DSGVO-INFO

DIE UMFASSENDE INFORMATIONSPLATTFORM

STIFTUNG DATENSCHUTZ

Dossier VII: Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen

Stand: August 2018

Rechtsgrundlage:

Artikel 44 bis Artikel 49 Datenschutzgrundverordnung , Erwägungsgründe 101 bis 115

Werden personenbezogene Daten in Länder außerhalb der EU/EWR (so genannte Drittländer/Drittstaaten) übermittelt, muss dort ein Datenschutzniveau vorliegen, das dem in der Datenschutzgrundverordnung gewährleisteten Niveau gleichwertig ist. Die Frage, wie ein solches angemessenes Datenschutzniveau sichergestellt werden kann, wird unter Punkt A. behandelt. Im Anschluss erfolgt eine Zusammenfassung (B.). Weiterführende Links zu der Thematik sind unter Punkt C. zu finden.

A. Sicherstellung eines angemessenen Datenschutzniveaus:

Grundsätzlich kann die Sicherstellung eines angemessenen Datenschutzniveaus

- durch einen Angemessenheitsbeschluss der Europäischen Kommission herbeigeführt werden (siehe unter I.)

oder

- durch Garantien in Form von Binding Corporate Rules, Standarddatenschutzklauseln sowie von seitens der Aufsichtsbehörde genehmigten Verhaltensregeln, Zertifizierungsmechanismen oder individuellen Vertragsklauseln erfolgen (siehe unter II.).

Anderenfalls ist eine Datenverarbeitung in einem Drittland lediglich unter den Voraussetzungen der in der Datenschutzgrundverordnung abschließend aufgezählten Ausnahmen möglich (siehe unter III.).

I. Angemessenheitsbeschluss

Die Europäische Kommission kann das Bestehen eines angemessenen Schutzniveaus in einem bestimmten Drittland festzustellen, so dass ohne zusätzliche Garantien der freie Verkehr personenbezogener Daten aus der Europäischen Union in dieses Drittland ermöglicht wird. In der Vergangenheit wurden bereits Angemessenheitsbeschlüsse erlassen, die nach der Datenschutzgrundverordnung fortgelten. Folgende Länder sind bislang davon umfasst:

Schweiz, Andorra, die Färöer, Guernsey, Jersey, Isle of Man, Argentinien, Kanada, Israel, die Vereinigten Staaten, Neuseeland und Uruguay.

Bei den Vereinigten Staaten und Kanada ist jedoch die einschränkende Geltung der Angemessenheitsbeschlüsse zu beachten. Mangels allgemein geltender Datenschutzgesetze in den USA ist dieser nur auf Unternehmen anwendbar, die sich verpflichtet haben, den Datenschutzstandard des EU-US Privacy Shield einzuhalten, so dass diese Regelungen ebenso nach US-Recht durchsetzbar sind. Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz geht davon aus, dass das EU-US Privacy Shield trotz der von den Datenschutzaufsichtsbehörden geäußerten Kritik zurzeit als Grundlage genutzt werden kann, um personenbezogene Daten aus Europa an solche U.S.-Unternehmen zu transferieren, die sich gemäß dem Privacy Shield zertifiziert haben.

Im Hinblick auf Kanada muss die Einschränkung berücksichtigt werden, dass der Angemessenheitsbeschluss für private Unternehmen gilt, die unter den so genannten „Personal Information Protection and Electronic Documents Act“ fallen.

II. Geeignete Garantien

Neben dem gerade erwähnten Angemessenheitsbeschluss der Europäischen Kommission sieht die Datenschutzgrundverordnung die Möglichkeit der „geeigneten Garantien“ vor, um ein angemessenes Datenschutzniveau sicherzustellen. Von zentraler Bedeutung ist hierbei, dass den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen müssen.

Im Einzelnen können geeignete Garantien wie folgt umgesetzt werden:

- **Binding Corporate Rules**

Geeignete Garantien können in Form von verbindlichen internen Datenschutzvorschriften (Binding Corporate Rules) erfolgen, welche in der Vergangenheit bereits gemäß BDSG-alt angewandt wurden. Der Mindestinhalt ist nun in Artikel 47 Absatz 2 DSGVO klar und konkret festgelegt. Insgesamt müssen die Garantien den nach der Datenschutzgrundverordnung vorgesehenen Schutz widerspiegeln und den betroffenen Personen durchsetzbare Rechte übertragen. Die Genehmigung solcher Binding Corporate Rules erfolgt gemäß dem Kohärenzverfahren durch die zuständige Aufsichtsbehörde. Vor allem weltweit tätige Unternehmensgruppen können hiermit ihren internen Datenfluss regeln.

- **Standarddatenschutzklauseln**

Die Europäische Kommission hat in der Vergangenheit EU-Standardvertragsklauseln zur Sicherstellung eines angemessenen Datenschutzniveaus unter der Richtlinie 95/46/EG veröffentlicht. Auch wenn in den Vertragstexten seitens des Verantwortlichen Ergänzungen vorgenommen werden müssen, stellt ihre Verwendung grundsätzlich eine einfache Handhabe dar, um die Datenverarbeitung in einem Drittstaat zu legitimieren.

Diese Regelungen bleiben zudem vorerst in Kraft, es sei denn, die EU-Kommission ersetzt diese durch einen neuen Beschluss. Die Datenschutzgrundverordnung verwendet im Übrigen nicht mehr den Begriff der „EU-Standardvertragsklauseln“ sondern „Standarddatenschutzklauseln“. Standarddatenschutzklauseln dürfen ohne vorherige Zustimmung der zuständigen Datenschutz-Aufsichtsbehörden verwendet werden. Aufsichtsbehörden können ebenso eigene Standarddatenschutzklauseln veröffentlichen. Unternehmen müssen bei der Verwendung dieser Standarddatenschutzklauseln allerdings berücksichtigen, dass nicht allein der Abschluss eines Vertrages die Angemessenheit des Datenschutzniveaus sicherstellt, sondern (erst) die Umsetzung und Einhaltung der damit verbundenen Pflichten in der Praxis: Der Empfänger der Daten verpflichtet sich, die Standards des europäischen Datenschutzrechts einzuhalten. Aus datenschutzrechtlicher Sicht wird als problematisch eingestuft, dass nicht jedes Land aufgrund seiner Rechtsordnung die entsprechenden Voraussetzungen dafür schafft. So muss in jedem Drittland zusätzlich geprüft werden, inwieweit die dort geltenden innerstaatlichen Rechtsvorschriften und Möglichkeiten des gerichtlichen Rechtsschutzes überhaupt ein der Datenschutzgrundverordnung gleichwertiges Schutzniveau garantieren können. Kritisch ist, wenn die Rechtsordnung keine Kontrollrechte des Bürgers vorsieht, die sich auf Zugang, Berichtigung oder Löschung seiner Daten beziehen. Auf diese Problematik im Zusammenhang mit der Rechtslage in den USA und der damit einhergehenden umfassenden staatlichen Überwachung hatte der Europäische Gerichtshof bereits im Rahmen seines Urteils vom 6. Oktober 2015 hingewiesen und festgestellt, dass

die Safe Harbor-Entscheidung der Europäischen Kommission ungültig ist (http://curia.europa.eu/juris/document/document.jsf?docid=169195&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=DE&cid=703941). Da in Bezug auf die Standardvertragsklauseln und deren Durchsetzbarkeit in der Praxis eine ähnliche Problematik vorliegt, wird erwartet, dass der Europäische Gerichtshof auch über die Rechtswirksamt der EU-Standardvertragsklauseln entscheiden wird. Dies sollten Unternehmen daher im Auge behalten, sofern sie Datenübermittlungen in Drittstaaten, insbesondere in die USA, auf der Grundlage der derzeit existierenden EU-Standardvertragsklauseln vornehmen.

- **Genehmigte Verhaltensregeln und genehmigter Zertifizierungsmechanismus**

In der Datenschutzgrundverordnung wurden die Instrumente der genehmigten Verhaltensregeln und des genehmigten Zertifizierungsmechanismus neu eingeführt, um die Verarbeitung von Daten in Drittstaaten zu legitimieren. Darin müssen rechtsverbindliche und durchsetzbare Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters festgelegt werden, die außerdem seitens der zuständigen Aufsichtsbehörde zu genehmigen sind.

Die praktische Relevanz dieser beiden Instrumentarien bleibt abzuwarten.

- **Genehmigte Vertragsklauseln**

Vertragsklauseln, die zwischen dem Verantwortlichen oder dem Auftragsverarbeiter und dem Verantwortlichen, dem Auftragsverarbeiter oder dem Empfänger der personenbezogenen Daten im Drittland vereinbart wurden, können gleichermaßen die Datenübermittlung unter der Voraussetzung legitimieren, dass die Aufsichtsbehörde diese zuvor genehmigt hat und das Kohärenzverfahren nach Artikel 63 DSGVO durchgeführt wurde.

III. Ausnahmen

Liegen weder ein Angemessenheitsbeschluss noch geeignete Garantien vor, kann eine Datenverarbeitung in einem Drittland dennoch zulässig sein. Diesbezüglich sind in der Datenschutzgrundverordnung explizite und abschließende Ausnahmetatbestände genannt, etwa wenn die betroffene Person ihre ausdrückliche Einwilligung erteilt hat oder wenn der Übermittlung ein zwingendes berechtigtes Interesse des Verantwortlichen zugrunde liegt und die Übermittlung nicht wiederholt erfolgt. Im zuletzt genannten Fall muss sowohl die Aufsichtsbehörde als auch die betroffene Person informiert werden.

Weitere Ausnahmefälle beziehen sich darauf, dass die Übermittlung aus folgenden Gründen erforderlich sein muss:

- zur Erfüllung eines Vertrages mit der betroffenen Person oder zum Abschluss oder zur Erfüllung eines Vertrages im Interesse der betroffenen Person
- aus wichtigen Gründen des öffentlichen Interesses (z.B. Steuer- und Zollbehörden)
- zur Verfolgung von Rechtsansprüchen
- zum Schutz lebenswichtiger Interessen

Die Aufsichtsbehörden vertreten die Auffassung, dass diese Ausnahmen eng auszulegen sind (Artikel-29-Datenschutzgruppe). Daher kann sich für Unternehmen eine sorgfältige Prüfung dahingehend empfehlen, ob beispielsweise der Abschluss von Standarddatenschutzklauseln oder Bindung Corporate Rules, vorrangig in Betracht kommen kann. Zwar wird häufig in der Praxis darauf verwiesen wird, dass es sich bei den Leitlinien der Artikel-29-Datenschutzgruppe um rechtlich nicht bindende Vorgaben handelt. Dennoch sollten Unternehmen bedenken, dass die nationalen Aufsichtsbehörden, die für die Verhängung von Bußgeldern zuständig sind, diese als Orientierungshilfen im Rahmen ihrer Aufgabenerfüllung zugrunde legen.

B. In Kürze:

Übermittelt der Verantwortliche personenbezogene Daten in Länder außerhalb der EU/EWR (Drittländer/Drittstaaten), muss dort ein Datenschutzniveau vorliegen, das dem in der Datenschutzgrundverordnung gewährleisteten Niveau gleichwertig ist. Dieses gleichwertige Datenschutzniveau kann mittels eines so genannten Angemessenheitsbeschlusses von der Europäischen Kommission festgestellt werden oder die Verantwortlichen müssen geeignete Garantien vorlegen. Möglichkeiten für geeignete Garantien bieten die Vorlage von internen Datenschutzvorschriften (Binding Corporate Rules), von Verhaltensregeln, Zertifizierungsmechanismen oder Vertragsklauseln. Diese Instrumente müssen von der zuständigen Aufsichtsbehörde zuvor genehmigt werden. Die Europäische Kommission hat in der Vergangenheit außerdem EU-Standardvertragsklauseln zur Sicherstellung eines angemessenen Datenschutzniveaus veröffentlicht, die vorerst in Kraft bleiben, es sei denn, die EU-Kommission ersetzt diese durch einen neuen Beschluss.

In Bezug auf die Übermittlung von Daten in die USA aufgrund des EU-US Privacy Shield geht der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz davon aus, dass dieses trotz der von den Datenschutzaufsichtsbehörden geäußerten Kritik als Grundlage genutzt werden kann, um personenbezogene Daten aus Europa an solche U.S.-Unternehmen zu transferieren, die sich gemäß dem Privacy Shield zertifiziert haben (https://www.datenschutz.rlp.de/de/themenfelder-themen/privacy-shield/).

Ein Verantwortlicher kann gemäß der Datenschutzgrundverordnung im Übrigen einen Auftragsverarbeitungsvertrag ebenso mit einem Dienstleister abschließen, der seinen Geschäftssitz nicht innerhalb der Europäischen Union hat (z.B. Cloudanbieter), sofern dort **zusätzlich** ein **angemessenes Datenschutzniveau** festgestellt werden kann.

Ergänzend:

Die Datenschutzgrundverordnung gilt für alle Datenverarbeitungstätigkeiten, die im Rahmen der Tätigkeiten eines Verantwortlichen oder Auftragsverarbeiters mit Hauptsitz oder Niederlassung in der Europäischen Union erfolgen. Dabei ist unerheblich, an welchem Ort die Datenverarbeitung konkret erfolgt. Die Datenschutzgrundverordnung findet außerdem Anwendung, wenn der Verantwortliche seinen Geschäftssitz *nicht* innerhalb der Europäischen Union hat, er aber personenbezogene Daten im Zusammenhang mit einem Waren- und Dienstleistungsangebot verarbeitet (Artikel 3 DSGVO).

C. Weitere Links und Materialien

- **Datenschutzkonferenz:**

  Unter https://www.lda.bayern.de/media/dsk_kpnr_4_drittlaender.pdf ist das Kurzpapier der Datenschutzkonferenz abrufbar, in welchem die Voraussetzungen der Datenschutzgrundverordnung an eine Datenübermittlung in einen Drittstaat erläutert werden.

- **Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz**

  Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz hat unter https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Privacy_Shield_Betroffenenrechte.pdf die Rechte von betroffenen Personen unter dem EU-US Privacy Shield erläutert. Auf seiner Webseite (https://www.datenschutz.rlp.de/de/themenfelder-themen/privacy-shield/) sind im Übrigen weitere Informationen zum Privacy Shield mit weiterführenden Links veröffentlicht.

  In Bezug auf die Übermittlung von Daten in die USA aufgrund des EU-US Privacy Shield geht der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz davon aus, dass dieses trotz der von den Datenschutzaufsichtsbehörden geäußerten Kritik als Grundlage genutzt werden kann, um personenbezogene Daten aus Europa an solche U.S.-Unternehmen zu transferieren, die sich gemäß dem Privacy Shield zertifiziert haben (https://www.datenschutz.rlp.de/de/themenfelder-themen/privacy-shield/)

- **Artikel-29-Datenschutzgruppe**

  Die Artikel-29-Datenschutzgruppe hat ein Arbeitspapier veröffentlicht (WP 261), abrufbar unter http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49771 Sie befasst sich in dieser Orientierungshilfe mit den Ausnahmen zu Artikel 45 und 46 DSGVO, d.h. sofern weder ein Angemessenheitsbeschluss der Europäischen Kommission noch geeignete Garantien zur Sicherstellung eines angemessenen Datenschutzniveaus vorliegen. Die Artikel-29-Datenschutzgruppe ist der Auffassung, dass diese Ausnahmen eng auszulegen sind.

  Die Artikel-29-Datenschutzgruppe hat außerdem eine Stellungnahme zur Anwendbarkeit der EU-Standardvertragsklauseln verfasst, abrufbar unter https://www.bfdi.bund.de/SharedDocs/Publikationen/Sachthemen/SafeHarbor/Art29ZuSchremUrteil.pdf?__blob=publicationFile&v=1

  Zum EU-US Privacy Shield hat die Artikel-29-Datenschutzgruppe das Arbeitspapier WP 245 veröffentlicht (vom 13.12.2016), abrufbar unter http://www.ec.europa.eu/newsroom/document.cfm?doc_id=40933 . Eine nicht-amtliche Arbeitsübersetzung ist abrufbar unter https://www.bfdi.bund.de/SharedDocs/ExterneLinks/Sachthemen/Art29DSK_Unternehmen_deutsch.pdf;jsessionid=B2FFCAB3D576B8C4837C8089883437ED.2_cid344?__blob=publicationFile&v=4 .

- **bitkom (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.)**

  Die bitkom hat einen Leitfaden mit dem Titel „Verarbeitung personenbezogener Daten in Drittländern“ veröffentlicht, abrufbar unter

https://www.bitkom.org/noindex/Publikationen/2017/Leitfaden/LF-Verarbeitung-personenbezogener-Daten-DE-online-final.pdf

Der bereits im Jahre 2005 erstellte und im Jahr 2016 aktualisierte Leitfaden „Übermittlung personenbezogener Daten – Inland, EU-Länder, Drittländer“ https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/161124-Uebermittlung-pers-Daten-Entwurf-04.pdf) wird damit ersetzt. Bei der im Sommer 2016 aktualisierten Version handelte es sich um eine Orientierung für die Übergangsphase bis zur endgültigen Anwendung der EU-Datenschutz-Grundverordnung ab 25. Mai 2018. Dennoch erfolgt in diesem Dokument bereits ein Ausblick auf die Datenschutzgrundverordnung und es werden Informationen zu den Auswirkungen des EuGH-Urteils zu Safe Harbor und der Anwendung von Standardvertragsklauseln bereitgestellt.

- **BvD (Berufsverband der Datenschutzbeauftragten Deutschlands e.V.)**

  Der BvD informiert unter https://www.bvdnet.de/eu-standardvertragsklauseln-kommen-vor-dem-eugh/ darüber, dass Facebook-Irland nun die EU-Standardvertragsklauseln zur Legitimierung des Datentransfers seiner Benutzer zum Mutterkonzern in die USA verwendet, nachdem Europäische Gerichtshof in einem Urteil festgestellt hat, dass die Safe Harbor-Entscheidung der Europäischen Kommission ungültig ist. Auf dieser Grundlage dürfen daher keine Daten in die USA übermittelt werden. Der BvD geht außerdem davon aus, dass der EUGH auch über die Wirksamkeit der EU-Standardvertragsklauseln entscheiden wird, da sich derzeit der oberste Gerichtshof in Irland (High Court) damit befasst.

- **Europaweite Links**

- **Europäische Kommission und angemessenes Datenschutzniveau**

Die Europäische Kommission hat EU-Standardvertragsklauseln zur Sicherstellung eines **angemessenen Datenschutzniveaus** (Datenverarbeitung in Drittstaaten) veröffentlicht. Diese stammen aus den Jahren 2001 und 2004 und 2010: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:181:0019:0031:DE:PDF sowie http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:DE:PDF sowie https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32010D0087&from=DE

Zur Einstufung von **Drittländern** ist die Mitteilung der Europäischen Kommission vom 10. Januar 2017 zu beachten: MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT -Austausch und Schutz personenbezogener Daten in einer globalisierten Welt- http://ec.europa.eu/transparency/regdoc/rep/1/2017/DE/COM-2017-7-F1-DE-MAIN-PART-1.PDF

Beispiele zu Drittländern und Angemessenheitsbeschlüssen:

Vereinigtes Königreich:

Gemäß einer Mitteilung der Europäischen Kommission vom Januar 2018 handelt es sich bei dem Vereinigten Königreich ab 30. März 2019 ebenso um ein Drittland. Bislang ist noch kein Angemessenheitsbeschluss seitens der Europäischen Kommission erfolgt. Siehe die Mitteilung der Europäischen Kommission, abrufbar unter: http://ec.europa.eu/newsroom/just/document.cfm?action=display&doc_id=49245

Kanada:

Für Kanada hat die Europäische Kommission einen Angemessenheitsbeschluss unter der Einschränkung erlassen, dass dieser nur für private Unternehmen gilt, die unter den so genannten „Personal Information Protection and Electronic Documents Act“ fallen. Siehe Entscheidung der Kommission vom 20. Dezember 2001 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzes, den das kanadische Personal Information Protection and Electronic Documents Act bietet (Bekannt gegeben unter Aktenzeichen K(2001) 4539), **abrufbar unter** http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32002D0002&from=DE

Vereinigte Staaten:

Der Angemessenheitsbeschluss der Europäischen Kommission gilt einschränkend für Unternehmen, , die sich verpflichtet haben, den Datenschutzstandard des Privacy Shield einzuhalten. Siehe Bekanntmachung C(2016) 4176 final zum EU-US Privacy Shield, abrufbar unter https://www.ftc.gov/system/files/documents/plain-language/annexes_eu-us_privacy_shield_en1.pdf sowie 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 (Bekannt gegeben unter Aktenzeichen C(2016) 4176, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016D1250&from=DE

Eine offizielle Liste der Unternehmen, die eine Zertifizierung nach dem Privacy Shield erworben haben, ist unter https://www.privacyshield.gov/list abrufbar.

- Webseite des Privacy Shield

https://www.privacyshield.gov/welcome

- Leitfaden der EU-Kommission zum Privacy Shield

http://ec.europa.eu/newsroom/document.cfm?doc_id=47786

- **Europäische Kommission**

  Die Europäische Kommission stellt außerdem auf ihrer Webseite Informationen zum Datentransfer in Nicht-EU-Mitgliedstaaten zur Verfügung, abrufbar unter https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu_de (Data Transfer outside the EU)

- **ICO: Britische Datenschutzbehörde (Information Commissioner's Office)**

  Die Voraussetzungen einer Datenverarbeitung in Drittstaaten werden zudem von der britischen Datenschutzbehörde erläutert (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/)

- **Information Commissioner (Datenschutzbehörde Isle of Man)**

Die Datenschutzbehörde der Isle of Man informiert ebenfalls über die Voraussetzungen einer Datenübermittlung in Drittstaaten, abrufbar unter https://www.inforights.im/information-centre/data-protection/the-general-data-protection-regulation/gdpr-in-depth/transfers-to-third-countries/