Globaler Datentransfer: Die neuen Standard-datenschutzklauseln – Was ist zu tun?

FÜR DIE ÜBERMITTLUNG PERSONENBEZOGENER DATEN IN DRITTSTAATEN HAT DIE EU KOMMISSION NEUE STANDARDDATENSCHUTZKLAUSELN VERABSCHIEDET

Executive Summary

- Am 4. Juni 2021 hat die EU-Kommission neue Standarddatenschutzklauseln (auch Standardvertragsklauseln (SCC) genannt) verabschiedet.
- Die grundlegende Überarbeitung der SCC wurde durch die gestiegenen Anforderungen nach der EU Datenschutzgrundverordnung (DSGVO) und dem Schrems-II-Urteil des EuGH erforderlich.
- Die neuen SCC sind flexibler einsetzbar und öffnen sich für einen größeren Anwendungskreis.
- Maßgebliche Neuerungen sind eine obligatorische Folgenabschätzung sowie Mitteilungspflichten an Betroffene. Das Erfordernis des separaten Abschlusses von Auftragsverarbeitungsverträgen entfällt zukünftig.
- Es gilt eine Übergangsfrist. Bei bestehenden Verträgen müssen die neuen SCC bis spätestens Ende 2022 vereinbart werden.

I. Hintergrund – Grundlage des Datentransfers in Drittstaaten, insbes. Datenübermittlung in die USA

Eine Übermittlung personenbezogener Daten in ein Land außerhalb der EU / des EWR – in einen Drittstaat (insbesondere in die USA) – ist nur zulässig, wenn neben den allgemeinen Anforderungen für eine Datenübermittlung nach der DSGVO darüber hinaus sichergestellt ist, dass die personenbezogenen Daten beim Empfänger in diesem Drittstaat ausreichend geschützt werden. Insoweit gelten die allgemeinen und spezifischen Anforderungen der Art. 44 ff. DSGVO. Für die Praxis hatte die EU Kommission bereits unter dem alten Datenschutzrecht im Jahr 2010 mit dem Beschluss 2010/87/EU sogenannte Standardvertragsklauseln erlassen, deren Verwendung sicherstellen sollte, dass alle personenbezogenen Daten, die die EU oder den EWR verlassen, in Übereinstimmung mit dem geltenden Datenschutzrecht übermittelt und verarbeitet werden. Für den Datentransfer in die USA konnte alternativ auch das EU-US Privacy Shield Abkommen herangezogen werden. Das Privacy Shield enthielt einen Mechanismus, der den darunter zertifizierten US-Unternehmen ein in der EU vergleichbares Datenschutzniveau attestiert, um so Datenübermittlungen in die USA zu legitimieren.

Durch das Schrems-II-Urteil des Gerichtshofes der Europäischen Union (EuGH) vom 16. Juli 2020 wurde jedoch die Datenübertragung basierend auf dem EU-US Privacy Shield ohne Übergangsregelung für ungültig erklärt. Ab diesem Zeitpunkt war damit eine Datenübermittlung in die USA basierend auf dem Privacy Shield-Mechanismus nicht mehr möglich.

Zwar lies der EuGH in seinem Urteil die SCC grundsätzlich unangetastet. Allerdings wies das Gericht deutlich darauf hin, dass über die bloße Verwendung der SCC hinaus die Datenexporteure ab sofort dafür verantwortlich sind, im Einzelfall angemessene Garantien für Datenschutz und Datensicherheit in den Drittländern zu prüfen und ergänzende Maßnahmen zu ergreifen, die diese Schutzlücken schließen und den Standard auf das von der DSGVO geforderte Niveau bringen.

Damit stellte das Schrems-II-Urteil für die datenschutzrechtlichen Anforderungen an den Drittstaatentransfer eine Zäsur dar. Die EU Kommission war als Reaktion gehalten, ihre SCC insgesamt grundlegend zu überprüfen und zu überarbeiten, damit für die Übermittlung personenbezogener Daten in Drittstaaten wieder ein angemessenes Schutzniveau besteht. Auch die fortschreitenden

Entwicklungen in der digitalen Wirtschaft erforderten eine Überarbeitung und Anpassung der SCC.

II. Höhere Anforderungen für den Datentransfer nach dem Schrems-II-Urteil

Entscheidend für einen zulässigen Datentransfer auf Grundlage der bisherigen SCC ist laut EuGH, dass die vertraglichen Regelungen eingehalten und im Drittstaat die Transferschutzanforderungen des Art. 45 Abs. 2 DSGVO tatsächlich angemessen berücksichtigt werden. Das Augenmerk richtete der EuGH dabei auf den besonderen Schutz vor dem Zugriff ausländischer Sicherheitsbehörden auf personenbezogene Daten. Betroffenen Personen müssten durchsetzbare Rechte sowie wirksame Rechtsbehelfe zur Verfügung stehen, so wie dies nach Art. 47 der Charta der Grundrechte der Europäischen Union statuiert ist. Die Datenübermittlung sei auszusetzen oder zu verbieten, wenn die zuständigen Aufsichtsbehörden in der EU der Auffassung sind, dass die SCC im Drittstaat nicht eingehalten oder nicht eingehalten werden können.

Die bisherigen SCC wurden diesen Anforderungen nicht mehr gerecht, was insbesondere in Bezug auf die USA deutlich wurde. In den USA kann aufgrund der weitreichenden Zugriffsmöglichkeiten von Sicherheitsbehörden auf personenbezogene Daten nicht der notwendige EU-Schutzstandard gewährleistet werden, da z.B. Sicherheitsbehörden ohne richterlichen Beschluss auf personenbezogene Daten zugreifen können. Auch die Möglichkeit, sich an einen Ombudsmann in den USA zur Ahndung von Rechtsverstößen zu wenden, reicht zur Gewährleistung effektiven Rechtsschutzes nicht (mehr) aus. Dem EuGH zufolge sei ein Ombudsmann nicht mit einem unabhängigen Richter gleichzustellen.

III. Grundlegende Änderungen in den neuen Standarddatenschutzklauseln

1. Modulare Gliederung

Mit den neuen SCC erhalten Verwender einen größeren Gestaltungsspielraum. Die neuen SCC bieten mehr Flexibilität und öffnen sich für einen größeren Anwendungskreis. Umfassten die bisherigen SCC nur Regelungen zu einem Datentransfer zwischen zwei Verantwortlichen und dem Verantwortlichen und einem Auftragsverarbeiter, so werden nun neben den allgemeinen Klauseln, die folgenden 4 Vertragsmodule bzw. Anwendungsfälle für einen Datentransfer differenzierter erfasst:

Modul 1: Verantwortlicher an Verantwortlichen (controller to controller)

Modul 2: Verantwortlicher an Auftragsverarbeiter (controller to processor)

Modul 3: Auftragsverarbeiter an Auftragsverarbeiter (processor to processor)

Modul 4: Auftragsverarbeiter an Verantwortlichen (processor to controller)

2. Maßgebliche Änderungen

Da die bisherigen SCC noch aus Vor-DSGVO-Zeiten stammen, wurden die neuen SCC insgesamt an den Wortlaut und die Anforderungen der DSGVO angepasst. Die wichtigsten Neuerungen sind die Folgenden:

a. Obligatorische Folgenabschätzung

Eine maßgebliche Neuerung der SCC ist die obligatorische Datenschutzfolgenabschätzung.

Beide Parteien, der Datenexporteur und der Datenimporteur, müssen versichern, dass sie keine Bedenken hinsichtlich des Datenschutzstandards im Land des Datenimporteurs haben. Hierbei gilt es insbesondere die datenschutzrechtlichen Vorgaben und Sicherheiten im Drittstaat (Land des Datenimporteurs) – einschließlich der Offenlegungspflichten von personenbezogenen Daten gegenüber Behörden – kritisch zu prüfen.

Die Folgenabschätzung ist zu dokumentieren und auf Anfrage den Aufsichtsbehörden zur Verfügung zu stellen.

b. Mitteilung an Betroffene

Der Datenimporteur hat den Datenexporteur und den Betroffenen zu informieren, wenn er von einer öffentlichen Stelle eine rechtsverbindliche Aufforderung zur

Herausgabe von personenbezogenen Daten erhält. Der Datenimporteur hat zudem die Rechtmäßigkeit dieser Herausgabeaufforderung zu prüfen. Kommt er zu dem Schluss, dass das Ersuchen rechtswidrig ist, muss er es anfechten und ggf. die zur Verfügung stehenden Rechtsmittel ausschöpfen.

c. Schutzwirkung für Dritte

Mit gewissen Ausnahmen können Betroffene selbst ihre Rechte gegenüber allen Verwendern ihrer personenbezogenen Daten in der Datentransferkette geltend machen; also auch direkt gegenüber Auftragsverarbeitern.

d. Nachträglicher Beitritt weiterer Vertragsparteien möglich

Zukünftig ist der Beitritt eines Dritten, als Datenimporteur oder -exporteur, nach Abschluss der SCC möglich, sofern beide Parteien zustimmen.

3. Kein separater Auftragsverarbeitungsvertrag mehr notwendig

In den neuen Vertragsmodulen für den Datentransfer an Auftragsverarbeiter sind die Vorgaben für eine Auftragsverarbeitung nach Art. 28 Abs. 3 DSGVO gleich mit enthalten. Schließen Unternehmen die neuen SCC ab, so bedarf es keines weiteren Vertrages zur Auftragsverarbeitung (AVV) mehr. Eine individuelle Vereinbarung im Hinblick auf den AVV wird jedoch erschwert, da hierfür die starr vorgegebenen SCC abgeändert werden müssten. Dies ist jedoch nur zulässig, sofern etwaige zusätzliche Klauseln den SCC nicht widersprechen.

IV. Umsetzungsfristen

Die neuen SCC werden mit der Veröffentlichung im Amtsblatt der EU in den nächsten Wochen in Kraft treten.

Die bisherigen SCC basierend auf dem Beschluss 2010/87/EU werden damit jedoch nicht sofort obsolet. Diese können für eine Übergangsfrist von 3 Monaten nach Inkrafttreten der neuen SCC weiterverwendet werden.

Für die sich bereits in Verwendung befindlichen bisherigen SCC gilt folgendes: Nach Ablauf der Übergangsfrist von 3 Monaten behalten die bisherigen SCC für bereits abgeschlossene Datentransferverträge für weitere 15 Monate ihre Gültigkeit. Voraussetzung dafür ist, dass die Verarbeitungsvorgänge, die Gegenstand des Datentransfervertrages sind, unverändert bleiben und durch zusätzliche Maßnahmen sichergestellt ist, dass die Anforderungen des Art. 46 Abs. 1 DSGVO eingehalten werden. Die bisherigen SCC gelten in bereits abgeschlossenen Datentransferverträgen mithin nur dann fort, wenn gemäß dem Schrems-II-Urteil sichergestellt ist, dass die dort festgehaltenen Anforderungen, bspw. durch zusätzlich vereinbarte Maßnahmen, hinreichend umgesetzt werden.

V. Ausblick und Handlungsempfehlung für Unternehmen

Zunächst ist zu begrüßen, dass die neuen SCC eine aktualisierte und hinreichende Grundlage für Datentransfers in Drittländer bieten. Allerdings genügt der Abschluss der SCC alleine noch nicht, um Rechtssicherheit zu erlangen. Das Datenschutzniveau im Drittland muss im Einzelfall aktiv geprüft werden.

Für Unternehmen mit Datentransfers in Drittstaaten ist akutes Handeln geboten. Insbesondere sollten folgende Maßnahmen initiiert bzw. umgesetzt werden:

(1) **Verträge:** Bei Neuverträgen müssen die neuen SCC nach der dreimonatigen Übergangsfrist berücksichtigt werden. Bei Altverträgen müssen die derzeitigen SCC spätestens im Dezember 2022 durch die neuen SCC ersetzt werden.

(2) **Bestandsaufnahme:** Es ist (vorsorglich nochmals) zu prüfen, ob und inwieweit Dienstleister in Drittländern eingesetzt werden und ein entsprechender Datentransfer stattfindet (auch diese Dienstleister müssen überprüfen, ob sie wiederum mit Subunternehmen in Drittländern arbeiten, die für den Vertag relevant sind).

(3) **Abfrage der Sicherheitsmaßnahmen:** Es sind (vorsorglich nochmals) die technischen und organisatorischen Sicherheitsmaßnahmen für den Datenschutz abzufragen, einschließlich des datenschutzbezogenen Rechtsschutzes im Drittland.

(4) **Prüfung des Datenschutzniveaus:** Anhand der erteilten Auskünfte zu den Sicherheitsmaßnahmen ist zu prüfen, ob ein hinreichendes Datenschutzniveau gegeben ist bzw. gewährleistet werden kann.

(5) **Protokollierung:** Aus Nachweisgründen ist die durchgeführte Prüfung des Datenschutzniveaus zu protokollieren.

(6) **Datenschutzfolgenabschätzung:** Da dies bei den neuen SCC ohnehin obligatorisch wird, ist zu erwägen, diese Folgenabschätzung bei bereits bestehenden Verträgen mit den bisherigen SCC durchzuführen; insbesondere dann, wenn das Datenschutzniveau ohnehin (nochmals) überprüft werden muss.

Da die deutschen Datenschutzbehörden – unabhängig von den neuen SCC – damit begonnen haben, proaktiv zu kontrollieren, ob die Anforderungen, die der EuGH in dem Schrems-II-Urteil für den Datentransfer in Drittstaaten aufgestellt hat, umgesetzt werden[1], sollten Unternehmen mit Datentransfers in Drittstaaten schnell aktiv werden. Aufgrund der ohnehin anstehenden Überprüfungen empfiehlt es sich, nicht die Übergangsfrist abzuwarten, sondern die bestehenden SCC möglichst zeitnah auszutauschen.

[1] Siehe z. B. Ankündigung der Berliner Datenschutzbehörde: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/presse-mitteilungen/2021/20210601-PM-Schrems_II_Pruefung.pdf

Dr. Jörg Kahler
Rechtsanwalt, Partner
Standort Berlin
joerg.kahler@gsk.de

Dr. Martin Hossenfelder
Rechtsanwalt, Counsel
Standort Berlin
martin.hossenfelder@gsk.de

Simonié Schlombs
Rechtsanwältin
Standort Berlin
simonie.schlombs@gsk.de

GSK
STOCKMANN

Haftungsausschluss
Diese Mandanteninformation enthält ausschließlich allgemeine Informationen, die nicht geeignet sind, den besonderen Umständen eines Einzelfalles gerecht zu werden. Sie hat nicht den Sinn, Grundlage für wirtschaftliche oder sonstige Entscheidungen jedweder Art zu sein. Sie stellt keine Beratung, Auskunft oder ein rechtsverbindliches Angebot auf Beratung oder Auskunft dar und ist auch nicht geeignet, eine persönliche Beratung zu ersetzen. Sollte jemand Entscheidungen jedweder Art auf Inhalte dieser Mandanteninformation oder Teile davon stützen, handelt dieser ausschließlich auf eigenes Risiko.

GSK Stockmann und auch die in dieser Mandanteninformation namentlich genannten Partner oder Mitarbeiter übernehmen keinerlei Garantie oder Gewährleistung, noch haftet GSK Stockmann und einzelne Partner oder Mitarbeiter in irgendeiner anderen Weise für den Inhalt dieser Mandanteninformation. Aus diesem Grund empfehlen wir, in jedem Fall eine persönliche Beratung einzuholen.

www.gsk.de

GSK Stockmann

BERLIN
Mohrenstrasse 42
10117 Berlin
T +49 30 203907-0
F +49 30 203907-44
berlin@gsk.de

HEIDELBERG
Mittermaierstrasse 31
69115 Heidelberg
T +49 6221 4566-0
F +49 6221 4566-44
heidelberg@gsk.de

FRANKFURT / M.
Taunusanlage 21
60325 Frankfurt am Main
T +49 69 710003-0
F +49 69 710003-144
frankfurt@gsk.de

MÜNCHEN
Karl-Scharnagl-Ring 8
80539 München
T +49 89 288174-0
F +49 89 288174-44
muenchen@gsk.de

HAMBURG
Neuer Wall 69
20354 Hamburg
T +49 40 369703-0
F +49 40 369703-44
hamburg@gsk.de

LUXEMBURG
GSK Stockmann SA
44, Avenue John F. Kennedy
L-1855 Luxemburg
T +352 271802-00
F +352 271802-11
luxembourg@gsk-lux.com