STIFTUNG DATENSCHUTZ

INTERNATIONALE DATENTRANSFERS

Eine Handreichung

UMSETZUNG DER DATENSCHUTZ-RECHTLICHEN VORGABEN BEI INTERNATIONALEN TRANSFERS PERSONENBEZOGENER DATEN

AUTOREN

Wiebke Reuter, LL.M. (London)
Rechtsanwältin, Taylor Wessing

Dr. Paul Voigt, Lic. en Derecho, CIPP/E
Rechtsanwalt und Fachanwalt für IT-Recht, Taylor Wessing

INHALT

DARSTELLUNG DER RECHTLICHEN HINTERGRÜNDE UND GRUNDLAGEN

HINTERGRUND

Am 16. Juli 2020 hat der Europäische Gerichtshof (EuGH) eine wegweisende Entscheidung zur Übermittlung personenbezogener Daten[1] an Datenimporteure in Drittländern ohne angemessenes Datenschutzniveau verkündet. Die Entscheidung hat nicht nur Auswirkungen auf die Weitergabe von Daten in die USA, sondern auch andere Staaten außerhalb der Europäischen Union (EU) bzw. des Europäischen Wirtschaftsraumes (EWR).

Ausgangspunkt des Urteils war eine Beschwerde des Österreichers Maximilian Schrems bei der irischen Datenschutzbehörde gegen Facebook, in der Maximilian Schrems behauptete, dass die interne Übermittlung personenbezogener Daten durch Facebook aus der EU in die USA gegen das EU-Datenschutzrecht verstoße. Facebook stützte den Transfer auf das sogenannte Safe-Harbor-Abkommen, ein Abkommen zwischen der EU und den USA über Datenschutzanforderungen für die Verarbeitung von EU-Daten in den USA. In einem ersten Urteil vom Oktober 2015 erklärte der EuGH das Safe-Harbor-Abkommen für ungültig, weil es nicht den Anforderungen der Europäischen Grundrechtecharta entsprach (Urteil vom 6. Oktober 2015, C-362/14 – *Schrems I*[2]). Daraufhin einigten sich die EU und die USA auf das EU-US-Privacy Shield, den Nachfolger des Safe-Harbor-Abkommens, um Datenübermittlungen aus der EU in die USA zu rechtfertigen. In einem weiteren Verfahren hat der EuGH jedoch im Juli 2020 auch das EU-US Privacy Shield aufgehoben (Urteil vom 16. Juli 2020, C-311/18 – *Schrems II*[3]). Der Gerichtshof begründete seine Entscheidung damit, dass personenbezogene Daten in den USA nicht ausreichend vor den US-Behörden geschützt seien und es keine hinreichenden Rechtsschutzmöglichkeiten gebe. Zum einen hätten die US-Geheimdienste zu weitreichende Befugnisse, auf Datenbestände zuzugreifen, insbesondere in Bezug auf Nicht-US-Bürger. Zum anderen gebe es keinen hinreichenden Rechtschutz für Personen aus der EU. Seit Verkündung des Urteils können Datenübermittlungen in die USA daher nicht mehr auf das Privacy Shield gestützt werden.

Der EuGH äußerte sich in seinem Urteil daneben auch zu einem weiteren Instrument der Absicherung von Drittlandtransfers, den sogenannten Standardvertragsklauseln der Europäischen Kommission, welche ebenfalls verwendet werden können, um Drittlandtransfers abzusichern. Mit Abschluss der Standardvertragsklauseln verpflichtet sich der Datenempfänger, die empfangenen Daten nach mit europäischem Recht vergleichbaren Standards zu behandeln. Der EuGH sah die Standardvertragsklauseln als weiterhin wirksam an. Die Richter betonten jedoch, dass die Vereinbarung der Standardvertragsklauseln als solches nicht genüge, ein angemessenes Datenschutzniveau im Drittland sicherzustellen. Vielmehr müssen Datenexporteur und -importeur sicherstellen, dass die transferierten Daten im Zielland tatsächlich einen vergleichbaren Schutz wie nach der DSGVO im Lichte der europäischen Grundrechtecharta genießen. Dafür sei die bilaterale Vereinbarung der Standardvertragsklauseln nicht immer hinreichend: Soweit behördliche Zugriffsrechte im Empfängerland bestünden, könnten diese durch die vertragliche Vereinbarung der Standardvertragsklauseln zwischen Datenexporteur in der EU und Datenimporteur außerhalb der EU nicht ausgehebelt werden.

Das Urteil hat für betroffene Unternehmen viele Unsicherheiten mit sich gebracht, wie in Zukunft mit Datenübermittlungen in Drittländer umzugehen ist. Diese Handreichung soll einen Überblick über den rechtlichen Hintergründen und die Auswirkungen des Urteils für die Praxis sowie entsprechende Hinweise für Unternehmen geben.

1 Personenbezogene Daten bezeichnen alle Informationen, die sich auf eine natürliche Person beziehen, die direkt oder indirekt identifiziert werden kann, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, einer Kennnummer, Standortdaten oder einer Online-Kennung.
2 https://curia.europa.eu/juris/liste.jsf?language=de&num=C-362/14.
3 https://curia.europa.eu/juris/liste.jsf?language=de&num=C-311/18.

DATENÜBERMITTLUNGEN IN DRITTLÄNDER NACH DER DSGVO

Werden personenbezogene Daten an andere Empfänger weitergegeben, so ist dies gemäß Art. 6 der DSGVO unabhängig davon zu rechtfertigen, wo der Empfänger niedergelassen ist. Auch an Datenweitergaben innerhalb der EU/des EWR werden somit hohe Anforderungen gestellt. Zusätzlich zu diesen für Datenübermittlungen innerhalb der EU/des EWR geltenden Anforderungen kommen jedoch weitere Verpflichtungen hinzu, wenn personenbezogene Daten an Empfänger außerhalb der EU/des EWR weitergegeben werden sollen.

Die Anforderungen an solch eine Datenübermittlung in ein Drittland sind in den Art. 44 der Datenschutz-Grundverordnung (DSGVO) geregelt. Die Vorgaben gelten für alle Transfers personenbezogener Daten, bei denen der Datenexporteur der Daten (in Bezug auf diese Daten) der DSGVO unterfällt (siehe hierzu unter Abschnitt A.II.1.) und der Datenimporteur in einem Drittland ansässig ist (siehe hierzu unter A.II.2.).

DATENEXPORTEUR IST ADRESSAT DER DSGVO

Der Datenexporteur ist Adressat der DSGVO, wenn er

- in der EU niedergelassen ist;

  Beispiel: Datenexporteur ist in Deutschland ansässig und betreibt einen Online-Shop.

  → Die DSGVO findet Anwendung auf die Verarbeitung aller personenbezogenen Daten, die im Rahmen des Online-Shops verarbeitet werden, unabhängig davon, wo die betroffenen Personen ansässig sind.

- nicht in der EU niedergelassen ist, aber Daten von natürlichen Personen in der EU verarbeitet im Zusammenhang mit dem Angebot von Waren oder Dienstleistungen an diese; oder

  Beispiel: Datenexporteur ist in Großbritannien ansässig und betreibt einen Online-Shop, der sich gezielt auch an Kunden in Deutschland richtet.

  → Die DSGVO findet Anwendung auf die Verarbeitung der personenbezogenen Daten der Nutzer aus Deutschland.

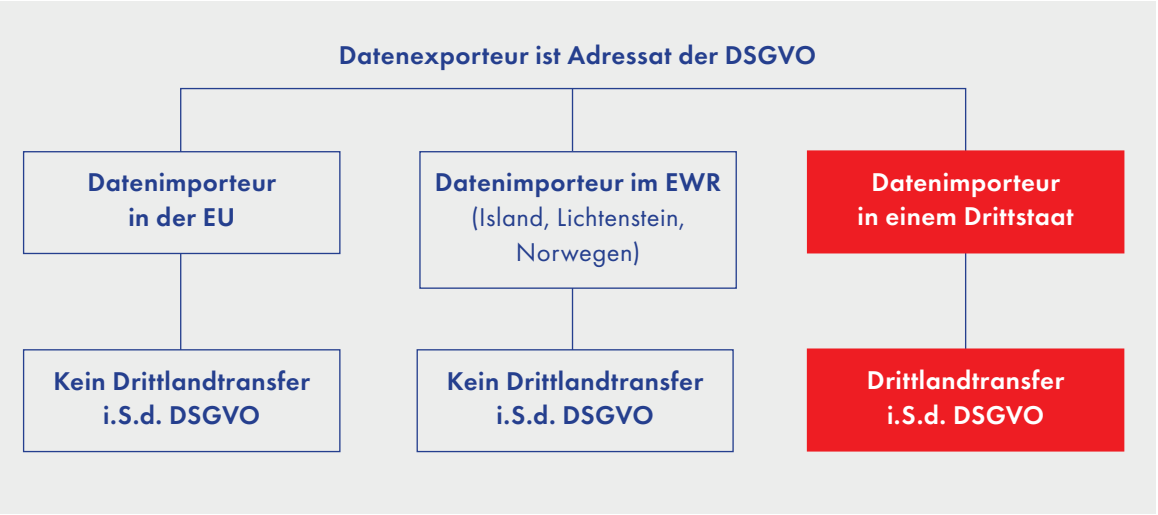
- nicht in der EU niedergelassen ist, aber Daten von Personen in der EU verarbeitet, um deren Verhalten zu beobachten.

  Beispiel: Datenexporteur ist in Großbritannien ansässig und betreibt einen Online-Shop, der sich auch an Kunden in Deutschland richtet. Im Rahmen des Online-Shops setzt der Anbieter Analysetools ein, um die Nutzung des Shops durch Kunden zu analysieren.

  → Die DSGVO findet Anwendung auf die Verarbeitung der personenbezogenen Daten der Nutzer aus Deutschland.

DATENIMPORTEUR IST IM DRITTLAND ANSÄSSIG

Als Drittländer im Sinne der Normen gelten alle Staaten, die nicht Mitgliedstaat der EU oder des Europäischen Wirtschaftsraumes (EWR) ist. Zu den Mitgliedern des EWR gehören außerhalb der EU Island, Liechtenstein und Norwegen. Datentransfers in diese Staaten fallen somit nicht unter die strengen Anforderungen der Art. 44 DSGVO an Drittlandübermittlungen. Es sind daher folgende Konstellationen zu unterscheiden:



Praxistipp: Vor jeder Datenübermittlung sollte kurz geprüft werden, ob der Datenimporteur in der EU oder dem EWR (Island, Liechtenstein, Norwegen) niedergelassen ist. Ist dies der Fall, bedarf es keiner weiteren Schutzmaßnahmen. Die Daten können wie geplant übermittelt werden. Nur wenn der Datenimporteur in einem Staat außerhalb der EU/des EWR ansässig ist, muss sichergestellt werden, dass Schutzmaßnahmen zur Sicherstellung eines angemessenen Datenschutzniveaus im Drittland bestehen (siehe zu den verschiedenen Mechanismen unter Abschnitt A.III.).

INSTRUMENTE ZUR ABSICHERUNG VON DRITTLANDTRANSFERS NACH DER DSGVO

Sofern ein Drittlandtransfer i.S.d. DSGVO vorliegt (siehe hierzu oben unter Abschnitt A.II.), sieht die DSGVO verschiedene Instrumente vor, mit denen dieser Drittlandtransfer abgesichert werden kann. Im Folgenden sollen die relevantesten Instrumente kurz dargestellt werden:

- Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses;
- Datenübermittlung auf der Grundlage der Standarddatenschutzklauseln;
- Datenübermittlung auf der Grundlage verbindlicher interner Datenschutzvorschriften;
- Ausnahmen für bestimmte Fälle.

ANGEMESSENHEITSBESCHLUSS DER EUROPÄISCHEN KOMMISSION

Art. 45 DSGVO bietet die Rechtsgrundlage für die Europäische Kommission, festzustellen, ob ein Land außerhalb der EU bzw. des EWR ein angemessenes Datenschutzniveau bietet. Ergibt die Prüfung, dass ein angemessenes Datenschutzniveau besteht, erlässt die Europäische Kommission einen Angemessenheitsbeschluss. Ein solcher Beschluss hat zur Folge, dass personenbezogene Daten aus der EU sowie den weiteren Ländern des EWR (Island, Liechtenstein und Norwegen) in das betreffende Drittland übermittelt werden können, ohne dass weitere Schutzmaßnahmen erforderlich sind. Faktisch werden Datenübermittlungen in Drittstaaten, für die ein Angemessenheitsbeschluss erlassen wurde, somit Datenübermittlungen innerhalb der EU bzw. des EWR gleichgestellt.

Derzeit besteht ein Angemessenheitsbeschluss für folgende Staaten: Andorra, Argentinien, Kanada (kommerzielle Organisationen), die Färöer-Inseln, Großbritannien, Guernsey, Israel, die Isle of Man, Japan, Jersey, Neuseeland, die Schweiz und Uruguay. Daneben läuft ein Verfahren für Südkorea. Die aktuelle Liste der bestehenden Angemessenheitsbeschlüsse ist online einsehbar.[4]

Praxistipp: Sofern Daten an einen Empfänger außerhalb der EU/des EWR übermittelt werden sollen, sollte zunächst die aktuelle Liste der Europäischen Kommission überprüft werden, ob für das Empfängerland bereits ein Angemessenheitsbeschluss ergangen ist. Ist dies der Fall, sind keine weiteren Schutzmaßnahmen erforderlich. Die Daten können dann an den Empfänger übermittelt werden.

STANDARDDATENSCHUTZKLAUSELN

Eine weitere Möglichkeit, Datenübermittlungen in ein Drittland abzusichern, bieten die sogenannten Standarddatenschutzklauseln. Hierbei handelt es sich um Klauseln, die die Europäische Kommission erlässt und die bestimmte Verpflichtungen für den Datenexporteur und -importeur vorsehen. Die Europäische Kommission hat von dieser Möglichkeit Gebrauch gemacht und im Juni 2021 die sogenannten Standardvertragsklauseln[5] (häufig auch als Standard Contractual Clauses („SCC") bezeichnet) veröffentlicht. Bis zu diesem Zeitpunkt galten noch die „alten" Standardvertragsklauseln, die bereits vor Inkrafttreten der DSGVO unter der vorherigen Rechtslage erlassen wurden. Im Rahmen der neuen Standardvertragsklauseln hat die Europäische Kommission die Klauseln auf die Vorgaben der DSGVO angepasst und auch das Schrems II-Urteil des EuGH berücksichtigt.

Die Absicherung von Datentransfers basierend auf den Standardvertragsklauseln stellt in der Praxis den mit Abstand relevantesten Transfermechanismus dar. Ein Großteil der Datentransfers beruht auf diesen Klauseln.

Praxistipp: Bestehende Datenübermittlungen, für die bisher die alten Standardvertragsklauseln abgeschlossen wurden, müssen bis zum 26. Dezember 2022 auf die neuen Standardvertragsklauseln umgestellt werden. Neue Datenübermittlungen, die ab dem 27. September 2021 aufgenommen werden, können nur noch über die neuen Standardvertragsklauseln abgesichert werden.

VERBINDLICHE INTERNE DATENSCHUTZVORSCHRIFTEN

Einen weiteren Schutzmechanismus für die Absicherung von Drittlandtransfer bieten verbindliche interne Datenschutzvorschriften, häufig auch als Bindung Corporate Rules („BCR") bezeichnet. Hierbei handelt es sich um eine Form der Selbstverpflichtung eines Unternehmens zum Umgang mit personenbezogenen Daten.

Die verbindlichen internen Datenschutzvorschriften haben in der Praxis nur bedingt Relevanz. Die Erstellung und Implementierung erfordern einen erheblichen Aufwand. Ferner müssen die Datenschutzvorschriften von der zuständigen Datenschutzaufsichtsbehörde genehmigt werden. Dieses Verfahren kann mehrere Monate bis Jahre dauern. Faktisch eignen sich verbindliche interne Datenschutzvorschriften daher regelmäßig nur bei großen Unternehmensgruppen mit umfangreichen Datentransfers.

AUSNAHMEN FÜR BESTIMMTE FÄLLE

Sofern kein anderes Instrument für die Absicherung von Drittlandtransfers in Betracht kommt, sieht die DSGVO bestimmte Ausnahmen vor, in denen auch außerhalb der sonstigen Schutzmaßnahmen Drittlandtransfers erlaubt werden können. Diese sind in Art. 49 DSGVO verankert.

Relevanz in der Praxis haben vor allem die Datenübermittlung basierend auf einer Einwilligung der Betroffenen sowie die Datenübermittlung zum Zwecke der Vertragserfüllung. Zu beachten ist jedoch, dass die Datenschutzaufsichtsbehörden den Ausnahmecharakter dieser Schutzmechanismen in den Vordergrund stellen. Sie vertreten daher

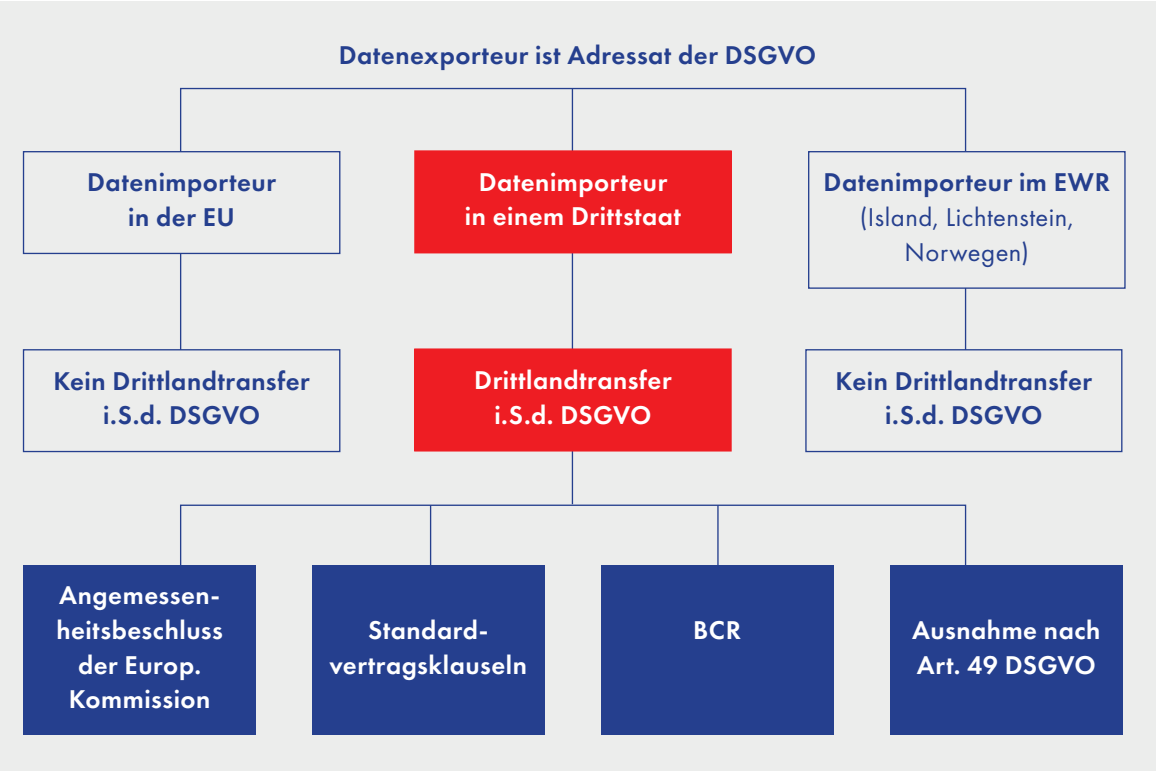
4 https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_de.
5 https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en.

die Ansicht, dass eine Übermittlung basierend auf einer der Ausnahmen nur in Betracht kommt, wenn es sich um vereinzelte Datenübermittlungen handelt, nicht jedoch bei regelmäßigen Datentransfers ins Drittland. Es ist zumindest streitbar, ob eine entsprechend restriktive Auslegung gerechtfertigt ist. Dennoch besteht eine gewisse rechtliche Unsicherheit, sodass in der Praxis eine besondere Prüfung erforderlich ist, wenn ein Datentransfer auf eine der Ausnahmen des Art. 49 DSGVO gestützt werden soll.

Praxistipp: Bevor ein Drittlandtransfer auf eine der Ausnahmen des Art. 49 DSGVO gestützt wird, sollte geprüft werden, ob eines der anderen Instrumente, insbesondere die Standardvertragsklauseln, in Betracht kommen. Ferner ist insbesondere bei der Einwilligung darauf zu achten, dass die strengen Anforderungen der DSGVO an eine Einwilligung (Transparenz, Freiwilligkeit) erfüllt werden.

ZUSAMMENFASSUNG DER INSTRUMENTE

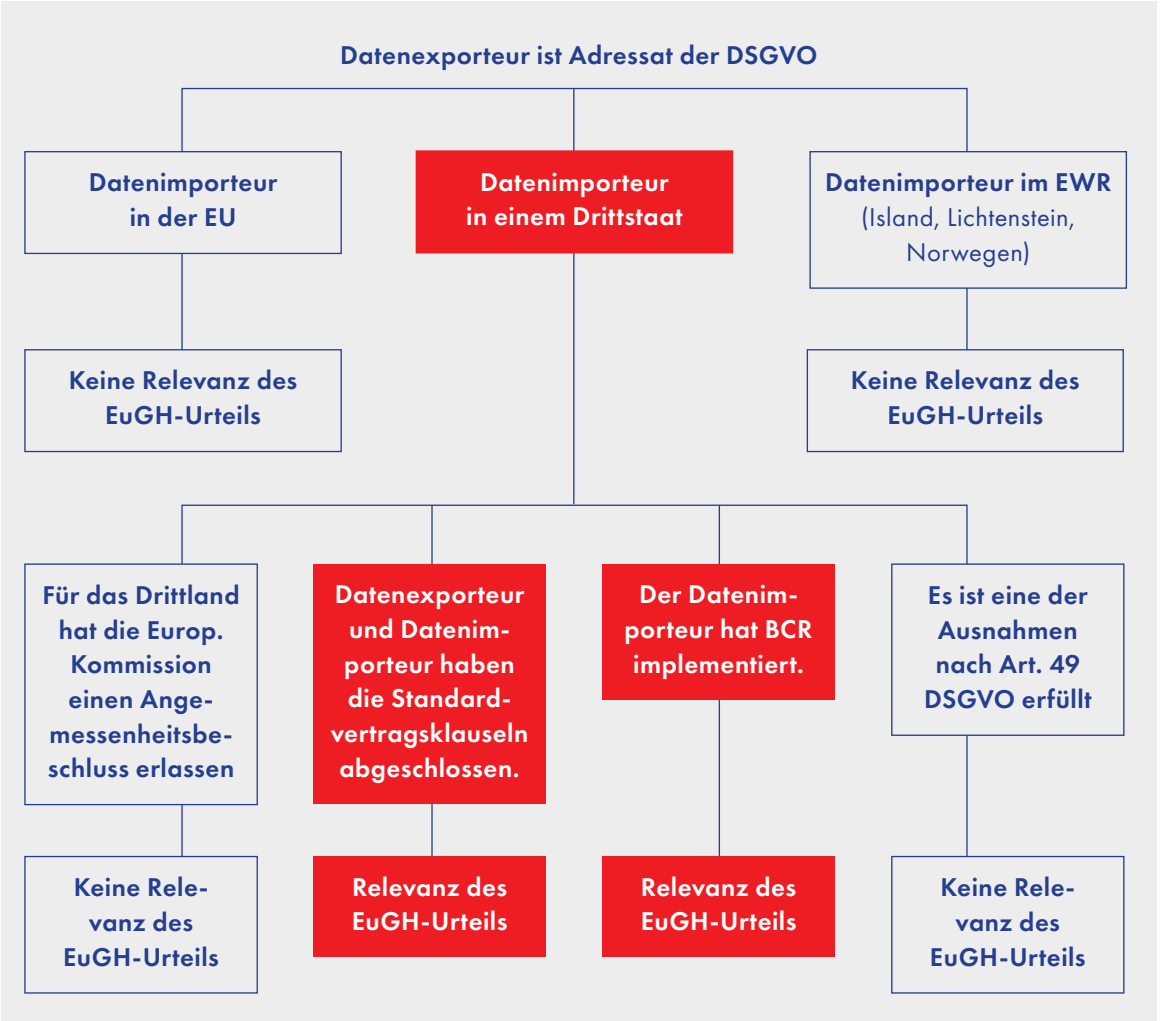
Die folgenden Instrumente können eine Datenübermittlung an einen Datenimporteur im Drittland absichern:



RELEVANZ DES EUGH-URTEILS FÜR DIE DATENÜBERMITTLUNG

Das Urteil des EuGH hat nicht für jede der oben dargestellten Datenübermittlungen in Drittländer Auswirkungen. Betroffen sind ausschließlich solche Transfers, bei denen der Datenimporteur in einem Staat ansässig ist, der aus Sicht des EU-Datenschutzrechts kein angemessenes (= mit dem Standard des EU-Rechts vergleichbares) Datenschutzniveau bietet. Zu unterscheiden sind insofern die folgenden Konstellationen:

- **Der Datenimporteur ist in einem Mitgliedstaat der EU ansässig:** Es liegt keine Drittlandübermittlung im Sinne der DSGVO vor. Für den Datenimporteur gilt die DSGVO. Das EuGH-Urteil hat keine Relevanz für den Transfer.
- **Der Datenimporteur ist in einem Staat des EWR ansässig:** Es liegt keine Drittlandübermittlung im Sinne der DSGVO vor. Für den Datenimporteur gilt die DSGVO. Das EuGH-Urteil hat keine Relevanz für den Transfer.
- **Der Datenimporteur ist in einem Staat ansässig, für den die Europäische Kommission einen Angemessenheitsbeschluss erlassen hat:** Es liegt eine Drittlandübermittlung im Sinne der DSGVO vor. Durch den Angemessenheitsbeschluss bedarf es aber keiner weiteren Schutzmaßnahmen. Das EuGH-Urteil hat keine Relevanz für den Transfer.
- **Der Datenimporteur ist in einem sonstigen Drittstaat ansässig:** Es liegt eine Drittlandübermittlung im Sinne der DSGVO vor. Es bedarf Schutzmaßnahmen nach der DSGVO, um die Datenübermittlung abzusichern.
  - **Der Datentransfer wird mit den Standardvertragsklauseln abgesichert:** Das EuGH-Urteil hat Relevanz für den Transfer.
  - **Der Datentransfer wird mit BCR abgesichert:** Das EuGH-Urteil hat Relevanz für den Transfer.
  - **Der Datentransfer wird mit einer Ausnahme nach Art. 49 DSGVO abgesichert:** Das EuGH-Urteil hat keine Relevanz für den Transfer.



Die Übersicht zeigt, dass das EuGH-Urteil bei der Absicherung von Drittlandtransfers basierend auf Standardvertragsklauseln sowie verbindlichen internen Datenschutzvorschriften Relevanz hat. Da die verbindlichen internen Datenschutzvorschriften in der Praxis nur in sehr begrenzten Fällen in Betracht kommen, beschränkt sich die folgende Darstellung auf die Auswirkungen des EuGH-Urteils auf die Verwendung der Standardvertragsklauseln.

UMGANG MIT DEM EUGH URTEIL BEI DER DATENÜBERMITTLUNG INS DRITTLAND

Bei der Umsetzung der Vorgaben des EuGH zum Drittlandtransfer bieten insbesondere die Empfehlungen des Europäischen Datenschutzausschusses („EDSA"), dem Zusammenschluss aller EU-Datenschutzbehörden, Hilfestellung (siehe hierzu unter Abschnitt A.V.1.). Einige der Vorgaben haben auch bereits Einzug in die neuen Standardvertragsklauseln erhalten (siehe hierzu unter Abschnitt A.V.3.).

EMPFEHLUNGEN DES EUROPÄISCHEN DATENSCHUTZAUSSCHUSSES („EDSA")

Der Europäische Datenschutzausschusses („EDSA") hat im Zusammenhang mit dem Drittlandtransfer zwei Empfehlungen veröffentlicht:

1. Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten[6]
2. Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen[7]

Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten

Die Empfehlungen 01/2020 enthalten einen 6-Stufen-Plan zur Identifizierung und Evaluierung von Datentransfers (siehe hierzu unter Abschnitt A.V.1.a)aa)) sowie Beispiele für mögliche Zusatzmaßnahmen zur Absicherung von Datentransfers in Drittländer (siehe hierzu unter Abschnitt A.V.1.a) bb)). Im Rahmen der Beispiele nennt der EDSA auch verschiedene Fallkonstellationen, in denen Zusatzmaßnahmen einen Drittlandtransfer absichern können sowie Fälle in denen „aus Sicht des EDSA" keine Zusatzmaßnahmen zur Verfügung stehen, die eine ausreichende Absicherung bieten.

6-Stufen-Plan zur Identifizierung und Evaluierung von Datentransfers

Der 6-Stufen-Plan des EDSA unterteilt sich in die folgenden Schritte:

Stufe 1: Datentransfers identifizieren

Werden personenbezogene Daten an Empfänger übermittelt?
→ Ist dies nicht der Fall, ist die Prüfung abgeschlossen.

Wo verarbeiten diese Empfänger die Daten (in der EU, im EWR oder in Drittländern)?
→ Bei der Übermittlung der Daten an Empfänger in der EU/des EWR ist die Prüfung abgeschlossen. Ansonsten ist auf der nächsten Stufe zu prüfen, welche Übermittlungsinstrumente den Transfer absichern.

Stufe 2: Übermittlungsinstrumente

Welche Instrumente werden eingesetzt, um den Datentransfer an den Empfänger im Drittland abzusichern, insbesondere Angemessenheitsbeschluss, Standardvertragsklauseln, verbindliche interne Datenschutzvorschriften, Ausnahmen nach Art. 49 DSGVO?
→ Sofern der Transfer auf Standardvertragsklauseln oder verbindlichen internen Datenschutzvorschriften beruht, ist im nächsten Schritt die Wirksamkeit dieser Instrumente im konkreten Fall zu bewerten.

6 https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_de.
7 https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_de.

Stufe 3: Beurteilung der Wirksamkeit des ausgewählten Übermittlungsinstruments im Hinblick auf die Gesamtumstände der Übermittlung

Wird die Wirksamkeit des gewählten Übermittlungsinstruments durch Vorschriften des nationalen Rechts im Land des Datenimporteurs beeinträchtigt?

Zu prüfen ist, ob das nationale Recht die wesentlichen Garantien des EU-Rechts gewährleistet. Der Prozess wird als „Transfer Impact Assessment" bezeichnet. Er stellt die Parteien in der Praxis vor erhebliche Schwierigkeiten. Faktisch bedeutet die Durchführung eines Transfer Impact Assessment die Prüfung der konkreten rechtlichen Vorschriften im relevanten Drittland in Bezug auf den konkreten Transfer. Anhaltspunkte an den Prüfungsumfang bieten die Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen (siehe hierzu unten unter Abschnitt A.V.1.b)). Die Prüfung kann zu folgenden Ergebnissen führen:

1. Das gewählte Übermittlungsinstrument kann wirksam gewährleisten, dass die übermittelten personenbezogenen Daten in dem Drittland ein Schutzniveau genießen, das dem im EWR garantierten Niveau der Sache nach gleichwertig ist. Die Regelungen des Drittlandes stehen der Einhaltung dieses Schutzniveaus durch den Datenimporteur nicht entgegen.
   → Eine Datenübermittlung ist möglich.

2. Das gewählte Übermittlungsinstrument kann nicht wirksam gewährleisten, dass die übermittelten personenbezogenen Daten in dem Drittland ein Schutzniveau genießen, das dem im EWR garantierten Niveau der Sache nach gleichwertig ist. Die Regelungen des Drittlandes stehen der Einhaltung dieses Schutzniveaus durch den Datenimporteur entgegen.
   → Es müssen zusätzliche Schutzmaßnahmen implementiert werden, um den Datentransfer zu ermöglichen (siehe hierzu unter Abschnitt A.V.1.a)aa)(4)).

Aufgrund der Komplexität der Prüfung kann es in Einzelfällen praktikabler sein, direkt ein unzureichendes Schutzniveau anzunehmen und mit Stufe 4 fortzufahren.

Stufe 4: Zusätzliche Schutzmaßnahmen

Welche zusätzlichen vertraglichen, technischen oder organisatorischen Maßnahmen kommen in Betracht, um den Datentransfer ausreichend abzusichern?

Kommt man im Rahmen der Stufe 3 zu dem Schluss, dass das gewählte Übermittlungsinstrument nicht wirksam gewährleisten kann, dass die übermittelten personenbezogenen Daten in dem Drittland ein Schutzniveau genießen, das dem im EWR garantierten Niveau der Sache nach gleichwertig ist, so sind zusätzliche Schutzmaßnahmen zu ergreifen, um den Drittlandtransfer zu rechtfertigen. Solche Maßnahmen können grundsätzlich technischer (z.B. Verschlüsselung), vertraglicher oder organisatorischer Natur sein (siehe hierzu unter Abschnitt A.V.1.a)bb)).

Wenngleich sich dies nicht direkt aus der EuGH-Entscheidung „Schrems II" ergibt, sind nach Ansicht des EDSA organisatorische Maßnahmen allein nicht ausreichend, um ein angemessenes Schutzniveau sicherzustellen. Es bedarf nach Ansicht der Aufsichtsbehörden immer auch technischer Maßnahmen, die die Einhaltung der EU-Garantien im Drittland sicherstellen. Der EDSA zeigt ferner verschiedene Fallbeispiele auf, in denen angemessene Zusatzmaßnahmen seiner Ansicht nach in Betracht kommen oder nicht (siehe hierzu unter Abschnitt A.V.1.a)bb)).

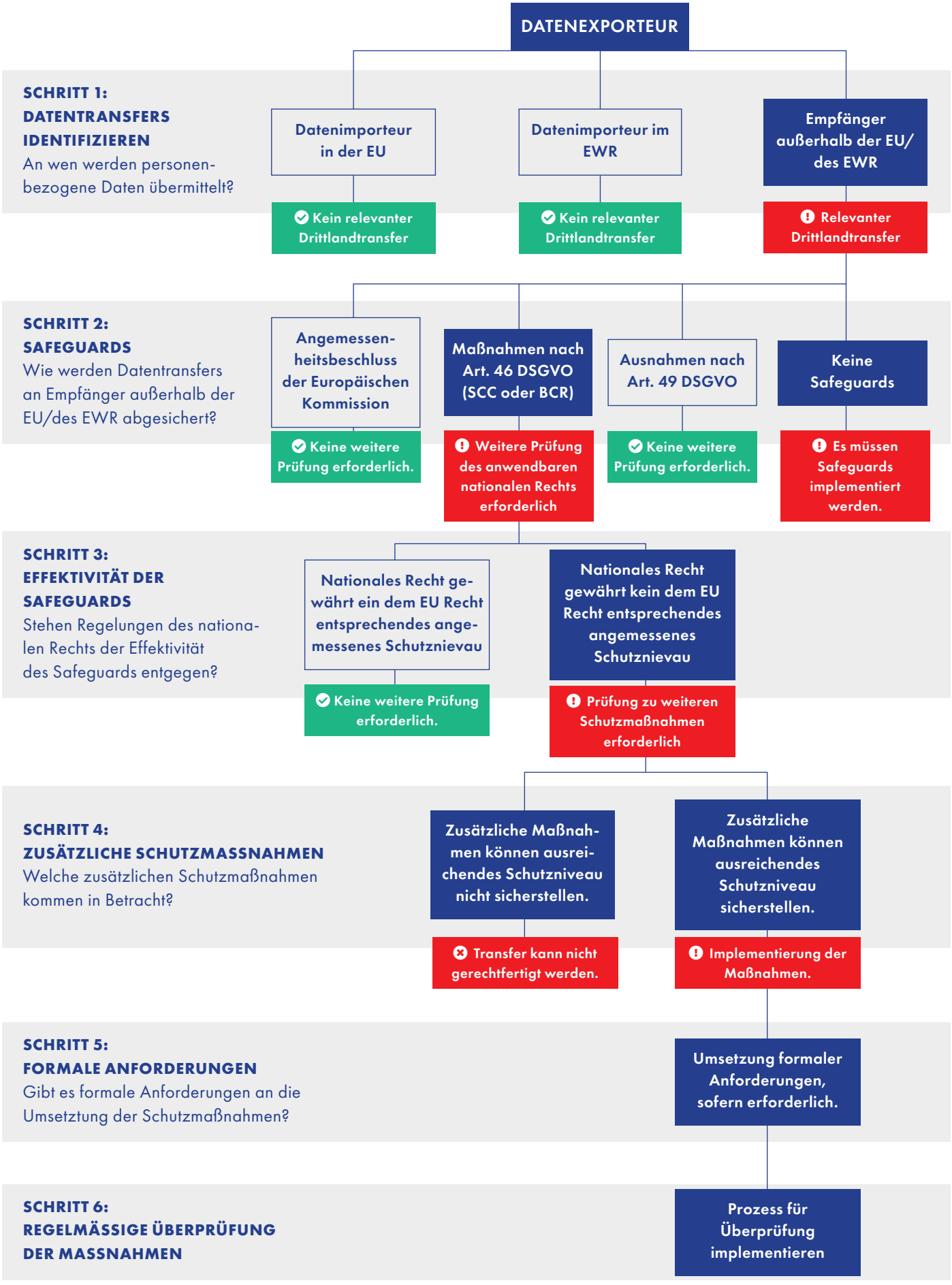
Stufe 5: Formale Anforderungen umsetzen

Müssen bei der Umsetzung der Zusatzmaßnahmen formale Anforderungen beachtet werden?

Im Einzelfall kann eine Genehmigung durch die Datenschutzaufsichtsbehörden erforderlich werden, um den Drittlandtransfer durchzuführen. Bei der Ergänzung von zusätzlichen Schutzmaßnahmen in den Standardvertragsklauseln bedarf es in der Regel jedoch keiner separaten Genehmigung durch die zuständige Datenschutzaufsichtsbehörde.

Stufe 6: Regelmäßige Überprüfung

Die Bewertung des Drittlandtransfers muss in regelmäßigen Abständen überprüft werden.


DATENEXPORTEUR
SCHRITT 1:
DATENTRANSFERS IDENTIFIZIEREN
An wen werden personenbezogene Daten übermittelt?
Datenimporteur in der EU
Datenimporteur im EWR
Empfänger außerhalb der EU/ des EWR
Kein relevanter Drittlandtransfer
Kein relevanter Drittlandtransfer
Relevanter Drittlandtransfer
SCHRITT 2:
SAFEGUARDS
Wie werden Datentransfers an Empfänger außerhalb der EU/des EWR abgesichert?
Angemessenheitsbeschluss der Europäischen Kommission
Maßnahmen nach Art. 46 DSGVO (SCC oder BCR)
Ausnahmen nach Art. 49 DSGVO
Keine Safeguards
Keine weitere Prüfung erforderlich.
Weitere Prüfung des anwendbaren nationalen Rechts erforderlich
Keine weitere Prüfung erforderlich.
Es müssen Safeguards implementiert werden.
SCHRITT 3:
EFFEKTIVITÄT DER SAFEGUARDS
Stehen Regelungen des nationalen Rechts der Effektivität des Safeguards entgegen?
Nationales Recht gewährt ein dem EU Recht entsprechendes angemessenes Schutznievau
Nationales Recht gewährt kein dem EU Recht entsprechendes angemessenes Schutznievau
Keine weitere Prüfung erforderlich.
Prüfung zu weiteren Schutzmaßnahmen erforderlich
SCHRITT 4:
ZUSÄTZLICHE SCHUTZMASSNAHMEN
Welche zusätzlichen Schutzmaßnahmen kommen in Betracht?
Zusätzliche Maßnahmen können ausreichendes Schutzniveau nicht sicherstellen.
Zusätzliche Maßnahmen können ausreichendes Schutzniveau sicherstellen.
Transfer kann nicht gerechtfertigt werden.
Implementierung der Maßnahmen.
SCHRITT 5:
FORMALE ANFORDERUNGEN
Gibt es formale Anforderungen an die Umsetztung der Schutzmaßnahmen?
Umsetzung formaler Anforderungen, sofern erforderlich.
SCHRITT 6:
REGELMÄSSIGE ÜBERPRÜFUNG DER MASSNAHMEN
Prozess für Überprüfung implementieren

Beispiele für Zusatzmaßnahmen

Der EDSA bietet in seinen Empfehlungen 01/2020 Hilfestellung zu den möglichen zusätzlichen Schutzmaßnahmen. In Betracht kommen vertragliche, organisatorische und technische Maßnahmen. In den folgenden Beispielen ist der Datentransfer in Drittländer nach Ansicht des EDSA gerechtfertigt, auch wenn Stufe 3 der Prüfung ergeben hat, dass die Regelungen des Drittlandes der Einhaltung des erforderlichen Schutzniveaus durch den Datenimporteur entgegenstehen, da in diesen Fällen ausreichend wirksame Zusatzmaßnahmen ergriffen wurden:

- **Fallbeispiel 1: Die Daten werden im Drittland gespeichert, sie sind jedoch nach dem Stand der Technik verschlüsselt und die Hoheit über den Schlüssel liegt beim Datenexporteur in der EU/EWR, sodass der Datenimporteur keinen Zugriff auf unverschlüsselte Daten hat.**

  In der Praxis ist eine solche Konstellation „wenn überhaupt" regelmäßig nur bei der Übermittlung von Daten zur Backup-Sicherung relevant. In den wenigsten Fällen ermöglichen die Anbieter jedoch, dass der Verschlüsselungsschlüssel ausschließlich beim Exporteur verbleibt.

- **Fallbeispiel 2: Der Datenexporteur übermittelt ausschließlich pseudonyme Daten (die der Datenimporteur also nicht mehr identifizierbaren Personen zuordnen kann) und der Datenimporteur hat keine Möglichkeit der De-Pseudonymisierung.**

  Abhängig vom konkreten Zweck der Datenübermittlung benötigt der Datenimporteur in der Regel Zugriff auf sog. „Klardaten", sodass die Übermittlung von pseudonymisierten Daten nur ausnahmsweise in Betracht kommen wird.

- **Fallbeispiel 3: Die Daten „durchlaufen" das Drittland nur im Transit und sind ferner nach dem Stand der Technik verschlüsselt, wobei die Hoheit über den Schlüssel wiederum beim Datenexporteur liegt, sodass der Datenimporteur keinen Zugriff auf unverschlüsselte Daten hat.**

  In der Praxis kommt diese Konstellation so gut wie nie vor.

- **Fallbeispiel 4: Die Daten werden an einen Datenexporteur übermittelt, der nach dem Recht des betreffenden Landes besonderen Schutz genießt.**

  Die Bewertung hängt wiederum eng mit der Prüfung des nationalen Rechts in Stufe 3 des Stufenplans zusammen. In Ausnahmefällen kann dies Konstellation einschlägig sein, z.B. bei Übermittlungen an Empfänger, die einer besonderen Berufsgruppe angehören, die spezifischen beruflichen Pflichten unterliegen (z.B. Ärzte, Rechtsanwälte). Bei den meisten Dienstleistern im Drittland wird die Ausnahme jedoch irrelevant sein.

- **Fallbeispiel 5: Die Daten werden „aufgeteilt" und an verschiedene Empfänger übermittelt, wobei jeder Empfänger mit dem erhaltenen Datensatz allein keinen Rückschluss auf die betroffenen Personen ziehen kann. Die Ergebnisse fügt der Datenexporteur selbst zusammen.**

  In der Praxis kommt diese Konstellation so gut wie nie vor.

  Der EDSA hat daneben zwei Fallbeispiele aufgeführt, die nach Ansicht des EDSA auch bei der Implementierung entsprechender technischer Maßnahmen nicht gerechtfertigt werden können. Hierbei handelt es sich um die in der Praxis mit Abstand relevantesten Konstellationen:

Fallbeispiel 6: Die Daten werden an einen Datenimporteur übermittelt, der Zugriff auf unverschlüsselte Daten benötigt.

Es gibt kaum Dienstleister, die ihren Service ausschließlich basierend auf verschlüsselten oder pseudonymisierten Daten anbieten (können). Ein weit überwiegender Teil der Dienstleister im Drittland fällt daher in diese Kategorie.

Fallbeispiel 7: Die Daten werden an ein anderes Unternehmen derselben Unternehmensgruppe zu gemeinsamen Geschäftszwecken übermittelt.

In der Praxis kommt eine konzerninterne Datenübermittlung regelmäßig vor und ist daher besonders relevant.

Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen

Die Empfehlungen 02/2020 bieten Hilfestellungen für die Prüfung, ob das nationale Recht im Land des Datenimporteurs ein angemessenes Schutzniveau bietet (Stufe 3 des 6-Stufen-Plans des EDSA, siehe oben unter Abschnitt A.V.1.a)aa)(3)). Die Hilfestellung orientiert sich dabei den vier wesentlichen Garantien im EU-Recht, die eingehalten werden müssen, um einen Eingriff bzw. eine Einschränkung der Rechte und Freiheiten der Betroffenen zu rechtfertigen:

- Die durch die Sicherheitsbehörden im Drittland vorgenommene Datenverarbeitung muss auf klaren, präzisen und zugänglichen Vorschriften beruhen.
- Die durch die Sicherheitsbehörden im Drittland vorgenommene Datenverarbeitung muss erforderlich und angemessen sein im Hinblick auf die verfolgten legitimen Ziele.
- Es muss ein unabhängiger Aufsichtsmechanismus bezüglich der Datenverarbeitung der Sicherheitsbehörde bestehen.
- Dem Betroffenen müssen wirksame Rechtsbehelfe zur Verfügung stehen, um sich gegen Eingriffe zu verteidigen bzw. diese überprüfen zu lassen.

Die Durchführung der Prüfung unter Berücksichtigung der entsprechenden Garantien erfordert umfangreiche Kenntnisse des nationalen Rechts und

kann daher in der Regel nur durch einen Juristen aus der jeweiligen Jurisdiktion sinnvoll durchgeführt werden. Je nach Zahl der Drittlandtransfers müssen Unternehmen hier einen sinnvollen Ansatz finden, der ein ausreichendes Maß an Datenschutz-Compliance bei vertretbarem Aufwand gewährleistet.

DARSTELLUNG DER SICHTWEISE DER DATENSCHUTZBEHÖRDEN

Innerhalb Europas haben neben dem EDSA zahlreiche Aufsichtsbehörden Stellungnahmen zum EuGH-Urteil in der Sache *Schrems II* abgegeben. Dabei sind unterschiedliche Strömungen auszumachen. Einige Datenschutzaufsichtsbehörden (darunter z.B. Berlin) legen die Entscheidung sehr streng aus und folgen auch der sehr restriktiven Bewertung des EDSA zu den verschiedenen Konstellationen. Faktisch ist nach Ansicht der Datenschutzaufsichtsbehörde Berlin daher eine Datenübermittlung ins Drittland außerhalb der vom EDSA dargestellten Fallbeispiele kaum zu rechtfertigen. Andere Datenschutzaufsichtsbehörden (z.B. Baden-Württemberg) scheinen einen weniger strengen Ansatz zu verfolgen und berücksichtigen auch die wirtschaftliche Relevanz der Datentransfers, wonach die Unterbindung von Drittlandtransfers erhebliche negative Auswirkungen haben könnte.

UMSETZUNG DER ANFORDERUNGEN DES EUGH IM RAHMEN DER NEUEN STANDARDVERTRAGSKLAUSELN

Wie der EuGH in seinem Urteil festgestellt und der EDSA in seinen Empfehlungen ebenfalls betont hat, ist der Abschluss der Standardvertragsklauseln allein nicht ausreichend, um Datentransfers in Drittländer abzusichern. Vielmehr müssen die Parteien sicherstellen, dass das nationale Recht im Land des Datenimporteurs der Einhaltung der Regelungen aus den Standardvertragsklauseln nicht entgegensteht. Das gilt sowohl für Datenübermittlungen, die noch über die „alten“ Standardvertragsklauseln abgesichert werden als auch solche, für die die „neuen“ Standardvertragsklauseln abgeschlossen wurden. Die neuen Standardvertragsklauseln sehen für diese Prüfung einen konkreten Prozess vor, in dem die Parteien insbesondere folgende Aspekte zu berücksichtigen haben[8]:

- die besonderen Umstände der Übermittlung, einschließlich der Länge der Verarbeitungskette, der Anzahl der beteiligten Akteure und der verwendeten Übertragungskanäle, beabsichtigte Datenweiterleitungen, die Art des Empfängers, den Zweck der Verarbeitung, die Kategorien und das Format der übermittelten personenbezogenen Daten, den Wirtschaftszweig, in dem die Übertragung erfolgt, den Speicherort der übermittelten Daten (Stufe 3 des 6-Stufen-Plans des EDSA, siehe oben unter Abschnitt A.V.1.a) aa)(3)),
- die angesichts der besonderen Umstände der Übermittlung relevanten Rechtsvorschriften und Gepflogenheiten des Bestimmungsdrittlandes (einschließlich solcher, die die Offenlegung von Daten gegenüber Behörden vorschreiben oder den Zugang von Behörden zu diesen Daten gestatten) sowie die geltenden Beschränkungen und Garantien (Stufe 3 des 6-Stufen-Plans des EDSA, siehe oben unter Abschnitt A.V.1.a)aa)(3)), sowie
- alle relevanten vertraglichen, technischen oder organisatorischen Garantien, die zur Ergänzung der Garantien gemäß den Klauseln eingerichtet wurden, einschließlich Maßnahmen, die während der Übermittlung und bei der Verarbeitung personenbezogener Daten im Bestimmungsland angewandt werden (Stufe 4 des 6-Stufen-Plans des EDSA, siehe oben unter Abschnitt A.V.1.a) aa)(4)).

Daneben enthalten die neuen Standardvertragsklauseln in Klausel 15 bereits konkrete Verpflichtungen für den Datenimporteur, wie er mit Zugriffen nationaler Behörden im Drittland umzugehen hat. In dieser Klausel spiegeln sich ebenfalls die Empfehlungen des EDSA wider. Die Formulierung der Klauseln 14 und 15 legt insofern nahe, dass ein risikobasierter Ansatz vertretbar erscheint, wonach bei der Bewertung des Drittlandtransfers zu berücksichtigen ist, inwiefern der Datenimporteur in der Vergangenheit überhaupt Adressat von Zugriffen durch nationale Behörden war und ob sich daraus für die Zukunft eine entsprechende Gefahr ergibt.

8 Vgl. Klausel 14 der Standardvertragsklauseln.

PRAXISTIPPS ZUR VERWENDUNG VON STANDARDVERTRAGSKLAUSEN

In der Praxis ist die Nutzung der Standardvertragsklauseln als Übermittlungsinstrument besonders relevant. Im Folgenden sollen die neuen Standardvertragsklauseln daher etwas näher beleuchtet werden:

STRUKTUR DER STANDARDVERTRAGSKLAUSELN

Die Europäische Kommission hat im Juni 2021 Standardvertragsklauseln zur Absicherung von Datenübermittlungen in Drittländer veröffentlicht. Die Standardvertragsklauseln sind nicht „wie bei den bisherigen Standardvertragsklauseln" in separate Vertragsklauseln unterteilt, sondern folgen einem „Baukastensystem", das die unterschiedlichen Konstellationen abdeckt. Die Standardvertragsklauseln bestehen somit aus vier verschiedenen Modulen:

- Modul 1: Übermittlung von einem Verantwortlichen an einen Verantwortlichen

  Wie bereits die alten Standardvertragsklauseln enthalten auch die neuen Klauseln ein Modul für die Datenübermittlung von einem Verantwortlichen[9] an einen Verantwortlichen. Dieses Modul ist immer dann relevant, wenn der Datenimporteur die Daten zu eigenen Zwecken verarbeiten soll.
  Beispiel: Der Datenexporteur übermittelt Personaldaten an die Muttergesellschaft in den USA, damit diese eine Bewertung der Mitarbeiterleistungen durchführen kann.

- Modul 2: Übermittlung von einem Verantwortlichen an einen Auftragsverarbeiter

  Die Konstellation des Modul 2 gab es ebenfalls bereits unter den alten Standardvertragsklauseln und stellt den in der Praxis wohl relevantesten Fall der Drittlandübermittlung dar. Erfasst sind alle Fälle, in denen der Empfänger Daten des Exporteurs ausschließlichen in dessen Auftrag und auf dessen Weisung verarbeitet.[10]
  Beispiel: Der Datenexporteur beauftragt einen Dienstleister zur Erbringung von Analysediensten in den USA oder der Datenexporteur speichert Daten bei einem Hosting-Anbieter in China.

- Modul 3: Übermittlung von einem Auftragsverarbeiter an einen Auftragsverarbeiter

  Die neuen Standardvertragsklauseln bilden in Modul 3 die in der Praxis häufig relevante Konstellation einer Datenübermittlung von einem Auftragsverarbeiter an einen (Unter-)Auftragsverarbeiter ab.
  Beispiel: Der Datenexporteur bietet Hosting-Dienste gegenüber seinen Kunden (= Verantwortliche der Datenverarbeitung) an und bedient sich dafür eines Cloud-Anbieters im Drittland (=Unterauftragsverarbeiter).

- Modul 4: Übermittlung von einem Auftragsverarbeiter an einen Verantwortlichen

  Das Modul 4 ist in der Praxis nur begrenzt relevant. Erfasst werden sollen solche Konstellationen, in denen der Verantwortliche im Drittland ansässig ist und einen Auftragsverarbeiter in der EU mit der Datenverarbeitung beauftragt. Der Auftragsverarbeiter muss dabei regelmäßig die Daten, die er im Auftrag des Verantwortlichen verarbeitet an diesen (zurück) übermitteln, sodass wiederum ein Drittlandtransfer gegeben ist.
  Beispiel: Verantwortlicher ist in den USA ansässig und beauftragt Auftragsverarbeiter in der EU, Datenanalysen durchzuführen. Der Auftragsverarbeiter übermittelt die Daten im Anschluss zurück an den Auftraggeber in den USA.

Zusammenfassung

9 Verantwortliche bestimmen die Zwecke und Mittel der Datenverarbeitung allein gemeinsam mit anderen.
10 Auftragsverarbeiter verarbeiten personenbezogene Daten im Auftrag und auf Weisung des Verantwortlichen.

UMSETZUNG DER VORGABEN IN DER PRAXIS

Die folgende Checkliste bietet eine grobe Orientierung bei der Überprüfung, inwiefern Vorgaben des Drittlandtransfers für Ihr Unternehmen relevant sind und welche Schritte sie ergreifen müssen:

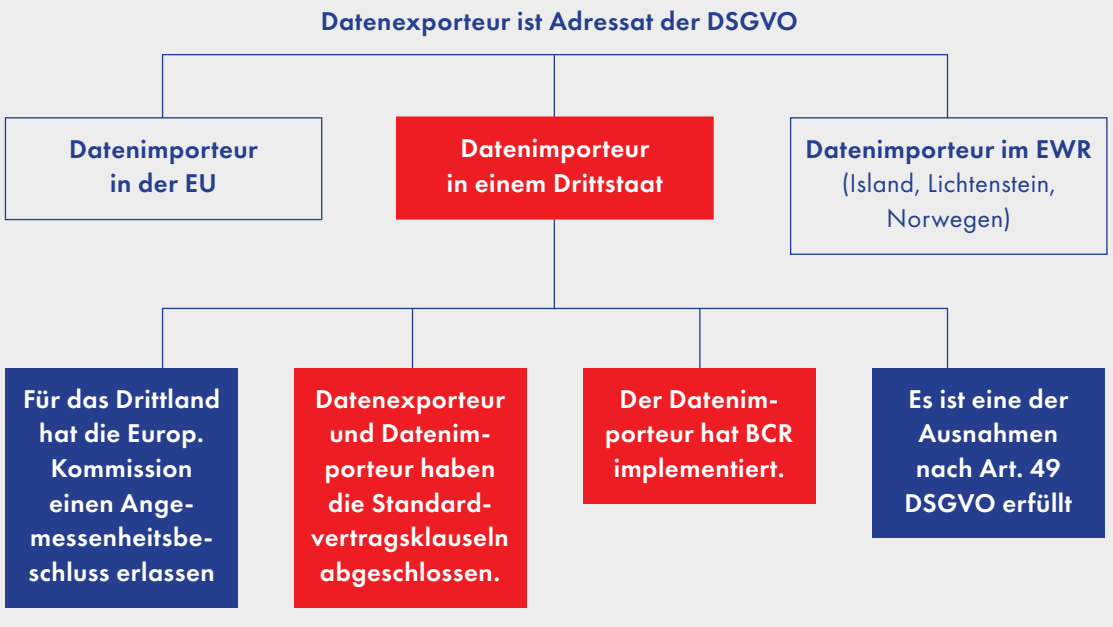
DATA MAPPING

Die Datenflüsse des Unternehmens müssen identifiziert werden. Dieser Schritt ist zwingende Grundlage für die Bewertung möglicher Drittlandtransfers. Nur wenn bekannt ist, an wen Ihr Unternehmen personenbezogene Daten übermittelt, kann eine weitere Prüfung stattfinden. Ausgangspunkt kann hier das sogenannte „Verarbeitungsverzeichnis“ nach Art. 30 DSGVO sein, falls ein solches vorliegt. In diesem müssen regelmäßig alle Datenverarbeitungsvorgänge im Unternehmen detailliert beschrieben werden.

Als Ergebnis des data mapping sollten folgende Informationen vorliegen:

Name des Empfängers	Adresse des Empfängers	Ort der Datenverarbeitung	Bei Datenverarbeitung außerhalb des EWR: Übermittlungsinstrument
		Verarbeitet der Datenimporteur die Daten außerhalb des EWR? Wenn ja, in welchem Land?	› Angemessenheitsbeschluss › Standardvertragsklauseln › BCR › Ausnahmen nach Art. 49 DSGVO

Anhand des data mapping sind solche Datenübermittlungen herauszufiltern, bei denen (1) der Datenimporteur die Daten außerhalb des EWR verarbeitet und (2) die Datenübermittlung mit Standardvertragsklauseln (oder BCR) abgesichert werden.



DURCHFÜHRUNG EINES TRANSFER IMPACT ASSESSMENT

Für Datentransfers, bei denen sich ergibt, dass die Übermittlung auf Standardvertragsklauseln (oder BCR) gestützt werden, muss ein Transfer Impact Assessment durchgeführt werden. Das bedeutet, es muss geprüft werden, ob das nationale Recht im Staat des Datenimporteurs die Wirksamkeit des gewählten Übermittlungsinstruments beeinfluss, sodass kein angemessenes Datenschutzniveau gewährleistet werden kann.

Für das Transfer Impact Assessment gelten die Ausführungen zu Stufe 3 des 6-Stufen-Plans des EDSA (siehe hierzu Abschnitt A.V.1.a)aa)(3)).

In der Regel bedarf es hier Unterstützung eines Juristen aus der jeweiligen Jurisdiktion. Mittelfristig ist zu erwarten, dass Dienstleister ihrerseits eine Bewertung vornehmen und diese dem Datenexporteur zur Verfügung stellen. Bis dahin hängt der Umfang des Transfer Impact Assessment von den verfügbaren Ressourcen sowie der Bewertung des faktischen Risikos ab. Wenn kein Transfer Impact Assessment durchgeführt werden kann, oder dieses zu unklaren Ergebnissen führt, ist von einem mangelnden Schutzniveau beim Datenimporteur auszugehen.

IDENTIFIZIERUNG ETWAIGER ZUSATZMASSNAHMEN

Basierend auf dem Transfer Impact Assessment sind etwaige Zusatzmaßnahmen zu bestimmen. Wie bereits ausgeführt, ist nach Ansicht des EDSA bei den on der Praxis besonders relevanten Fällen eine Datenübermittlung in der Regel nicht zu rechtfertigen. Die Standardvertragsklauseln lassen jedoch wohl stärker als die Richtlinien des EDSA – Raum für eine risikobasierte Bewertung. Jedes Unternehmen sollte ferner überlegen, inwiefern pragmatische Lösungen in Betracht kommen, die wenngleich sie nicht in gleicher Art und Weise Rechtssicherheit bieten, einen Umgang mit Drittlandtransfers in der Praxis erleichtern (z.B. einheitliche Zusatzmaßnahmen für sämtliche Drittlandtransfers).

ABSCHLUSS DER NEUEN STANDARDVERTRAGSKLAUSELN

Neue Datentransfers können ab dem 27. September 2021 regelmäßig nur noch mit den neuen Standardvertragsklauseln abgesichert werden. Etwaige interne Prozesse sind entsprechend umzustellen.

Für bestehende Datentransfers basierend auf den alten Standardvertragsklauseln müssen die alten Standardvertragsklauseln bis einschließlich 26. Dezember 2022 ausgetauscht werden.

ZUSAMMENFASSUNG

SCHRITT 1:
Relevante Datentransfers identifizieren

SCHRITT 2:
Transfer Impact Assessment durchführen

SCHRITT 3:
Sofern erforderlich: Zusatzmaßnahmen implementieren

SCHRITT 2:
Sofern erforderlich: Bestehende Standardvertragsklauseln bis 26. Dezember 2022 auf die neuen Standardvertragsklauseln umstellen

Alle Schritte dokumentieren

STIFTUNG DATENSCHUTZ

Stiftung Datenschutz
rechtsfähige Stiftung bürgerlichen Rechts
Karl-Rothe-Straße 10–14
04105 Leipzig
Deutschland

Telefon 0341 / 5861 555-0
mail@stiftungdatenschutz.org
www.stiftungdatenschutz.org

gestiftet von der Bundesrepublik Deutschland
vertreten durch den Vorstand Frederick Richter

Die Arbeit der Stiftung Datenschutz wird aus dem Bundeshaushalt gefördert (Einzelplan des BMI).

Bundesministerium des Innern, für Bau und Heimat