausgabe von personenbezogenen Daten verlangte, obwohl diese Daten auf Servern außerhalb der USA gespeichert waren. Bis zu diesem Zeitpunkt war umstritten, ob auf den SCA auch ein Herausgabeverlangen von Daten gestützt werden könne, die zwar dem Zugriff und der Kontrolle eines US-Unternehmens unterlagen, sich aber auf ausländischen Servern befanden. Bevor der Supreme Court über den Rechtsstreit entscheiden konnte, verabschiedete der US-Kongress den CLOUD Act, sodass der Rechtsstreit für erledigt erklärt wurde und eine abschließende Entscheidung ausblieb.

Der CLOUD Act stellt klar, dass US-amerikanische Unternehmen für **strafrechtliche Zwecke** verpflichtet sind, sämtliche in ihrem Besitz, Gewahrsam oder ihrer Kontrolle befindlichen Daten gegenüber US-Behörden offenzulegen. Dies gilt unabhängig davon, ob die Daten innerhalb oder außerhalb der USA

gespeichert sind. Die US-Behörden haben somit das Recht, für strafrechtliche Zwecke auch ohne das Vorliegen eines internationalen Rechtshilfeabkommens auf personenbezogene Daten von US-Unternehmen, die im Ausland gespeichert sind, zuzugreifen.

Dieses Herausgabeverlangen kann von den US-amerikanischen Unternehmen nur in seltenen Fällen abgelehnt werden. Eine **Ablehnung** kommt nur in Betracht, wenn das Herausgabeverlangen personenbezogene Daten von Nicht-US-Bürgern oder nicht in den USA ansässigen Personen betrifft und die Offenlegung das erhebliche Risiko der Verletzung der Gesetze einer „qualifizierten ausländischen Regierung" begründet. Der Begriff der „qualifizierten ausländischen Regierung" erfasst nur solche Staaten, mit denen die USA ein sog. „Executive Agreement" abgeschlossen haben. Diesbezüglich steht die EU seit einiger Zeit in Verhandlungen mit den USA. Ein Ergebnis liegt bislang nicht vor. Zwischenzeitlich haben jedoch die USA und Großbritannien ein solch wechselseitiges Abkommen geschlossen. Dieses wird vom EDSA jedoch kritisiert, da befürchtet wird, dass das Abkommen zu einer Aushebelung des Datenschutzes führe. Auch wird bezweifelt, dass die in dem Abkommen getroffenen Schutzbestimmungen überhaupt greifen würden.

Die Europäische Kommission plant zurzeit mit der sog. **E-Evidence-Verordnung** ein zum CLOUD Act vergleichbares EU-Gesetz zu schaffen. Der Entwurf sieht vor, dass Strafverfolgungsbehörden in den Mitgliedsstaaten der EU in strafrechtlichen Verfahren berechtigt wären, Anbieter von Telekommunikations- und Internetdienstleistungen in anderen Mitgliedstaaten der EU und in Drittstaaten zur Übermittlung von Bestands-, Verkehrs- und Inhaltsdaten zu verpflichten. Ihnen soll der (Direkt-)Zugriff zu „elektronischen Beweismitteln" erleichtert werden. Bislang stößt der Entwurf jedoch bei den europäischen Aufsichtsbehörden auf Kritik, insbesondere, weil der Entwurf eine Umgehung der Justizbehörden des Landes vorsieht, in dem der Provider seinen Sitz hat.

Fraglich ist, ob der **CLOUD Act** und die **DSGVO miteinander vereinbar** sind. Entscheidend ist diesbezüglich **Art. 48 DSGVO**. Gemäß Art. 48 DSGVO darf eine Datenübermittlung auf der Grundlage einer Entscheidung eines ausländischen Gerichts nur erfolgen, wenn sie auf eine in Kraft befindliche internationale Übereinkunft (z. B. Rechtshilfeabkommen) zwischen ersuchendem Drittland und Mitgliedsstaat oder auf andere Ermächtigungen des Kapitels V der DSGVO gestützt werden kann. Eine internationale Übereinkunft, die in diesem Fall zum Tragen käme, gibt es gegenwärtig nicht.

Die Datenübermittlung könnte aber zulässig sein, wenn die Voraussetzungen des **Art. 49 DSGVO** vorliegen. Der EDSA sowie der EDSB haben dies bereits geprüft und im Rahmen einer Stellungnahme festgestellt, dass eine Datenübermittlung in die USA auf der Grundlage von Art. 49 DSGVO aufgrund des CLOUD Acts nur in **extrem gelagerten Einzelfällen** in Betracht kommt. Neben den Voraussetzungen des Art. 49 DSGVO müssten dann auch die Voraussetzungen von Art. 5 und 6 DSGVO erfüllt sein.

Bei der Prüfung ist darüber hinaus auch **Erwägungsgrund 115** der DSGVO zu beachten. Danach muss ein Unterlaufen des Schutzniveaus der DSGVO durch Rechtsakte von Drittländern verhindert werden. Daraus folgt, dass Datenübermittlungen nur dann zulässig sind, wenn die Bedingungen der DSGVO für einen Drittlandtransfer eingehalten werden.

Ein US-amerikanisches Unternehmen, das aufgrund des Marktortprinzips der DSGVO unterfällt, unterliegt zugleich auch dem CLOUD Act. Verlangt eine US-Behörde von einem US-Unternehmen die Herausgabe von personenbezogenen Daten, die auf Servern außerhalb der USA gespeichert sind, so muss sich das US-Unternehmen entscheiden, ob es gegen den CLOUD Act oder gegen die Vorschriften der DSGVO verstößt.

Abschließende Beurteilung

Erfolgt eine Übermittlung personenbezogener Daten in die USA auf der Grundlage von § 10 Abs.1 DSG-EKD, so muss gewährleistet werden, dass in den USA ein gleichwertiges Schutzniveau besteht. Nach dem Wegfall des EU-US Privacy Shield-Abkommens gibt es aktuell keinen Angemessenheitsbeschluss, auf den die Datenübermittlung gestützt werden kann. Gegenwärtig wird von den zuständigen Stellen an einem Angemessenheitsbeschluss gearbeitet.

Eine Übermittlung von personenbezogenen Daten kann auf die zwischenzeitlich von der Europäischen Kommission beschlossenen Standarddatenschutzklauseln gestützt werden. Dabei ist zu beachten, dass die Standarddatenschutzklauseln stets an den Einzelfall angepasst und durch vertragliche, technische und organisatorische Maßnahmen ergänzt werden müssen. Auch sind die Parteien verpflichtet, in regelmäßigen Abständen zu prüfen, ob die in den Standarddatenschutzklauseln festgelegten Garantien weiterhin eingehalten werden. Darüber hinaus können personenbezogene Daten auf der Grundlage von § 10 Abs. 2 Nr. 1 bis 6 DSG-EKD in die USA übermittelt werden.

Werden personenbezogene Daten an ein US-Unternehmen übermittelt, so ist zu beachten, dass US-Behörden unter anderem auf der Grundlage des CLOUD Acts zu strafrechtlichen Zwecken auf diese Daten zugreifen können. Dies gilt unabhängig davon, ob die personenbezogenen Daten auf Servern in den USA oder auf europäischen Servern gespeichert sind. Ausreichend ist, wenn das US-Unternehmen Zugriff auf bzw. Besitz oder Gewahrsam an den personenbezogenen Daten hat. Irrelevant ist ebenfalls, ob das US-Unternehmen aufgrund des Marktortprinzips der DSGVO unterfällt oder nicht. Unterfällt das US-Unternehmen der DSGVO, so muss es sich entscheiden, ob es im Falle eines Zugriffs durch US-amerikanische Behörden gegen die Vorschriften der DSGVO oder gegen den CLOUD Act verstößt.

Übermittelt eine verantwortliche Stelle personenbezogene Daten an ein US-Unternehmen, so muss die verantwortliche Stelle prüfen, ob die Datenübermittlung im Hinblick auf die geltenden Sicherheitsgesetze vertretbar ist. Dabei ist insbesondere zu berücksichtigen, um welche Art von personenbezogenen Daten es sich handelt und ob die Daten gegebenenfalls durch weitere technische und organisatorische Maßnahmen vor dem Zugriff der US-Behörden geschützt werden können.

Hannover, den 15. Oktober 2021
Die Beauftragten für den Datenschutz in der EKD