DSGVO-INFO

DIE UMFASSENDE INFORMATIONSPLATTFORM

STIFTUNG DATENSCHUTZ

DATENÜBERMITTLUNG AN DRITTSTAATEN

Juni 2020
Prof. Dr. Anne Riechert

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 feststellen, 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,Uruguay und Japan.

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

Hinsichtlich der Vereinigten Staaten ist zu beachten, dass dort keine allgemeinen Datenschutzgesetze gelten. So wurde dort bislang ein angemessenes Datenschutzniveau bei Unternehmen unterstellt, die sich verpflichtet haben, den Datenschutzstandard des so genannten EU-US Privacy Shield einzuhalten. Diese Vereinbarung wurde als ausreichende Rechtsgrundlage dafür betrachtet, um personenbezogene Daten aus Europa an solche U.S.-Unternehmen zu transferieren, sofern sich diese gemäß dem Privacy Shield zertifiziert hatten. Aufgrund einer Entscheidung des Europäischen Gerichtshofs vom 16.07.2020 wurde das Privacy Shield allerdings für ungültig erklärt (https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091de.pdf), so dass auf dieser Grundlage keine personenbezogenen Daten in die USA übermittelt werden dürfen.

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 die Vertragstexte seitens des Verantwortlichen ergänzt 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 (siehe Artikel 46 Absatz 5 Satz 2 DSGVO). Die Datenschutzgrundverordnung verwendet im Übrigen nicht mehr den Begriff der „EU-Standardvertragsklauseln" sondern „Standarddatenschutzklauseln". Aufsichtsbehörden können ebenso eigene Standarddatenschutzklauseln veröffentlichen. Standarddatenschutzklauseln dürfen ohne vorherige Zustimmung der zuständigen Datenschutz-Aufsichtsbehörden verwendet werden.

So verweist auch der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz darauf, dass die Datenübermittlungen im Falle der Verwendung der Standardvertrags- bzw. Standarddatenschutzklauseln in unveränderter Form genehmigungsfrei sind. Außerdem gelte dies gemäß Erwägungsgrund 109 auch dann, wenn ihnen weitere Klauseln oder zusätzliche Garantien hinzugefügt werden, solange diese weder mittelbar noch unmittelbar im Widerspruch zu den Standardklauseln

stehen und die Grundrechte und Grundfreiheiten der betroffenen Personen nicht beschneiden. Allerdings weist der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz ebenso darauf hin, dass Unternehmen bei solchen Hinzufügungen eine gewisse Vorsicht walten lassen sollten, da im Falle eines inhaltlichen Widerspruchs zu den Standardvertrags- bzw. Standarddatenschutzklauseln die Übermittlung genehmigungspflichtig werde (https://www.datenschutz.rlp.de/de/themenfelder-themen/standarddatenschutzklauseln-der-eu-kommission-oder-einer-aufsichtsbehoerde/).

Insgesamt müssen Unternehmen bei der Verwendung von Standarddatenschutzklauseln 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).

Wie oben bereits dargestellt, hat nun der Europäische Gerichtshof ebenso die Nachfolgeregelung dieser Safe-Harbor-Entscheidung, das EU-US Privacy Shield, in seiner Entscheidung vom 16.07.2020 für ungültig erklärt. Hintergrund dieser Entscheidung ist ein Vorabentscheidungsverfahren, welches von der irischen Datenschutzaufsichtsbehörde angestoßen wurde. Die Behörde hatte aufgrund einer Beschwerde gegen Facebook Ireland beim irischen High Court einen Antrag auf Ersuchen einer Vorabentscheidung gestellt. In seiner Entscheidung hat der Europäische Gerichtshof allerdings ausdrücklich klargestellt, dass die Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern auch weiterhin wirksam sind (https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091de.pdf).

Klarstellend verweist er dabei darauf, dass die Standarddatenschutzklauseln wirksame Mechanismen enthalten, die in der Praxis gewährleisten können, dass das vom Unionsrecht verlangte Schutzniveau eingehalten werde und dass auf solche Klauseln gestützte Übermittlungen personenbezogener Daten ausgesetzt oder verboten werden, wenn gegen diese Klauseln verstoßen wird oder ihre Einhaltung unmöglich ist. Dabei betont der Europäische Gerichtshof, dass gemäß der Datenexporteur und der Empfänger der Übermittlung vorab prüfen müssen, ob das erforderliche Schutzniveau im betreffenden Drittland eingehalten wird, und dass der Empfänger dem Datenexporteur gegebenenfalls mitteilen müsse dass er die Standardschutzklauseln nicht einhalten kann. Wenn dies der Fall sei, müsse der Exporteur die Datenübermittlung aussetzen und/oder vom Vertrag zurücktreten. So hatte im Verlauf dieses Verfahrens bereits der Generalanwalt des Europäischen Gerichtshofs die Pflichten der Verantwortlichen

zur Sicherstellung rechtskonformer Datenübermittlung betont (http://curia.europa.eu/juris/document/document.jsf;jsessionid=72A050A2D16AC08EDAE3715F65E02279?text=&docid=221826&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1&cid=8330814).

Weiterführende Hinweise zu Standarddatenschutzklauseln sind abrufbar beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, abrufbar unter https://www.datenschutz.rlp.de/de/themenfelder-themen/standarddatenschutzklauseln-der-eu-kommission-oder-einer-aufsichtsbehoerde/ , sowie unter Punkt C. in diesem Dokument.

Genehmigte Verhaltensregeln und genehmigter Zertifizierungsmechanismus

In der Datenschutzgrundverordnung sind weiterhin die Instrumente der genehmigten Verhaltensregeln und des genehmigten Zertifizierungsmechanismus neu eingeführt worden, 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. So weist etwa der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz darauf hin, dass die europäischen Aufsichtsbehörden die für eine praktische Anwendung dieser Instrumente notwendigen weiteren Einzelheiten im Hinblick auf rechtliche Rahmenbedingungen und Verfahrensfragen noch erarbeiten werden (https://www.datenschutz.rlp.de/de/themenfelder-themen/genehmigte-verhaltensregeln-genehmigter-zertifizierungsmechanismus-und-einzeln-ausgehandelte-vertragsklauseln/).

Außerdem hat der Europäische Datenschutzausschuss Leitlinien zu Verhaltensregeln und Überwachungsstellen gemäß Artikel 40 DSGVO veröffentlicht (https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf).

Praxisrelevant ist ebenso, dass die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen gemäß Artikel 40 Absatz 6 DSGVO ein Verzeichnis über die von ihr genehmigten Verhaltensregeln führt. Bislang sind diesem Verzeichnis ausschließlich die Verhaltensregeln für die Prüf- und Löschfristen von personenbezogenen Daten durch die deutschen Wirtschaftsauskunfteien enthalten, die von der Behörde nach der Zustimmung der Datenschutzkonferenz genehmigt wurden (siehe unter https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/Verhaltensregeln_-Code-of-Coduct/Inhalt/Verhaltensregeln-und-Akkreditierung-von-Ueberwachungsstellen-nach-der-DS-GVO/DW_CoC_Loeschfristen_180418.pdf sowie unter https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/Verhaltensregeln-_-Code-of-Coduct/Inhalt/Verhaltensregeln-und-Akkreditierung-von-Ueberwachungsstellen-nach-der-DS-GVO/DW_Genehmigung_Loeschfristen_.pdf).

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.

Ausnahmen

Liegen weder ein Angemessenheitsbeschluss noch geeignete Garantien vor, kann eine Datenverarbeitung in einem Drittland dennoch zulässig sein. In der Datenschutzgrundverordnung sind 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

Der Europäische Datenschutzausschuss vertritt die Auffassung, dass diese Ausnahmen restriktiv auszulegen sind (Leitlinien 2/2018 vom 25.05.2018, abrufbar unter https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_de.pdf). 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. Unternehmen sollten 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. Geeignete Garantien umfassen folgende Möglichkeiten: interne Datenschutzvorschriften (Binding Corporate Rules), Verhaltensregeln, Zertifizierungsmechanismen und 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.

Für Datenübermittlungen in die USA ist zu beachten, dass der Europäische Gerichtshof in seiner Entscheidung vom 16.07.2020 das EU-US Privacy Shield für ungültig erklärt hat. Die Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern sind hingegen weiterhin gültig (https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091de.pdf).

Ein Verantwortlicher kann gemäß der Datenschutzgrundverordnung einen Auftragsverarbeitungsvertrag ebenso mit einem Dienstleister abschließen, der seinen Geschäftssitz nicht innerhalb der Europäischen

Union hat (z.B. Cloudanbieter), vorausgesetzt, dass dort **zusätzlich** ein **angemessenes Datenschutzniveau** vorliegt.

Ergänzender Hinweis: 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://datenschutzkonferenz-online.de/media/kp/dsk_kpnr_4.pdf ist das Kurzpapier der Datenschutzkonferenz abrufbar, in welchem die Voraussetzungen der Datenschutzgrundverordnung an eine **Datenübermittlung in einen Drittstaat** erläutert werden.

Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen

Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen führt gemäß Artikel 40 Absatz 6 DSGVO ein Verzeichnis über die von ihr genehmigten Verhaltensregeln: Prüf- und Löschfristen von personenbezogenen Daten durch die deutschen Wirtschaftsauskunfteien (siehe hierzu https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/Verhaltensregeln-_-Code-of-Coduct/Inhalt/Verhaltensregeln-und-Akkreditierung-von-Ueberwachungsstellen-nach-der-DS-GVO/DW_CoC_Loeschfristen_180418.pdf sowie https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/Verhaltensregeln-_-Code-of-Coduct/Inhalt/Verhaltensregeln-und-Akkreditierung-von-Ueberwachungsstellen-nach-der-DS-GVO/DW_Genehmigung_Loeschfristen_.pdf).

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg stellt unter https://www.baden-wuerttemberg.datenschutz.de/ueberblick-eu-u-s-privacy-shield/einen Überblick „**EU-U.S.-Privacy Shield**“ zur Verfügung.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz

Unter https://www.datenschutz.rlp.de/de/themenfelder-themen/standarddatenschutzklauseln-der-eu-kommission-oder-einer-aufsichtsbehoerde/ sind Informationen zu **Standarddatenschutzklauseln** zusammengestellt. Ebenso erfolgt ein Hinweis des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz zum Vorabentscheidungsverfahren zu Standarddatenschutzklauseln (dieses wurde auf Ersuchen der irischen Datenschutzaufsichtsbehörde vor dem EuGH geführt). Ein Verweis auf weitere Dokumente zum Verfahren, einschließlich der Schlussanträge des Generalanwalts des EuGH ist unter folgenden Links zu finden:

http://curia.europa.eu/juris/documents.jsf?num=C-311/18 http://curia.europa.eu/juris/document/document.jsf;jsessionid=72A050A2D16AC08EDAE3715F65E02279?text=&docid=221826&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1&cid=8330814).

Auch bezüglich der **genehmigten Verhaltensregeln** stellt der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz unter https://www.datenschutz.rlp.de/de/themenfelder-themen/genehmigte-verhaltensregeln-genehmigter-zertifizierungsmechanismus-und-einzeln-ausgehandelte-vertragsklauseln/ weitere Informationen bereit.

Europäischer Datenschutzausschuss

Der Europäische Datenschutzausschuss hat Leitlinien zu den **Ausnahmen nach Artikel 49 DSGVO** veröffentlicht (2/2018 vom 25.05.2018, abrufbar unter https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_de.pdf). Diese befassen sich 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. Der Europäische Datenschutzausschuss ist der Auffassung, dass diese Ausnahmen restriktiv auszulegen sind.

Als Vorgängerin des Europäischen Datenschutzausschusses hat die Artikel-29-Datenschutzgruppe außerdem Empfehlungen verfasst, die vom Europäischen Datenschutzausschuss bestätigt wurden (https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_de):

- Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, WP 264, abrufbar unter https://edpb.europa.eu/our-work-tools/our-documents/recommendation-standard-application-approval-controller-binding_en.
- Recommendation on the Standard Application form for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, WP 265, abrufbar unter http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623848.

Außerdem hat die Artikel-29-Datenschutzgruppe Arbeitsdokumente mit einer Übersicht über die Bestandteile und **Grundsätze verbindlicher interner Datenschutzvorschriften** veröffentlicht, die ebenso vom Europäischen Datenschutzausschuss bestätigt wurden:

- „Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules", WP 256 rev.01, abrufbar unter http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109.
- "Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules", WP 257 rev.01, abrufbar unter http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110 (Arbeitsdokument für Auftragsverarbeiter).

Europäischer Datenschutzbeauftragter (EDPS – European Data Protection Supervisor)

Der Europäische Datenschutzbeauftragte hat einen Informationsvermerk zu **internationalen Datenübermittlungen nach dem Brexit** veröffentlicht, abrufbar unter https://edps.europa.eu/sites/edp/files/publication/19-07-16_for_translation_note_on_personal_data_transfers_post-brexit_de.pdf.

Er verweist darauf, dass derzeit **drei** Zusammenstellungen von **Standarddatenschutzklauseln** zur Verfügung stehen, die gemäß DSGVO so lange gültig bleiben, bis sie durch einen Beschluss der Kommission geändert, ersetzt oder aufgehoben werden. Im Einzelnen sind dies:

- Datenübermittlung von einem Verantwortlichen in einem EU-Land an einen Verantwortlichen in einem Drittland (Nicht-EU-/EWR) (z.B. Vereinigtes Königreich):
  Hierzu sind zwei Zusammenstellungen verfügbar:
  - 2001/497/EG, abrufbar unter https://eur-lex.europa.eu/legal-content/de/ALL/?uri=CELEX:32001D0497
  - 2004/915/EG, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32004D0915
- Datenübermittlung von einem Verantwortlichen in einem EU-Land an einen Auftragsverarbeiter in einem Drittland (Nicht-EU-/EWR) (z. B. Vereinigtes Königreich): 2010/87/EG, abrufbar unter https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:32010D0087“

Der Europäische Datenschutzbeauftragte stellt außerdem weiterführende Hinweise zu **internationalen Datenübermittlung** unter folgendem Link bereit: https://edps.europa.eu/data-protection/data-protection/reference-library/international-transfers_de („Was Sie über internationale Übermittlungen wissen sollten; Welches sind die wichtigsten Datenschutzfragen?; Garantien für die Übermittlung personenbezogener Daten an Länder, in denen ein angemessener Datenschutz nicht gewährleistet ist“).

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

Die bitkom hat einen Leitfaden mit dem Titel „Processing of Personal Data in Third Countries“ (Verarbeitung personenbezogener Daten in Drittländern) veröffentlicht, abrufbar unter https://www.bitkom.org/sites/default/files/file/import/171120-LF-Verarbeitung-personenbezogener-Daten-ENG-online.pdf und https://www.bitkom.org/sites/default/files/file/import/LF-Verarbeitung-personenbezogener-Daten-DE-online-final.pdf.

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. Der BvD stellt außerdem weiterführende Links zu diesem Sachverhalt in diesem Beitrag bereit.

Europaweite Links

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 Angemessenheitsbeschlüssen in Bezug auf Drittländer:

Japan hat seine Datenschutzvorschriften modernisiert. Daraufhin leitete die Europäische Kommission im September 2018 das Verfahren ein und hat den Angemessenheitsbeschluss am 23.01. 2019 angenommen. Es ist der erste, der seit Geltungsbeginn der Datenschutz-Grundverordnung erlassen wurde. Weitere Informationen sind abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/de/IP_19_421 und https://ec.europa.eu/commission/presscorner/detail/de/MEMO_19_422.

Das Vereinigte Königreich von Großbritannien und Nordirland ist am 31. 01. 2020 aus der Europäischen Union ausgetreten. Mit diesem Austritt wurden ebenso Regelungen zum Datenschutzrecht getroffen (siehe unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:12020W/TXT&from=DE und https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:22020X0131(02)). Bis zum 31.12.2020 gilt weiterhin die DSGVO, sofern nicht zuvor ein Angemessenheitsbeschluss seitens der Europäischen Kommission erfolgt. Während dieses Übergangszeitraum gilt das Vereinigte Königreich nicht als Drittland. Weitere Informationen zu diesem Thema stellt der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz zur Verfügung (https://www.datenschutz.rlp.de/de/themenfelder-themen/brexit/). Er verweist darauf, dass die Empfehlungen der Datenschutzaufsichtsbehörden vom 12. Februar 2019 und vom 30. März 2019 gelten (https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/EDSA_Info_NoDealBrexit_Deutsch__Arbeitsuebersetzung_.pdf und https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/DSK_Brexit-Positionspapier.pdf).

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 galt einschränkend für Unternehmen, die sich verpflichtet hatten, 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 .

Aufgrund einer Entscheidung des Europäischen Gerichtshofs vom 16.07.2020 wurde das Privacy Shield allerdings für ungültig erklärt, so dass auf dieser Grundlage keine personenbezogenen Daten in die

USA übermittelt werden dürfen. Die Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern sind hingegen weiterhin gültig (https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091de.pdf).

Europäische Kommission

Die Europäische Kommission stellt auf ihrer Webseite außerdem weitere 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 über die Voraussetzungen einer Datenübermittlung in Drittstaaten unter „**Eighth Principle - transfer of data abroad**“, abrufbar unter https://www.inforights.im/organisations/data-protection-law-2018/legislation-and-case-law/data-protection-act-2002/data-protection-principles/eighth-principle-transfer-of-data-abroad.