

Drittlandsübertragung von personenbezogenen Daten

Die neuen Standardvertragsklauseln (SCC) sollen mehr Sicherheit beim Datentransfer in ein Drittland ohne Angemessenheitsbeschluss schaffen. Jedoch herrscht Unsicherheit, wie dies in der Praxis datenschutzkonform umzusetzen ist und wie die damit einhergehenden datenschutzrechtlichen Herausforderungen gemeistert werden sollen.

Historie oder was bisher geschah

Bereits mit der Datenschutzrichtlinie 95/46/EG war es verboten, personenbezogene Daten (pbD) aus EU-Staaten in einen Drittstaat, also einen Staat außerhalb der EU, zu übertragen, wenn das Schutzniveau des Drittstaates nicht mit dem der EU vergleichbar war.

Daher galt bis 2015 das Safe-Harbour-Abkommen zwischen der EU und den USA. Es regelte die Einhaltung der Datenschutzgrundsätze durch US-Unternehmen. Dies geschah durch einen Eintrag auf die entsprechende Liste des US-Handelsministeriums (<http://safeharbor.export.gov/list.aspx>). Dadurch sollte eine Äquivalenz des Datenschutzniveaus in dem jeweiligen US-Unternehmen zum europäischen Datenschutz hergestellt werden und den Unternehmen die Übermittlung von personenbezogenen Daten aus der Europäischen Union in die USA ermöglicht werden.

Durch das Schrems-I-Urteil vom 6. Oktober 2015 wurde das Abkommen jedoch für nicht bindend und ungültig erklärt. In der Folge waren die US-Unternehmen, auch wenn sie sich der Einhaltung unterworfen hatten, verpflichtet,

personenbezogene Daten jederzeit an die Sicherheitsbehörden herauszugeben. Daraufhin wurde das Privacy-Shield-Abkommen als Angemessenheitsbeschluss zwischen der EU und den USA eingeführt, das jedoch wiederum durch das Schrems-II-Urteil am 20. Juli 2020 für ungültig erklärt wurde.

Schlussendlich wurden die Anforderungen aus Art. 44 ff. DSGVO hinsichtlich der Datenübermittlung in Drittländer konkretisiert und in neue EU-Standardvertragsklauseln – Standard Contractual Clauses (SCC) – gefasst. Sie wurden zum 27. September 2021 in Kraft gesetzt. Sämtliche Verträge, die noch alte Standardvertragsklauseln enthalten, sind danach bis zum 27. Dezember 2022 durch neue zu ersetzen.

Die neuen EU-Standardvertragsklauseln

Am 4. Juni 2021 verabschiedete die EU-Kommission die neuen SCC, die als geeignete Garantien gemäß Art. 46 abs. 2 lit. c DSGVO gelten (Beschluss 2021/914/EU der Europäischen Kommission). Die neuen Standardvertragsklauseln legen die Rechtsgrundlage für den Daten-

transfer in Staaten fest, deren Datenschutzniveau nicht dem der EU gleichgestellt ist, und zu denen es auch keinen Angemessenheitsbeschluss der Europäischen Kommission gibt.

Bereits vor dem Schrems-II-Urteil des EuGH gab es Standardvertragsklauseln. Im Vergleich zu den alten Standardvertragsklauseln, die aus mehreren Sets bestanden und insgesamt zwölf Klauseln aufwiesen, gibt es nun ein Regelwerk aus insgesamt 18 Klauseln. Es ist modular aufgebaut und richtet sich an der jeweiligen Konstellation der Vertragsbeziehung und den entsprechenden Rollen der Vertragspartner aus.

Beispielsweise ist in Klausel 14 nun schriftlich geregelt, dass „bevor“ Daten in ein Drittland transferiert werden, der jeweilige Stand und die Qualität des Datenschutzes im Verhältnis zum Europäischen Datenschutzniveau zu bewerten sind. Dies erfolgt unter dem Prüfungspunkt Transfer Impact Assessment (TIA).

Ferner ist in Klausel 15 neu reguliert, dass dem Datenimporteur eine Informationspflicht gegenüber dem Datenexporteur auferlegt ist. Dem Exporteur wird hierdurch die Möglichkeit der Überprüfung der Rechtmäßigkeit eines Auskunftersuchens einer nationalen Behörde geschaffen.

Eine weitere Neuregulierung ist die in Klausel 7 eröffnete Möglichkeit, weitere Parteien zu den Standardvertragsklauseln beitreten zu lassen, die sogenannten „Kopplungsmöglichkeit“.

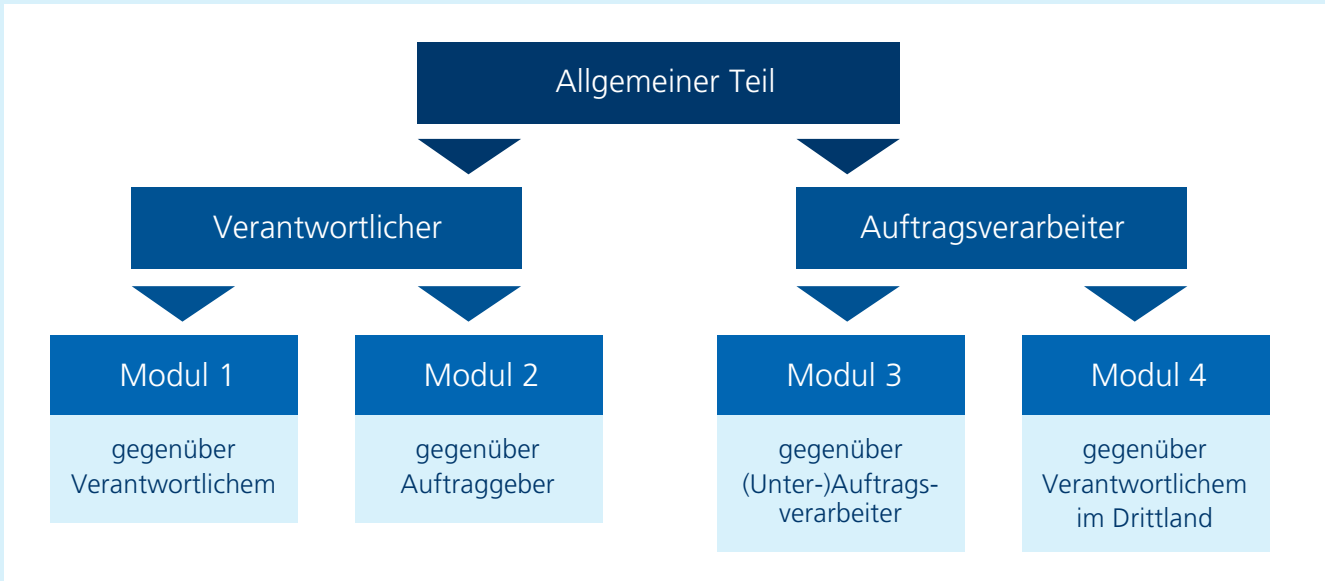
Zudem besteht nun in Klausel 12 lit. b eine Haftungsregelung bei Verletzung von Betroffenenrechten.

Durch den modularen Aufbau, unter strenger Einhaltung des allgemeinen Teils, werden nun verschiedene Situationen von Vertragspartnern abgebildet und wird daher eine flexible Gestaltung des Vertrages erwirkt.

Dieser Beitrag (Teil II)
beschreibt die Standardvertrags-
klauseln (Methodik)
Teil I: Regulatorische Vorgaben aus
Heft 2/2022 finden Sie hier:



Abb. 1. **Aufbau Standardvertragsklauseln**



Vorgehensweise

Ob Daten in Staaten außerhalb der EU rechtmäßig übermittelt werden können, ist in einem mehrstufigen Prüfungsverfahren festzustellen.

1. Taugliche Rechtsgrundlage

Zunächst ist festzuhalten, dass es auch für die Übermittlung, die eine Verarbeitung von personenbezogenen Daten im Sinne des Art. 4 Nr. 2 DSGVO darstellt, einer Rechtsgrundlage bedarf. Dies ergibt sich ebenso aus den Vorschriften des Art. 6 Abs. 1 lit. a bis f DSGVO zur Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten, da die Regeln des Art. 44 ff. DSGVO lediglich die Übermittlung von personenbezogenen Daten in ein Drittland regeln und legitimieren.¹ Die Verarbeitung ist daher weiterhin an die Voraussetzungen der DSGVO geknüpft, Art. 44 HS. 4 DSGVO.

Ebenso gilt dies für die Einhaltung der rechtlichen Vorgaben hinsichtlich der Informationspflicht gemäß Art. 12 ff. DSGVO sowie der technisch-organisatorischen Maßnahmen gemäß Art. 32 DSGVO.

2. Angemessenes Schutzniveau

Nachdem die Rechtsgrundlage der Verarbeitung und die weiteren Voraussetzungen der DSGVO eingehalten sind, bedarf es der Prüfung, ob ein Angemessenheitsbeschluss für das konkrete Drittland vorliegt und hierdurch die Einstufung als sicheres Drittland bereits besteht.²

Sollte dies gegeben sein, dann bedarf es keiner weiteren Prüfung.

Besteht jedoch kein Angemessenheitsbeschluss, kommen die neuen Standardvertragsklauseln in Betracht, sofern keine anderen geeigneten Garantien gemäß Art. 46 ff. DSGVO vorliegen sollten.

3. Standardvertragsklauseln

Wichtig ist, dass das richtige Modul der Standardvertragsklauseln genutzt wird. Je nach Vertragsbeziehung der Parteien ist das entsprechende Modul auszuwählen und ist unveränderbar. Daher besteht bei Standardvertragsklauseln keinerlei Vertragsgestaltungsspielraum zwischen den Parteien.

4. Transfer Impact Assessment (TIA)

Durch das Transfer Impact Assessment soll eine risikobasierte individuelle Betrachtung des Drittlandtransfers erfolgen.

Gemäß der Klausel 14 der neuen Standardvertragsklauseln ist die Bewertung und Prüfung des Datenschutzniveaus im Zielland nun verpflichtend. Insbesondere die Zugriffsbefugnisse seitens staatlicher Behörden sind hierbei von Bedeutung.

Bei einer solchen Prüfung ist daher die Zugriffsmöglichkeit der staatlichen Behörde auf die personenbezogenen Daten sowie die Prüfung, wie der Datenimporteur im Drittland diese abwendet und vermeidet, miteinzubeziehen.

Bei der Bewertung hinsichtlich des Datenschutzniveaus bedarf es daher der Unterstützung des Datenimporteurs, denn nur dieser kann beurteilen, ob und wie Zugriffe staatlichen Behörden möglich sind und durchsetzbar sind. Diese Mitwirkung ist in Klausel 14 c auch schriftlich reguliert.

Auch ist der Datenimporteur verpflichtet, notwendige Informationen für die Prüfung bereitzustellen

sowie der gemeinsamen Dokumentationspflicht nach Klausel 14 e nachzukommen.

Daher müssen beide Parteien das Transfer Impact Assessment gemeinsam durchführen.

Es ist darüber hinaus sinnvoll, eine Datenschutz-Folgenabschätzung (DSFA) gemeinsam mit dem jeweiligen Vertragspartner durchzuführen. Dadurch können alle wichtigen Punkte entsprechend gewürdigt und in die Bewertung einbezogen werden.

Weitere mögliche Maßnahmen zu den Standardvertragsklauseln

Aufgrund der kritischen Stimmen der deutschen Aufsichtsbehörden vor allem hinsichtlich des Drittlandtransfers in die USA sollten insbesondere die technisch-organisatorischen Maßnahmen eine hohe Beachtung bei der Prüfung finden.³ Eine Vorlage des Datenschutz- und Sicherheitskonzepts des Vertragspartners im Drittland ist daher von Vorteil.



Derya Isikli

Beauftragte Informationssicherheit & Datenschutz,
E-Mail: derya.isikli@dz-cp.de



Benjamin Wellnitz

Bereichsleiter Informationssicherheit & Datenschutz,
E-Mail: benjamin.wellnitz@dz-cp.de

Weitere Maßnahmen sind die Speicherung und der Support in der EU. Von Bedeutung sind auch eine spezielle Risikoanalyse und eine Datenschutz-Folgenabschätzung für den Transfer in ein Drittland.

Zudem könnte eine geeignete Maßnahme darin bestehen, die Daten nach der Einstufung des jeweiligen Risikos bei der Verarbeitung aufzuteilen.

Im Rahmen von Dienstleisterketten sollte der Verantwortliche das Transfer Impact Assessment zwischen den Dienstleistern im Rahmen des Auftragsverarbeitungsvertrages gemäß Art. 28 DSGVO überprüfen.

Besonderheit bei Drittlandtransfer von personenbezogenen Daten in die USA

Am 7. Oktober 2022 hat der derzeitige Präsident Joe Biden den „Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities“ unterzeichnet. Hierdurch soll eine Grundlage geschaffen werden, dass der Datentransfer zwischen europäischen und US-Unternehmen wieder DSGVO-konform, ohne rechtlichen und umständlichen Mehraufwand, erfolgen kann.⁴

Zwar können sich danach EU-Bürger beim „Civil Liberties Protection Officer“ der US-Geheimdienste über möglichen Datenmissbrauch beschweren und auf der zweiten Ebene dann die jeweilige Entscheidung beim „Data

Protection Review Court“ anfechten. Jedoch besteht das eigentliche Problem weiterhin: Die US-Sicherheitsgesetze, wie der Foreign Intelligence Surveillance Act (FISA) oder Cloud Act, ermöglichen die Überwachung von EU-Bürgern, sofern die Daten im Zugriff eines US-Konzerns liegen.

Wie sich die EU-Kommission hierzu letztlich äußern wird, bleibt offen.

Resümee

Hinsichtlich der personenbezogenen Datenverarbeitung sowie des Datentransfers in ein Drittland gelten besondere Anforderungen gemäß der DSGVO. Es ist ratsam, regelmäßig den Datenschutzbeauftragten einzubinden und Verarbeitungen, die im Verzeichnis für Verarbeitungstätigkeiten gemäß Art. 30 DSGVO dokumentiert sein sollten, auf Drittlandsübertragungen zu überprüfen. Im Anschluss sollten die Verträge hierzu geprüft werden, inwiefern diese die aktuellen Standardvertragsklauseln verwenden. Sofern alte Standardvertragsklauseln verwendet werden, sollten diese zeitnah durch die aktuellen Standardvertragsklauseln ersetzt werden.

Eine gesonderte stichprobenartige Überprüfung durch die Landesdatenschutzbehörden kann in diesem Zusammenhang nicht ausgeschlossen werden.⁵ ■

¹ Übertragung personenbezogener Daten in ein Drittland | DSGVO (keyed.de), abgerufen am 14.11.2022

² Beispiele für Drittländer mit bestehendem Angemessenheitsbeschluss: Andorra, Argentinien, Färöer, Guernsey, Isle of Man, Israel, Japan, Jersey, Neuseeland, Schweiz, Uruguay

³ <https://www.it-daily.net/it-sicherheit/datenschutz-grc/was-beim-tia-transfer-impact-assessment-beachtet-werden-muss>, abgerufen am 14.11.2022

⁴ Neues EU-US-Datentransfer-Abkommen nimmt erste Hürde | heise online, abgerufen am 14.11.2022

⁵ <https://fd.niedersachsen.de/startseite/infotehk/presseinformationen/neue-standardvertragsklauseln-frist-fur-die-umstellung-von-altvertragen-endet-demnachst-216765.html>, abgerufen am 14.11.2022