Ausarbeitung

DSGVO und Nutzung US-amerikanischer Cloud-Dienste

DSGVO und Nutzung US-amerikanischer Cloud-Dienste

Aktenzeichen: WD 3 - 3000 - 102/21
Abschluss der Arbeit: 3. Juni 2021
Fachbereich: WD 3: Verfassung und Verwaltung

Inhaltsverzeichnis

1. Einleitung und Fragestellung

Der Europäische Gerichtshof (EuGH) hat am 16. Juli 2020 entschieden, dass das zwischen der EU und den USA geschlossene Datenschutzabkommen EU-US-Privacy-Shield ungültig ist. Das Datenschutzniveau in den USA sei insbesondere aufgrund der weiten Eingriffsbefugnisse der amerikanischen Nachrichtendienste auf personenbezogene Daten und der fehlenden Rechtsschutzmöglichkeiten für EU-Bürger nicht mit dem der EU gleichwertig.[1]

Dies hat Auswirkungen auf die Zulässigkeit der Übermittlung von personenbezogenen Daten aus der EU in die USA, unter anderem im Bereich des **Cloud-Computings.** Cloud-Computing ist die Vermietung eines Online-Zugangs zu Computerressourcen durch einen Cloud-Anbieter. Bei den Computerressourcen kann es sich beispielsweise um Server, Speicherplatz, Datenbanken oder Online-Anwendungen handeln.[2] Große US-amerikanische Cloud-Anbieter sind Unternehmen wie Microsoft, Amazon und Google.

Gefragt wird, welche rechtlichen Voraussetzungen erfüllt sein müssen, damit die deutsche Bundesverwaltung die Dienste US-amerikanischer Cloud-Anbieter bzw. die Dienste von Unternehmen mit Sitz in Deutschland, die die Dienste solcher Anbietern nutzen, im Einklang mit der Datenschutzgrundverordnung (DSGVO)[3] nutzen können.

2. Rechtliche Voraussetzungen für die Nutzung von Diensten US-amerikanischer Cloud-Anbieter

Nach der DSGVO ist die Übermittlung personenbezogener Daten an einen in einem **Drittland** (d.h. **außerhalb** der **EU** oder des **EWR**) niedergelassenen Empfänger,[4] nur unter den in Kapitel V (Art. 44 ff. DSGVO) geregelten Bestimmungen zulässig. Die Art. 44 ff. DSGVO setzen voraus, dass die Übermittlung mit den allgemeinen Vorschriften der DSGVO im Einklang steht.

2.1. Anwendungsbereich der DSGVO

Grundlegende Voraussetzung ist zunächst, dass der Anwendungsbereich der DSGVO eröffnet ist.

2.1.1. Sachlicher Anwendungsbereich

Der sachliche Anwendungsbereich der DSGVO erstreckt sich auf die ganz oder teilweise **automatisierte Verarbeitung personenbezogener Daten** sowie auf die nichtautomatisierte Verarbeitung

---

1 EuGH, Urteil vom 16. Juli 2020 – Az. C-311/18 – (Schrems II), juris.

2 Vgl. Brockhaus, „Cloud-Computing“, abrufbar unter https://brockhaus.de/ecs/enzy/article/cloud-computing; Microsoft, Was ist Cloud Computing?, abrufbar unter https://azure.microsoft.com/de-de/overview/what-is-cloud-computing/ (letzter Abruf jeweils 3. Juni 2021).

3 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119 S. 1, ber. L 314 S. 72, 2018 L 127 S. 2 und 2021 L 74 S. 35.

4 Siehe dazu Kamp/Beck, in: Wolff/Brink, BeckOK Datenschutzrecht, 35. Edition, Stand: 1. November 2020, Art. 44 DSGVO Rn. 23 ff.

personenbezogener Daten, die in einem **Dateisystem gespeichert** sind oder gespeichert werden sollen, Art. 2 Abs. 1 DSGVO.

2.1.1.1. Personenbezogene Daten

Der Begriff der **personenbezogenen Daten** ist **weit** zu verstehen.[5] Gemäß Art. 4 Nr. 1 DSGVO sind personenbezogene Daten **alle Informationen,** die sich auf eine **identifizierte oder identifizierbare natürliche Person** (im Folgenden „betroffene Person") **beziehen;** als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann. Unter den Begriff personenbezogene Daten fallen sowohl persönliche Angaben wie Name, Alter, Herkunft, als auch sachliche Angaben wie die Beziehungen des Betroffenen zu Dritten, die finanzielle Situation oder das Konsum- und Kommunikationsverhalten.

Die Übermittlung von Daten an ein Unternehmen durch die deutsche Bundesverwaltung kann eine **Vielzahl an Daten** betreffen, die einen Personenbezug aufweisen. Es kommen unter anderem Beschäftigtendaten, staatlich erhobene Daten von Bürgern, Fotos von Personen mit Namenszuordnung und gespeicherte E-Mail-Adressen in Betracht. Bei Kommunikationsdaten sind sowohl die Inhalts- als auch die Metadaten umfasst.[6] Auch IP-Adressen sind potentiell personenbezogen, soweit der Provider sie einem Benutzer zuordnen kann und dieses Zusatzwissen des Providers für andere (juristische) Personen zugänglich und erreichbar ist.[7] Weiter können sich personenbezogene Daten in Erlaubnissen, Genehmigungen, Strafverfahrensakten o.Ä. befinden.

Lediglich reine Sachinformationen oder Unternehmensdaten, mit denen man auch nicht mittelbar eine natürliche Person identifizieren könnte, fallen aus dem Anwendungsbereich der DSGVO.[8]

2.1.1.2. Verarbeitung

Datenverarbeitung i.S.d. Art. 2 Abs. 1 DSGVO ist **jeder Umgang mit personenbezogenen Daten.**[9] Nach der weiten Begriffsbestimmung des Art. 4 Nr. 2 DSGVO umfasst die Verarbeitung „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die

---

5 Ernst, in: Paal/Pauly, DS-GVO BDSG, 3. Auflage 2021, Art. 4 DSGVO Rn. 3.

6 Ernst, in: Paal/Pauly, DS-GVO BDSG, 3. Auflage 2021, Art. 4 DSGVO Rn. 14.

7 Schild, in: Wolff/Brink, BeckOK Datenschutzrecht, 35. Edition Stand: 1. Februar 2021, Art. 4 DSGVO Rn. 19.

8 Ernst, in: Paal/Pauly, DS-GVO BDSG, 3. Auflage 2021, Art. 4 DSGVO Rn. 6.

9 Vgl. Gola, in: Gola, Datenschutz-Grundverordnung, 2. Auflage 2018, Art. 4 Rn. 30.

Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“.

Bei einem Transfer von personenbezogenen Daten durch die deutsche Bundesverwaltung an ein anderes Unternehmen kommen insbesondere die Tatbestände der „Bereitstellung“ sowie der „Offenlegung durch Übermittlung“ in Betracht. Es liegt in der Natur der Sache des Cloud-Computings, dass dieser Vorgang **automatisiert** abläuft.

2.1.2. Räumlicher Anwendungsbereich

Der räumliche Anwendungsbereich der DSGVO ist eröffnet, soweit die Datenverarbeitung **im Rahmen** der **Tätigkeiten** einer **Niederlassung** eines **Verantwortlichen** oder eines **Auftragsverarbeiters in der Union** erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet, Art. 3 Abs. 1 DSGVO.

Verantwortlicher ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere **Stelle, die** allein oder gemeinsam mit anderen **über** die **Zwecke** und **Mittel** der **Verarbeitung von personenbezogenen Daten entscheidet,** Art. 4 Nr. 7 DSGVO.

Dahingegen verarbeitet der **Auftragsverarbeiter** die personenbezogenen Daten **im Auftrag des Verantwortlichen,** Art. 4 Nr. 8 DSGVO. Cloud-Dienstleistungen sind typischer Weise Auftragsverarbeitungen. Soweit die Bundesverwaltung ein Unternehmen mit Cloud-Computing beauftragt, welches dafür die Dienste eines US-amerikanischen Cloud-Anbieters nutzt, wird es sich bei dem von der Verwaltung beauftragten Unternehmen regelmäßig um einen Auftragsverarbeiter handeln. Etwas anderes kann dann gelten, wenn das beauftragte Unternehmen die personenbezogenen Daten für eigene Zwecke verarbeitet.[10]

Im Falle der Datenübermittlung an einen Empfänger in einem Drittland durch die deutsche Bundesverwaltung oder ein Unternehmen mit Sitz in Deutschland ist die DSGVO nach dem Niederlassungsprinzip in räumlicher Hinsicht anwendbar.

2.2. Voraussetzungen für die Datenübermittlung

Die Voraussetzungen, um Daten verarbeiten zu dürfen, finden sich in Art. 6 Abs. 1 DSGVO. Darin werden **Erlaubnistatbestände** aufgezählt, die eine Datenverarbeitung möglich machen. Dies gilt ganz unabhängig davon, ob die Datenübermittlung an einen Empfänger in einem Drittland erfolgt oder nicht. Bei einem **Drittlandbezug** müssen **zusätzlich zu den allgemeinen Anforderungen** der

10 Zum Ganzen Spoerr, in: Wolff/Brink, BeckOK Datenschutzrecht, 35. Edition Stand: 1. Februar 2021, Art. 28 DSGVO Rn. 24c.

DSGVO die **speziellen Bestimmungen** der Art. 44 ff. DSGVO beachtet werden.[11] Welcher Erlaubnistatbestand in Betracht kommt, hängt von den Umständen im Einzelfall ab. Allgemein lässt sich mit Blick auf das Cloud-Computing Folgendes zu den Erlaubnistatbeständen festhalten:

2.2.1. Einwilligung, Art. 6 Abs. 1 S. 1 lit. a) DSGVO[12]

Gemäß Art. 6 Abs. 1 S. 1 lit. a) DSGVO ist eine Verarbeitung rechtmäßig, wenn die betroffene Person ihre **Einwilligung** zur der Verarbeitung gegeben hat. Eine Einwilligung der betroffenen Person ist jede **freiwillig** für den **bestimmten Fall, in informierter Weise** und **unmissverständlich abgegebene Willensbekundung** in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, Art. 4 Nr. 11 DSGVO. Gemäß Art. 7 DSGVO muss die Einwilligungserklärung insbesondere ausdrücklich erklärt werden sowie unmissverständlich und nachweisbar sein. Der Verantwortliche muss zudem gewährleisten, dass die Einverständniserklärung **freiwillig**, d.h. ohne jeden Druck und Zwang erfolgt.[13]

In der Literatur wird bezweifelt, ob die Einwilligung eine geeignete Grundlage für den Datentransfer an Cloud-Anbieter sein kann. So wird darauf hingewiesen, dass in einigen Fällen die Verantwortlichen keinen direkten **Zugang zu den betroffenen Personen** hätten, sodass das Einholen der Einwilligung Schwierigkeiten bereite.[14] Dies sei insbesondere dann der Fall, wenn beauftragte Unternehmen bzw. der Cloud-Anbieter selbst sich die Einwilligung einholen müssten. Mit Blick auf die personenbezogenen Daten von Beschäftigten werden Zweifel an der **Freiwilligkeit** der Einwilligungen geäußert, weil diese im Rahmen von Über-/Unterordnungsverhältnissen getätigt würden.[15] Dieses Argument lässt sich auf den Datentransfer von personenbezogenen Daten von Bürgerinnen und Bürgern durch Behörden an Cloud-Anbieter übertragen.

2.2.2. Zur Erfüllung eines Vertrages, Art. 6 Abs. 1 S. 1 lit. b) DSGVO

Die Verarbeitung kann auch aufgrund von Art. 6 Abs. 1 S. 1 lit. b) DSGVO erfolgen, wenn sie für die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen, erforderlich ist. Art. 6 Abs. 1 S. 1 lit. b) DSGVO gilt jedoch nur, wenn der **Vertrag mit der betroffenen Person selbst geschlossen** wird bzw. die Anfrage durch die betroffene Person erfolgt. Dies ist bei den hier zu erörternden Fällen jedoch nicht der Fall.

---

11 Schantz, in: Schantz/Wolff, Das neue Datenschutzrecht, 1. Auflage 2017, Rn. 755; Kamp/Beck, in: Wolff/Brink, BeckOK Datenschutzrecht, 35. Edition, Stand: 1. November 2020, Art. 44 DSGVO Rn. 47 f.

12 Gemäß Art. 6 Abs. 1 S. 2 DSGVO gilt der Erlaubnistatbestand der Einwilligung gemäß Art. 6 Abs. 1 S. 1 lit. a) DSGVO **nicht** für die von **Behörden** in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

13 Schulz, in: Gola, Datenschutz-Grundverordnung, 2. Auflage 2018, Art. 7 Rn. 21.

14 Determann/Weigl, EuZW 2016, S. 811 (S. 814).

15 Paal/Kumkar, MMR 2020, S. 733 (S. 737).

2.2.3. Zur Erfüllung einer rechtlichen Verpflichtung, Art. 6 Abs. 1 S. 1 lit. c) DSGVO

Gemäß Art. 6 Abs. 1 S. 1 lit. c) DSGVO dürfen Daten verarbeitet werden, wenn die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt. Art. 6 Abs. 3 S. 2 DSGVO präzisiert, dass **als Rechtsgrundlage nur Unionsrecht** oder das **nationale Recht** der **Mitgliedstaaten** in Betracht kommt. Ein US-amerikanischer Cloud-Anbieter mit Niederlassung in der EU könnte sich daher nicht auf eine mögliche rechtliche Verpflichtung aus US-Recht berufen.

2.2.4. Allgemeine Interessensabwägung, Art. 6 Abs. 1 S. 1 lit. f) DSGVO

Schließlich kommt der Erlaubnistatbestand der **allgemeinen Interessenabwägung** des Art. 6 Abs. 1 S. 1 lit. f) DSGVO in Betracht. Dafür muss die Übermittlung der Daten zur Wahrung der **berechtigten Interessen des Verantwortlichen** erforderlich sein, wobei die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, nicht überwiegen dürfen. Ob ein berechtigtes Interesse vorliegt, ist rein normativ zu entscheiden. Dafür wird zunächst der Zweck der Verarbeitung ermittelt und beurteilt. Dadurch, dass Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO einen Ausgleich zwischen den Interessen des Betroffenen und denen des Verantwortlichen schaffen möchte, werden nicht nur rechtliche Interessen berücksichtigt. Vielmehr können **auch wirtschaftliche oder ideelle Interessen** Beachtung finden.[16] Ein berechtigtes Interesse kommt daher in Betracht, wenn die Verwaltung aus Kostengründen auf Speicherplatz in einer Cloud zurückgreifen will. In einem zweiten Schritt ist dieses berechtige Interesse mit den Interessen und Grundrechten und Grundfreiheiten des Betroffenen **abzuwiegen**. Als schutzwürdige Interessen der betroffenen Personen sind deren allgemeines Persönlichkeitsrecht (Art. 2 Abs. 1 Grundgesetz (GG)) sowie das Recht auf den Schutz personenbezogener Daten (Art. 8 der Charta der Grundrechte der Europäischen Union (GRCh)) zu berücksichtigen. Das Ergebnis der Abwägung hängt dabei vom jeweiligen Einzelfall ab.

2.3. Datenübermittlung in ein Drittland

Sollen personenbezogene Daten an Drittländer oder an internationale Organisationen übermittelt werden, sind **zusätzlich** die Anforderungen der Art. 44 ff. DSGVO zu beachten. Auf diese Weise soll ausgeschlossen werden, dass die Regelungen der DSGVO unterlaufen werden, indem die Datenverarbeitung in ein Drittland ausgelagert wird.[17] Die Bestimmungen des Kapitels V sind gemäß Art. 44 S. 2 DSGVO so anzuwenden, dass das **durch die DSGVO gewährleistete Schutzniveau** für natürliche Personen **nicht untergraben** wird.

Der Begriff der **Übermittlung** wird in der DSGVO nicht ausdrücklich definiert. Mit Blick auf den Sinn und Zweck der Art. 44 ff. DSGVO ist der Begriff weit zu verstehen. Daher dürfte **jede Offenlegung personenbezogener Daten gegenüber Empfängern in Drittländern** oder internationalen

16 Albers/Veit, in: Wolff/Brink, BeckOK Datenschutzrecht, 35. Edition Stand: 1. Mai 2020, Art. 6 DSGVO, Rn. 49.

17 Schantz, in: Schantz/Wolff, Das neue Datenschutzrecht, 1. Auflage 2017, Rn. 754.

Organisationen erfasst sein.[18] In der Literatur wird vertreten, dass auch solche Fälle erfasst sind, in denen die personenbezogenen Daten an einen unselbständigen Unternehmensteil oder einen Auftragsverarbeiter in einem Drittland übermittelt werden.[19]

2.3.1. Angemessenheitsbeschluss, Art. 45 Abs. 3 DSGVO

Gemäß Art. 45 Abs. 1 DSGVO darf eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation vorgenommen werden, wenn die **EU-Kommission** „beschlossen hat, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet". Soweit ein solcher **Angemessenheitsbeschluss** besteht, bedarf die Datenübermittlung keiner besonderen Genehmigung durch die zuständigen Aufsichtsbehörden. Die Beurteilung des angemessenen Schutzniveaus erfolgt anhand des in Art. 45 DSGVO vorgegebenen Kriterienkatalogs. Nach der Rechtsprechung des **EuGH** muss das Schutzniveau des Drittlandes bzw. der internationalen Organisation **im Vergleich zur europäischen Lage gleichwertig** sein, wobei die Mittel, wie dies erreicht wird, von denen in der EU verwendeten Mitteln unterschiedlich sein können.[20]

Der Angemessenheitsbeschluss der EU-Kommission betreffend die **USA** wurde am 16. Juli 2020 vom **EuGH** im sog. Schrems II-Urteil[21] für **ungültig** erklärt.[22] Dies begründet das Gericht damit, dass keine ausreichenden Beschränkungen bestehen, die die Eingriffsbefugnisse US-amerikanischer Nachrichtendienste auf das erforderliche Maß begrenzen.[23] Zudem hätten die betroffenen Personen keine Möglichkeit, einen wirksamen Rechtsbehelf einzulegen, um sich gegen die Zugriffe der Behörden oder US-Nachrichtendienste auf ihre personenbezogenen Daten zu schützen.[24] Auch der US-amerikanische Ombudsmechanismus könne den mangelnden Rechtsschutz nicht ausgleichen, da Zweifel an der Unabhängigkeit der Ombudsperson bestehen würden.[25]

---

18 Schantz, in: Schantz/Wolff, Das neue Datenschutzrecht, 1. Auflage 2017, Rn. 757; Zerdick, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Auflage 2018, Art. 44 DSGVO Rn. 7.

19 Schantz, in: Schantz/Wolff, Das neue Datenschutzrecht, 1. Auflage 2017, Rn. 757; Kamp/Beck, in: Wolff/Brink, BeckOK Datenschutzrecht, 35. Edition, Stand: 1. November 2020, Art. 44 DSGVO Rn. 21.

20 EuGH, Urteil vom 6. Oktober 2015 – C-362/14 – (Schrems I), Rn. 73 f., juris.

21 EuGH, Urteil vom 16. Juli 2020 – C-311/18 – (Schrems II), juris.

22 Zum Ganzen siehe Beck, in: Wolff/Brink, BeckOK Datenschutzrecht, 35. Edition Stand: 1. November 2020, Art. 45 DSGVO Rn. 53 ff.

23 Ebenda.

24 EuGH, Urteil vom 16. Juli 2020 – Az. C-311/18 – (Schrems II), Rn. 187, Rn. 191, juris.

25 EuGH, Urteil vom 16. Juli 2020 – Az. C-311/18 – (Schrems II), Rn. 195, Rn. 196, juris.

2.3.2. Datenübermittlung vorbehaltlich geeigneter Garantien nach Art. 46 Abs. 1 DSGVO

Liegt für einen Drittstaat kein Angemessenheitsbeschluss nach Art. 45 DSGVO vor, ist eine Übermittlung von personenbezogenen Daten an einen Empfänger in einem Drittstaat unter den Voraussetzungen des Art. 46 DSGVO zulässig. Gemäß Art. 46 Abs. 1 DSGVO darf ein Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten an ein Drittland oder eine internationale Organisation übermitteln, sofern er **geeignete Garantien** vorgesehen hat und sofern den betroffenen Personen **durchsetzbare Rechte** und **wirksame Rechtsbehelfe** zur Verfügung stehen. Geeignete Garantien liegen laut dem Erwägungsgrund 108 bei Vorkehrungen vor, mit denen sichergestellt wird, dass die Datenschutzvorschriften auf eine der Verarbeitung innerhalb der Union angemessene Art und Weise beachtet werden. Nach der Rechtsprechung des **EuGH** muss auch bei den geeigneten Garantien ein Schutzniveau gewährleistet sein, das mit dem der Europäischen Union der Sache nach **gleichwertig** ist.[26]

Generell bedürfen geeignete Garantien einer **Genehmigung im Einzelfall** durch die **zuständigen Aufsichtsbehörden,** Art. 46 Abs. 3 DSGVO.

Eine solche **Genehmigung** ist jedoch **nicht erforderlich,** wenn eine geeignete Garantie nach Art. 46 Abs. 2 DSGVO vorliegt; dazu gehören:

- **rechtlich verbindliche Verwaltungsvereinbarungen** zwischen den Behörden oder öffentlichen Stellen,
- **verbindliche interne Datenschutzvorschriften** gemäß Art. 47 DSGVO,
- **Standarddatenschutzklauseln,** die von der EU-Kommission gemäß dem Prüfverfahren nach Art. 93 Abs. 2 DSGVO erlassen werden bzw. genehmigt wurden,
- genehmigte Verhaltensregeln gemäß Art. 40 DSGVO **(Code of Conduct)** bzw. ein **genehmigter Zertifizierungsmechanismus** gemäß Art. 42 DSGVO.

In der Praxis sind bei der Datenübermittlung an eine private Stelle insbesondere die Standarddatenschutzklauseln sowie die verbindlichen internen Datenschutzklauseln (Binding Corporate Rules) von großer Bedeutung. Fraglich ist jedoch, inwieweit sich Behörden nach dem sog. Schrems II-Urteils des EuGH noch auf die von der EU-Kommission beschlossenen Standarddatenschutzklauseln[27] bzw. auf Binding Corporate Rules als geeignete Garantien berufen können, wenn sie Dienste eines US-Cloud-Anbieters nutzen bzw. mit einem Unternehmen zusammenarbeiten wollen, das diese Dienste nutzt.

---

26 EuGH, Urteil vom 16. Juli 2020 – C-311/18 – (Schrems II), Rn. 96, Rn. 105, juris.

27 Beschluss der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates.

2.3.2.1. Standarddatenschutzklauseln

Der EuGH hat sich in dem sog. Schrems II-Urteil auch mit den Standarddatenschutzklauseln beschäftigt. Er stellt zunächst fest, dass die von der EU-Kommission festgelegten Standarddatenschutzklauseln aus dem SDK-Beschluss **prinzipiell wirksame Mechanismen** für die Aussetzungen und das Verbot der Übermittlung der personenbezogenen Daten vorsehen und hält diese für grundsätzlich zulässig.[28]

Das Gericht betont jedoch, dass der Verantwortliche und der Empfänger im Drittland **in jedem Einzelfall verpflichtet** sind, zu überprüfen, ob das **Recht des Bestimmungsdrittlands** nach Maßgabe des Unionsrechts einen **angemessenen Schutz** der **personenbezogenen Daten gewährleiste.**[29] Der EUGH stellt weiter fest:

> „Kann der in der Union ansässige Verantwortliche bzw. sein dort ansässiger Auftragsverarbeiter keine hinreichenden zusätzlichen Maßnahmen ergreifen, um einen solchen Schutz zu gewährleisten, ist er – bzw. in zweiter Linie die zuständige Aufsichtsbehörde – verpflichtet, die Übermittlung personenbezogener Daten in das betreffende Drittland auszusetzen oder zu beenden. Dies ist insbesondere dann der Fall, wenn das Recht dieses Drittlands dem Empfänger aus der Union übermittelter personenbezogener Daten Verpflichtungen auferlegt, die den genannten Klauseln widersprechen und daher geeignet sind, die vertragliche Garantie zu untergraben, dass ein angemessener Schutz vor dem Zugang der Behörden dieses Drittlands zu diesen Daten besteht.“[30]

Für den Fall der **USA** hat der EuGH entschieden, dass allein über die Verwendung der Standarddatenschutzklauseln **kein angemessenes Schutzniveau** hergestellt werden könne.[31] Nach Ansicht des EUGH müssen die Standarddatenschutzklauseln durch **zusätzliche Maßnahmen** ergänzt werden, die die übermittelten Daten im konkreten Einzelfall angemessen vor dem unbeschränkten Zugriff der US-Sicherheitsbehörden schützen. Der EUGH macht keine Vorgaben, welche dies sind bzw. sein können. Er betont, dass in jedem Einzelfall die passenden Maßnahmen zu ermitteln sind.

2.3.2.2. Zusätzliche Maßnahmen

In Literatur und Praxis werden unterschiedliche Lösungsansätze diskutiert, durch welche zusätzlichen Maßnahmen ein Datentransfer an einen Empfänger in den USA rechtmäßig erfolgen kann.

Der **Europäische Datenschutzausschuss (EDSA),** der aus Vertretern der nationalen Datenschutzbehörden und dem Europäischen Datenschutzbeauftragten (EDSB) besteht und der zur einheitlichen Anwendung der Datenschutzvorschriften in der EU beitragen und die Zusammenarbeit zwischen den EU-Datenschutzbehörden fördern soll, hat diesbezüglich **Empfehlungen** veröffentlicht. Darin

---

28 EuGH, Urteil vom 16. Juli 2020 – Az. C-311/18 – (Schrems II), Rn. 148, juris.

29 EuGH, Urteil vom 16. Juli 2020 – Az. C-311/18 – (Schrems II), Rn. 134, juris.

30 EuGH, Urteil vom 16. Juli 2020 – Az. C-311/18 – (Schrems II), Rn. 135, juris.

31 EuGH, Urteil vom 16. Juli 2020 – Az. C-311/18 – (Schrems II), Rn. 168, juris.

wird festgehalten, dass zusätzliche Maßnahmen grundsätzlich sowohl vertraglicher, technischer als auch organisatorischer Art sein können, wobei auch eine Kombination verschiedener Maßnahmen möglich ist.[32] Von entscheidender Bedeutung für die Frage, welche zusätzlichen Maßnahmen für die Gewährleistung des im Wesentlichen gleichwertigen Schutzniveaus geeignet sind, sei dabei die Beurteilung der Rechtslage im Drittland. So müsse der Datenexporteur – ggfs. mit Unterstützung des Datenimporteurs – prüfen, ob die Effektivität der gewählten Maßnahmen möglicherweise durch das Recht oder die Praxis des Drittlands beeinträchtigt wird.

Nach den Empfehlungen des EDSA kommen als **technische Maßnahmen** beispielsweise die **Verschlüsselung,** die **Übermittlung pseudonymisierter Daten** und die Transportverschlüsselung in Kombination mit End-to-End-Verschlüsselung in Betracht.[33] Der EDSA weist darauf hin, dass der Datenexporteur – mit Unterstützung des Datenimporteurs – **sehr genau prüfen** muss, **welchen Verpflichtungen letzterer unterliegt.** So gelte für Datenimporteure in den USA, die 50 USC § 1881a (FISA 702)[34] unterliegen würden, hinsichtlich der importierten Daten, die sich in ihrem Besitz oder Gewahrsam oder unter ihrer Kontrolle befänden, eine **direkte Verpflichtung,** den **Zugriff** darauf zu **gewähren** oder diese **herauszugeben.** Diese Verpflichtung könne sich auch auf die kryptografischen Schlüssel erstrecken, ohne die die Daten nicht lesbar seien.[35] Der EDSA stellt zudem fest, dass die empfohlenen technischen Maßnahmen in bestimmten Bereichen nicht in Betracht kommen, beispielsweise wenn der Cloud-Service-Anbieter oder andere Verarbeiter den Zugang zu unverschlüsselten Daten benötigen oder wenn personenbezogene Daten an Unternehmen in einem Drittland für gemeinsame Geschäftszwecke bereitgestellt werden sollen.[36]

Bezüglich zusätzlicher **vertraglicher Maßnahmen** stellt der EDSA fest, dass diese grundsätzlich nicht die Behörden des Drittlands binden können, wenn diese nicht selbst Vertragspartei sind. Daher kämen diese nur in Kombination mit zusätzlichen technischen und/oder organisatorischen Maßnahmen in Betracht.[37] Dies gilt entsprechend für die zusätzlichen **organisatorischen Maßnahmen.** Dabei handelt es sich um interne Strategien, Organisationsmethoden und Standards, die die Datenexporteure bei sich selbst anwenden oder den Datenimporteuren auferlegen (beispielsweise interne Grundsätze für Berichtswesen, Standardarbeitsanweisungen, Maßnahmen zur Datenminimierung).

---

32 EDSA, Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, angenommen am 10. November 2020, Rn. 47, abrufbar unter https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_de (letzter Abruf 3. Juni 2021).

33 EDSA (Fn. 32), Rn. 79 ff.

34 Die Section 702 des FISA ermöglicht das Überwachen von Zielpersonen für einen Zeitraum von bis zu einem Jahr. In dieser Zeit wird die ganze elektronische Kommunikation von und zu der Zielperson sowie über die Zielperson aufgefangen und anschließend analysiert.

35 EDSA (Fn. 32), Rn. 76.

36 EDSA (Fn. 32), Rn. 87 ff.

37 EDSA (Fn. 32), Rn. 93.

Nach den Empfehlungen des EDSA kann durch diese allein nicht bereits systematisch sichergestellt werden, dass ein im Wesentlichen gleichwertiges Schutzniveau gewährleistet wird.[38] Auch hier gilt es zu prüfen, welchen Verpflichtungen der Datenimporteur unterliegt und ob im Einzelfall durch die Zusammenschau der ergriffenen Maßnahmen der Schutz der personenbezogenen Daten ausreichend sicher gestellt ist.

In der Literatur wird als zusätzliche Maßnahme die Ergänzung der Standarddatenschutzklauseln um Regelungen vorgeschlagen, wonach der **Datenimporteur** im Falle staatlichen Zugriffs **verpflichtet** werde, hiergegen den **Rechtsweg zu beschreiten.**[39] Auf diese Weise soll das vom EUGH festgestellte Defizit bei den Rechtsschutzmöglichkeiten ausgeglichen werden. Ob dies allein durch vertragliche Regelungen mit dem Datenimporteur gelingen kann, kann hier nicht abschließend beurteilt werden. In jedem Fall würde sich jedoch weiterhin das Problem der weitreichenden Befugnisse der US-Sicherheitsbehörden stellen, die nicht mit dem erforderlichen Datenschutzniveau vereinbar sind.

Zum Teil wird auch vorgeschlagen, dass der **Cloud-Anbieter** seinen **Sitz in der EU** einrichtet oder eine Niederlassung in der EU gründet, um einem Eingriff der US-Sicherheitsbehörden vorzubeugen.[40] Hierzu ist allerdings anzumerken, dass sich die Zugriffsbefugnisse der US-Sicherheitsbehörden nicht allein nach dem Sitz des Unternehmens bestimmen. Vielmehr kann auch eine rechtliche Verknüpfung des Unternehmens mit den USA ausreichen. Dies ist laut Literatur beispielsweise dann der Fall, wenn der Server des Cloud-Anbieters seinen Standort in den USA hat.[41] Auch bei einem Konzernverbund, bei dem der Mutterkonzern seinen Sitz in den USA hat, oder bei einer (Zweig)Niederlassung des Unternehmens sind Zugriffe der US-Sicherheitsbehörden möglich.[42] In der Literatur wird zudem darauf hingewiesen, dass das US-Recht teilweise sogar dann für anwendbar erklärt wird, wenn ein Mitarbeiter des Unternehmens in den USA anwesend war, z.B. durch eine Dienstreise.[43] Auch das kontinuierliche und systematische Betreiben von Geschäften in den USA könne einen Anknüpfungspunkt bilden.[44] Damit ist festzuhalten, dass nur, weil der Cloud-Anbieter oder die Server, welche die Cloud bilden, in der EU gelegen sind, nicht schon davon ausgegangen werden kann, dass keine Zugriffsmöglichkeit der USA auf die Daten besteht.[45]

---

38 EDSA (Fn. 32), Rn. 122.

39 Schulz, PharmR 2020, S. 600 (S. 602).

40 Zum Ganzen Schulz, PharmR 2020, S. 600 (S. 602).

41 Schuppert/von Reden, ZD 2013, S. 210 (S. 217).

42 Voigt, MMR 2014, S. 158 (S. 160).

43 Ebenda.

44 Schuppert/von Reden, ZD 2013, S. 210 (S. 217).

45 Schuppert/von Reden, ZD 2013, S. 210 (S. 220); Voigt, MMR 2014, S. 158 (S. 160).

2.3.3. Binding Corporate Rules

Die vom EuGH aufgestellten Maßstäbe für eine Datenübermittlung auf Grund von Standarddatenschutzklauseln sind auch auf die anderen in Art. 46 Abs. 2 DSGVO geeigneten Garantien übertragbar. Dies bedeutet, dass auch bei der Nutzung von verbindlichen internen Datenschutzvorschriften (Binding Corporate Rules) gemäß Art. 46 Abs. 2 lit. b), 47 DSGVO zusätzliche Maßnahmen getroffen werden müssen.[46]

2.3.4. Ausnahmen nach Art. 49 DSGVO

Liegt weder ein Angemessenheitsbeschluss der EU-Kommission vor noch eine geeignete Garantie, kann die Datenübermittlung nach einem der in Art. 49 DSGVO geregelten Ausnahmetatbestände zulässig sein.

Art. 49 Abs. 1 DSGVO sieht folgende Ausnahmefälle vor:

- Besonders informierte, ausdrückliche Einwilligung der betroffenen Person, Abs. 1 UAbs. 1 lit. a),
- zur Erfüllung eines Vertrages oder vorvertraglicher Maßnahmen mit dem Betroffenen, Abs. 1 UAbs. 1 lit. b),
- zur Erfüllung eines im Interesse der betroffenen Person abgeschlossenen Vertrages, Abs. 1 UAbs. 1 lit. c),
- wichtige Gründe des öffentlichen Interesses, Abs. 1 UAbs. 1 lit. d),
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen, Abs. 1 UAbs. 1 lit. e),
- zum Schutz lebenswichtiger Interessen, Abs. 1 UAbs. 1 lit. f),
- Übermittlung aus einem Register, das gemäß EU-Recht oder dem Recht der Mitgliedstaaten zur Information der Öffentlichkeit bestimmt ist, Abs. 1 UAbs. 1 lit. g),
- zur Wahrung zwingender berechtigter Interessen des Verantwortlichen erforderlich, Abs. 1 UAbs. 2 S. 1.

---

46 Siehe hierzu auch das Informationsschreiben zur Auswirkung der Rechtsprechung des EuGH auf den internationalen Datentransfer (Rechtssache C-311/18 „Schrems II“) des Bundesbeauftragten für den Datenschutz und die Informationssicherheit (BfDI), abrufbar unter https://www.bfdi.bund.de/DE/Europa_International/International/Artikel/Auswirkungen-Schrems-II-Urteil.html (letzter Abruf 3. Juni 2021); Lange/Filip, in: Wolff/Brink, BeckOK Datenschutzrecht, 35. Edition Stand: 1. August 2020, Art. 47 DSGVO Rn. 62.

Die in Art. 49 DSGVO normierten **Ausnahmetatbestände** sind **eng auszulegen.**[47] Nach dem Erwägungsgrund 111 DSGVO sollen die Tatbestände des Art. 49 Abs. 1 UAbs. 1 lit. b), lit. c) und lit. e) DSGVO **nur bei gelegentlich erfolgenden Übermittlungen** in Betracht kommen. Eine Übermittlung ist gelegentlich, wenn sie nicht wiederholt oder im Rahmen einer Vielzahl ähnlicher Fälle erfolgt.

Welche Ausnahmetatbestände konkret in Betracht kommen, hängt maßgeblich von der Art der Informationen und den konkreten Umständen der Datenübermittlung ab. Insofern sind hier nur einige allgemeine Ausführungen möglich. So wird in der Literatur der Ausnahmetatbestand der **Einwilligung** gemäß Art. 49 UAbs. 1 lit. a) DSGVO als wenig praktikabel bewertet.[48] Art. 49 Abs. 1 UAbs. 1 lit. a) DSGVO setzt voraus, dass die betroffene Person über die Risiken der Datenübermittlung aufgeklärt werden muss. Die Betroffenen sollen sich darüber im Klaren sein, dass ihre Daten im Drittland nicht mehr geschützt sind.[49] Diese Aufklärung dürfte die Unternehmen sowie die Behörden jedoch vor große Herausforderungen stellen, da nicht nur die geplante Verwendung der Daten, sondern auch die Erhebungs- und Verarbeitungspraxis in dem Drittland so detailliert beschrieben werden muss, dass sich der Betroffene den Konsequenzen einer Übermittlung seiner Daten in ein Land mit abweichendem Schutzniveau bewusst wird.[50] Hinzu kommen die oben unter 2.2.1. beschriebenen praktischen Nachteile und Unsicherheiten. Eine weitere Unsicherheit besteht zudem dadurch, dass die Einwilligung jederzeit widerruflich ist.[51]

2.3.5. Überprüfungs- sowie Dokumentations- und Transparenzpflicht

Grundsätzlich gilt zu beachten, dass die vorgenommenen Maßnahmen in regelmäßigen Abständen **überprüft** werden müssen, insbesondere darauf, ob sie noch effektiv sind.[52] Die Überprüfung der Rechtmäßigkeit des Datentransfers in Drittländer muss so **dokumentiert** werden, dass die Aufsichtsbehörde die Einhaltung der Bestimmungen der Art. 44 ff. DSGVO prüfen kann, Art. 5 Abs. 2, Art. 30 Abs. 1 S. 1 lit. e) DSGVO.[53]

---

47 Lange/Filip, in: Wolff/Brink, BeckOK Datenschutzrecht, 35. Edition BeckOK Stand: 1. August 2020, Art. 49 DSGVO Rn. 2.

48 Lange/Filip, in: Wolff/Brink, BeckOK Datenschutzrecht, 35. Edition BeckOK Stand: 1. August 2020, Art. 49 DSGVO Rn. 11.

49 Lange/Filip, in: Wolff/Brink, BeckOK Datenschutzrecht, 35. Edition BeckOK Stand: 1. August 2020, Art. 49 DSGVO Rn. 6.

50 Schulz, PharmR 2020, S. 600 (S. 602); Paal/Kumkar, MMR 2020, S. 733 (S. 737).

51 Lange/Filip, in: Wolff/Brink, BeckOK Datenschutzrecht, 35. Edition BeckOK Stand: 1. August 2020, Art. 49 DSGVO Rn. 11.

52 Kamp/Beck, in: Wolff/Brink, BeckOK Datenschutzrecht, 35. Edition, Stand: 1. November 2020, Art. 44 DSGVO Rn. 44.

53 Siehe hierzu auch das Prüfschema Drittstaatentransfers des Bundesbeauftragten für den Datenschutz und die Informationssicherheit (BfDI), abrufbar unter https://www.bfdi.bund.de/DE/Europa_International/International/Artikel/Auswirkungen-Schrems-II-Urteil.html (letzter Abruf 3. Juni 2021).

2.3.6. Besondere Pflichten bei der Auftragsverarbeitung, Art. 28 DSGVO

Soweit die Bundesverwaltung ein Unternehmen mit Sitz in Deutschland mit Cloud-Diensten beauftragen will, welches hierfür die Dienste eines US-amerikanischen Cloud-Anbieters nutzt, sind die besonderen Pflichten aus Art. 28 DSGVO zu beachten. So darf der Verantwortliche nur mit solchen Auftragsverarbeitern zusammenarbeiten, die **hinreichenden Garantien für** eine **ordnungsgemäße Verarbeitung** bieten, Art. 28 Abs. 1 DSGVO. Der Verantwortliche muss den Auftragsverarbeiter also sorgfältig auswählen **(Auswahlverantwortung)** und durch **„geeignete technische und organisatorische Maßnahmen“** sicherstellen, dass der Schutz der Rechte der betroffenen Person gewährleistet ist.[54]

Für den Auftragsverarbeiter gilt grundsätzlich das Prinzip der eigenhändigen Leistungserbringung. Die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters ist nur mit vorheriger, gesonderter oder allgemeiner **schriftlicher Genehmigung des Verantwortlichen** möglich, Art. 28 Abs. 2 DSGVO. Dem Unterauftragsnehmer müssen dieselben Datenschutzpflichten auferlegt werden, die zwischen dem Verantwortlichen und dem Auftragsverarbeiter bestehen, Art. 28 Abs. 4 DSGVO. Auch der Unterauftragnehmer muss hinreichende Garantien dafür bieten, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt.[55]

3. Fazit

Ein Transfer personenbezogener Daten im Zusammenhang mit Cloud-Computing an einen Empfänger in der USA ist nur unter den besonderen Voraussetzungen der Art. 44 ff. DSGVO zulässig. Seit dem sog. Schrems II-Urteil des EUGH ist es nicht mehr möglich, die Übermittlung auf einen Angemessenheitsbeschluss der EU-Kommission gemäß Art. 45 DSGVO zu stützen. Eine Übermittlung auf der Grundlage von geeigneten Garantien nach Art. 46 DSGVO, wie beispielsweise Standarddatenschutzklauseln oder Binding Corporate Rules, bleibt grundsätzlich möglich. In diesem Fall müssen aber zusätzliche Maßnahmen getroffen werden, die die übermittelten Daten im konkreten Einzelfall angemessen vor dem unbeschränkten Zugriff der US-Sicherheitsbehörden schützen. Als zusätzliche Maßnahmen kommen insbesondere verschiedene Formen der Datenverschlüsselung in Betracht. Diese werden jedoch nicht in jedem Fall praktikabel oder ausreichend sein. Kann der in der Union ansässige Verantwortliche bzw. sein dort ansässiger Auftragsverarbeiter keine hinreichenden zusätzlichen Maßnahmen ergreifen, um einen solchen Schutz zu gewährleisten, ist er verpflichtet, die Übermittlung personenbezogener Daten in die USA auszusetzen oder zu beenden. Neben den geeigneten Garantien des Art. 46 DSGVO besteht die Möglichkeit der Datenübermittlung nach einem der in Art. 49 DSGVO normierten Ausnahmetatbestände. Diese sind jedoch eng auszulegen, da das von der DSGVO vorgesehene Regel-Ausnahmeverhältnis nicht missachtet werden darf. Zudem bestehen Zweifel an der Praktikabilität des Ausnahmetatbestandes der Einwilligung, die hier am ehesten in Betracht zu ziehen sein dürfte.

***

54 Spoerr, in: Wolff/Brink, BeckOK Datenschutzrecht, 35. Edition Stand: 1. Februar 2021, Art. 28 DSGVO Rn. 33 f.

55 Spoerr, in: Wolff/Brink, BeckOK Datenschutzrecht, 35. Edition Stand: 1. Februar 2021, Art. 28 DSGVO Rn. 43.