Gesellschaft für Datenschutz
und Datensicherheit e.V.

GDD-Praxishilfe DS-GVO

Datenschutzrechtliche Anforderungen an internationale Datentransfers

INHALT

Datenschutzrechtliche Anforderungen an internationale Datentransfers

Der europäische Gesetzgeber hat vor dem Hintergrund der Ausweitung des internationalen Handels die Übermittlung personenbezogener Daten an Datenempfänger in Drittländern unter besondere datenschutzrechtliche Anforderungen gestellt, um Rechte und Freiheiten von Betroffenen zu schützen. Ziel ist es, das durch die Datenschutz-Grundverordnung (DS-GVO) unionsweit gewährleistete Schutzniveau für natürliche Personen nicht zu untergraben, wenn personenbezogene Daten in ein Drittland transferiert werden. Die Art. 44 ff. aus Kapitel V der DS-GVO geben die Bedingungen vor, nach denen Verantwortliche oder Auftragsverarbeiter, die der DS-GVO unterliegen, personenbezogene Daten in Drittländer übermitteln dürfen.

Die vorliegende Praxishilfe der GDD soll Rechtsanwendern einen Überblick über die zur Verfügung stehenden Mechanismen beim sog. „Datenexport" geben und bei der Einhaltung der datenschutzrechtlichen Anforderungen Unterstützung leisten.[1]

1 Der Fokus der Praxishilfe liegt auf Hinweisen für nicht-öffentliche Stellen, daher wird im weiteren Verlauf nicht näher auf die Übermittlung an sog. „internationale Organisationen" gem. Art. 4 Nr. 26 DS-GVO im Drittland eingegangen.

A. Voraussetzungen einer Übermittlung personenbezogener Daten an Empfänger in Drittländern

Adressaten der DS-GVO, die personenbezogene Daten in ein Drittland[2] übermitteln möchten, haben die sog. **2-Stufen-Prüfung** zu durchlaufen. Dies ergibt sich aus Art. 44 S. 1 DS-GVO, der von Verantwortlichen oder Auftragsverarbeitern die Einhaltung der Vorgaben von Kapitel V sowie die Einhaltung der „sonstigen Bestimmungen dieser Verordnung" verlangt.

Hinweis:

Ein Exporteur von personenbezogenen Daten nach Kapitel V der DS-GVO kann nur der Verantwortliche gem. Art. 4 Nr. 7 DS-GVO oder der Auftragsverarbeiter gem. Art. 4 Nr. 8 DS-GVO, nicht der Betroffene selbst sein. Registriert sich bspw. ein Betroffener aus der EU mit seinen personenbezogenen Daten auf einer Internetseite eines Anbieters aus den USA, liegt kein Datentransfer nach Kapitel V der DS-GVO vor. Vielmehr erhebt der Anbieter aus den USA personenbezogene Daten unmittelbar beim Betroffenen selbst. Ob für den US-amerikanischen Anbieter die DS-GVO gilt, ist gesondert zu prüfen.

Von einen Übermittlung durch einen Verantwortlichen oder Auftragsverarbeiter ist auszugehen, wenn personenbezogene Daten einem anderen Verantwortlichen oder Auftragsverarbeiter im Drittland offengelegt oder zum Abruf bereitgehalten werden. Hierzu sind auch vertraglich vorgesehene bzw. nicht auszuschließende Zugriffsmöglichkeiten bspw. im Bereich der Systemadministration zu zählen oder sonstige Abrufverfahren (z.B. Download oder Bereitstellung von Daten an einem Terminal). Ebenso kann eine Übermittlung bei einem Zugriff mittels VPN aus einem Drittland heraus auf personenbezogene Daten bei einem Verantwortlichen im EWR[3] vorliegen.

I. Einhaltung der „sonstigen" Bestimmungen der DS-GVO (1. Prüfstufe)

Der Datenexporteur hat im Zuge der **ersten Prüfstufe** sicherzustellen, dass die geplante Übermittlung den allgemeinen Anforderungen der DS-GVO bzw. denen des Bundesdatenschutzgesetzes (BDSG) oder einer bereichsspezifischen Norm entspricht.

Hierzu zählt die Einhaltung der Datenschutzgrundsätze gemäß Art. 5 DS-GVO ebenso, wie das Vorhandensein einer Rechtsgrundlage hinsichtlich der Verarbeitung personenbezogener Daten. Im Bereich der Transparenzvorgaben aus Artt. 13 u. 14 DS-GVO sind Betroffene über die Absicht, personenbezogene Daten in ein Drittland zu übermitteln ebenso zu informieren, wie über die hierbei verwendeten Mechanismen zur Einhaltung von Kapitel V zur Gewährleistung eines angemessenen Datenschutzniveaus.

Hinweis:

Bei bestimmten Mechanismen aus Kapitel V haben Betroffene das Recht, eine Kopie der verwendeten Garantie zu erhalten bzw. haben Anspruch auf Informationen, wie diese zu bekommen ist (vgl. Art. 13 Abs. 1 lit. f DS-GVO).

Unter die „sonstigen Bestimmungen" fallen ebenfalls weitere Pflichten aus der DS-GVO, so die Anforderungen an die Auftragsverarbeitung gem. Art. 28 DS-GVO oder an eine gemeinsame Verantwortlichkeit nach den Vorgaben des Art. 26 DS-GVO.

2 Drittländer sind alle Länder, die nicht Teil des Europäischen Wirtschaftsraums (EWR) sind.

3 Aktuelle Mitglieder des EWR sind die 27 Mitgliedstaaten der Europäischen Union sowie Liechtenstein, Island und Norwegen.

Die erste Prüfstufe unterscheidet sich nicht wesentlich von den Prüfanforderungen an eine Verarbeitung personenbezogener Daten innerhalb des EWR. Mit dem Verweis auf die „sonstigen Bestimmungen" möchte der Gesetzgeber sicherstellen, dass die Erfüllung von Kapitel V alleine nicht ausreicht, um personenbezogene Daten in das Drittland zu übermitteln. Der Verweis auf die „sonstigen Bestimmungen" führt im Übrigen nicht zu einer Anwendbarkeit der DS-GVO auf Seiten des Datenempfängers im Drittland. Fragen zur räumlichen Anwendbarkeit der DS-GVO sind ausschließlich nach Art. 3 DS-GVO zu beurteilen.

II. Vorgaben von Kapitel V der DS-GVO (2. Prüfstufe)

Im Rahmen der **zweiten Prüfstufe** sind die spezifischen Anforderungen aus Kapitel V an die Datenübermittlung an den Verantwortlichen oder Auftragsverarbeiter im Drittland zu prüfen. Dies erfolgt anhand der Maßgabe, dass ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet sein muss oder ein solches ausnahmsweise entbehrlich ist.

1. Angemessenheitsbeschluss der Europäischen Kommission

Die Kommission kann gem. Art. 45 Abs. 1 S. 1 DS-GVO beschließen, dass ein Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland ein angemessenes Schutzniveau aufweisen. Liegt ein solcher Beschluss vor, darf eine Übermittlung personenbezogener Daten in das betroffene Drittland, das Gebiet oder den Sektor im Rahmen der zweiten Prüfstufe erfolgen.

Hinweis: Einschränkungen der Angemessenheitsbeschlüsse in ihrem Geltungsbereich

Angemessenheitsbeschlüsse können, abseits der gesetzlich vorgesehenen Konkretisierungen, einen eingeschränkten Anwendungsbereich haben oder einer bestimmten Gültigkeitsdauer unterliegen. So gilt der Angemessenheitsbeschluss für Kanada beispielsweise nur für Datenweitergaben an Empfänger, die dem Personal Information Protection and Electronic Documents Act (PIPEDA) unterfallen[4]. Der Beschluss zu UK verfügt bspw. lediglich über eine Gültigkeit von 4 Jahren und muss danach erneuert werden. Daher sollte der Anwendungsbereich des jeweiligen Beschlusses und seine Gültigkeit vorab des Datenexports geprüft werden.

Hinweis: Neuer Angemessenheitsbeschluss nach Schrems II

Der EuGH hatte in seiner Entscheidung zu Schrems II[5] das EU-US Privacy Shield für ungültig erklärt. Weitere Angemessenheitsbeschlüsse der Kommission waren nicht Bestandteil des Urteils. Für Datenexporteure bestehen besondere Prüfpflichten im Hinblick auf das Datenschutzniveau in Drittländern mit Angemessenheitsbeschluss gerade nicht.[6] Es ist allein zu überwachen, ob der Angemessenheitsbeschluss insgesamt gültig ist und den vorgesehenen Datentransfer abdeckt.

4 Vgl. Beschluss 2002/2/EG, Art. 1.

5 Urteil vom 16. Juli 2020, Facebook Ireland und Schrems, C-311/18.

6 Vgl. EDSA, Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten vom 10. November 2020, Rn. 19.

Infolge der „Schrems II"-Entscheidung wurde zwischen EU und USA ein neues Datenschutzabkommen ausgehandelt, das EU-US Data Privacy Framework (EU-US DPF). Um Bedenken auszuräumen, welcher der EuGH gegen das Vorgängerabkommen hatte, wurden neue Datenschutzmechanismen eingeführt, darunter ein Gericht zur Datenschutzüberprüfung in den USA (Data Protection Review Court) sowie beschränkte Zugriffsbefugnisse für Strafverfolgungs- und Sicherheitsbehörden. Die Einführung erfolgte über eine am 07.10.2022 von US-Präsident Biden unterzeichnete Durchführungs-verordnung (Executive Order).[7]

Mittels des am 10.07.2023 verabschiedeten Angemessenheitsbeschlusses hat die EU-Kommission nunmehr festgestellt, dass im Hinblick auf den Transfer personenbezogener Daten an unter dem neuen EU-US Datenschutzrahmen (EU-US Data Privacy Framework – EU-US DPF) (selbst-)zertifizierte US-Unternehmen aus ihrer Sicht ein angemessenes Datenschutzniveau besteht. Unternehmen in Europa steht nunmehr wieder eine unbürokratische Methode zur Legitimierung des Transfers personenbezogener Daten in die USA zur Verfügung.

Inwiefern das Abkommen dauerhaft Bestand haben wird, wird sich zeigen. So wird die EU-Kommission die Umsetzung des EU-US Datenschutzrahmens im jährlichen Turnus überprüfen und könnte das Abkommen auch aussetzen. Größere Gefahr für das Abkommen dürfte allerdings durch Max Schrems drohen und die wohl unausweichliche „Schrems III"-Entscheidung des EuGH.

Bis zu dieser Entscheidung haben die europäischen Datenexporteure nun aber erstmal „Verschnaufpause", können doch auf Grundlage der Angemessenheitsentscheidung der Kommission Datentransfers in die USA ohne zusätzliche Vorkehrungen im Verhältnis zu innereuropäischen Datentransfers durchgeführt werden.

Folgende Länder weisen derzeit ein angemessenes Datenschutzniveau per Kommissionsbeschluss auf:

- Andorra (ABl. EU v. 21.10.2010, Nr. L 277),
- Argentinien (ABl. EG v. 5.7.2003, Nr. L 68/19),
- Australien (Nur eingeschr. für Flugpassagierdaten, ABl. EU v. 08.08.2008, Nr. L 213/47)
- Färöer-Inseln (ABl. EU v. 09.03.2010, Nr. L 58),
- Guernsey (ABl. EG v. 25.11.2003, Nr. L 08/27),
- Isle of Man (ABl. EG v. 30.4.2004, Nr. L 51/51 sowie Berichtigung in ABl. EG v. 10.6.2004, Nr. L 208/47),
- Israel (ABl. EU v. 01.02.2011, Nr. L 27/39),
- Japan (ABl. EU v. 19.3.2019, Nr. L 76),
- Jersey (ABl. EU v. 28.05.2008, Nr. L 138),
- Kanada (ABl. EG v. 4.1.2000, Nr. L 2/13),
- Neuseeland (ABl. EU v. 30.01.2013, Nr. L 028),
- Schweiz (ABl. EG v. 25.8.2000, Nr. L 215/1),
- Uruguay (ABl. EU v. 23.08.2012, Nr. L),
- USA (gilt nur für Datentransfers an US-Unternehmen, die sich unter dem neuen EU-US DPF zertifizieren lassen können und dies auch tatsächlich machen, ABl. EU v. 10.07.2023, Nr. L 207/1; für Flugpassagierdaten, ABl. EU v. 11.08.2012, Nr. L 215),
- Großbritannien/Vereinigtes Königreich (UK) (ABl. EU v. 11.10.2021, Nr. L 360/1),
- Republik Korea (Brüssel, 17.12.2021 - C 2021) 9316 final - bislang keine Veröffentlichung im Amtsblatt der EU.

Vertreter der europäischen Kommission und der US-Regierung verhandeln derzeit über das Trans-Atlantic Data Privacy Framework als Nachfolgeregelung

7 The White House, Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities.

zum ungültigen EU-US Privacy Shield. Auch nach dem neuen Abkommen sollen Unternehmen in den USA über eine Zertifizierung von einem angemessenen Datenschutzniveau profitieren können.[8] Das Abkommen soll voraussichtlich zum Ende des Jahres 2022 zum Anschluss gebracht werden.

Datenübermittlungen auf Basis eines Angemessenheitsbeschlusses bedürfen keiner besonderen Genehmigung durch eine Aufsichtsbehörde (vgl. Art. 45 Abs. 1 S. 2 DS-GVO).

2. Datenübermittlung vorbehaltlich geeigneter Garantien (Art. 46 DS-GVO)

Sollte kein Angemessenheitsbeschluss der Kommission für den Datenexport vorliegen, ist gem. Art. 46 Abs. 1 DS-GVO eine Datenübermittlung in Drittländer zulässig, wenn der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorsehen und wenn den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung gestellt werden. Die Absätze 2 und 3 des Art. 46 DS-GVO führen im Weiteren aus, welche geeigneten Garantien überhaupt in der DS-GVO zur Verfügung stehen. Ohne eine gesonderte Genehmigungspflicht seitens der zuständigen Aufsichtsbehörde für den Datenexport sind dies

- rechtlich bindende und durchsetzbare Dokumente zwischen den Behörden oder öffentlichen Stellen (Art. 46 Abs. 2 lit. a DS-GVO)[9],
- verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b DS-GVO),
- Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c DS-GVO),
- von einer Aufsichtsbehörde angenommene Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. d DS-GVO),
- genehmigte Verhaltensregeln gem. Art. 40 DS-GVO (Art. 46 Abs. 2 lit. e DS-GVO) sowie
- genehmigte Zertifizierungsmechanismen gem. Art. 42 DS-GVO (Art. 46 Abs. 2 lit. f) DS-GVO.

Garantien, die unter dem Vorbehalt einer vorherigen Genehmigung durch die zuständige Aufsichtsbehörde stehen, sind

- Vertragsklauseln, die zwischen dem Verantwortlichen oder dem Auftragsverarbeiter und dem Verantwortlichen, dem Auftragsverarbeiter oder dem Empfänger der personenbezogenen Daten im Drittland oder internationalen Organisation vereinbart wurden (sog. „Ad-hoc-Vertragsklauseln“, Art. 46 Abs. 3 lit. a DS-GVO)
- Bestimmungen, die in Verwaltungsvereinbarungen zwischen Behörden oder öffentlichen Stellen aufzunehmen sind und durchsetzbare und wirksame Rechte für die betroffenen Personen einschließen (Art. 46 Abs. 3 lit. b DS-GVO).

Hinweis:

Verantwortliche oder Auftragsverarbeiter müssen, ggf. in Zusammenarbeit mit dem Datenimporteur, bei Datenexporten in ein Drittland auf Basis von Art. 46 DS-GVO prüfen, ob beim Empfänger ein der Sache nach gleichwertiges Datenschutzniveau gegeben ist. Hierbei sind die besonderen Umstände im Drittland zu berücksichtigten (z.B. bestehende Rechtsvorschriften hinsichtlich behördlicher Datenzugriffe oder andere Praktiken der Datenverarbeitung im Drittland), welche die Wirksamkeit der in Art. 46 DS-GVO genannten Garantien beeinträchtigen können.[10] Dies läuft auf eine Prüfung anhand der Frage hinaus, ob die Garantie im jeweiligen Drittland auch effektiv ist. Bieten die Garantien nach Art. 46 DS-GVO kein der Sache nach gleichwertiges Schutzniveau für die Verarbeitung personenbezogenen Daten, müssen **zusätzliche „geeignete Garantien“** geprüft und implementiert werden.

8 https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/.

9 Aufgrund der Schwerpunktsetzung auf den nicht öffentlichen Bereich werden die Voraussetzungen von Art. 46 Abs. 2 lit. a DS-GVO nicht weiter ausgeführt.

10 Empfehlungen 01/2020 über Maßnahmen zur Gewährleistung des EU-Schutzniveaus bei der Übertragung von personenbezogenen Daten, Rn. 29, 30.

a. Verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b i.V.m. Art. 47 DS-GVO)

Für Datenexporte innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen mit gemeinsamer Wirtschaftstätigkeit können verbindliche interne Datenschutzvorschriften (sog. „Binding Corporate Rules" (BCR)) zur Gewährleistung eines angemessenen Datenschutzniveaus eingesetzt werden. Eine Unternehmensgruppe ist eine Gruppe, die aus einem herrschenden Unternehmen und von diesem abhängigen Unternehmen besteht (Art. 4 Nr. 19 DS-GVO). Während die Unternehmensgruppen bereits vor Inkrafttreten der Grundverordnung Adressat möglicher interner Datenschutzvorschriften waren, ist die Gruppe von Unternehmen mit gemeinsamer Wirtschaftstätigkeit ergänzend aufgenommen worden. Das Vorliegen einer gemeinsamen wirtschaftlichen Tätigkeit kann bereits bei einer andauernden Geschäftspartnerschaft vermutet werden. Nicht ausreichend ist hingegen ein loses, sporadisches oder einzelnes Zusammenarbeiten. Allen voran werden Unternehmensstrukturen im Rahmen von Joint Ventures vom Begriff der gemeinsamen Wirtschaftstätigkeit erfasst, ohne dass diese im eigentlichen Sinne eine klassische Konzernstruktur aufweisen müssen.[11]

aa. Varianten

BCR existieren in zwei Varianten:
Interne Datenschutzvorschriften für Datenübermittlungen zwischen Verantwortlichen (Controller BCR): Soll ein angemessenes Datenschutzniveaus bei Datenübermittlungen zwischen Verantwortlichen gem. Art. 4 Nr. 7 DS-GVO einer Unternehmensgruppe oder einer Gruppe von Unternehmen mit gemeinsamer Wirtschaftstätigkeit und Verantwortlichen oder Auftragsverarbeitern dieser Gruppe im Drittland hergestellt werden, spricht man von „Controller BCR". Über ihren Anwendungsbereich wird definiert, für welche Daten bzw. für welche Personengruppen sie Anwendung finden sollen (z.B. Übermittlungen von Beschäftigtendaten).

Interne Datenschutzvorschriften für Datenübermittlungen zwischen Auftragsverarbeitern (Processor BCR): Processor BCR werden zwischen Unternehmen einer Unternehmensgruppe oder einer Gruppe von Unternehmen mit gemeinsamer Wirtschaftsaktivität verwendet, die in ihrer Eigenschaft als Auftragsverarbeiter nach Art. 4 Nr. 8 DS-GVO ein angemessenes Datenschutzniveau bei der Datenübermittlung an Gesellschaften der Gruppe, d.h. weitere Auftragsverarbeiter, im Drittland gewährleisten möchten.

Beispiel

Kundendaten sollen von einer Konzerngesellschaft, die ein Customer Relationship Management System als Cloud-Lösung anbietet, an weitere Auftragsverarbeiter des Konzerns in ein Drittland übermittelt werden. Zu diesem Zweck können Processor BCR eingesetzt werden.

Hinweis:

Verantwortliche, die der DS-GVO unterliegen, sollten den Anwendungsbereich von Processor BCR prüfen, bevor personenbezogene Daten an den Dienstleister weitergegeben werden.

Datenverarbeiter, die BCR unter Aufsicht der britischen Datenschutzaufsichtsbehörde (ICO) genehmigen ließen, müssen diese durch eine federführende Aufsichtsbehörde aus dem EWR erneut genehmigen lassen.

11 Gola DS-GVO/Klug, 2. Aufl. 2018, DS-GVO Art. 47 Rn. 3.

Verantwortliche oder Auftragsverarbeiter, die nicht Teil der Unternehmensgruppe oder der Gruppe von Unternehmen mit gemeinsamer Wirtschaftsaktivität sind, können nicht von den BCR profitieren. Für Datenexporte an solche Empfänger müssen andere Mechanismen aus Kapitel V der DS-GVO verwendet werden.

bb. Anforderungen

Der Gesetzgeber hat Anforderungen an BCR in Art. 47 Abs. 1 DS-GVO formuliert. Hiernach müssen die internen Datenschutzvorschriften

- >> für alle beteiligten Unternehmen rechtlich bindend sein und durchgesetzt werden,
- >> Wirkung bei den Beschäftigten entfalten,
- >> den betroffenen Personen ausdrücklich durchsetzbare Rechte in Bezug auf die Verarbeitung ihrer personenbezogenen Daten übertragen und
- >> die in Art. 47 Abs. 2 DS-GVO genannten Mindestanforderungen erfüllen.

Die Art.-29-Datenschutzgruppe hat über Working Paper (WP) umfangreiche Hinweise zur Konkretisierung der gesetzlichen Anforderungen und zur Genehmigung von BCR erarbeitet.

BCR im Allgemeinen:

- >> WP 263 rev.01 (ehemals WP 107, übergreifende Erläuterungen für ein Koordinierungsverfahren der europäischen Datenschutzaufsichtsbehörden für BCR[12])
- >> WP 155 rev.04 (Antworten auf häufig gestellte Fragen sowohl zur BCR für Verantwortliche als auch für Auftragsverarbeiter[13])

Controller BCR:

- >> WP 264 (Antragsformular für den EU-weiten Koordinierungsprozesses für die Genehmigung von BCR für Verantwortliche[14])
- >> WP 256 rev.01 (tabellarische Darstellung über die notwendigen Inhalte von BCR für Verantwortliche[15])

Processor BCR:

- >> WP 204 (allgemeine Erläuterungen zu verbindlichen Konzernregelungen für Auftragsverarbeiter[16]
- >> WP 265 (Antragsformular zum Start des EU-weiten Koordinierungsprozesses für die Genehmigung von BCR für Auftragsverarbeiter[17])
- >> WP 257 rev.01 (tabellarische Darstellung über die notwendigen Inhalte von BCR für Auftragsverarbeiter[18])

Auswirkungen von Schrems II:

Bei BCR muss, wie bei den übrigen Garantien des Art. 46 DS-GVO auch, im Einzelfall geprüft werden, ob sie mit Blick auf die Rechtsvorschriften und die Praktiken im Drittland eine effektive Garantie darstellen oder ob zusätzliche technische oder organisatorische Maßnahmen notwendig sind. Der EDSA prüft derzeit, ob unter Umständen zusätzliche Verpflichtungen in die in den WP 256/257 enthaltenen Referenzgrundlagen aufgenommen werden müssen.[19]

12 https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/ExtLink/WP_263.html
13 https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/ExtLink/WP_155_neu.html
14 https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/ExtLink/WP_264.html
15 https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/ExtLink/WP_256.html
16 https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/ExtLink/WP_204.html
17 https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/ExtLink/WP_265.html
18 https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/ExtLink/WP_257.html
19 Empfehlungen 01/2020 über Maßnahmen zur Gewährleistung des EU-Schutzniveaus bei der Übertragung von personenbezogenen Daten, Rn. 59.

cc. Genehmigung

Zwingend erforderlich zur Verwendung von BCR ist, dass die jeweils zuständige federführende Aufsichtsbehörde (engl.: Lead Authority) die internen Vorschriften im Hinblick auf ihre datenschutzrechtliche Belastbarkeit sowie auf die Herstellung eines angemessenen Datenschutzniveaus ausdrücklich genehmigt. Nur nach ihrer erfolgreichen Genehmigung können BCR für den Datenexport eingesetzt werden.

Hinweis:

Einzelgenehmigungen für Datenübermittlungen im Unternehmensverbund oder innerhalb der Gruppe von Unternehmen mit gemeinsamer Wirtschaftstätigkeit sind bei bereits genehmigten BCR nicht erforderlich.[20] Es bedarf jedoch im Rahmen des Genehmigungsprozesses einer allgemeine Beschreibung der Zwecke und Umstände der Datentransfers.

dd. Vor- und Nachteile

BCRs haben gegenüber anderen Garantien des Art. 46 DS-GVO den Vorteil, dass sie einen Beitrag zur Implementierung einer konzern- oder gruppenweiten Datenschutzkultur beitragen können. Hierdurch werden einheitliche und verbindliche Datenschutzstandards geschaffen. Gleichzeitig ist eine Anpassung an individuelle Bedürfnisse bspw. eines Konzerns möglich. Dies ermöglicht zum einen die Realisierung einer gewissen Kosteneffizienz der gesamten Datenschutzorganisation („Economies of Scale“) und zum anderen eine Professionalisierung des Datenschutzes („Economies of Scope“) durch die Konzentration von Know-how. Darüber hinaus kann eine gelebte Datenschutzkultur als Marketinginstrument dienen. Allerdings erfordert die erstmalige Implementierung einer gruppenweit einheitlichen Datenschutzkultur einen nicht zu vernachlässigenden Aufwand sowie Kosten für die Organisationsgestaltung.

b. Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c DS-GVO)

Art. 46 Abs. 2 lit. c DS-GVO ermöglicht es der Kommission, Standarddatenschutzklauseln (SCC) als eine Garantie für den Drittlandstransfer zu erlassen. Besagte Klauseln werden von der Kommission in Form eines Durchführungsbeschlusses entworfen und in einem Ausschussverfahren durch Vertreter der Mitgliedstaaten genehmigt (vgl. Art. 93 DS-GVO). Bei den SCC handelt es sich um einen Vertrag, der zwischen dem Datenexporteur als Adressat der DS-GVO und dem Datenimporteur im Drittland geschlossen wird und verbindliche Regeln zum Umgang mit personenbezogenen Daten festlegt. Die SCC müssen nicht gesondert durch eine Aufsichtsbehörde genehmigt werden.

Die Kommission hat jüngst neue Standarddatenschutzklauseln erlassen.[21] Der Beschluss trat am 27.06.2021 in Kraft (Art. 4 Abs. 2, 3 SCC-Beschluss). Dies führte am 27.09.2021 zu einer Aufhebung der bisherigen Entscheidungen 2001/497/EG, 2004/915/EG (Datenübermittlung an einen Verantwortlichen im Drittland) sowie der Entscheidung 2010/87/EU (Datenübermittlung an einen Auftragsverarbeiter im Drittland), die verbreitet als „EU-Standardvertragsklauseln“ bezeich-

20 Vgl. Datenschutzkonferenz, Kurzpapier Nr. 4 S. 2.

21 Durchführungsbeschluss (EU) der Kommission v. 4.6.2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates („SCC-Beschluss“), ABl. EU v. 7.6.2021, Nr. L 199/31.

net wurden.[22] Neuverträge müssen auf Basis der neuen Standarddatenschutzklauseln abgeschlossen werden.

Auswirkungen von Schrems II:

Verträge, die noch auf Basis der bisherigen Entscheidungen vereinbart wurden, sind bis zum 27.12.2022 auf die neuen Standarddatenschutzklauseln zu aktualisieren. Hierzu müssen die Verarbeitungsvorgänge jedoch unverändert geblieben sein sowie der Transfer geeigneten Garantien nach Art. 46 Abs. 1 DS-GVO unterliegen. Insbesondere müssen, i.S.d. Rechtsprechung des EuGHs zu Schrems II, die SCC um zusätzliche Maßnahmen ergänzt worden sein. Ist dies nicht der Fall, müssen seit dem 27.09.2022 die neuen SCC abgeschlossen sein. Diese greifen die Rechtsprechung des EuGHs bereits auf, so dass eine frühestmögliche Umstellung auf die neuen Klauseln empfohlen wird.

aa. Modularer Ansatz

Die SCC sind in vier Abschnitte gegliedert. Im Gegensatz zu den bisherigen Klauseln sind nunmehr sämtliche Transferkonstellationen in einem einzigen Vertragsset integriert. Insgesamt umfassen die SCC nunmehr eine Sammlung von 18 Klauseln, aus der die Vertragsparteien jene Inhalte wählen müssen, die der Rolle ihres Zusammenwirkens entsprechen. Hierbei verfolgt die Kommission einen modularen Ansatz. Die einzelnen Module bilden jeweils eine der vier Konstellationen zwischen Datenimporteur und Datenexporteur ab:

- Datenübermittlung von einem Verantwortlichen an einen Verantwortlichen im Drittland (Controller-to-Controller, C2C)
- Datenübermittlung von einem Verantwortlichen an einen Auftragsverarbeiter im Drittland (Controller-to-Processor, C2P)
- Datenübermittlung von einem Auftragsverarbeiter an einen weiteren Auftragsverarbeiter im Drittland (Processor-to-Processor, P2P)
- Datenübermittlung von einem Auftragsverarbeiter an einen Verantwortlichen im Drittland (Processor-to-Controller, P2C)

Einige allgemeine Klauseln gelten für alle Konstellationen, andere sind modulspezifisch. Ergänzt werden die SCC weiterhin durch zu individualisierende Anlagen, um die Umstände und die Beteiligten des Datentransfers zu beschreiben.

bb. Überblick über die einzelnen Abschnitte und ausgewählte Klauseln

Abschnitt 1 (Klauseln 1 – 7 SCC) enthält allgemeine, modulunabhängige Rahmenbedingungen für den Datentransfer (Umstände der Datenverarbeitung, Drittbegünstigtenklauseln, Beitritt neuer Vertragsparteien etc.). Besonders hervorzuheben sind folgende Klauseln:

Klausel 2 trifft Regelungen zur Wirkung und Unabänderbarkeit der Klauseln. Entscheidender Unterschied zu vorherigen Klauseln ist, dass diese nun die Anforderungen des Art. 28 Abs. 3 u. 4 DS-GVO „ermöglichen sollten“ (vgl. EG 9 SCC). Hierdurch bedarf es nicht mehr notwendigerweise des Abschlusses eines separaten Vertrages zur Auftragsverarbeitung, wobei weitere vertragliche Vereinbarungen gerade auch nicht ausgeschlossen sind.

Die Inhalte der SCC dürfen grundsätzlich nicht verändert werden. Konkretisierungen bzw. Ergänzungen sind bei den SCC jedoch notwendig, so

- bei der Auswahl des relevanten Moduls,

22 Standardisierte Verträge für die Auftragsverarbeitung innerhalb des EWR gem. Art. 28 Abs. 7 DS-GVO werden nunmehr als „Standardvertragsklauseln“ bezeichnet. Sie unterscheiden sich inhaltlich von den SCC. Die Kommission hat bereits ein solches Vertragsset erlassen (abrufbar unter https://ec.europa.eu/info/law/law-topic/data-protection/publications/standard-contractual-clauses-controllers-and-processors_de).

- bei der erforderlichen Vervollständigung von Texten (durch eckige Klammern gekennzeichnet), z.B. um die die zuständigen Gerichte und die Aufsichtsbehörde anzugeben und Fristen festzulegen,
- beim Ausfüllen der Anhänge zu den Umständen der Verarbeitung sowie
- beim Hinzufügen zusätzlicher Garantien, um das Schutzniveau für die Daten zu erhöhen (soweit erforderlich).

Solche Anpassungen werden nicht als Änderung des Kerntextes betrachtet und sind daher unproblematisch.[23]

Bestehen parallele Regelungen zu den Vertragsinhalten der SCC, muss geprüft werden, ob diese mittelbar oder unmittelbar im Widerspruch zu den Klauseln stehen (s. auch EG 109 S. 1 DS-GVO).

Beispiel

Cloudanbieter X führt in seinen allgemeinen Geschäftsbedingungen aus, dass er im Notfall Unterauftragnehmer ohne vorherige Information bzw. Genehmigung des Kunden einsetzen darf. Eine solche Regelung steht im direkten Widerspruch zu Klausel 9 (a) der SCC.

Vereinbaren die Parteien ergänzende, den SCC widersprechende Klauseln, verlieren die SCC ihre Eigenschaft als „geeignete Garantie nach Art. 46 Abs. 2 lit. c DS-GVO. Sie sind in der Folge als Ad-hoc-Vertrag gem. Art. 46 Abs. 3 lit. a DS-GVO anzusehen, der einer Genehmigungspflicht durch die zuständige Aufsichtsbehörde unterliegt.

Die Drittbegünstigtenklausel (*Klausel 3*) ermöglicht betroffenen Personen, zahlreiche Klauseln der SCC als Drittbegünstigte gegenüber dem Datenexporteur und/oder dem Datenimporteur geltend zu machen und durchsetzen zu können.

Klausel 5 bestimmt ein Rangverhältnis zwischen individuellen Vereinbarungen der Parteien und den SCC. Demnach gelten die Klauseln der SCC immer vorrangig. Konflikte sind zu Gunsten der Regelungsinhalte der SCC aufzulösen. Dies ist jedoch nicht so zu verstehen, dass im Widerspruch stehende vertragliche Vereinbarungen hinter den Vereinbarungen der SCC zurücktreten. Vielmehr verlieren in diesem Fall die SCC nach Klausel 2 SCC wiederum ihre Wirkung als „geeignete Garantie".

Neu in dieser Form ist die Kopplungsklausel (*Klausel 7*), die vereinbart werden kann. Eine Pflicht hierzu besteht nicht. Sie ermöglicht den nachträglichen Beitritt neuer Parteien, mit Zustimmung der bisherigen Parteien. Modalitäten des Beitritts (z.B. das Erfüllen einer Beitrittsbedingung sowie die Form der Genehmigung) sind in Klausel 7 nicht detailliert geregelt, so dass sich die Erstellung einer eigenen Kopplungsklausel z.B. in einer gesonderten Datenschutzrahmenvereinbarung anbietet.

Abschnitt 2 (*Klauseln 8 – 13 SCC*) regelt zunächst die Pflichten der Vertragsparteien in Abhängigkeit zur jeweiligen Transferkonstellation. Insbesondere Empfänger personenbezogener Daten im Drittland, die als Verantwortlicher für die Daten agieren, haben sich mit weitreichenden Anforderungen auseinander zu setzen, die an der DS-GVO angelehnt sind.

Durch die Datenschutzgarantien aus *Klausel 8* werden die Verarbeitungsgrundsätze des Art. 5 Abs. 1 DS-GVO, inklusive der Rechenschaftspflicht gem. Art. 5 Abs. 2 vereinbart. Auch versichert der Datenexporteuer nach der allgemeingültigen Klausel 8 Abs. 1 SCC, dass er sich „im Rahmen des Zumutbaren" davon überzeugt hat, dass der Datenimporteur – durch die Umsetzung geeigneter technischer und organisatorischer Maßnahmen – in der Lage ist, seinen Pflichten aus diesen Klauseln nachzukommen. In den *Klauseln 10, 11 und 13* finden sich Regelungen zu den Rechten der betroffenen Personen, den Rechtsbehelfen sowie zur Aufsicht.
Hervorzuheben sind die Haftungsregelungen im In-

23 Vgl. EU-Kommission, the new Standard Contractual Clauses - Questions and Answers, Ziff. 7, abrufbar unter https://ec.europa.eu/info/sites/default/files/questions_answers_on_sccs_en.pdf.

nenverhältnis (*Klausel 12*). Diese sehen im Grunde vor, dass die Parteien im Innenverhältnis unbeschränkt haften bzw. sich gegenseitig entsprechend freistellen. Aufgrund fehlender Konkretisierungen der Kommission kann Klausel 12 so verstanden werden, dass eine Beschränkung der Haftung im Innenverhältnis eine unzulässige Änderung der SCC darstellt.

Abschnitt 3 (*Klauseln 13, 14 SCC*) enthält spezifische Regelungen zum sog. „Transfer Impact Assessment (TIA)" und zum Umgang mit sicherheitsbehördlichen Zugriffen auf übermittelte Daten im Empfängerland. Dies ist eine direkte Reaktion auf das EuGH Urteil „Schrems II" und als „zusätzliche Maßnahme" vertraglicher Natur anzusehen.

Datenexporteur und Datenimporteur erklären in den SCC, dass sie sich mit der Rechtslage im Drittland im Hinblick auf den Datentransfer auseinandergesetzt haben und garantieren können, dass nach ihrem Wissen keine Gesetze bestehen, welche den Datenimporteur an der Einhaltung der Klauseln hindern. Der Datenexporteur soll zudem durch den Datenimporteur bei der Gesetzesanalyse nach „besten Kräften" (durch größtmögliche Informationen) unterstützt werden. Im Fall von entgegenstehenden Gesetzen muss der Datenexporteur für geeignete technische und organisatorische Maßnahmen Sorge tragen.

Hinweis:

In den Fällen, in den ein Verantwortlicher gem. Art. 4 Nr. 7 DS-GVO nicht Vertragspartei der SCC ist (so in der Variante „P2P"), bleibt er weiterhin rechenschaftspflichtig bezüglich der Wirksamkeit der SCC als geeignete Garantie. Hier bietet es sich an, beim Auftragsverarbeiter Informationen zum Transfer Impact Assessment einzuholen.

Hervorzuheben und besonders (praxis-)relevant ist *Klausel 14* lit. b sublit. ii i.V.m. Fußnote 12. Demnach sind neben den lokalen Rechtsvorschriften und den relevanten vertraglichen, technischen und organisatorischen Garantien, auch die „Gepflogenheiten" (engl. „Practices") des jeweiligen Drittlands zu berücksichtigen. Dies ermöglicht (wohl) eine risikobasierte Gesamtbeurteilung der Übermittlung. Demnach dürfte eine Übermittlung in ein der Rechtslage nach „problematisches" Drittland nicht vollkommen ausgeschlossen sein. Die Vereinbarkeit dieses risikobasierten Ansatzes mit der Rechtsprechung des EuGH bleibt abzuwarten. Die gesamte Prüfung ist in einem umfassenden TIA zu dokumentieren und den zuständigen Aufsichtsbehörden auf Verlangen vorzulegen.

Hinweis:

Nach Mitteilung der EU-Kommission sollen die von der US-Regierung eingeführten neuen Datenschutzgarantien (Rechtsmittelverfahren, eingeschränkter Zugriff durch US-Sicherheitsbehörden etc.) unabhängig von der Zertifizierung des Datenimporteurs nach dem EU-US DPF gelten. Auch der Datentransfer an US-Unternehmen unter Verwendung von SCCs oder auch BCRs wird insofern erleichtert.

Nicht eindeutig geklärt ist bislang, ob mit dem Angemessenheitsbeschluss der EU-Kommission auch die seit der „Schrems II"-Entscheidung bestehende Verpflichtung entfallen ist, zusätzlich zum Abschluss der SCC ein sog. Transfer Impact Assessment (TIA) durchzuführen.

Hierfür spricht, dass vor der „Schrems II"-Entscheidung des EuGH die Zertifizierung des Datenimporteurs nach dem Privacy Shield bzw. der Abschluss von SCC jeweils gleichwertige Möglichkeiten waren, um einen Datentransfer in die USA zu legitimieren und dies in beiden Fällen, ohne ein zusätzliches Risiko-Assessment durchzuführen und ggf. zusätzliche Schutzmaßnahmen zu ergreifen.

Fortsetzung Hinweis:

Wenn die neu eingeführten Datenschutzmechanismen dies also wieder für Datentransfers unter dem Abkommen ermöglichen, dann sollte dies auch für Datenübermittlungen aufgrund der SCC zutreffen. Gleichwohl gibt es eine Reihe von Vertretern von Großkanzleien, die dies anders beurteilen und da-von ausgehen, dass beim Abschluss von SCC weiterhin ein TIA notwendig ist. Die weitere Entwicklung insofern bleibt abzuwarten.

CHECKLISTE FÜR EIN TRANSFER IMPACT ASSESSMENT[24]

A. Umstände der Übermittlung

- ☐ **Verfahrensbeschreibung** *(z.B. systematische Beschreibung der verfolgten Ziele sowie der eingesetzten Hard- und Software; Erstellung von Datenflussdiagrammen)*
- ☐ **Verantwortlicher Geschäftsbereich** *(z.B. Human Resources)*
- ☐ **Prüfung von Alternativen** zur Übermittlung personenbezogener Daten in das Drittland *(z.B. Verweis auf gesichtete alternative Angebote mit einem ausschließlichen Bezug zur Europäischen Union)*
- ☐ **Herkunft der Daten** *(z.B. Angabe des Quellsystems)*
- ☐ **Verarbeitungsart und Speicherort** *(z.B. Speicherung von Daten im Data Center im Land X, Wartungszugriff aus Land Y)*
- ☐ **Art der Daten** *(z.B. Kategorien und Format, z.B. Personalstammdaten, Log-Dateien etc.)*

24 Aus Schwartmann/Benedikt/ Reif, Datenschutz im Internet 1. Aufl. 2022 (noch nicht erschienen).

A. Fortsetzung

- ☐ **Betroffene Personen** *(z.B. Kunden, Beschäftigte, Lieferanten etc.)*
- ☐ **Beteiligte Akteure sowie Art des Empfängers** *(z.B. Auftragsverarbeiter X, weiterer Auftragsverarbeiter Y, öffentl. Stelle Z etc.)*
- ☐ **Sektor** *(z.B. Telekommunikation, Gesundheit etc.)*
- ☐ **Verwendete Übertragungskanäle** *(z.B. Webeingabe per HTTPS)*
- ☐ **Verwendete vertragliche, technische oder organisatorische Garantien** *(z.B. Weiterleitung behördlicher Auskunftsersuchen an den Verantwortlichen, Richtlinie zum Umgang mit behördlichen Anfragen, Transportverschlüsselung, Encryption-at-Rest etc.)*

B. Lokale Rechtsvorschriften im Drittland, Beschränkungen und Garantien

- ☐ **Relevante Rechtsvorschrift im Drittland**[25] hinsichtlich **behördlicher Zugriffsmöglichkeiten** auf personenbezogene Daten und deren Voraussetzungen *(z.B. Sect. 702 FISA)*
- ☐ **Gesetzliche Ausnahmen** für einen behördlichen Datenzugriff sowie **Garantien für Betroffene** *(z.B. Geltung gesetzlicher Ermächtigungen nur für bestimmte Gesetzesverstöße, durchsetzbare Rechte und Rechtsschutzmöglichkeiten für Betroffene)*
- ☐ **Verhältnismäßigkeitsprüfung** *(z.B. Verhältnismäßigkeit identifizierter behördlicher Zugriffsmöglichkeiten anhand der EDSA Empfehlungen 02/202[26])*

C. Praktische Erfahrungen

- ☐ Berücksichtigung von Erfahrungen des Datenexporteurs oder –importeurs *(z.B. veröffentlichte Security Reports des Datenimporteurs)*

---

25 Der EDSA hat eine Studie zu behördlichen Zugriffen und der diesbezüglichen Gesetzeslage in den Ländern China, Indien und Russland veröffentlicht, vgl. https://edpb.europa.eu/system/files/2022-01/legalstudy_on_government_access_0.pdf.

26 EDSA, Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen v. 10.11.2020, abrufbar unter https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_de.pdf.

D. Ergänzende Maßnahmen

☐ Prüfung der Notwendigkeit ergänzender Maßnahmen[27] in Abhängigkeit des Ergebnisses von A.-C.

E. Gesamtbewertung

☐ Evaluierung der Feststellungen unter A.-D.

Der Datenimporteur wird zudem verpflichtet, jegliche behördlichen Anfragen anzufechten und mittels Ausschöpfung aller Rechtsmittel (bei begründeten Anhaltspunkten) anzugreifen.

Der Exporteur hat durch den Datenimporteur unverzüglich informiert zu werden, wenn nach Wissen des Importeurs eine Verarbeitung im Einklang mit den Klauseln nicht mehr gewährleistet werden kann.

Abschnitt 4 (*Klausel 16 – 18 SCC*) der Standarddatenschutzklauseln enthält Schlussbestimmungen, so unter anderem zu Kündigungsmöglichkeiten der Parteien, die Festlegung einer zuständigen Aufsichtsbehörde für die Klauseln sowie zum anwendbaren Recht.

cc. Überblick über die Anlagen

Ergänzt werden die Standarddatenschutzklausen weiterhin durch Anlagen, welche ebenfalls Vertragsbestandteil sind und von den Parteien individualisiert werden müssen. Die neuen Standarddatenschutzklausen enthalten drei Anhänge:

In Anhang I ist eine Liste der Vertragsparteien inkl. umfangreicher Angaben zu diesen sowie eine detaillierte Beschreibung der Datenübermittlungen aufzunehmen. Ergänzend ist die zuständige Aufsichtsbehörde i.S.d. Klausel 13 zu benennen.

27 Ausführlich zu den ergänzen Maßnahmen vgl. EDSA, Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten Version 2.0 v. 18.06.2021, abrufbar unter https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_de.pdf.

Anhang I der SCC (Muster)

A. LIST OF PARTIES

MODULE THREE: Transfer processor to processor

Data exporter(s): *[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name: Kölner Bauzeichner

Address: John Doe Str. 12, 50827 Köln

Contact person's name, position and contact details: Max Muster, Owner and Partner, +49 0000000, name@email

Activities relevant to the data transferred under these Clauses: Data Exporter captures digital imagery of requested Property. For each requested Property, Data Exporter delivers a shareable 3D model to its Customers acting as Data Controllers.

Signature and date: Max Muster, 28.06.2022

Role (controller/processor): Processor

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

Name: 3D Models Cloud LLC

Address: 111 E. John Doe Dr., Anonymouscity , MT 00000 USA

Contact person's name, position and contact details: Max Muster, General Counsel, name@email, +1 00000

Activities relevant to the data transferred under these Clauses: Data Importer acts as a service provider to host and display 3D models using a cloud environment.

Signature and date: Max Muster, 28.06.2022

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Inhabitants of Properties, Customers who have requested Services from Data Exporter, Employees of Data Exporter.

Categories of personal data transferred

Digital Imagery, location and type of property, name, email, phone number, company name, device identification and traffic data

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

No special categories of data are processed.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous basis.

Nature of the processing

By operating (hosting, backing up data), maintaining and supporting (including processing logs) the Services, Data Importer will process Personal Data contained in 3D models managed by the Services.

Purpose(s) of the data transfer and further processing

Allow for use of cloud based solution to host and display 3D models.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Duration of the related underlying main agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

See Annex III

Anhang II fordert eine Beschreibung der konkreten technischen und organisatorischen Maßnahmen (TOMs) des Datenimporteurs sowie etwaiger Auftrags-/Unterauftragsverarbeiter. Es ist davon auszugehen, dass auch etwaige Maßnahmen des Datenexporteurs aufzulisten sind.

In *Anhang III* sind schließlich für die Module 2 und 3 sämtliche Unterauftragsverarbeiter mit Namen, Anschrift und einer Beschreibung der jeweiligen Verarbeitungsschritte zu benennen. Hierbei wird der Praxis regelmäßig auf Online-Quellen (z.B. ein Kundenportal) verwiesen.

c. Genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit. e DS-GVO)

Auch genehmigte Verhaltensregeln (sog. „Codes of Conduct", CoC) gem. Art. 46 Abs. 2 lit. e DS-GVO können als geeignete Garantie für den Drittlandstransfer eingesetzt werden. Sie werden von Verbänden und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, entwickelt. Wird ein CoC für das Gewährleisten eines angemessenen Schutzniveaus im Drittland eingesetzt, geht der Datenempfänger im Drittland mittels vertraglicher oder sonstiger rechtlich bindender Instrumente die verbindliche und durchsetzbare Verpflichtung ein, die geeigneten Garantien anzuwenden, auch im Hinblick auf die Rechte der betroffenen Personen. Dies ist wichtig, um für ein angemessenes Schutzniveau im Drittland zu sorgen. Der Datenexporteur im EWR muss einem solchen CoC nicht zwingend beitreten. CoCs bedürfen der vorherigen Genehmigung durch die zuständige Aufsichtsbehörde.

Auswirkungen von Schrems II:

Auch im Hinblick auf CoC ist eine Prüfung bezüglich zusätzlicher Maßnahmen/Garantien vor dem Hintergrund der Schrems II-Entscheidung erforderlich.

Der Europäische Datenschutzausschuss hat eine Checkliste mit verpflichtenden Bestandteilen eines CoC für den Drittlandstransfer veröffentlicht.[28]

d. Zertifizierung (Art. 46 Abs. 2 lit. f DS-GVO)

Auch eine Zertifizierung kann, zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters, eine geeignete Garantie für einen Datenexport darstellen. Die Genehmigung erfolgt durch die zuständige Aufsichtsbehörde oder eine akkreditierte Zertifizierungsstelle (vgl. Art. 42 Abs. 2 und 5 DS-GVO). Der Europäische Datenschutzausschuss hat Leitlinien bezüglich einer Zertifizierung als Transfermechanismus in Drittländer veröffentlicht. Dort finden ich Hinweise zu erforderlichen zusätzlichen Kriterien, um für ein angemessenes Schutzniveau beim zertifizeirten Datenimporteur zu sorgen.[29]

Auswirkungen von Schrems II:

Im Falle eines Zertifizierungsverfahrens für den Drittlandstransfer muss das Erfordernis von zusätzlichen Maßnahmen/Garantien hinsichtlich der Schrems II-Entscheidung geprüft werden.

28 EDSA, Guidelines 04/2021 on Codes of Conduct as tools for transfers Version 2.0, Ziff. 6.2, abrufbar unter https://edpb.europa.eu/system/files/2022-03/edpb_guidelines_codes_conduct_transfers_after_public_consultation_en_1.pdf.

29 hhttps://edpb.europa.eu/system/files/2022-06/edpb_guidelines_202207_certificationfortransfers_en_1.pdf, Ziff. 3.2).

e. Ad-hoc-Verträge (Art. 46 Abs. 3 lit. a DS-GVO)

Datenexporteure und -importeure können, über die bisher genannten Mechanismen hinaus, individuelle Garantien über einen Individualvertrag vereinbaren (sog. "Ad-hoc-Vertrag"). Der Vorteil einer Ad-hoc-Vereinbarung liegt darin, dass die Vertragsparteien ihre individuellen Bedürfnisse in das Vertragswerk einfließen lassen können. Eine solche Vereinbarung muss jedoch durch die zuständige Aufsichtsbehörde im Rahmen des Kohärenzverfahrens vorab genehmigt werden (vgl. Art. 46 Abs. 3 lit. a DS-GVO i.V.m. Art. 46 Abs. 4 DS-GVO).

Hinweis:

Einen belastbaren Orientierungsmaßstab für genehmigungsfähige Ad-hoc-Verträge bieten die SCC, welche auch übernommen und angepasst werden können. Werden Änderungen an den SCC vorgenommen, welche im Widerspruch zu den Klauseln stehen, dann führt dies dazu, dass sie als Ad-hoc-Vertragsklauseln angesehen werden.

3. Ausnahmen für bestimmte Fälle (Art. 49 DS-GVO)

Besteht kein Angemessenheitsbeschluss der Kommission und können keine geeigneten Garantien gem. Art. 46 DS-GVO für den Datenexport eingesetzt werden (z.B. weil sich der Empfänger weigert, die SCC abzuschließen oder die Garantie nicht wirksam im Drittland durchgesetzt werden kann), können personenbezogene Daten unter den Voraussetzungen von Art. 49 DS-GVO in ein Drittland übermittelt werden. Bei manchen der in Art. 49 DS-GVO aufgeführten Sonderfälle besteht die Einschränkung, dass die Datenübermittlung in das Drittland nur gelegentlich erfolgen darf (vgl. EG 111).

a. Einwilligung (Art. 49 Abs. 1 S. 1 lit. a DS-GVO)

Art. 49 Abs. 1 S. 1 lit. a DS-GVO gestattet eine Übermittlung in ein Drittland, wenn der Betroffene hierzu seine ausdrückliche Einwilligung erteilt hat. Neben den allgemeinen Anforderungen an die Einwilligung (vgl. Art. 4 Nr. 11 DS-GVO sowie Art. 7 u. Art. 8 DS-GVO) tritt im Rahmen der Übermittlung personenbezogener Daten in ein Drittland das Merkmal der „Ausdrücklichkeit". Nicht jede Willensbekundung genügt für den Drittlandstransfer, vielmehr muss sich die Einwilligung ausdrücklich auf die Risiken einer Datenübermittlung in ein Drittland oder an eine internationale Organisation ohne das Vorliegen eines Angemessenheitsbeschlusses oder anderer geeigneter Garantien beziehen. Der Betroffene muss entsprechend vor der Übermittlung über die Risiken in Kenntnis gesetzt werden.

Hinweis:

Eine Einschränkung der Einwilligung auf gelegentliche Übermittlungen findet sich in der DS-GVO nicht.

b. Erfüllung eines Vertrags mit dem Betroffenen (Art. 49 Abs. 1 S. 1 lit. b DS-GVO)

Ein Datenexport in ein Drittland kann zum Zwecke der Erfüllung eines zwischen dem Betroffenen und dem Verantwortlichen geschlossenen Vertrags oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag des Betroffenen legitimiert werden. Bei vorvertraglichen Maßnahmen und Verarbeitungen ist daher die aktive Mitwirkung des Betroffenen erforderlich (z.B. die Aufforderung durch den Betroffenen, ein Angebot abzugeben).

Im Rahmen eines Vertrags mit dem Betroffenen bedarf es nach Meinung des EDSA eines engen und erheblichen Zusammenhangs zwischen Vertrags-

zweck und der zu Grunde liegenden Datenverarbeitung.[30]

Beispiel

Erforderliche Datenübermittlungen zur Vertragserfüllung können etwa angenommen werden, wenn ein Kunde über ein deutsches Reisebüro eine Vermittlung von Hotelübernachtungen oder sonstigen Reiseleistungen im Drittland über das Internet bucht.

Die Übermittlung von Beschäftigtendaten von einem europäischen Tochterunternehmen zur Muttergesellschaft im Drittland zu Zwecken der zentralen Personalverwaltung kann in der Regel nicht über die Erfüllung arbeitsvertraglicher Pflichten legitimiert werden, da eine solche Datenübermittlung hierzu nicht in einem engeren Zusammenhang steht.

Eine Erforderlichkeit eines Drittlandstransfer kann sich dann ergeben, wenn dieser im Arbeitsvertrag zwischen Mitarbeiter und dem Unternehmen hinreichend deutlich angelegt ist (über eine sog. „Konzernbezugsklausel"). Allerdings muss hierbei weiterhin das Prinzip der Erforderlichkeit einer Verarbeitung beachtet werden. Dies gilt auch für Zugriffe auf Beschäftigtendaten nach dem „Need-to-know-Prinzip".

Im Zusammenhang mit Art. 49 Abs. 1 S. 1 lit. b DS-GVO ist zudem zu beachten, dass mit Blick auf den Wortlaut von EG 111 S. 1 DS-GVO nur gelegentliche Übermittlungen möglich sind. Eine systematische Übermittlung zählt hierzu nicht.

c. Erfüllung eines Vertrags im Interesse des Betroffenen (Art. 49 Abs. 1 S. 1 lit. c DS-GVO)

Datenübermittlungen in Drittländer sind gestattet, wenn sie zum Abschluss oder zur Erfüllung von Verträgen erforderlich sind, die im Interesse des Betroffenen vom Verantwortlichen mit einem Dritten geschlossen wurden oder geschlossen werden sollen. Gemeint sind damit Verträge, an denen die Betroffenen zwar nicht beteiligt sind, von denen sie aber begünstigt werden. Typische Anwendungsfälle für die Norm ergeben sich insbesondere im Bereich des Beschäftigtendatenschutzes, z.B. der Abschluss von Mitarbeiterversicherungen bei ausländischen Gesellschaften oder die Weitergabe von Beschäftigtendaten durch den Arbeitgeber im Rahmen eines Reisevertrags an ein Hotel im Drittland. Auch im Fall von Verträgen mit Dritten darf die Übermittlung erforderlicher personenbezogener Daten nur gelegentlich erfolgen (vgl. EG 111 S. 1 DS-GVO).

d. Wichtige Gründe des öffentlichen Interesses (Art. 49 Abs. 1 S. 1 lit. d DS-GVO)

Zur Wahrung wichtiger öffentlicher Interessen können personenbezogenen Daten an Empfänger in Drittländern auch ohne angemessenes Schutzniveau übermittelt werden. Diese Interessen müssen sich allerdings aus einer gesetzlichen Grundlage eines europäischen bzw. nationalen Mitgliedstaates ergeben. Wichtige Gründe des öffentlichen Interesses eines Drittlandes fallen nicht hierunter.

Beispiel

Anfragen einer Behörde wegen Ermittlungen im öffentlichen Interesse des Drittlands sind im Rahmen von Art. 49 Abs. 1 S. 1 lit. d DS-GVO unzulässig, so beispielsweise FISA Orders oder National Security Letters, da sie ihren Ursprung im US-amerikanischen Recht haben und nicht über ein Rechtshilfeabkommen mit der Europäischen Union oder einem Mitgliedstaat geregelt sind (s. auch Art. 48 DS-GVO).

30 Vgl. Leitlinien 2/2018, S. 10.

e. Geltendmachung von Rechtsansprüchen (Art. 49 Abs. 1 S. 1 lit. e DS-GVO)

Eine Datenübermittlung kann ausnahmsweise zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich sein. Der in der EU-Datenschutzrichtlinie 95/46/EG noch vorhandene Verweis auf Rechtsansprüche vor Gericht ist entfallen, wodurch auch Datenübermittlungen an Behörden sowie Datenübermittlungen zwischen privaten Rechtsträgern im Rahmen der obigen Zweckverfolgung nunmehr möglich sind. Voraussetzung ist jedoch, dass die Übermittlung einem konkreten Verfahren zugeordnet werden kann. Damit können beispielsweise auch sog. Pre-Trial-Discovery-Verfahren nach US-amerikanischem Recht grundsätzlich unter die gesetzliche Ausnahme fallen.

Ein „klassischer" Fall einer erforderlichen Datenübermittlung in ein Drittland kann sich im Kontext der Rechtsansprüche ergeben, wenn beispielsweise die im Drittland niedergelassene Muttergesellschaft von einem Angestellten des Konzerns, der in einem europäischen Tochterunternehmen arbeitet, verklagt wird.

Die jeweiligen Datenübermittlungen sind jedoch auf das erforderliche Maß zur Ausübung der eigenen Rechte zu beschränken. Hierbei ist wiederum EG 111 S. 1 zu beachten, der nur gelegentliche Übermittlungen erlaubt. Da auch die Rechteausübung, Rechtsverfolgung oder Rechtsverteidigung im Kontext der „Sonderfälle" des Art. 49 DS-GVO angesiedelt ist, sollten vorrangig Garantien i.S.d. Art. 46 DS-GVO eingesetzt werden. Ferner ist die Übermittlung anonymisierter oder zumindest pseudonymisierter Daten vorzugswürdig.

f. Schutz lebenswichtiger Interessen (Art. 49 Abs. 1 S. 1 lit. f DS-GVO)

Ein Datenexport in ein Drittland kann zur Wahrung lebenswichtiger Interessen des Betroffenen oder anderer Personen erforderlich sein. Dies betrifft jedoch nur Einzelfälle, in denen der Betroffene beispielsweise bewusstlos ist und dringend ärztliche Hilfe benötigt. Denkbar wäre etwa der Fall, dass nur der in einem Land der Europäischen Union niedergelassene behandelnde Arzt die für die akut notwendige Behandlung im Drittland erforderlichen Informationen liefern kann und dann dementsprechend in das Drittland übermitteln darf.

g. Übermittlung aus einem öffentlichen Register (Art. 49 Abs. 1 S. 1 lit. g DS-GVO)

Die DS-GVO erlaubt eine Datenübermittlung aus Registern in ein Land ohne angemessenes Schutzniveau, wobei diese Register gemäß den Rechts- oder Verwaltungsvorschriften des jeweiligen Mitgliedstaats zur Information der Öffentlichkeit bestimmt sein müssen (z.B. das Handels- oder Vereinsregister in Deutschland). Ebenso erfasst sind solche Register, die auf Basis eines berechtigten Interesses bestimmter Personen zur Einsicht offenstehen (z.B. das Grundbuch).

h. Wahrung zwingender berechtigter Interessen des Verantwortlichen (Art. 49 Abs. 1 S. 2 DS-GVO)

Für den Fall, dass keine der Ausnahmen für bestimmte Fälle bei der Datenübermittlung greift, kein Angemessenheitsbeschluss der Kommission vorliegt und keine Garantien des Art. 46 DS-GVO zugunsten des Betroffenen geschaffen werden können, ermöglicht Art. 49 Abs. 1 S. 2 DS-GVO eine Datenübermittlung in ein Drittland unter engen Voraussetzungen. Der Verantwortliche hat hierbei die folgende Anforderungen kumulativ zu erfüllen:

- Die Übermittlung betrifft nur eine begrenzte Zahl von betroffenen Personen,
- sie ist zur Wahrung seiner zwingenden berechtigten Interessen erforderlich,
- die Interessen oder Rechten und Freiheiten der Betroffenen überwiegen nicht,

>> der Verantwortliche hat alle Umstände der Datenübermittlung beurteilt und auf Grundlage der Beurteilung angemessene Garantien in Bezug auf den Schutz personenbezogener Daten vorgesehen.

Welche Garantien als angemessen zu erachten sind, spezifiziert die DS-GVO nicht. Diese können grundsätzlich vertraglicher, aber auch technisch-organisatorischer Natur sein. Letztlich dürfen die Übermittlungen im Rahmen des Art. 49 Abs. 1 S. 2 DS-GVO nicht wiederholt erfolgen. In welchem Umfang diese Ausnahme für Verantwortliche mit Blick auf zwingende berechtigte Interessen nutzbar ist, bleibt offen. Die Aufsichtsbehörden sehen den Auffangtatbestand des Art. 49 DS-GVO beispielsweise dann als erfüllt an, wenn ein Verantwortlicher gezwungen ist, personenbezogene Daten in das Drittland zu übermitteln, um seine Organisation oder seine Systeme vor einem unmittelbar bevorstehenden, schwerwiegenden Schaden oder vor einer empfindlichen Strafe zu schützen, die sein Geschäft erheblich beeinträchtigen würde.[31] Art. 49 Abs. 1 S. 2 DS-GVO sollte daher nur für außergewöhnliche Umstände angewendet werden, in denen ein Datenexport in ein Drittland realisiert werden muss. Hierbei ist im Sinne der Rechenschaftspflicht des Art. 5 Abs. 2 DS-GVO darauf zu achten, dass die geforderten zwingenden berechtigten Interessen und realisierten Garantien ausreichend dokumentiert sind. Ferner ist die zuständige Aufsichtsbehörde über die Übermittlung im Rahmen des Art. 49 Abs. 1 S. 2 DS-GVO zu informieren. Betroffenen sind die zwingenden berechtigten Interessen, die mit der Übermittlung verfolgt werden zusätzlich zu den allgemeinen Informationspflichten der Artt. 13 u. 14 DS-GVO zu kommunizieren.

B. 6 Prüfschritte zur Umsetzung

Der EDSA hat in seinen Empfehlungen zu den zusätzlichen Maßnahmen[32] im Bereich der Drittlandsübermittlungen sechs Prüfschritte empfohlen, die Datenexporteure zur Einhaltung von Kapitel V anwenden können:

1. Bestandsaufnahme der Datenflüsse („data mapping“)

2. Bestandsaufnahme des verwendeten Mechanismus nach Kapitel V („transfer tools verification“)

Für den Fall, dass kein Angemessenheitsbeschluss der Kommission für das Land, das Gebiet oder den Sektor vorliegt, sind zusätzlich die Schritte 3-5 zu durchlaufen:

3. Effektivität geeigneter Garantien nach Art. 46 DS-GVO: Evaluierung der Rechtslage im Drittland, insbes. bezüglich behördlicher Datenzugriffe (vgl. Recommendations 02/2020 zur Verhältnismäßigkeit von Überwachungsmaßnahmen)

4. Implementierung zusätzlicher Garantien (falls erforderlich)

5. Einhaltung der sonstigen formalen Anforderungen an geeignete Garantien nach Art. 46 DS-GVO (z.B. die Genehmigung einer Ad-hoc-Vereinbarung durch eine zuständige Aufsichtsbehörde)

6. Regelmäßiges Monitoring

31 Vgl. Leitlinien 2/2018, S. 18.

32 Vgl. Empfehlungen 01/2020.

Gesellschaft für Datenschutz
und Datensicherheit e.V.

Mitglied werden? Mehr Informationen?

https://www.gdd.de/service/mitglied-werden oder eine E-Mail an: info@gdd.de

Eine Mitgliedschaft bietet wesentliche Vorteile:

>> Mitglieder-Nachrichten mit aktuellen Fachinformationen
>> Bezug der Fachzeitschrift RDV (Recht der Datenverarbeitung)
>> Beratung bei konkreten Einzelfragen
>> Zugriff auf Rechtsprechungs- und Literaturarchiv
>> Online-Service „DataAgenda Plus“ (Muster, Checklisten, RDV ONLINE Archiv, Arbeitspapiere etc.)
>> Mitarbeit in Erfahrungsaustausch- und Arbeitskreisen
>> Teilnahme an den kostenfreien GDD-Informationstagen sowie Vergünstigungen bei Seminaren u.v.m.

Schließen Sie sich unseren mehr als 3.800 Mitgliedern an. Eine Mitgliedschaft erhalten Sie schon ab 150,- EUR/Jahr für Privatpersonen und ab 300,- EUR/Jahr für Firmen.

Herausgeber:
Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.
Heinrich-Böll-Ring 10
53119 Bonn
Tel.: +49 0228 96 96 75-00
Fax: +49 0228 96 96 75-25
www.gdd.de
info@gdd.de
Satz: C. Wengenroth, GDD-Geschäftsstelle, Bonn
Ansprechpartner: RA Yvette Reif, LL.M. / Maximilian Olker

Stand:
Version 2.0 (August 2023)