[Nicholas Vollmer: Verfasser und Datum werden hier im Dokument nicht genannt. Es ist wohl die EU-Kommission, die das Dokument vermutlich am 23.05.2022 zuletzt geändert hatte. Quelle: https://ec.europa.eu/info/sites/default/files/questions_answers_on_sccs_en.pdf

Im Folgenden werden speziell die letzten 4 Fragestellungen präsentiert. Hier handelt es sich um den wohl wichtigsten Aspekt: Kann der Drittland-Importeur zusichern, dass die Gesetze und Gepflogenheiten seines Landes den hier zugesagten Datenschutz nicht torpedieren?

Man könnte glauben, dass die EU-Kommission diesen Aspekt bewusst vage ausdrückt und erst ganz zum Schluss erwähnt, um die Verantwortlichen in falscher Sicherheit zu wiegen und die EU-Wirtschaft (zulasten des Datenschutzes) zu schonen.]

DIE NEUEN STANDARDVERTRAGSKLAUSELN - FRAGEN UND ANTWORTEN IM ÜBERBLICK

[...]

LOKALE GESETZE UND ZUGANG DER BEHÖRDEN

40. Sind bei der Verwendung der neuen SCC besondere Maßnahmen erforderlich, um dem Urteil in der Rechtssache Schrems II nachzukommen? Ist es weiterhin notwendig, die Leitlinien des EDPB zu berücksichtigen?

Im Einklang mit dem Urteil des Gerichtshofs der Europäischen Union in der Rechtssache *Schrems II* (C-311/18) verpflichtet **Klausel 14** die Parteien, vor dem Abschluss der SCC zu prüfen, ob die für die Verarbeitung der personenbezogenen Daten durch den Datenimporteur geltenden Rechtsvorschriften und Praktiken des Bestimmungsdrittlandes letzteren daran hindern könnten, die Klauseln einzuhalten. Bei der Durchführung dieser **"Folgenabschätzung für die Übermittlung"** sollten die Parteien insbesondere die besonderen Umstände der Übermittlung (z. B. die Kategorien und das Format der Daten, die Art des Empfängers, den Wirtschaftssektor, in dem die Übermittlung erfolgt, und die Länge der Verarbeitungskette) sowie die in diesem Zusammenhang relevanten Gesetze und Praktiken berücksichtigen. Die letztgenannte Bewertung umfasst die geltenden Beschränkungen und Garantien, um insbesondere festzustellen, ob die Gesetze und Praktiken nicht über das hinausgehen, was in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist, um eines der in Artikel 23 Absatz 1 DSGVO aufgeführten Ziele zu schützen (in diesem Fall wird davon ausgegangen, dass sie die Einhaltung der SCC nicht beeinträchtigen).

Was die Auswirkungen auf die Einhaltung der SCC betrifft, so können die Parteien im Rahmen einer Gesamtbeurteilung **verschiedene Elemente berücksichtigen** (siehe Klausel 14, Fußnote 12), wie z. B. verlässliche Informationen über die Anwendung des Gesetzes in der Praxis (z. B. Rechtsprechung und Berichte unabhängiger Aufsichtsgremien), das Vorhandensein bzw. Nichtvorhandensein von Ersuchen im selben Sektor und - unter strengen Voraussetzungen - die dokumentierte praktische Erfahrung des Datenexporteurs und/oder Datenimporteurs. **Im Falle einer negativen Beurteilung** dürfen die Parteien nur dann Daten auf der Grundlage der SCC übermitteln, wenn sie **zusätzliche ("ergänzende") Garantien** (z. B. technische Maßnahmen zur Gewährleistung der Datensicherheit, wie z. B. eine Ende-zu-Ende-Verschlüsselung) einführen, die der Situation gerecht werden und somit die Einhaltung der Klauseln gewährleisten. Das Gleiche gilt, wenn der Datenexporteur später feststellt, dass der Datenimporteur nicht mehr in der Lage ist, die SCC einzuhalten, auch infolge einer Änderung der Rechtsvorschriften des Drittlandes. Der Datenexporteur ist verpflichtet, die Übermittlung auszusetzen, wenn er der Ansicht ist, dass keine angemessenen Garantien gewährleistet werden können, oder wenn er von der zuständigen Aufsichtsbehörde dazu angewiesen wird.
[Nicholas Vollmer: Die deutschen Aufsichtsbehörden haben am 21.06.2021 in einer gemeinsamen Pressemeldung bereits das Ergebnis für eine USA-Risikoanalyse veröffentlicht:

Es seien regelmäßig ergänzende Maßnahmen erforderlich, die aber überhaupt nur für wenige Fälle denkbar seien. Dies wird auf Seite 230 des PrivazyPlan® als “Der letzte Sargnagel für US-Datentransfer” bezeichnet.]

Die SCC (Klausel 14) sollten nicht isoliert gelesen werden, sondern **zusammen mit den ausführlichen Leitlinien des Europäischen Datenschutzausschusses (EDPB) verwendet werden**. Siehe Empfehlungen 01/2020 zu Maßnahmen, die die Übermittlungsinstrumente ergänzen, um die Einhaltung des EU-Schutzniveaus für personenbezogene Daten zu gewährleisten (18. Juni 2021) (verfügbar unter: https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf). Die Empfehlung enthält einen schrittweisen Fahrplan für die Bewertungsphase, eine Liste möglicher Informationsquellen für diese Bewertung (Anhang 3) und verschiedene Beispiele für ergänzende Maßnahmen (Anhang 2).
[Nicholas Vollmer: Siehe im obigen Dokument ab RdNr. 84 (“use case 1”), wobei insbesondere der „Use Case 6“ in RdNr. 93-94 dem klassischen US-Cloud-Modell eine klare Absage erteilt.]

[Nicholas Vollmer: Das Gesamtfazit an dieser Stelle muss wohl lauten: Die EU Kommission möchte es nicht klar aussprechen, sondern sich lieber hinter verklausulierten Forderungen verstecken. Die Rechtsanwender müssen selbst zu dem Ergebnis kommen, dass die klassischen US-Clouddienste nicht mit den neuen EU Standardvertragsklauseln zu legitimieren sind. Es bleibt also nur noch die explizite Einwilligung gemäß Artikel 49 (1a); allerdings erteilen die deutschen Aufsichtsbehörden auch diesem Ansatz einen deutlichen Dämpfer, da die Einwilligung nur in Ausnahmefällen zulässig sei (siehe PrivazyPlan® im Kapitel 7.6.2a… wobei die restliche Fachwelt – inkl. EDPB - diese Rechtsauffassung allerdings zumeist nicht teilt.]

41. Inwieweit muss der Datenimporteur den Datenexporteur über Auskunftsersuchen von Behörden (z. B. Strafverfolgungs- oder nationale Sicherheitsbehörden) informieren?

Erstens sehen die SCC **vor, dass der Datenimporteur die Behörden über den Zugang zu den** übermittelten Daten **informieren muss** (entweder auf Anfrage oder direkt).

Gemäß Klausel 15.1 sollte der Datenimporteur den Datenexporteur unverzüglich benachrichtigen, wenn er eine **rechtsverbindliche Aufforderung einer Behörde** oder eines Gerichts in dem Drittland zur Offenlegung der übermittelten personenbezogenen Daten erhält. Ebenso sollte er den Exporteur benachrichtigen, wenn er von einem **direkten Zugriff** (z. B. Abfangen) von Behörden auf diese Daten erfährt. In diesem Zusammenhang berücksichtigen die SCC, dass es dem **Datenimporteur nach nationalem Recht untersagt sein kann,** dem Datenexporteur (bestimmte) Informationen zu übermitteln. Insbesondere wenn der Datenimporteur nicht befugt ist, bestimmte Fälle des staatlichen Zugriffs zu melden, sollte er sich nach besten Kräften bemühen, eine Befreiung von diesem Verbot zu erwirken, um so schnell wie möglich so viele Informationen wie möglich zu übermitteln. Ist der Datenexporteur selbst ein Auftragsverarbeiter, muss er die Meldung an seinen für die Verarbeitung Verantwortlichen weiterleiten.

Darüber hinaus sollte der **Datenimporteur dem Datenexporteur in regelmäßigen Abständen aggregierte Informationen** über die bei ihm eingegangenen Auskunftsersuchen zur **Verfügung stellen** (Klausel 15.1(c)). Auch diese Verpflichtung gilt nur**, wenn der Importeur nach seinem nationalen Recht berechtigt ist**, solche Informationen zu erteilen. Ist der Datenexporteur selbst ein Auftragsverarbeiter, so muss er diese Informationen an seinen für die Verarbeitung Verantwortlichen weiterleiten.

Zweitens enthalten die SCC **zusätzliche Meldepflichten** für den Fall, dass der Datenimporteur **Gesetzen und/oder Praktiken** unterliegt**, die ihn daran hindern, die** Klauseln einzuhalten.

Gemäß Klausel 14(e) **verpflichtet sich** der **Datenimporteur, den Datenexporteur**

unverzüglich zu **benachrichtigen,** wenn er nach Zustimmung zu den Klauseln und während der Laufzeit des Vertrags Grund zu der Annahme hat, dass **er Gesetzen oder Praktiken unterliegt oder unterlegen ist, die nicht mit den Anforderungen gemäß Klausel 14(a) übereinstimmen**. Dies gilt auch für Fälle, in denen sich die Rechtsvorschriften des Drittlandes nach der ursprünglichen Bewertung ändern oder in denen der Datenimporteur in dem Drittland einer Maßnahme (z. B. einer Aufforderung zur Offenlegung) unterliegt, die darauf hindeutet, dass die Anwendung dieser Rechtsvorschriften in der Praxis nicht mit der ursprünglichen Bewertung übereinstimmt. Handelt es sich bei dem Datenexporteur um einen Auftragsverarbeiter, der im Namen eines für die Verarbeitung Verantwortlichen handelt, muss er die Meldung an seinen für die Verarbeitung Verantwortlichen weiterleiten.

Die SCC **berücksichtigen** auch hier**, dass der Datenimporteur** nach nationalem Recht **möglicherweise nicht befugt ist**, über spezifische staatliche Auskunftsersuchen/direkten Zugang zu informieren. Insbesondere Klausel 16(a) enthält eine allgemeine Meldepflicht, wonach der **Datenimporteur den Datenexporteur unverzüglich informieren muss**, wenn er die Klauseln - **aus welchen Gründen auch immer - nicht einhalten kann**. Unter Berufung auf diese Klausel muss der Datenimporteur dem Datenexporteur mitteilen, dass er die SCC nicht mehr einhalten kann, ohne dass er notwendigerweise spezifische Informationen über den Zugang der Behörden geben muss. Der Datenexporteur wird dann in der Lage sein, die erforderlichen Maßnahmen zu ergreifen, einschließlich der möglichen Aussetzung der Übermittlung oder der Beendigung der SCCs.

42. Muss der Datenimporteur Einzelpersonen über Auskunftsersuchen einer Behörde informieren? Was ist, wenn der Datenimporteur nach nationalem Recht nicht berechtigt ist, diese Informationen zu erteilen?

Gemäß Klausel 15.1(a) **muss** der **Datenimporteur die betroffenen Personen benachrichtigen**, wenn er eine **rechtsverbindliche Aufforderung einer Behörde** oder eines Gerichts in dem Drittland erhält, sie betreffende personenbezogene Daten offenzulegen. Darüber hinaus sollte er den Exporteur benachrichtigen, wenn er von einem **direkten Zugriff** (z. B. Abhören) von Behörden auf diese Daten erfährt. Gleichzeitig **berücksichtigen** die **SCC, dass die Bereitstellung dieser Informationen aus rechtlichen oder praktischen Gründen möglicherweise nicht möglich ist.**

Insbesondere **kann es dem Datenimporteur** (nach nationalem Recht) **untersagt sein**, über bestimmte Fälle des staatlichen Zugriffs zu informieren. In diesem Fall sollte er sich nach Kräften bemühen, eine Befreiung von diesem Verbot zu erwirken, um so schnell wie möglich so viele Informationen wie möglich zu übermitteln.

Darüber hinaus **kann es in der Praxis schwierig sein**, die betroffenen Personen zu kontaktieren (z. B. weil der Datenimporteur keine direkte Beziehung zu den Personen hat). In dieser Hinsicht stellt Klausel 15.1(a) klar, dass der Datenimporteur die Hilfe des Datenexporteurs in Anspruch nehmen kann (der möglicherweise eine direkte Beziehung zu den Personen hat).

43. Ist der Datenimporteur vertraglich verpflichtet, jedem Antrag auf Offenlegung, den er von einer Behörde erhält, zu widersprechen?

Nein. Gemäß Klausel 15.2 der SCC **muss** der Datenimporteur **prüfen**, ob die bei ihm eingehenden Anfragen nach dem geltenden innerstaatlichen Recht rechtmäßig sind. Ist der Importeur der Ansicht, dass es **berechtigte Gründe gibt, die Anfrage als rechtswidrig zu betrachten** (z. B. wenn die anfragende Behörde offensichtlich ihre Befugnisse überschritten hat), sollte er die nach seinem innerstaatlichen Recht verfügbaren Verfahren nutzen, um die Anfrage anzufechten. Hat der Datenimporteur ein Ersuchen angefochten und ist er der Ansicht, dass es **genügend Gründe gibt, um** das Ergebnis des erstinstanzlichen Verfahrens

anzufechten, so sollte er diesem Rechtsbehelf nachgehen.

44. Muss man Abschnitt III der SCC einhalten, wenn man sich auf Modul 4 beruft?

Abschnitt III der SCC enthält eine spezielle Ausnahme für den Fall, dass Modul 4 von einem **EWR-Verarbeiter** verwendet wird**, um Daten, die er von seinem für die Verarbeitung Verantwortlichen außerhalb des EWR erhalten hat,** an diesen **zurückzusenden**. In diesem Szenario wurden die personenbezogenen Daten ursprünglich außerhalb des EWR verarbeitet, wo sie bereits dem nationalen Rechtsrahmen unterlagen. Die Parteien müssen daher weder eine "Folgenabschätzung für die Übermittlung" (Klausel 14) durchführen noch die Verpflichtungen in Bezug auf den Zugang von Behörden zu den Daten erfüllen (Klausel 15).

Beispiel: Ein marokkanisches Unternehmen nutzt Cloud-Dienste, die von einem luxemburgischen Unternehmen angeboten werden, um Daten in seiner Kundendatenbank zu speichern. Die SCCs (Modul 4) können verwendet werden, um die Daten von Luxemburg (durch den Datenexporteur) zurück nach Marokko (zum Datenimporteur) zu übertragen. Da der Datenexporteur nur die Daten zurücksendet, die er von Marokko erhalten hat, muss er Abschnitt III nicht einhalten.

Umgekehrt **gilt** die **Ausnahme nicht** (und die Parteien müssen daher Abschnitt III einhalten), **wenn die Daten, die vom Auftragsverarbeiter** (Datenexporteur) an seinen für die Verarbeitung Verantwortlichen (Datenimporteur) **übermittelt werden, auch personenbezogene Daten mit Ursprung in Europa enthalten**.

Beispiel: Ein chilenisches Unternehmen beauftragt einen spanischen Auftragsverarbeiter mit der Durchführung von Marktforschung und der Entwicklung von Marketingmaterial unter Verwendung von Kundendaten, die es von dem chilenischen Unternehmen erhalten hat, und von Kundendaten, die es in Spanien gesammelt hat. Modul 4 der SCC kann von dem spanischen Auftragsverarbeiter verwendet werden, um aggregierte Daten über die beiden Datensätze nach Chile zu übermitteln. Da der Datenexporteur auch in Europa erhobene Daten (und nicht nur die Daten, die er von Chile erhalten hat) an den Datenimporteur übermittelt, muss er Abschnitt III einhalten. Dies gilt für den gesamten Datensatz, der nach Chile übermittelt wird (d. h. sowohl für die aus Chile erhaltenen als auch für die in Spanien erhobenen Daten).