VISCHER

FREQUENTLY ASKED QUESTIONS (FAQ)

NEUE EU STANDARDVERTRAGSKLAUSELN FÜR DATENTRANSFERS IN UNSICHERE DRITTLÄNDER

unter Berücksichtigung von Version 2.0 der Empfehlung 01/2020 des EDSA

Von David Rosenthal, VISCHER AG[1] (available also in English[2])

Die folgenden Fragen beziehen sich auf die von der Europäischen Kommission am 4. Juni 2021 verabschiedeten Standardvertragsklauseln für die Datenübermittlung in Drittländer (**SCC**), d.h. im Sinne von Art. 46 EU-Datenschutz-Grundverordnung (**DSGVO**). Zu den Standardvertragsvertragsklauseln für Auftragsbearbeiter (**SCC-ADV**) siehe Ziff. 47. Die Kommentierung basiert auf der englischen Fassung der SCC. Praktische Hinweise zur Umsetzung der neuen SCC finden sich in Ziff. 48. Mehr Information zur Entwicklung von Intra-Group Data Transfer Agreements (**IGDTA**) (einschliesslich einer ausführlichen Checkliste) sind in Ziff. 49 und zu Transfer Impact Assessments (**TIA**) in Ziff. 44.

Am 27. August 2021 hat auch der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (**EDÖB**) die neuen SCC unter dem Schweizer Datenschutzgesetz (**DSG**) anerkannt. Dazu äussert sich diese FAQ auch.

Diese FAQ wird von Zeit zu Zeit aufdatiert.[3]

Version	Wichtigste Anpassung
22. Juni 2021	Erster Entwurf
13. Juli 2021	Neue eingefügte Ziff. 8 (Übermittlungen in unsichere Drittländer, wenn der Importeur der DSGVO untersteht); Klarstellung betr. die Natur einer Bearbeitung (Ziff. 19); die neue Ziff. 21 (EU Mitgliedstaaten), Ziff. 35 (Subprocessor in Europa) und Ziff. 49 (IGDTA); weitere Details zu den Ziff. 43 und 44 (Schrems II und TIA) und die Liste der Mängel der SCC (Ziff. 45).
1. August 2021	Neu eingefügte Ziff. 7 (für welche Fälle es die EU SCC und TIAs braucht), neues TIA-Formular und weitere Anpassungen zum Behördenzugriff (Ziff. 43 und 44), Erweiterung der IGDTA-Checkliste (Ziff. 49)
5. September 2021	Anpassungen nach erfolgter Anerkennung der EU SCC durch den EDÖB (diverse Ziffern); Anpassung der TIA-Grafik und Anpassungen zur Vernehmlassung des ICO.
27. September 2021	Kleinere Anpassungen und Korrekturen, inbesondere bei den Links und der TIA-Grafik.
17. Oktober 2021	Ergänzte/neue Ziff. 26, 33, 36 und 37.

---

1 Mitwirkung: Samira Studer, Mladen Stojiljkovic, Elias Elmiger, David Koelliker (alle VISCHER). Vielen Dank für den fachlichen Input zu dieser FAQ an Phil Lee (FieldFisher), Christian Schröder (Orrick), John Magee (DLA Piper), David Vasella (WalderWyss) und diverse weitere Personen. Der Autor ist zu erreichen unter drosenthal@vischer.com.

2 Inoffizieller Permalink: https://www.rosenthal.ch/downloads/VISCHER-faq-scc-en.pdf.

3 Inoffizieller Permalink: https://www.rosenthal.ch/downloads/VISCHER-faq-scc.pdf.

28. Dezember 2021	Anpassungen aufgrund der EDSA Richtlinien 05/2021 (Ziff. 8, 36 und 37), Hinweis auf zusätzliche neue SCC (Ziff. 1 und 8), neue Frage in Ziff. 34, Erweiterung der Ausführungen zu Schrems II und TIAs aufgrund von Praxiserfahrungen, neuem Erhebungsformular und neuer Übersichtsgrafik (Ziff. 43, 44).

Fragen und Feedback: dataprivacy@vischer.com

Die Fragen:

1. Was sind die wichtigsten Neuerungen?

Die wichtigsten Neuerungen gegenüber den bisherigen Standardvertragsklauseln sind:

- Es werden neu mit einem einzelnen, modularen Dokument mehr Konstellationen von Datenübermittlungen in unsichere Drittländer als bisher abgedeckt (Ziff. 13). Sogar der Auftragsbearbeiter im Europäischen Wirtschaftsraum (**EWR**), der einen Kunden in einem unsicheren Drittland hat, wird künftig die SCC einsetzen können und müssen (Ziff. 33). Die neuen SCC regeln auch inhaltlich mehr als bisher. Es braucht neu keinen separaten Auftragsbearbeitungsvertrag (**ADV**) mehr, da die neuen SCC alle erforderlichen Bestimmungen enthalten (Ziff. 47).
- Es besteht eine unbeschränkte Haftung für Datenschutzverstösse, sowohl unter den Parteien wie auch gegenüber betroffenen Personen (Ziff. 41). Die SCC dürfen nicht verändert oder eingeschränkt werden. Trotzdem wird aber bereits darüber diskutiert, ob und inwieweit sich diese Haftung doch noch einschränken lässt, wenigstens zwischen den Vertragsparteien. Die Frage wird vor allem für Service-Provider wichtig sein (ihr Workaround: Sie werden ihre Verträge mit europäischen Kunden nur über ihre europäischen Gesellschaften schliessen – so kommen die neuen SCC kundenseitig nicht mehr zum Einsatz).
- Die SCC sehen zusätzliche präventive und reaktive Bestimmungen zum Schutz der Daten vor ausländischen Behördenzugriffen vor (Ziff. 43). Die Parteien müssen zusichern, dass sie keinen "Grund zu der Annahme haben" ("no reason to believe"), dass es im Zielland solche Zugriffe ohne Rechtsweggarantie (und gewisse weitere Garantien) gibt, und falls doch eine Behörde den Zugriff versucht, die betroffenen Personen informieren und den Zugriff abzuwehren versuchen. Hierzu muss ein *Transfer Impact Assessment* (**TIA**) durchgeführt werden. Damit vertritt die Europäische Kommission (richtigerweise) einen risikobasierten Ansatz, den inzwischen (mit etwas Zurückhaltung) auch der Europäische Datenschutzausschuss (**EDSA**) akzeptiert[4].
- Die Informations- und Meldepflichten nehmen zu. Neu müssen sogar Unterauftragsbearbeiter die betroffenen Personen über eine Kontaktmöglichkeit informieren (Ziff. 38) und über Zugriffsversuche von ausländischen Behörden (Ziff. 43). Betroffene Personen können auch Einsicht in die von den Parteien abgeschlossenen SCC verlangen. Alle Pflichten zugunsten der betroffenen Personen können diese neu direkt einklagen – oder von Organisationen wie

[4] https://edpb.europa.eu/news/news/2021/edpb-adopts-final-version-recommendations-supplementary-measures-letter-eu_en.

dem *European Center for Digital Rights* (**NOYB**)[5] einklagen lassen (Ziff. 39).

- Leider wird es nicht bei den neuen SCC bleiben. Die Europäische Kommission hat angekündigt, mindestens noch einen weiteren Satz an SCC zu publizieren, weil nach ihrer Ansicht Übermittlungen an Empfänger in unsicheren Drittstaaten, die selbst der DSGVO unterstehen, anderer SCC bedürfen als jene, die bereits genehmigt wurden (Ziff. 8). Dies sorgt mehrheitlich für Unverständnis. Es wird den Umgang mit den neuen SCC noch weiter verkomplizieren.

2. Welche Risiken bringt der Abschluss der SCC für den Exporteur und den Importeur mit sich?

Der Abschluss der neuen SCC birgt unter anderem folgende neue oder erhöhte Risiken:

- Eine unbeschränkte vertragliche Haftung für Datenschutzverstösse, sowohl gegenüber den anderen Parteien im SCC als auch gegenüber den betroffenen Personen. Diese können auch vor einer Vielzahl ausländischer Gerichte geltend gemacht werden.
- Weil die SCC nicht geändert werden dürfen und mehr Themen abdecken als bisher, kann ihre Einführung in bestehenden Vertragsverhältnissen dazu führen, dass die bisherige "Balance" eines Vertragsverhältnisses nicht mehr stimmt – etwa bezüglich Kostentragung, Risikoverteilung und Haftung.
- Betroffene Personen oder Organisationen wie NOYB können die Einhaltung der SCC klageweise durchsetzen. Sie können auch Einblick in die abgeschlossenen SCC nehmen, auch wenn gewisse Teile geschwärzt werden dürfen. Da es mehr Pflichten als bisher gibt, kann auch mehr geltend gemacht werden.
- Der Exporteur ist letztlich für die Einhaltung der SCC auch seitens des Importeurs verantwortlich.
- Der Aufwand zur korrekten Implementation wird deutlich zunehmen. Die Parteien müssen zum Beispiel alle Aktivitäten dokumentieren und diese Dokumentation auf Verlangen der Aufsichtsbehörde vorlegen. Auch müssen sie sich über falsche oder unvollständige Daten gegenseitig informieren. Auch werden für nicht EWR-Länder mit Datenschutzgesetzen länderspezifische Anpassungen gemacht werden müssen, was die Sache weiter verkompliziert. Für die Schweiz hat der EDÖB die neuen SCC mit geringen Anpassungen immerhin bereits anerkannt; der UK ICO dürfte dasselbe tun.

---

5 https://noyb.eu/.

- Service-Provider in Europa müssen ihren Kunden in unsicheren Drittstaaten die SCC in einer reduzierten Variante künftig ebenfalls aufzwingen, sobald sie für sie Personendaten bearbeiten. Ihr Haftungsrisiko nimmt dabei zu – und so auch jenes ihrer Kunden.

3. Ab wann müssen wir die neuen SCC einsetzen?

Hierzu muss unterschieden werden, ob damit ein Datentransfer unter der DSGVO stattfindet oder unter dem DSG.

Unter der DSGVO müssen die neuen SCC in neuen Verträgen ab dem 28. September 2021 eingesetzt werden. Bis zum 27. September 2021 unterzeichnete (alte) SCC müssen bis zum 27. Dezember 2022 abgelöst sein. Wer also noch unbedingt die alten SCC einsetzen will, muss dies vor dem 28. September 2021 getan haben.

Die lange Frist bis zum 27. Dezember 2022 täuscht: Der Einsatz der alten SCC ist ab dem 28. September 2021 nur zulässig, sofern und soweit sich die betreffende Datenbearbeitung nicht verändert und sie weiterhin hinreichend geschützt ist[6]. In der Praxis dürften diese Bedingungen in vielen Fällen nicht erfüllt sein, jedenfalls nicht nach der traditionell strengen Interpretation mancher EU-Datenschutzbehörden. Fast nie der Fall sein wird dies bei einem Intra-Group Data Transfer Agreement (**IGDTA**), über welches schon der Natur der Sache nach sehr viele Datentransfers abgewickelt werden, die Datenbearbeitungen sich nach allgemeiner Lebenserfahrung bis 27. Dezember 2022 auch ändern werden und die Parteien ebenso (z.B. Hinzukauf einer neuen Gesellschaft). Hinzu kommt, dass die EU-Datenschutzbehörden vermutlich den Standpunkt einnehmen werden, dass ohne Zusatzklauseln (wie eine "Defend-your-data"-Klausel, Ziff. 43) die bisherigen SCC ungenügenden Schutz bieten. Daher sollten insbesondere IGDTA bis zum 27. September 2021 auf die neuen SCC überführt werden.

Unter dem DSG ist die Situation im Ergebnis vergleichbar. Die von der Europäischen Kommission gesetzten Fristen haben für die Schweiz zwar keine Verbindlichkeit. Der EDÖB hat mittlerweile jedoch ähnliche Fristen kommuniziert. Für den "Normalfall" gilt grob gesagt: Die alten SCC sollten in der Schweiz nach dem 27. September 2021 nicht mehr neu abgeschlossen werden und die bestehenden Verträge, welche die alten SCC noch nutzen, sollten bis zum 31. Dezember 2022 abgelöst sein oder schon vorher, falls die Datenbearbeitung bzw. der Vertrag "wesentlich verändert" werden (was dies genau bedeutet, sagt er nicht). Dies hat der EDÖB am 27. August 2021 bekanntgegeben.[7]

---

6 Artikel 4 des Beschlusses C(2021) 3972 vom 4. Juni 2021: "[…] provided the processing operations that are the subject matter of the contract remain unchanged and that reliance on those clauses ensures that the transfer of personal data is subject to appropriate safeguards."

7 https://bit.ly/3zQarff.

Rechtlich gesehen muss differenziert werden. Soweit die alten SCC materiell als hinreichend betrachtet werden können, was derzeit unseres Erachtens nach wie vor der Fall ist, können sie rechtlich gesehen beliebig lange eingesetzt werden. Das gilt auch unter dem revidierten DSG (**revDSG**), denn es erhöht die Anforderungen an eine grenzüberschreitende Bekanntgabe von Personendaten nicht. Was sich ändert ist der Mechanismus der Vorlagepflicht gegenüber dem EDÖB (siehe Ziff. 26). An dieser legalistischen Sichtweise hat der EDÖB jedoch aus diversen Gründen kein Interesse. Darum erweckt er den Eindruck, dass künftig nur noch die neuen SCC eingesetzt werden dürfen, während die alten SCC nach seiner Ansicht nunmehr ungenügend werden. Dementsprechend hat er ihre Anerkennung mit Wirkung ab dem 28. September 2021 widerrufen, was aber rechtlich nur bedeutet, dass eine vereinfachte Meldung der alten SCC nach Art. 6 Abs. 3 der Verordnung zum DSG (**VDSG**) ab diesem Tag nicht mehr möglich ist. Sie können dementsprechend nur noch als Garantien "sui generis" gemeldet werden, d.h. unterliegen dann einer Prüfung durch den EDÖB (aber nach wie vor keiner Genehmigung). Seine Ansicht zur Frage, ob die alten SCC noch genügend Schutz bieten, ist zwar nicht verbindlich, aber sie wird ihre Wirkung haben: Im Zusammenspiel mit dem Fakt, dass in der EU nur noch die neuen SCC zum Einsatz kommen dürfen, werden sich diese auch in der Schweiz rasch durchsetzen. Ein Schweizer Sonderweg ist unrealistisch; auch die eigenen SCC des EDÖB haben sich nie wirklich an breiter Front durchgesetzt. Es ist einfacher, dieselbe Vorlage zu verwenden wie (fast das ganze) das restliche Europa. Daher wird sich faktisch die Ansicht durchsetzen, dass die neuen SCC auch nach DSG erforderlich sind, auch wenn es dafür rechtlich keine Basis gibt, da sich weder die Rechts- noch Sachlage geändert hat und es somit keinen (rechtlichen) Grund gibt, warum die bisherigen SCC plötzlich nicht mehr genügen sollten. Wenn dem aber so ist, werden viele Unternehmen sich bemüht sehen, bis zum Inkrafttreten des revidierten DSG mutmasslich am 1. Januar 2023 die neuen SCC auch für die Zwecke des DSG einzuführen und Verträge mit den alten SCC ersetzt zu haben (deshalb hat der EDÖB auch seine Frist auf den 31. Dezember 2022 gesetzt, auch wenn er nicht befugt ist, ein Verfalldatum für den Einsatz der bestehende Garantien verbindlich festzulegen). Treibende Kraft wird hierbei sein, dass unter dem revidierten DSG eine (eventual-)vorsätzliche grenzüberschreitende Bekanntgabe von Personendaten ohne angemessene Schutzmassnahmen strafbar wird. Dieses Risiko wird kaum jemand eingehen wollen. Bis dahin wird aber einem Schweizer Datenbearbeiter kaum Ungemach drohen, wenn er noch die alten SCC einsetzt – selbst wenn die Bedingungen der Europäischen Kommission nicht erfüllt sind und der EDÖB diese nunmehr auch vertritt. Hat er die Verwendung der alten SCC dem EDÖB noch bis zum 27. September 2021 in generischer Weise mitgeteilt (wie wir dies jeweils empfohlen haben und was der EDÖB auch akzeptiert hat), kann der Schweizer Datenbearbeiter die alten SCC rein rechtlich sogar noch nach dem 27. September 2021 neu abschliessen. Selbst nach dem Pa-

pier des EDÖB ist lediglich die *Meldung* der alten SCC nach dem 27. September 2021 nicht mehr möglich; ist sie aber wegen bereits erfolgter Meldung gar nicht nötig, spielt diese Frist für die betreffenden Unternehmen auch keine Rolle, jedenfalls soweit nur die Exportbestimmungen des DSG und nicht auch der DSGVO zu beachten sind.

Unternehmen, die sowohl die DSGVO als auch das DSG befolgen müssen, sollten sich angesichts dieser Ausgangslage an den Vorgaben der DSGVO ausrichten. Dies kann auch Unternehmen betreffen, die "nur" aufgrund von Art. 3 Abs. 2 DSGVO der DSGVO unterliegen und nur in der Schweiz Daten bearbeiten: Unterliegt eine Bearbeitung von Personendaten der DSGVO, müssen die Vorgaben der DSGVO auch bei der Übermittlung von der Schweiz aus in ein Drittland beachtet werden (hier unterscheidet sich die DSGVO von der Schweizer Regelung, die an die Bekanntgabe aus der Schweiz heraus anknüpft).

4. Ab wann dürfen wir die neuen SCC einsetzen?

Die neuen SCC dürfen für die Zwecke von Art. 46 DSGVO seit dem 27. Juni 2021 eingesetzt werden.

In der Schweiz konnten sie seit ihrer Bekanntgabe durch die Europäische Kommission eingesetzt werden. Mittlerweile hat der EDÖB sie auch anerkannt, was ihre Meldung erleichtert (Ziff. 10). Sie ist mittels eines einfachen Briefs möglich (Art. 6 Abs. 3 VDSG).

5. Wo kann ich die neuen SCC herunterladen?

Unter https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj können sie in allen Sprachen der EU heruntergeladen werden, dies sowohl im Format HTML als auch PDF. Es ist zudem ein Sprachenvergleich möglich. Mehrere private Anbieter halten inzwischen auch vorkonfektionierte Fassungen und "Generatoren" bereit (dazu Ziff. 13).

6. In welchen Fällen sind wir zur Verwendung der neuen SCC verpflichtet?

Es gibt rechtlich keinen Zwang, die neuen SCC einzusetzen.

Die neuen SCC werden aber unter der DSGVO in manchen Konstellationen die einzige vernünftige Methode sein, eine Bekanntgabe von Personendaten in ein unsicheres Drittland unter der DSGVO rechtsgenüglich abzusichern. Andere Methoden wie "Binding Corporate Rules" (**BCR**), Einwilligungen oder die weiteren Ausnahmetatbestände werden in manchen Fällen nicht zielführend sein. Es kann sein, dass die Europäische Kommission mit der Zeit noch ein weiteres Set an SCC für die Bekanntgabe von Personendaten in unsichere Drittländer publiziert, aber das wird höchstens zu einem deutlich späteren Zeitpunkt passieren, sollten sich die bestehenden SCC als untauglich oder zu unpraktisch erweisen (vgl. die Mängel in Ziff. 45).

Es ist unter der DSGVO denkbar, dass einzelne Aufsichtsbehörden weitere SCC publizieren, welche von der Europäischen Kommission genehmigt werden müssen (Art. 46 Abs. 2 Bst. d DSGVO), aber damit ist im Moment nicht zu rechnen (mit Ausnahme betreffend ein Mangel der neuen SCC, siehe Ziff. 8).

Die DSGVO sieht schliesslich noch den Einsatz von individuellen Verträgen für Datentransfers in unsichere Drittstaaten vor, die aber von der jeweils zuständigen EU-Aufsichtsbehörde genehmigt werden müssen (Art. 46 Abs. 3 Bst. a DSGVO). Dieser Fall ist unseres Erachtens denkbar, etwa wenn die SCC in modifizierter Form zum Einsatz kommen müssen, um darin enthaltene Fehler zu korrigieren (Ziff. 23) oder weil der Einsatz der SCC wie vorgesehen rechtswidrig wäre, die Anpassung aber den Schutz der betroffenen Personen nicht tangiert.

Unter dem DSG ist die Situation weniger streng. Hier ist es ohne Weiteres denkbar, dass anstelle der SCC alternative Vertragsvorlagen eingesetzt werden – ggf. mit der Konsequenz, dass diese Garantien "sui generis" dem EDÖB vorgelegt werden müssen. Anders als unter der DSGVO ist bleibt unter dem heutigen und revidierten DSG der Datenexporteur dafür verantwortlich, dass die von ihm eingesetzten Verträge einen geeigneten Schutz sicherstellen. Immerhin wird es dem EDÖB unter dem revidierten DSG möglich sein, gegen, nach seiner Ansicht, ungenügende Verträge aufsichtsrechtlich vorzugehen. Es ist denkbar, dass der EDÖB Alternativen zu den SCC akzeptiert, wenn sich die SCC der EU in gewissen Punkten als mangelhaft oder untauglich erweisen. Denkbar ist auch, dass er die im Vereinigten Königreich geplanten eigenen SCC akzeptiert.

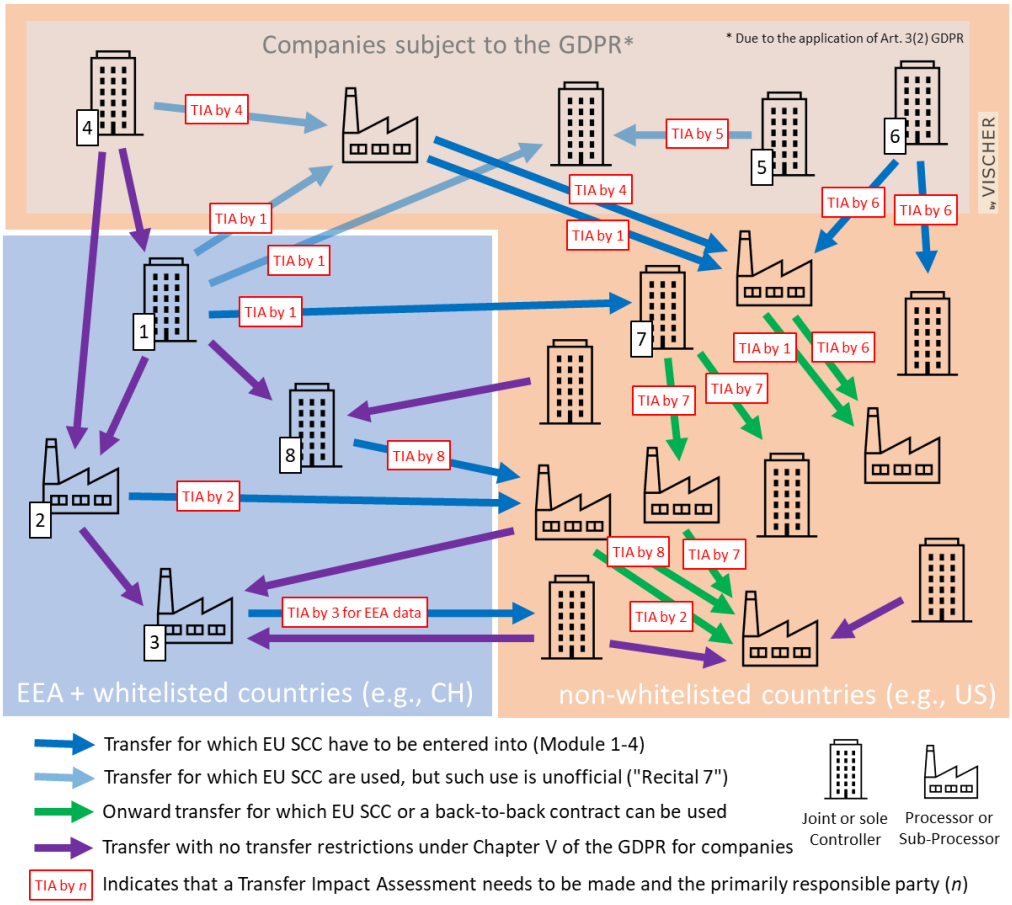
7. Welche Übermittlungen sollten mit den neuen SCC abgedeckt werden?

Es gibt im Wesentlichen drei Arten von Übermittlungen, für welche die Anwendung der neuen SCC in Betracht gezogen werden sollten:

- Personendaten werden von einem für Verantwortlichen oder einem Auftragsbearbeiter (jeweils einschliesslich Unterauftragsbearbeiter), welcher der DSGVO (oder dem DSG) unterliegt, an einen Empfänger in einem unsicheren Drittland übermittelt und der selbst nicht der DSGVO unterliegt. Dies sind die klassischen Fälle, für welche die Europäische Kommission die neuen SCC erlassen hat. Sie sind in der nachstehenden Abbildung als dunkelblaue Pfeile dargestellt.
- Ein für die Verantwortlicher oder ein Auftragsbearbeiter, welcher der DSGVO (oder dem DSG) unterliegt, übermittelt Personendaten an einen Empfänger in einem unsicheren Drittland, aber dieses Mal unterliegt der Empfänger der DSGVO. Offiziell hat die Europäische Kommission die Verwendung der neuen SCC für diese Übermittlungen (noch) nicht genehmigt, aber wir sind der Mei-

nung, dass sie in solchen Fällen trotzdem verwendet werden sollten (siehe dazu Ziff. 8). Diese Übermittlungen sind in der Abbildung als hellblaue Pfeile dargestellt.

- Schliesslich muss jeder Verantwortliche oder Auftragsverarbeiter, der personenbezogene Daten unter den neuen SCC erhält, zumindest unter bestimmten Umständen sicherstellen, dass für die Weiterübermittlung dasselbe Schutzniveau gilt wie nach den neuen SCC vorgesehen; dies kann durch einen Back-to-Back-Vertrag oder durch die Verwendung des neuen SCC geschehen. Diese Übermittlungen sind im Diagramm als grüne Pfeile dargestellt.



Das obige Diagramm veranschaulicht auch die verschiedenen Szenarien, in denen eine Transfer Impact Assessment (**TIA**) erforderlich wird, und wer in erster Linie für die Durchführung dieser Prüfung verantwortlich ist.

Weitere Einzelheiten hierzu finden Sie in Ziff. 43 und 44. Zusammenfassend lässt sich jedoch sagen, dass nach den neuen SCC eine TIA durchgeführt werden muss, bevor die Verträge geschlossen werden. Andernfalls können die Parteien nicht die in Clause 14(a)-(d) der neuen SCC vorgesehenen Zusicherungen geben (d.h. dass die Parteien keinen Grund zur Annahme haben, dass die im Zielland für den Datenimporteur geltenden Gesetze und Praktiken diesen daran hindern, bei der

Bearbeitung der Personendaten seinen Verpflichtungen gemäss den neuen SCC nachzukommen). Die vorgenommene Bewertung muss dokumentiert werden.

Das ist jedoch nicht alles. Eine TIA muss nicht nur für die Übermittlung an den (ersten) Empfänger der Personendaten in einem unsicheren Drittland durchgeführt werden. Eine TIA muss in der Regel auch vor jeder Weiterübermittlung von Personendaten an weitere Empfänger in unsicheren Drittländern erfolgen:

- Falls die Weiterübermittlung immer noch Teil der Bearbeitung des (ursprünglichen) Verantwortlichen ist, bleibt dieser für die Durchführung einer solchen TIA verantwortlich, da er für den Schutz "seiner" Personendaten entlang der Kette der Unterauftragsbearbeiter verantwortlich bleibt, auch wenn die Weiterübermittlung nicht von ihm selbst (sondern von seinem Auftragsbearbeiter oder Unterauftragsbearbeiter) durchgeführt wird.
- Erfolgt die Weiterübermittlung durch einen Verantwortlichen (als den ursprünglichen Empfänger) an einen anderen Verantwortlichen oder Auftragsbearbeiter, so ist dieser (weiterübermittelnde) Verantwortliche dafür verantwortlich, die Bestimmungen über die Weiterübermittlung der neuen SCC einzuhalten. Zu diesem Zweck muss der Verantwortliche selbst die neuen SCC oder einen Back-to-Back-Vertrag abschliessen, um den erforderlichen Schutz der Personendaten während der Weiterübermittlung zu gewährleisten (siehe oben), sofern nicht die Ausnahmen in den neuen SCC greifen. Im Rahmen dieser Verpflichtung muss er auch eine TIA durchführen.

Weitere Informationen zur Durchführung einer TIA finden Sie in Frage 44.

8. Können die neuen SCC für Übermittlungen in unsichere Drittländer auch dann benutzt werden, wenn der Importeur der DSGVO unterliegt?

Ja, aber diesbezüglich ist der Europäischen Kommission ein Fehler unterlaufen, der korrigiert werden wird, denn für diesen Fall sind die neuen SCC *nicht* genehmigt worden. Sanktionen sind hier jedoch vorerst nicht zu erwarten.

In Erwägung 7 des Umsetzungsbeschlusses C(2021) 3972 vom 4. Juni 2021 wird ausgeführt, in welchen Fällen die SCC eingesetzt werden "dürfen". Das ist nicht zum Nennwert zu nehmen, weil die DSGVO nur regelt, wo die SCC zur Erfüllung einer Anforderung der DSGVO benutzt werden kann, aber nicht, wo von der Europäischen Kommission verabschiedete Vertragsklauseln eingesetzt werden dürfen und wo nicht.

In Erwägung 7 wird sowohl der zulässige Exporteur als auch der zulässige Importeur umschrieben:

- Exporteur: Befindet er sich im EWR, ergeben sich keine weiteren Fragen. Das gilt an sich auch, wenn der Exporteur sich zwar nicht im EWR befindet, aber kraft Art. 3 Abs. 2 DSGVO der DSGVO untersteht. Für Exporte in unsichere Drittstaaten musste er schon bisher die Vorgaben von Art. 44 ff. DSGVO einhalten und für diese Zwecke können und sollen die SCC verwendet werden. Das ist in Clause 13 der SCC auch entsprechend abgebildet (dort wird noch zwischen demjenigen Verantwortlichen oder Auftragsbearbeiter unterschieden, der über einen Vertreter nach Art. 27 DSGVO verfügt und demjenigen, der keinen solchen bestellt hat).
- Importeur: Unsicherheiten sind aufgekommen, weil in der Erwägung 7 steht, dass die SCC nur in Fällen eingesetzt werden "dürfen", soweit die Bearbeitung der Daten durch den Importeur nicht unter die DSGVO fällt. Das ist falsch und unseres Erachtens unbeachtlich. Gemäss Art. 44 ff. DSGVO kommt es gerade *nicht* darauf an, ob der Importeur unter die DSGVO fällt, sondern ob er sich in einem sicheren oder unsicheren *Drittland* befindet. Selbst wenn der Empfänger im unsicheren Drittland unter die DSGVO fällt (z.B. ein US-Online-Dienst, der Benutzer im EWR trackt), wird das EWR-Unternehmen, welches ihm Daten sendet, mit ihm die SCC vereinbaren. Das war schon immer so und Hinweise auf einen Systemwandel sind nicht ersichtlich. Umgekehrt ist der Abschluss der SCC nicht nötig, wenn sich der Empfänger in einem *sicheren* Drittland befindet – und zwar gleichgültig, ob der Empfänger unter die DSGVO fällt oder nicht. Tun darf er es aber trotzdem, denn die DSGVO kennt keinen *numerus clausus* der Datenschutzverträge und verbietet auch deren Abschluss selbst dort nicht, wo solche Verträge unnötig sind – solange solche Verträge die Parteien nicht daran hindern die DSGVO anzuwenden, wo sie gilt. Ein überschiessender Einsatz der SCC muss somit entgegen Erwägung 7 erlaubt sein. Es muss sogar erlaubt sein, die SCC zwischen zwei Stellen innerhalb des EWR abzuschliessen, falls das in einem konkreten Einzelfall Sinn macht (z.B. als ADV bei multilateralen Verträgen, wo ein Teil der Parteien in Drittländern sind und andere nicht). Daran ändert auch der Umstand, dass der "Importer" in der Definition in Clause 1(b)(ii) als Stelle "in einem Drittland" bezeichnet wird, nichts.

  Hinzu kommt, dass dort wo die SCC mit Auftragsbearbeitern ausserhalb des EWR abgeschlossen werden, es in der Praxis äussert schwierig ist rechtssicher festzustellen, ob der Auftragsbearbeiter als solcher tatsächlich der DSGVO unterliegt oder nicht. Normalerweise wird er der DSGVO nicht unterliegen, da ein Auftragsbearbeiter natürliche Personen im EWR selbst weder "trackt" noch ein "Targeting" für (seine) Produkte oder Dienstleistungen betreibt. Der EDSA ist in seinen Leitlinien 3/2018 (S. 20 ff.) allerdings strenger und erachtet Auftragsbearbeiter mit Sitz in einem

Drittland, im Falle einer Mitwirkung am Targeting oder Tracking ihres Verantwortlichen, der DSGVO unterstellt.

Die Ausführungen der Kommission haben freilich einen tieferen Grund, der darauf hindeutet, dass es sich hier nicht nur um ein Versehen handelt. Es geht um die Grundsatzfrage, wann Kapitel V der DSGVO (welches die Auslandsübermittlung regelt) überhaupt zur Anwendung kommt. So gibt es Stimmen, die der Ansicht sind, es käme nicht zur Anwendung, wenn der Importeur selbst der DSGVO unterliegt. Eine solche Haltung erscheint nicht wirklich vernünftig. Wenn sie richtig wäre, hätte es "Schrems II" nie gegeben, denn dann wäre die Übermittlungen von Benutzerdaten an Facebook in den USA selbst ohne *Privacy Shield* oder den bisherigen SCC immer rechtens gewesen, da sie vom Kapitel V gar nicht erfasst gewesen wären, weil auch Facebook in den USA aufgrund von Art. 3(2) DSGVO wohl der DSGVO unterstellt ist. Diese Haltung ignoriert allerdings den Umstand, dass sich die Einhaltung der DSGVO in den USA – insbesondere im Falle von Behördenzugriffen – *für in den USA liegende Daten* nicht wirklich durchsetzen lässt.

In der gemeinsamen Stellungnahme des EDSA und des europäischen Datenschutzbeauftragten zum Entwurf der neuen SCC[8] hatten diese beiden Stellen die Kommission bereits gebeten, sich in diesem Punkt höchstens zur Frage zu äussern, für welchen Fall die neuen SCC genehmigt sind, nicht aber dazu, welche Übermittlungen in ein Drittland dem Kapitel V unterliegen. Inzwischen hat der EDSA eine eigene erste Stellungnahme publiziert, in welcher er zum Schluss kommt, dass auch die genannten Übermittlungen an der DSGVO unterstellte Importeure in unsicheren Drittländern dem Kapitel V der DSGVO unterliegen.[9] Er hat sich zudem mit der Kommission darauf geeinigt, dass diese für diesen Fall einen weiteren Satz an SCC erlassen wird. Es bleibt zu hoffen, dass auch die Genehmigung der schon erlassenen neuen SCC auf diesen Fall ausgedehnt wird, damit nicht mit einem zusätzlichen Satz von SCC gearbeitet werden muss; das würde die Handhabung unnötig verkomplizieren.

Bis dahin besteht das Problem, dass in Art. 1 Abs. 1 des derzeitigen Durchführungsbeschlusses zur Genehmigung der neuen SCC[10] festgehalten wird, dass die neuen SCC nur dort einen angemessenen Schutz

---

8 Darin schrieben sie (Teile durch uns hervorgehoben): "27. In view of the above and of the title [of] the Draft Decision, the EDPB and the EDPS understand that the Draft Decision **does not cover**: Transfers to a data importer not in the EEA but subject to the GDPR for a given processing under Article 3(2) GDPR […]. / 28. Keeping this in mind, for the avoidance of doubt, the EDPB and the EDPS **recommend** the Commission to clarify that these provisions are only intended to **address the issue of the scope** of the Draft Decision and the draft SCCs themselves, and **not the scope of the notion of transfers**." (https://bit.ly/3gSC27q).

9 European Data Protection Board (EDPB), Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, 18. November 2021 (Version for public consultation, https://bit.ly/3mDiWWx).

10 Vom 4. Juni 2021, C(2021) 3972.

gewähren, wo der Importeur nicht unter die DSGVO fällt. In der Praxis gibt es bis zur Klärung der Situation zwei Möglichkeiten:

- Es wird für die formal nicht abgedeckten Fälle weiterhin mit den bisherigen SCC gearbeitet, so wie im Falle von Transfers aus dem Vereinigten Königreich. Das geht, soweit die Verträge bis zum 27. September 2021 geschlossen werden, grundsätzlich bis zum 27. Dezember 2022 (vgl. aber Ziff. 3). Bis dahin sollte die obige Situation geklärt sein.
- Die neuen SCC werden verwendet, als wären sie für die hier diskutierten Fälle genehmigt. Verboten ist deren Verwendung mit Sicherheit nicht. Die Frage ist lediglich, ob die neuen SCC als für die hier diskutierten Fälle als genehmigt gelten und sich der Exporteur daher auf Art. 46 DSGVO berufen kann. Dies kann wie folgt begründet werden: Dass die neuen SCC genehmigt sind, ist unstrittig. Art. 46 DSGVO verlangt nur, dass SCC eingesetzt werden, welche erstens genehmigt sind und zweitens "geeignete" Garantien darstellen. Diese Anforderung erfüllen die neuen SCC materiell, denn wenn sie als für einen *keinen* gesetzlichen Regelungen unterstehenden Importeur als "geeignet" gelten, müssen sie *a maiore ad minus* erst recht bei einem Importeur einen geeigneten Schutz vermitteln, der sich zusätzlich an die DSGVO halten muss und ansonsten alle Voraussetzungen eines Importeurs unter den neuen SCC erfüllt. Dies macht die Tatsache, dass die neuen SCC formal nur für den problematischeren Fall genehmigt sind, unseres Erachtens wett und steht jedenfalls mit dem Wortlaut von Art. 46(2)(c) DSGVO nicht im Widerspruch.

Wir empfehlen grundsätzlich die letztere Vorgehensweise, wo ein Abwarten keine vernünftige Option ist. Wir gehen davon aus, dass die Datenschutzbehörden nicht gegen Unternehmen vorgehen werden, die auf diese Weise verfahren. Ein Vertreter des BayLDA hat sich bereits in dieser Richtung geäussert.

Der EDÖB hat sich zu dieser Frage bisher nicht geäussert.[11] Es ist aber davon auszugehen, dass aus seiner Sicht die SCC für alle Exporte in unsichere Drittstaaten verwendet werden können. In seinem Papier zur Anerkennung der neuen SCC spricht er lediglich davon, dass sie für Übermittlungen in "unsichere" Drittstaaten verwendet werden können, ohne danach zu differenzieren, ob der Empfänger noch dem DSG untersteht. Das würde aus denselben Gründen wie unter der DSGVO auch im DSG keinen Sinn machen. Es gibt hier also keine Einschränkung.

---

11 https://bit.ly/3zQarff.

9. Gibt es Fälle, in denen wir die neuen SCC nicht einsetzen dürfen?

Nein, die SCC dürfen rein rechtlich gesehen in jeder Konstellation eingesetzt werden. Aber: als "genehmigte" SCC im Sinne der DSGVO gelten sie nur in den von SCC selbst vorgesehenen Fällen. Es gibt somit einen offiziellen und einen inoffiziellen Einsatzbereich der SCC. Ein *offizieller* Einsatz erfolgt als Absicherung im Sinne von Art. 46 DSGVO zwischen einem Exporteur, welcher unter die DSGVO fällt, und einem Importeur der sich in einem unsicheren Drittland befindet. Ein *inoffizieller* Einsatz läge z.B. vor, wenn der Importeur neben seinem Hauptsitz in einem unsicheren Drittland (z.B. USA) auch eine Zweigniederlassung in einem sicheren Drittland (z.B. Schweiz) oder im EWR unterhält, welche natürlich ebenfalls an den Vertrag gebunden ist, auch wenn Datenübermittlungen an die Zweigniederlassung keine SCC erfordern.

Zur Frage der Verwendung der neuen SCC für den Fall, dass sich der Importeur zwar in einem unsicheren Drittland befindet, selbst aber der DSGVO untersteht, vgl. Ziff. 8.

Eine andere Frage ist, ob die SCC auch dann als genehmigte SCC für die Zwecke von Art. 28(7) DSGVO gelten, wenn sie als ADV zwischen zwei Parteien im EWR oder einem sicheren Drittland zum Einsatz kommen (dazu Ziff. 47). Diese Konstellation kann in einem IGDTA vorkommen (Ziff. 17).

10. Sind die neuen SCC vom EDÖB anerkannt? Braucht es überhaupt seine Anerkennung?

Ja, der EDÖB hat sie am 27. August 2021 anerkannt.[12]

Die Anerkennung ist rechtlich zwar nicht erforderlich – es liegt in der Verantwortung des Exporteurs von Personendaten, für einen angemessenen Schutz zu sorgen. Art. 6 Abs. 3 DSG sieht jedoch vor, dass vertragliche Garantien (und darum handelt es sich bei den SCC) dem EDÖB zur Stellungnahme vorgelegt werden müssen. Sind solche von ihm anerkannt (wie z.B. die bisherigen SCC dies waren), genügt ein einfacher Brief, in welchem dem EDÖB erklärt wird, dass das betreffende Unternehmen sie zum Einsatz bringt (Art. 6 Abs. 3 VDSG).

Es war zu erwarten, dass der EDÖB die SCC in der einen oder anderen Form anerkennen wird. Hätte er dies nicht getan, würde er mit Prüfungsgesuchen überschwemmt werden, was praktischerweise nicht zu handhaben wäre. Offen war, ob es er die SCC in ihrer "reinen" Form (wie von der Europäischen Kommission verabschiedet) anerkennt oder ob er Modifikationen zulässt oder verlangt, um sie an die schweizerischen Verhältnisse anzupassen. Er hat sich für einige wenige, jedoch

---

12 https://bit.ly/3zQarff.

einfach zu implementierte und DSGVO-kompatible Anpassungen entschieden.

Aus Schweizer Sicht führen die SCC im Übrigen dazu, dass für Importeure strengere Regeln gelten als für sie nach DSG gelten würde. Das liegt daran, dass die SCC sehr weitgehende Pflichten vorsehen, die mitunter sogar über das Niveau der DSGVO hinausgehen.

Unter dem revidierten DSG führt die Anerkennung durch den EDÖB dazu, dass dem EDÖB gar nichts mehr gemeldet werden muss (Art. 16 Abs. 2 Bst. d revDSG). Wer hingegen eine nicht oder nicht mehr anerkannte Vertragsvorlage einsetzt, der wird sie dem EDÖB weiterhin melden müssen (Art. 16 Abs. 2 Bst. b revDSG). Das gilt nun auch die alten SCC, deren Anerkennung am 27. September 2021 abläuft. Sie können zwar rechtlich noch eingesetzt werden, Neuabschlüsse oder Vertragsanpassungen werden ihm aber gemeldet werden müssen und ihm wohl auch erklärt werden muss, warum sie nach wie vor als hinreichend erachtet werden, einen "geeigneten Datenschutz" zu gewährleisten (was Art. 16 Abs. 2 revDSG verlangt). Wir gehen davon aus, dass dies ausser in Spezialkonstellationen niemand mehr tun wird. Bis zum Inkrafttreten des revDSG mutmasslich am 1. Januar 2023 werden die neuen SCC die alten weitgehend ersetzt haben.

11. Gibt es eine Rückwirkung der neuen SCC?

Formal haben die SCC keine Rückwirkung. Es sind aber zwei Dinge zu beachten:

- Erstens sehen die neuen SCC vor, dass die Parteien dafür einstehen müssen, dass sie zum Zeitpunkt der Vereinbarung der SCC keinen Anlass zur Annahme haben, dass sie die aufgrund des nationalen Rechts des Importeurs die SCC nicht eingehalten werden können (Clause 14(a), Einleitung von Clause 8). Weitere solche Zusicherungen gibt es im Gegensatz zu den bisherigen SCC nicht. Dies bedeutet, dass die SCC an sich nur und erst ohne Vertragsverletzung abgeschlossen werden können, wenn die bisherige Rechtslage diesbezüglich geklärt worden ist. In der Praxis dürfte dies allerdings häufig nicht vorkommen. Zu den Zusicherungen vgl. Ziff. 42.
- Zweitens sehen die neuen SCC primär seitens des Importeurs etliche Pflichten vor, die ab der ersten Minute gelten, einschliesslich bestimmter Informationspflichten (Ziff. 38). Auch dies bedeutet in der Praxis, dass die bisherigen Massnahmen des Importeurs in der Regel angepasst werden müssen, bevor die neuen SCC abgeschlossen werden können.

12. Gibt es eine "de minimis"-Regelung, d.h. Fälle, in denen die SCC nicht zu vereinbaren sind?

Nein. Dies ist jedoch nicht eine Frage der SCC, sondern der anwendbaren Bestimmungen der DSGVO oder des DSG zum Transfer von Personendaten in unsichere Drittstaaten. Die dort festgehaltenen Angaben gelten für alle Übermittlungen von Personendaten in unsichere Drittstaaten, auch wenn sie nur geringfügiger Natur oder nicht besonders heikel erscheinen. Dass dem in der Praxis häufig nicht nachgelebt wird (z.B. im Rahmen der Übermittlung einer einzelnen E-Mail an einen Empfänger in den USA) ist eine andere Frage.

13. Wie handhaben wir die neuen SCC praktisch? Wie "wählen" wir die Module aus?

Die neuen SCC können nicht integral, so wie sie sind, gültig vereinbart werden. Sie enthalten Vertragsklauseln für vier unterschiedliche Fallkonstellationen, die alternativ oder parallel zum Einsatz kommen. Dies bedeutet, es muss zuerst entschieden werden, welche Fallkonstellation(en) zum Einsatz kommt (bzw. kommen) und diese Komponenten müssen entsprechend bezeichnet werden. Gestützt darauf leitet sich aus der Vorlage dann der zu vereinbarende Vertragstext ab.

Eine anschauliche Darstellung der einzelnen Fallkonstellationen und welche Module der SCC zu verwenden sind (siehe Abbildung) haben die Kollegen von WalderWyss publiziert.[13]

Es gibt grundsätzlich drei Möglichkeiten, wie vor diesem Hintergrund die neuen SCC zum Einsatz kommen, d.h. vereinbart werden können:

- Es werden aus dem Vorlagentext jene Teile übernommen, die Geltung haben sollen. Es gibt bereits verschiedene Kanzleien, die solche vorkonfektionierte Vertragssätze bereits fixfertig anbieten oder Generatoren zur deren Erstellung betreiben.[14] Bei der Verwendung dieser Angebote ist allerdings genau darauf zu achten, ob nicht trotzdem noch Anpassungen vorgenommen werden müssen;

---

13 https://datenrecht.ch/neue-standardklauseln-uebersicht-wann-sind-welche-module-zu-verwenden/.

14 Öffentlich: https://www.essentialguarantees.com/scc/, http://scc.twobirds.com (Bird & Bird), https://www.oppenhoff.eu/de/legaltech/scc-generator (Oppenhoff), https://www.taylorwessing.com/de/online-services/scc-generator (TaylorWessing), https://www.lauxlawyers.ch/neue-eu-standardvertragsklauseln/ (LauxLawyers), https://bit.ly/3qeBI7b (WalderWyss).

nebst den vier Modulen gibt es noch diverse weitere Optionen, die gewählt werden müssen; es kann auch nicht nur auf die grau hervorgehobenen Modulbezeichnungen geachtet werden (Verweise auf die Module finden sich teilweise auch im Text, z.B. in Clause 14(e) und (f); Clause 7 wiederum ist für alle Module optional).

Einschränkend ist bei dieser Vorgehensweise ferner zu beachten, dass die Klausel der SCC, welche die Weitergabe von Daten durch den Importeur regelt ("Onward transfers") auf die vollständigen Klauseln verweist (d.h. die SCC mit *allen* Modulen), die bei dieser Vorgehensweise fehlen. Es besteht ein Restrisiko, dass das Weglassen der nicht verwendeten Module dazu führt, dass der Importeur sich nicht auf die weggelassenen Module berufen kann (da sie nicht mehr Bestandteil der "Clauses" sind) und damit weniger Möglichkeiten zur Weitergabe hat. Wir erachten das Risiko jedoch als relativ gering; dieser redaktionelle Fehler der SCC blieb bisher auch weitgehend unbemerkt.

- Es wird eine Vereinbarung geschlossen (z.B. in Form eines Deckblatts), an welche die vollständigen SCC angehängt werden und in welcher festgelegt wird, welches Modul bzw. welche Module der SCC in welcher Konstellation gelten sollen. Im Deckblatt kann auch bestimmt werden, welche Optionen gewählt werden und wie die einzelnen Felder und Anhänge auszufüllen sind. Diese Variante hat den Nachteil, dass sie zu einem längeren Vertragsdokument führt, aber es muss zugleich nicht kontrolliert werden, ob die Teile aus der SCC-Vorlage richtig zusammengestellt wurde; es kann der von der Europäischen Kommission verabschiedete Text integral übernommen werden.
- Es wird wie vorstehend mit einer separaten Vereinbarung gearbeitet, allerdings werden die SCC nicht als Anhang angehängt, sondern sie inklusive Auswahl der betreffenden Module und Optionen "nur" qua Referenz zum Vertragsbestandteil erklärt – so wie AGB ebenfalls Vertragsbestandteil werden können, wenn sie korrekt eingebunden werden.[15] Die Zulässigkeit dieser Vorgehensweise ist keine Frage der DSGVO, sondern des anwendbaren Vertragsrechts. Unter Schweizer Recht ist diese Vorgehensweise zulässig, da der Vertragsinhalt für die Parteien nicht nur klar bestimmbar, sondern auch jederzeit via Internet zugänglich ist, da es sich um eine behördliche Entscheidung handelt. Wichtig ist allerdings eine klare Referenz auf die Vorlage der SCC in der amtlichen Fassung, ggf. mit einem entsprechenden Internet-Link auf die offizielle Website der EU. Die Gültigkeit einer solchen Integra-

---

15 Gauch/Schluep/Schmid, Schweizerisches Obligationenrecht Allgemeiner Teil ohne ausservertragliches Haftpflichtrecht, 2008, N 1140b.

tion ist offenbar auch nach deutschem Recht gegeben. Diese "incorporation by reference" ist die schlankste Vorgehensweise.

Aus unserer Sicht sind alle drei Varianten rechtlich gleichwertig. In der Praxis rechnen wir damit, dass sich in Standardsituationen (z.B. Vereinbarung mit einem Cloud-Provider) die erste Variante durchsetzen wird. In einem IGDTA oder dort, wo mehrere Module parallel gelten, dürfte tendenziell die zweite oder dritte Variante zum Einsatz kommen.

14. Müssen die neuen SCC eigenhändig unterzeichnet werden oder genügt eine elektronische Unterschrift?

Nein, Verträge basierend auf den neuen SCC müssen nicht mit einer eigenhändigen Unterschrift versehen werden. In Annex I.A des Appendix ist zwar von der "Unterschrift" jeder einzelnen Partei die Rede; auch Clause 7 spricht davon, dass eine Partei die SCC "unterzeichnet".

Erforderlich ist unseres Erachtens aber lediglich – wie bisher – ein Nachweis durch Text, d.h. der Inhalt der Willenserklärung der Partei, die sich an die SCC bindet, muss textlich erkennbar und festgehalten sein. Diese Voraussetzung kann durch "Click"-Erklärungen erfüllt werden. In diese Kategorie fallen auch die mittels einfacher Signatur-Systeme wie "DocuSign" oder "Adobe Sign" bestätigten Verträge. Wäre dem nicht so, wäre der Abschluss der SCC im Online-Kontext faktisch nicht mehr möglich. Es gibt keinen Grund zu der Annahme, dass dies beabsichtigt gewesen wäre.

15. Was ist beim Anpassen bestehender Verträge mit den bisherigen SCC zu beachten?

Zu beachten sind insbesondere folgende Punkte:

- Der Appendix der neuen SCC erfordert mehr Angaben als für die bisherigen SCC benötigt wurde (Ziff. 19).
- Die technische und organisatorische Massnahmen (**TOMS**) müssen unter den neuen SCC zusätzliche Aspekte abdecken und detaillierter sein (Ziff. 18).
- Die neuen SCC regeln mehr als die bisherigen SCC (z.B. Haftung), und beanspruchen auch für diese zusätzlichen Regelungen Vorrang. Dies kann dazu führen, dass Teile der bisherigen Vereinbarung (z.B. ein ADV) plötzlich im Konflikt mit den neuen SCC stehen und es zu einer Veränderung der Risikoverteilung zwischen den Parteien kommt.
- Weil die neuen SCC in mehr Fallkonstellationen zum Einsatz kommen können, kann es erforderlich sein, diese ebenfalls abzudecken (Ziff. 16).
- Die neuen SCC sind derzeit erst für Übermittlungen von Daten unter der DSGVO und unter dem DSG (Ziff. 10) freigegeben. Ob

sie auch für die Absicherung von Datentransfers unter anderen Datenschutzgesetzen als den beiden benutzt werden können, ist separat zu prüfen. Für das Vereinigte Königreich ist dies z.B. noch nicht der Fall, aber mit Anpassungen vorgesehen (Ziff. 22).

Ferner sind die zeitlichen Vorgaben für Anpassungen zu berücksichtigen (Ziff. 3, Ziff. 4).

Es ist leider nicht möglich, in einem Vertrag die bisherigen SCC einfach durch einen Verweis auf die neuen SCC auszutauschen, da die neuen SCC aufwändiger als bisher "konfektioniert" werden müssen, da nicht nur das oder die betreffenden Module gewählt werden müssen, sondern auch die diversen Optionen. Anders als die bisherigen SCC kann die von der Europäischen Kommission verabschiedete Vorlage für die neuen SCC nicht integral als Vertragstext vereinbart werden; es ist dies nur eine Vorlage, die der jeweiligen Fallkonstellation anzupassen ist (Ziff. 13).

16. Können mehrere Module zwischen denselben Parteien zugleich vereinbart werden?

Ja, dies ist möglich. Clause 2(a) erwähnt explizit die Möglichkeit der Wahl mehrerer Module.

Konzernintern ist es z.B. üblich, dass eine Konzerngesellschaft gegenüber einer Konzerngesellschaft sowohl als Auftragsbearbeiterin wie auch als Verantwortliche auftritt. Diese Datenflüsse wurden bisher in einem einzigen Vertrag (IGDTA) geregelt, der bisher die jeweiligen SCC zur Anwendung brachte. Neu wird ein solches IGDTA die jeweiligen Module der SCC zur Anwendung bringen.

17. Wie ist mit mehreren Parteien umzugehen? Braucht es noch ein IGDTA?

Die neuen SCC können von mehr als nur zwei Parteien zugleich abgeschlossen werden. Das war auch bei den bisherigen SCC schon möglich und wurde regelmässig praktiziert. Neu sehen die neuen SCC die (optionale) Clause 7 vor, welche einen solchen späteren "Beitritt" weiterer Parteien ausdrücklich regelt. Der Beitritt erfolgt dadurch, dass kurzerhand die Liste der Parteien ergänzt und mit einer weiteren Unterschrift versehen wird.

Die Regelung in Clause 7 ist leider schlecht formuliert und nicht zu Ende gedacht. So heisst es zwar, dass eine neue Partei nur mit der Zustimmung (aller) anderen Parteien beitreten kann, aber wie diese Zustimmung der anderen Parteien zustande kommt und zum Ausdruck gebracht werden muss, bleibt offen. Laut Clause 7 genügt eine einseitige Willenserklärung der neu hinzutretenden Partei, um Partei zu werden. Das kann nicht ernsthaft so gemeint sein.

Wir empfehlen daher, auf Clause 7 zu verzichten (sie ist optional) und den Beitritt weiterer Parteien in Verhältnissen, wo es öfters zum Wechsel oder zur Erweiterung der Parteien kommt, in einer separaten Vereinbarung zu regeln.

In einer solchen separaten Vereinbarung kann auch das Verfahren der Vertragsanpassung geregelt werden, ebenso die Kostentragung, der Informationsaustausch und die weiteren Punkte, welche die SCC nicht regeln. Die neuen SCC sind daher kein Ersatz für ein IGDTA.

18. Können wir unsere bisherigen TOMS auch unter den neuen SCC weiterverwenden?

Ja, aber sie genügen nicht mehr.

Nach dem Titel nach enthält Annex II des Appendix zwar nach wie vor technischen und organisatorische Massnahmen der Datensicherheit. Die Beispiele und auch die SCC verlangen hier aber mehr als nur Massnahmen zur Datensicherheit. Die TOMS unter den neuen SCC müssen auch Massnahmen zur Umsetzung bzw. Gewährleistung der Betroffenenrechte und Bearbeitungsgrundsätze enthalten.

Das ist vor dem Hintergrund des "Privacy by Design" zwar sinnvoll, geht aber weiter als das, was die heutigen TOMS regelmässig vorsehen. Sie müssen daher um Massnahmen zur Datenminimierung, zur Datenqualität, zur Speicherbegrenzung, zur Rechenschaft und zu den Betroffenenrechten vorsehen (die Beispiele in Annex II beschränken sich auf Datenportabilität und Löschpflicht).

Ferner halten die Erläuterungen im Annex II fest, dass die TOMS "konkret (nicht allgemein) beschrieben" sein müssen. Die meisten heutigen TOMS in ADVs und SCC dürften diese Anforderung nicht erfüllen, da sie üblicherweise auf ein bis drei Seite vergleichsweise generisch abgefasst sind. Der Annex II zählt Kategorien von Massnahmen auf (wie z.B. "Massnahmen zur Identifizierung und Autorisierung der Nutzer"), die dann näher auszuführen sind. Gemäss den Erläuterungen ist "klar anzugeben, welche Massnahmen für jede Datenübermittlung bzw. jede Kategorie von Datenübermittlungen gelten".

19. Können wir unsere bisherigen Umschreibungen der Datenübermittlungen unter den neuen SCC weiterverwenden?

Ja, aber sie genügen nicht mehr.

Das Konzept ist dasselbe geblieben: Über Annex I.B des Appendix wird der "Transfer" umschrieben und damit zugleich definiert, für welche Übermittlung von Personendaten oder – breiter formuliert – für welche Bearbeitungsaktivitäten die konkret vereinbarten SCC gelten.

In diesem Zusammenhang war es bisher üblich, die Umschreibung der Datenübermittlungen sehr breit zu umfassen, damit garantiert alle er-

fasst waren ("catch all"). Dies wird vermutlich auch weiterhin so praktiziert werden.

Deckt eine Vereinbarung eine Mehrzahl von (Arten von) Datenübermittlungen ab, so wird künftig aber wohl erwartet werden, dass diese voneinander getrennt aufgeführt werden (z.B. in einzelnen Anhängen oder Abschnitten). Die SCC selbst halten in einer Erläuterung zum Appendix fest, dass es möglich sein müsse, "die für jede Datenübermittlung oder jede Kategorie von Datenübermittlungen geltenden Informationen klar voneinander zu unterscheiden und in diesem Zusammenhang die jeweilige(n) Rolle(n) der Parteien als Datenexporteur(e) und/oder Datenimporteur(e) zu bestimmen". Dies ist mit einer "catch all"-Formulierung nicht ohne weiteres möglich.

Hinzu kommt, dass die Aufzählung der zu liefernden Angaben umfassender als bisher ist. Zusätzlich erforderlich sind folgende Angaben:

- Die besonderen Beschränkungen, die für besonders schützenswerte Personendaten ("sensitive data", besondere Kategorien von Personendaten) gelten sollen. Für solche Personendaten verlangen die SCC nämlich, dass zusätzliche Massnahmen definiert werden.
- Die Häufigkeit der Bekanntgabe von Personendaten (einmalig, regelmässig).
- Die Aufbewahrungsfrist der Personendaten oder die Kriterien zu deren Berechnung.
- Die "Natur" der Bearbeitung (nach unserem Verständnis beschreibt dies die Vorgänge wie Erhebung, Erfassung, Veränderung, Strukturierung, Speicherung, Abruf, Abfrage, Weitergabe, Verbreitung, Verknüpfung, Abgleich, Einschränkung, Löschung, Übermittlung von personenbezogenen Daten).
- Im Falle einer Auftragsbearbeitung deren Dauer und Gegenstand (was sich allerdings bereits aus Art. 28(3) DSGVO ergibt).

Wir gehen davon aus, dass die Umschreibungen der einzelnen Datenübermittlungen trotz allem weiterhin vergleichsweise generisch sein werden, da sie primär dazu dienen, die Eckwerte der Bearbeitungsaktivitäten zu erfassen, nicht aber sie in der Sache näher zu regeln.

20. Welche Rechtswahl und welchen Gerichtsstand dürfen und sollen wir vereinbaren?

Werden die neuen SCC zur Absicherung von Transfers von Personendaten nach DSGVO abgeschlossen, so muss das Recht eines Mitgliedsstaats des EWR (Clause 17) und ein Gerichtsstand im EWR (Clause 18) gewählt werden – mit Ausnahme von Modul 4 (Processor-Controller).

Das gewählte Recht muss durch Dritte einklagbare Ansprüche ermöglichen, da die neuen SCC solche Rechte zugunsten Dritter für die be-

troffenen Personen vorsehen; Clause 17 hält dies ausdrücklich fest. Das irische Recht, das insbesondere bei grossen Online-Anbietern wie Microsoft beliebt ist, sah dies bisher beispielsweise nicht vor, wurde jetzt aber eigens für die neuen SCC angepasst (aber nur für die neuen SCC).

Welches Recht innerhalb des EWR gewählt wird, ist nicht vorgeschrieben. Es muss insbesondere nicht das Recht am Sitz des Exporteurs sein. Dies erlaubt es den Parteien, das für sie in Bezug auf Ansprüche von betroffenen Personen günstigste Recht zu wählen, um ihr Haftungsrisiko und Ansprüche auf Realerfüllung zu beschränken oder zu erschweren. Welches Recht sich hier am besten anbietet, können wir noch nicht beurteilen.

Mit Bezug auf den Gerichtsstand funktioniert dies nicht, denn dieser ist nicht abschliessend vereinbart. Auch wenn ein Land als Gerichtsstand gewählt wird, wird es in der Regel möglich sein, eine Partei auch an ihrem Sitz in einem anderen Land einzuklagen, wenn dies günstiger erscheint. Auf Klagen betroffener Personen hat der Gerichtsstand sowieso keine Auswirkung: Die betreffenden Clause 18(a) und Clause 18(b) gelten für sie gemäss Clause 3(a) nicht. Für sie gilt stattdessen Clause 18(c), welcher einen nicht ausschliesslichen Gerichtsstand an ihrem gewöhnlichen Aufenthaltsort begründet.

Unsauber an der gesamten Regelung von Clause 18 ist allerdings, dass immer jeweils nur auf das Land verwiesen wird, nicht den Gerichtsbezirk. Wer klagen will, muss daher zunächst nach dem innerstaatlichen Prozessrecht ermitteln, welches Gericht örtlich zuständig ist. Nach unserer Ansicht ist es hingegen zulässig, in Clause 18 dieses Gericht gleich festzuhalten – dies wirkt sich ohnehin nur *inter partes* aus.

Werden die neuen SCC (nur) für Schweizer Exporte von Personendaten abgeschlossen, können statt dem Recht eines EWR-Landes und einem EWR-Gerichtsstand auch Schweizer Gericht und ein Schweizer Gerichtsstand gewählt werden. Erforderlich ist dies aus Sicht des Schweizer Rechts aber nicht; auch der EDÖB verlangt dies nicht. Nach DSG kommt es nur darauf an, dass der Vertrag wie angedacht gilt und durchsetzbar ist – auch wenn dies unter fremden Recht und durch fremde Richter geschieht. Wesentlich ist nur, dass deren Entscheide in der Schweiz vollstreckt werden, was im Fall europäischer Gerichte kein Hindernis sein sollte. Wie die SCC vorsehen muss das gewählte Recht auch aus Schweizer Sicht Ansprüche von Drittbegünstigten zulassen.

Unterliegt lediglich der Auftragsbearbeiter der DSGVO (also im Falle von Modul 4), so kann er einen beliebigen Gerichtsstand und ein beliebiges Recht wählen (soweit es Ansprüche zugunsten Dritter zulässt), was insofern sinnvoll ist, dass er so wenigstens in diesem Punkt dem Verantwortlichen (typischerweise seinem Kunden) entgegenkommen kann. Hat also ein Hosting-Provider im EWR einen Kunden in den USA, so wird er zwar die neuen SCC abschliessen müssen (Ziff. 33), aber er

kann diese immerhin US-Recht unterstellen und als Gerichtsstand für Streitigkeiten unter den SCC der Gerichtsbarkeit die USA wählen – falls der Kunde dies wirklich will.

21. Umfasst der Verweis auf EU Mitgliedstaaten auch Mitgliedstaaten nur des EWR?

Ja, die DSGVO ist nicht nur Teil des Unionsrechts, sondern auch EWR-Rechts. Der EWR besteht aus der EU und den EFTA-Mitgliedstaaten ohne die Schweiz (Island, Liechtenstein und Norwegen). Die DSGVO gilt in diesen drei Ländern direkt. Sie sind auch keine Drittstaaten aus Sicht der EU. Wo in den SCC auf "EU Mitgliedstaaten" verwiesen wird, sind daher auch Mitgliedstaaten (nur) des EWR gemeint.

22. Was gilt mit Bezug auf das Vereinigte Königreich?

Für Transfers von Personendaten ins Vereinigte Königreich werden die neuen SCC weder aus Sicht des EWR noch aus der Schweiz erforderlich sein, da das Vereinigte Königreich als sicheres Drittland gilt.

Für Exporte aus dem Vereinigten Königreich in unsichere Drittstaaten gelten die neuen SCC nicht, d.h. sie dürfen in diesen Fällen nicht eingesetzt werden. Für solche Exporte müssen noch die alten SCC benutzt werden, was insbesondere im Falle der Erneuerung von IGDTAs zu beachten ist, sofern diese – wie häufig der Fall – auch Exporte aus dem Vereinigten Königreich abdecken sollen.

Hier bietet sich als Praktikerlösung an, dass neue IGDTA die in aller Regel bereits bestehenden IGDTAs nur soweit ablösen, als sie *nicht* Transfers von Personendaten aus dem Vereinigten Königreich in unsichere Drittstaaten betreffen. Bis eine neue Lösung auch für das Vereinigte Königreich vorliegt, bestehen bei dieser Vorgehensweise somit zwei parallele Verträge, was unseres Erachtens sinnvoller ist, als ein kombiniertes, dafür sehr kompliziertes IGDTA neu abzuschliessen – nur um es in Kürze wieder anpassen zu müssen.

Die britische Datenschutzbehörde ICO arbeitet derweil an eigenen SCC. Am 11. August 2021 hat sie eine Vernehmlassung für diese gestartet, die noch bis zum 4. Oktober 2021 dauert.[16] Neben eigenen SCC plant der ICO auch eine Anerkennung der SCC der Europäischen Kommission, wobei diese in einem Anhang auf die Bedürfnisse des UK GDPR angepasst werden müssen. Dies dürfte sich jedoch leicht umsetzen lassen. Viele haben damit schon begonnen, obwohl ein solcher Einsatz noch nicht genehmigt worden ist.

---

16 https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-on-data-transferred-outside-of-the-uk/.

23. Was ist, wenn uns eine Klausel in den neuen SCC nicht passt?

Clause 2(a) stellt klar, dass die SCC unverändert und integral übernommen werden müssen, soweit sie nicht selbst Bestimmungen als Optional vorsehen oder Wahlmöglichkeiten bieten. Die SCC dürfen zwar in einen umfangreicheren Vertrag eingebettet werden (z.B. ein IGDTA oder einen Providervertrag), aber dieser andere Vertrag darf den Bestimmungen der SCC weder direkt noch indirekt widersprechen oder die Rechte der betroffenen Personen einschränken. Hierzu hält Clause 5 fest, dass die Bestimmungen der SCC einem solchen Vertrag vorgeht.

Es wird in den kommenden Monaten zweifellos eine Diskussion darüber entstehen, inwiefern Ergänzungen oder Präzisierungen zu den SCC möglich sind. Aus unserer Sicht sind solche zulässig, ja sogar aus praktischer Sicht erforderlich (dazu Ziff. 24).

Auch wenn die SCC an sich unverändert übernommen werden müssen, so sind Anpassungen trotz allem in gewissen Ausnahmesituationen denkbar:

- Dort, wo die SCC für Fälle eingesetzt werden, für welche sie nicht gedacht sind, so z.B. für den Datentransfer zwischen Parteien, die sich im EWR oder in sicheren Drittstaaten befinden, oder für Datentransfers, die nicht der DSGVO unterliegen. Siehe auch Ziff. 8. Insbesondere in einem IGDTA kann es vorkommen, dass mit einem Set an Vertragsklauseln auch Datentransfers aus anderen Rechtsordnungen mit Datenschutzgesetzen geregelt werden müssen, für welche die SCC leicht anzupassen sind. In solchen Fällen können die SCC angepasst werden. Die unveränderte Übernahme gilt nur dort, wo auf sie als vertragliche Garantien nach Art. 46(2)(c) DSGVO abgestellt werden soll. Selbst wo die Klauseln als ADV verwendet werden, dürfen sie verändert werden (wer dies jedoch tut, kann sich nicht mehr auf die Anerkennung nach Art. 28(7) DSGVO abstützen).
- Abgeänderte SCC können zumindest theoretisch von einer zuständigen EWR-Datenschutzbehörde genehmigt werden (Art. 46(3)(a) DSGVO).

Die Unveränderlichkeit der SCC (und auch der SCC-ADV) ist im Übrigen nichts als konsequent: Es sind nicht bloss Hilfestellungen zur Vertragsredaktion, sondern sie gelten als für die Zwecke von Art. 46 DSGVO bzw. Art. 28 DSGVO hinreichend, selbst wenn sie es materiell nicht sein sollten. Dies bedingt naturgemäss, dass sie wie genehmigt eingesetzt werden müssen.

24. Können wir die SCC mit eigenen Regelungen ergänzen und präzisieren?

Ja, dies ist ohne Weiteres möglich, muss aber über einen separaten Vertrag erfolgen und die eigenen Regelungen dürfen den durch die SCC beabsichtigten Schutz nicht schwächen und den SCC auch nicht widersprechen. Clause 5 hält in diesem Zusammenhang zusätzlich fest, dass im Falle von Widersprüchen die Bestimmungen der SCC vorgehen.

Die SCC dürfen zwar als solche nicht verändert werden und auch dürfen sie nicht durch andere Bestimmungen übersteuert werden, aber sie dürfen Teil eines breiteren Vertragswerks sein, wie Clause 2(a) ausdrücklich festhält. In diesem Vertragswerk können durchaus auch Fragen des Datenschutzes geregelt sein.

Das können beispielsweise zusätzliche Aspekte sein, die in den neuen SCC nicht oder nur lückenhaft geregelt sind (wie beispielsweise die Folgen der Ablehnung eines Unterauftragsbearbeiters), aber auch ausführende Bestimmungen sein (wie beispielweise die Art und Weise, wie die Instruktionen des Verantwortlichen gegenüber dem Auftragsbearbeiter ermittelt werden, was insbesondere für Anbieter von standardisierten Dienstleistungen wichtig sein wird).

Wesentlich ist in Bezug auf solche Präzisierungen und Implementierungsregeln, dass sie den Datenschutz der betroffenen Personen nicht nachteilig beeinflussen und die SCC in ihrer (datenschutzrechtlichen) Wirkung nicht schwächen.

Hingegen muss es unseres Erachtens zulässig sein, dass die Parteien eine in der SCC nicht geregelte Risikoallokation oder Aufgabenverteilung zwischen ihnen selbst vornehmen – also etwa was passiert, wenn ein neuer Unterauftragsbearbeiter abgelehnt wird oder der Auftragsbearbeiter eine Instruktion nicht umsetzen will, weil sie nicht in sein Service-Konzept passt. Es muss ebenso zulässig sein, dass die Ausübung von Rechten unter den SCC zu datenschutzfremden Zwecken eingeschränkt wird (zur Haftung und der Möglichkeit deren Einschränkung vgl. Ziff. 41). Zulässig sein muss es auch, die Bearbeitungsmöglichkeiten des Importeurs von Daten weiter einzuschränken oder ihm in gewissen Situationen zu untersagen. So sehen die SCC zwar die Weitergabe von Personendaten vor, aber es muss ohne Weiteres zulässig sein, vertraglich zu vereinbaren, dass der Importeur die erhaltenen Personendaten nicht weitergibt – auch nicht an Unterauftragsbearbeiter. Das widerspricht zwar den SCC, aber nicht ihrem Schutzzweck. So gesehen darf den SCC wohl nur dort nicht widersprochen werden, wo dies ihrem Schutzzweck entgegenläuft. Problematisch wäre aus unserer Sicht hingegen eine Einschränkung, wonach Vor-Ort-Audits des Exporteurs zwingend und vollständig an einen Dritten delegiert werden müssen, wie dies Cloud-Provider heute regelmässig vorsehen (Ziff. 29).

Zur Anpassung der SCC im Falle gemeinsamer Verantwortlicher vgl. Ziff. 28.

25. Müssen die neuen SCC für den Einsatz unter dem DSG angepasst werden? Wie setzen wir sie unter dem DSG ein?

Die neuen SCC können so wie sie sind auch für die Zwecke des DSG verwendet werden und gewährleisten unseres Erachtens den erforderlichen Schutz, d.h. einen "geeigneten Datenschutz" (Art. 16 Abs. 2 revDSG).

Die SCC verweisen zunächst rund 45 Mal auf die DSGVO. Die Verweise führen jedoch nicht zu einer relevanten Schwächung des Schutzes betroffener Personen, deren Daten in der Schweiz bearbeitet werden und mit Hilfe der SCC exportiert werden sollen. Das gilt unseres Erachtens auch in folgenden Fällen:

- Die Weitergabe von Personendaten ist u.a. dann zulässig, wenn das Land des Empfängers zwar aus Sicht der DSGVO einen angemessenen Schutz bietet, nicht jedoch aus Sicht der Schweiz. Dies kommt jedoch kaum vor. Diese Differenz erscheint uns vernachlässigbar (betrifft derzeit nur Japan), da nicht derselbe Schutz wie nach DSG, sondern ein lediglich geeigneter Schutz sichergestellt werden muss.
- Im Falle einer Verletzung der Datensicherheit muss der Auftragsbearbeiter den Verantwortlichen nur bei der Erfüllung seiner Pflichten nach DSGVO unterstützen, nicht nach DSG. Die Grundpflicht (die Meldung an den Verantwortlichen) existiert unabhängig davon. Daher genügt dies.
- Im Falle einer Anfrage einer betroffenen Person muss der Auftragsbearbeiter den Verantwortlichen nur bei der Erfüllung der Betroffenenrechte nach DSGVO unterstützen, nicht das DSG. Da der Auftragsbearbeiter aber ohnehin gehalten ist, seinen Instruktionen zu folgen, genügt dies.
- Bezüglich der Bezeichnung der zuständigen Aufsichtsbehörde sieht Clause 13 ("Supervision") zwar keinen Text vor, der vollständig auf den EDÖB passt, aber alle Varianten verweisen auf Annex I.C, wo der "EDÖB" als "competent supervisory authority" vereinbart werden kann, was als Abrede zweifellos so gilt, auch wenn dem EDÖB selbstverständlich keine Funktion unter der DSGVO zukommt. Welche Variante in Clause 13(a) gewählt wird spielt daher für das DSG keine Rolle (wohl aber, wenn parallel die DSGVO zur Anwendung kommen sollte). Der Begriff der "competent supervisory authority" wird in den SCC an rund 14 Stellen aufgegriffen, so etwa bei der Pflicht zur Meldung von Verletzungen der Datensicherheit.

An rund 17 Stellen wird auf "Member State" verwiesen. Die Verweise beeinträchtigen das erforderliche Schutzniveau grundsätzlich nicht. Sie dienen primär der Festlegung des anwendbaren Rechts und des Gerichtsstands. Schon die bisherigen SCC verwendeten hierzu den Begriff des "Member State"[17] und sahen gar keinen Gerichtsstand vor, was ihrer Tauglichkeit keinen Abbruch tat. Auch in den neuen SCC bleibt es in den Parteien überlassen, das anwendbare Recht zu bezeichnen (Clause 17); hinzu kommt die Bezeichnung eines (nicht ausschliesslichen) Gerichtsstands (Clause 18). Vereinbaren die Parteien hier Schweizer Recht und als Gerichtsstand einen Ort in der Schweiz, so dürfte dies so als vereinbart gelten, auch wenn Vordruck der Klauseln festhält, dass der bezeichnete Gerichtsstand die Gerichte eines "EU Member State" sein müssen. Der wahre Wille der Parteien geht auch hier vor. Dasselbe gilt bezüglich der Rechtswahl, wobei in diesem Fall die "Option 1" von Clause 17 zu wählen ist.

Ist die Rechtswahl für die Schweiz getroffen, dürfte auch der ins Leere führende Verweis in Clause 11(e) den Schutz der betroffenen Personen und damit Drittberechtigten nicht schaden, denn ihre Klageberechtigung ergibt sich aus dem Vertrag und die Durchsetzbarkeit eines Urteils aus der Zuständigkeit des Schweizer Gerichts. Clause 18(c) gibt der betroffenen Person überdies einen Anspruch, vor einem EU-Gericht zu klagen, falls sie dort ihren gewöhnlichen Aufenthaltsort hat. Da Clause 18 keine der Zuständigkeiten als ausschliessliche Zuständigkeit vorsieht, bleibt weiterhin auch eine Klage gegen eine Schweizer Partei an ihrem Sitz bzw. Wohnsitz in der Schweiz möglich.

Für die Praxis stellt sich freilich die Frage, ob zwingend Schweizer Recht und ein Gerichtsstand in der Schweiz gewählt werden muss. Dies ist im Einklang mit der bisherigen Praxis zu verneinen. Es ist ohne Weiteres zulässig, die SCC auch unter dem Recht eines EU-Mitgliedsstaates und mit einer Zuständigkeit durch ein Zivilgericht in einem EU-Mitgliedsstaat zu vereinbaren. Dies wird sogar die Regel sein, wenn die neuen SCC in Fällen abgeschlossen werden, in welchen ein Vertragsschluss Datentransfers aus mehreren europäischen Ländern abdecken muss.

Im Ergebnis erfordert das bisher gesagte somit keine Anpassung der SCC sowohl für reine Schweizer Datenexporte als auch für gemischte EWR- und Schweizer-Datenexporte, sofern im Falle von Datenexporten aus der Schweiz Annex I.C einen Verweis auf den EDÖB als "competent supevisory authority" für Datenexporte aus der Schweiz enthält (und im Falle eines gemischten Datenexports einen Verweis auch auf eine EWR-Datenschutzbehörde für Datenexporte, welcher der DSGVO unterliegen).

---

[17] Vgl. etwa Clause 9 der Processor Model Clauses von 2010: "The Clauses shall be governed by the law of the EU Member State in which the data exporter is established, namely …"

Weiter stellt sich die Frage, ob die SCC um eine Klarstellung zu ergänzen sind, dass bei Datentransfers aus der Schweiz alle Verweise auf die "Regulation (EU) 2016/679" (= DSGVO) als Verweis auf das DSG, alle Verweise auf bestimmte Artikel der DSGVO als Verweis auf deren entsprechende Bestimmung im DSG und alle Verweise auf die EU als Verweis auf die Schweiz gelten. Dies mag aus Schweizer Sicht sinnvoll erscheinen, kann aber dort in Konflikt mit der DSGVO geraten, wo ein Datentransfer aus der Schweiz parallel der DSGVO unterliegt. In diesem Fall müssen die SCC unverändert gelten, damit sie wirksam sind. Wenn also eine solche Anpassung vorgenommen wird, muss klargestellt werden, dass diese Anpassung nur für Datentransfers aus der Schweiz gilt, soweit sie dem DSG unterstehen, wobei im Konfliktfalle mit der ursprünglichen Formulierung der SCC die ursprüngliche Formulierung vorgeht.

Der EDÖB hat sich dieser Beurteilung zwischenzeitlich weitgehend angeschlossen. Am 27. August 2021 kommunizierte er, welchen Anpassungsbedarf er sieht, damit die neuen SCC von ihm anerkannt sind und daher die vereinfachte Meldung nach Art. 6 Abs. 3 VDSG gilt.[18] Es sind dies nur wenige Anpassungen bzw. Klarstellungen, die er auch in einer Tabelle zusammengefasst hat:

[18] https://bit.ly/3zQarff.

	Fall 1: Die Datenübermittlung ist ausschliesslich dem DSG unterstellt[13]	Fall 2: Die Datenübermittlung ist sowohl dem DSG und als auch der DSGVO unterstellt[14]	
		Option 1: Parteien sehen zwei «separate» Regelungen jeweils für Datenübermittlungen unter DSG und solche unter DSGVO vor.	Option 2: Parteien übernehmen den Standard der DSGVO für alle Datenübermittlungen
Zuständige Aufsichtsbehörde in Anhang I.C gemäss Klausel 13	Zwingend EDÖB	Parallele Aufsicht: EDÖB, soweit die Datenübermittlung unter das DSG fällt; EU-Behörde, soweit die Datenübermittlung unter die DSGVO fällt (dabei sind die Kriterien von Klausel 13 a für die Auswahl der zuständigen Behörde zu beachten)	
Anwendbares Recht für vertragliche Ansprüche gemäss Klausel 17	Schweizer Recht oder Recht eines Landes, das Rechte als Drittbegünstigte zulässt und gewährt	Schweizer Recht oder Recht eines Landes, das Rechte als Drittbegünstigte zulässt und gewährt für vertragliche Ansprüche betreffend Datenübermittlungen gemäss DSG; Recht eines EU-Mitgliedstaats für solche gemäss DSGVO (freie Wahl bei Modul 4)	Recht eines EU-Mitgliedstaats (freie Wahl bei Modul 4)
Gerichtsstand für Klagen zwischen den Parteien gemäss Klausel 18 b[15]	Freie Wahl	Freie Wahl für Klagen betreffend Datenübermittlungen gemäss DSG; Gericht eines EU-Mitgliedstaats für Klagen betreffend Datenübermittlungen gemäss DSGVO (freie Wahl bei Modul 4)	Gericht eines EU-Mitgliedstaats (freie Wahl bei Modul 4)
Anpassungen bzw. Ergänzungen betreffend Gerichtsstand für Klagen von betroffenen Personen	Die SCC sind mit einem Anhang zu ergänzen, worin präzisiert wird, dass der Begriff «Mitgliedstaat» nicht so ausgelegt werden darf, dass betroffene Personen in der Schweiz von der Möglichkeit ausgeschlossen werden, ihre Rechte an ihrem gewöhnlichen Aufenthaltsort (Schweiz) gemäss Klausel 18 c einzuklagen.		
Anpassungen bzw. Ergänzungen betreffend Verweise auf die DSGVO	Die SCC sind mit einem Anhang zu ergänzen, worin präzisiert wird, dass die Verweise auf die DSGVO als Verweise auf das DSG zu verstehen sind	Die SCC sind mit einem Anhang zu ergänzen, worin präzisiert wird, dass die Verweise auf die DSGVO als Verweise auf das DSG zu verstehen sind, soweit die Datenübermittlungen dem DSG unterstellt sind	
Ergänzung bis zum Inkrafttreten des rev. DSG[16]	Die SCC sind mit einem Anhang zu ergänzen, worin präzisiert wird, dass die Klauseln bis zum Inkrafttreten des rev. DSG auch die Daten juristischer Personen schützen.		

Wie aus der Tabelle ersichtlich ist, unterscheidet der EDÖB korrekterweise zwischen den Fällen, in denen nur das DSG gilt und jenen, in welchen eine Datenübermittlung auch der DSGVO unterstellt ist. Er schreibt nur wenige Anpassungen vor:

- Erwähnung (auch) des EDÖB als Aufsichtsbehörde in Annex I.C (im Grund keine Anpassung);
- Anhang zu den SCC mit folgenden Regelungen bzw. Klarstellungen:
  - Verweise auf die DSGVO sind als Verweise auf das DSG zu betrachten sind, soweit die Datenübermittlung dem DSG untersteht (und die SCC für die Zwecke des DSG verwendet werden);
  - Der Verweis "Gerichte des Mitgliedsstaats" in Clause 18(c) umfasst auch Schweizer Gerichte;
  - Bis zum Inkrafttreten des revDSG schützen die Klauseln der SCC auch die Personendaten juristischer Personen; sie gelten daher ebenfalls als Personendaten.

Die beiden letzten Punkte sind oben nicht erwähnt. Der letzte Punkt wäre nach Schweizer Recht nicht nötig, da die Angemessenheit des

Schutzes im Ausland nicht von einem Schutz von Daten juristischer Personen abhängt.

Die SCC sollten entsprechend den Vorgaben des EDÖB ergänzt werden. Sie gelten dann auch als anerkannt. Wichtig ist jedoch darauf zu achten, dass die Bestimmungen des Anhangs so formuliert werden, dass sie nur gelten, soweit die Datenübermittlung im Rahmen des DSG reguliert wird. Das gilt wie erwähnt speziell für die erste Regelung des Anhangs: Soweit eine Datenübermittlung unter die DSGVO fällt, müssen Verweise auf die DSGVO weiterhin Verweise auf die DSGVO sein.

Pro memoria: Die Beschreibung der Datenübermittlung in Annex I.B des Appendix muss so abgefasst sein, dass auch die Schweizer Datenexporte davon erfasst sind. Denn Annex I.B legt letztlich den Gegenstand der konkret vereinbarten SCC fest. Diese Anpassung kann insbesondere bei auf europäischer Ebene abgeschlossenen SCC wichtig sein, weil hierbei die Schweiz gerne vergessen geht, wenn im Rahmen des Drafting nicht realisiert wird, dass die Schweiz nicht Teil des EWR ist.

26. Muss der Einsatz der neuen SCC dem EDÖB gemeldet werden?

Ja, der Einsatz der neuen SCC muss dem EDÖB nach Art. 6 Abs. 3 DSG gemeldet werden, jedenfalls wenn er im Sinne von Art. 6 Abs. 2 DSG zur Absicherung einer Bekanntgabe von Personendaten in ein unsicheres Drittland erfolgt.

Da der EDÖB die neuen SCC anerkannt hat, genügt hierzu ein einfacher Brief nach Art. 6 Abs. 3 VDSG – sofern die SCC so angepasst bzw. klargestellt wurden, wie der EDÖB dies verlangt hat (Ziff. 25). Auf eine früher schon erfolgte Meldung wird normalerweise nicht mehr abgestellt werden können, jedenfalls soweit sich diese "nur" auf die alten SCC bezog.

Wird ein IGDTA neu abgeschlossen, welches die neuen SCC zur Anwendung bringt, genügt ebenfalls die vereinfachte Meldung. Das IGDTA selbst enthält zwar wesentlich mehr Regelungen als die neuen SCC, bringt aber im Kern trotzdem "nur" die unveränderten SCC zur Anwendung, soweit es um Datenübermittlungen in unsichere Drittstaaten geht, weshalb keine Garantien "sui generis" vorliegen und die vereinfachte Meldung nach Art. 6 Abs. 3 VDSG zur Verfügung steht.

Für die vereinfachte Meldung genügt ein Brief, in welchem die Verwendung der neuen SCC mitgeteilt wird. Gemäss EDÖB sind ihm dabei folgende Angaben zu machen:

- Meldepflichtige(r) Verantwortlicher/Datenbearbeiter (wie bisher)
- Empfängerland bzw. Empfängerländer (wie bisher)
- Kategorien der Datenempfänger (z.B. Mutterhaus oder Tochtergesellschaft, wie bisher)
- verwendete Module (neu)

- Bestätigung, dass Anpassungen gemäss EDÖB Stellungnahme vom 27. August 2021 entsprechend der konkreten Vertragssituation gemacht wurden (neu)

Wir sind der Ansicht, dass für eine derart umfangreiche Meldung (nach wie vor) keine Pflicht besteht, da Art. 6 Abs. 3 VDSG keine solchen Angaben verlangt. Es genügt, dass der EDÖB "in allgemeiner Form über die Verwendung dieser Musterverträge oder Standardvertragsklauseln informiert" wird. Für unsere Klienten verzichten wir daher auf die Nennung des Empfängerlands und der Kategorien der Datenempfänger genannt werden und teilen dem EDÖB den Anlass der Meldung nur im Sinne einer über Art. 6 Abs. 3 DSG hinausgehenden Information mit. Damit bleibt die Meldung generisch und es sind keine neuerlichen Meldungen bei späteren Verwendungen der SCC nötig. Wir melden jeweils den Einsatz aller vier Module.

Unter dem revidierten DSG wird eine Meldung nur noch nötig sein, wenn die SCC in einer Ausführung eingesetzt werden, die vom EDÖB nicht anerkannt ist (z.B. mit nicht anerkannten Anpassungen oder ohne die von ihm verlangten Anpassungen). Für die meisten Fälle entfällt also die Meldepflicht mit dem revidierten DSG.

27. Welche Besonderheiten sind bei einem Controller-Controller-Transfer (Modul 1) unter den neuen SCC zu beachten?

Erhält ein Verantwortlicher im Rahmen der SCC Personendaten übermittelt, so unterliegt er nicht mehr wie bisher nur einigen allgemeinen Bearbeitungsgrundsätzen. Die neuen SCC formulieren die Anforderungen an ihn als Importeur vergleichsweise detailliert. Hervorzuheben sind insbesondere folgende Punkte:

- Der Importeur kann die erhaltenen Daten für weniger Zwecke verwenden, als dies einem Verantwortlichen unter der DSGVO erlaubt wäre (Modul 1, Clause 8.1). Es ist daher darauf zu achten, dass die im Appendix der SCC aufgeführten Zwecke genügend umfassend sind. Immerhin: Die Verwendung für behördliche oder gerichtliche Verfahren bleibt dem Empfänger erlaubt. Auch steht es den Parteien natürlich frei, den Appendix und damit auch die aufgeführten Zwecke jederzeit anzupassen. Der Importeur wird sich daher das Recht, solche Anpassungen zu verlangen, mit Vorteil vorbehalten lassen.
- Der Importeur muss betroffene Personen über seinen Namen und Kontaktdaten informieren, die übermittelten Datenkategorien und etwaige weitere Empfänger, der Zweck solcher Weiterübermittlungen und die Rechtsgrundlage gemäss den SCC (Modul 1, Clause 8.2(a)). Die SCC sehen vor, dass diese Informationen auch via Exporteur (und dessen Datenschutzerklärung) erfolgen kann, aber eine Pflicht zur Information hat der Exporteur nicht. Kann der Importeur zeigen, dass es unverhältnismässig wäre, dass er

die einzelnen betroffenen Personen selbst informiert, dann soll die "öffentliche" Information genügen. Mit anderen Worten: Ein Verantwortlicher in einem unsicheren Drittland wird unter den SCC mindestens eine Datenschutzerklärung auf seiner Website publizieren müssen.

- Über die DSGVO hinaus geht die Regelung zum Umgang mit falschen oder nicht mehr aktuellen Daten. Hier sehen die SCC vor, dass sich die beiden Verantwortlichen gegenseitig über Korrekturen in ihren Datenbeständen, soweit sie die transferierten Daten betreffen, auf dem Laufenden halten müssen (Modul 1, Clause 8.3(b)).
- Kommt es zu einer Verletzung der Datensicherheit, die mit relevanten Risiken für die betroffenen Personen verbunden ist, muss der Importeur neu nicht nur den Exporteur in Kenntnis setzen, sondern direkt an die betreffende Datenschutzbehörde gelangen, auf welche sich die Parteien gemäss Clause 13 verständigt haben (Modul 1, Clause 8.5(e)), und allenfalls auch an die betroffenen Personen. Der Exporteur muss selbst nicht melden, aber allenfalls den Prozess unterstützen.
- Der Importeur wird verpflichtet ein Protokoll der Verletzungen der Datensicherheit zu führen – letztlich auch für solche, die nicht gemeldet wurden (Modul 1, Clause 8.5(g)). Diese Pflicht sieht das DSG nicht vor. Doch auch bezüglich der restlichen Dokumentationspflicht gehen die SCC weiter: Der Importeur wird vertraglich zur Dokumentation seiner Bearbeitungsaktivitäten verpflichtet und muss auf Verlangen der Datenschutzbehörde Einblick geben (Modul 1, Clause 8.9).
- Die Weitergabe von Personendaten durch den Importeur ist unter den neuen SCC flexibler geregelt als unter den bisherigen SCC. Selbstverständlich ist sie möglich, wenn die SCC abgeschlossen werden, aber neu ist auch die Weitergabe im Rahmen von behördlichen und gerichtlichen Verfahren möglich, wo der Abschluss von SCC keine Chance hat (vgl. Ziff. 46). Auch die Verwendung abgeänderter SCC ist möglich, sofern der Importeur selbst nicht der DSGVO unterliegt.
- Speziell sind die Betroffenenrechte geregelt: Die betroffenen Personen haben ein Auskunfts-, Korrektur- und Löschrecht sowie ein Widerspruchsrecht gegen die Verwendung ihrer Daten für Marketingzwecke. Sie können diese Rechte direkt gegen den Importeur geltend machen. Das Auskunftsrecht umfasst auch einen Anspruch auf Herausgabe der Namen der Dritten, denen der Importeur die Daten weitergegeben hat, was bedeutet, dass diese Daten aufgezeichnet werden müssen. Auch das geht über das DSG hinaus. Einschränkungen der Betroffenenrechte sind möglich, aber welche Einschränkungen das sind, führen die SCC nicht nä-

her aus: Sie halten lediglich fest, dass der Importeur verweigern darf, wenn dies (i) nach dem Recht des Ziellands ("country of destination") erlaubt ist und (ii) nötig ist, um die (überwiegenden) Rechte anderer Personen (auch des Verantwortlichen) oder die weiteren, in Art. 23(1) DSGVO aufgezählten Grundwerte zu schützen[19]. Der Begriff des "Ziellands" ist nicht auf den ersten Blick klar, meint aber das Land des Importeurs, wie bei einem Blick im Clause 15.1(a) klar wird, wo der Begriff ebenfalls verwendet und weiter ausgeführt wird. Regelt dieses Heimatrecht des Importeurs das Auskunftsrecht nicht, so steht dieser Unterpunkt einer Verweigerung der Auskunft nicht entgegen, d.h. in der Praxis kann die Auskunft im Prinzip verweigert werden, wenn ihr andere überwiegende Interessen entgegenstehen.

Anders als unter Art. 13 f. DSGVO praktiziert, genügt es unter den neuen SCC nicht mehr, den betroffenen Personen in der eigenen Datenschutzerklärung einen Link auf die SCC anzubieten. Sie haben neu Anspruch auf Einsicht in die konkret vereinbarten SCC inklusive Appendix (Modul 1, Clause 8.2(c)). Zwar dürfen Geschäftsgeheimnisse und Personendaten geschwärzt werden, aber es muss stattdessen eine aussagekräftige Zusammenfassung geliefert werden, falls dies für die Beurteilung der Rechtmässigkeit der Regelung nötig ist. Die Datenflüsse müssen mit anderen Worten transparent gemacht werden, was über die normale Informationspflicht und das Auskunftsrecht nach DSGVO hinausgeht. Es wird allerdings nicht verlangt, dass in der Datenschutzerklärung die Herausgabe dieser Kopie konkret angeboten werden muss; die Datenschutzerklärung kann diesbezüglich also so bleiben, wie sie ist, mit Ausnahme des Nachführens des Links auf die neuen EU SCC.

Zur Frage der Durchsetzung und Haftung vgl. Ziff. 40 und Ziff. 41. Zu neuen Informationspflichten vgl. Ziff. 38. Zur Herausgabe an Behörden vgl. Ziff. 43. Zu den besonderen Fragen im Falle einer gemeinsamen Verantwortlichkeit vgl. Ziff. 28.

28. Was gilt im Falle einer Offenlegung an einen gemeinsamen Verantwortlichen in einem unsicheren Drittstaat?

Auch Übermittlungen von Personendaten zwischen gemeinsamen Verantwortlichen müssen die Anforderungen von Art. 44 ff. DSGVO und Art. 6 DSG einhalten. Die SCC können also auch zwischen gemeinsamen Verantwortlichen abgeschlossen werden. In diesem Fall kommt Modul 1 (Controller-Controller) zum Einsatz.

---

[19] Das sind neben dem Schutz der betroffenen Person und Rechte Dritter die nationale Sicherheit, Landesverteidigung, öffentliche Sicherheit, Verhütung, Ermittlung und Aufdeckung oder Verfolgung von Straftaten, Schutz sonstiger wichtiger Ziele des öffentlichen Interesses, Schutz der Justiz und Justizverfahren, Verhütung, Aufdeckung und Verfolgung der Verletzung von Standesregeln, Ausübung öffentlicher Gewalt und die Durchsetzung zivilrechtlicher Ansprüche.

Ob die Verteilung der Verantwortlichkeiten zwischen den gemeinsam Verantwortlichen, wie sie die SCC vorsehen, im konkreten Fall passen, muss einzelfallweise beurteilt werden. In der Mehrheit der Fälle dürften die SCC passen, denn wenn ein der DSGVO (oder dem DSG) unterstellter Verantwortlicher für eine Datenbearbeitung gemeinsam verantwortlich ist mit einer Gesellschaft, die gesetzlich nicht zur Einhaltung des Datenschutzes verpflichtet ist, wird sie schon aus reinem Eigennutz eine Regelung analog den SCC abschliessen wollen, um im Schadenfall wenigstens Rückgriff nehmen zu können auf den oder die anderen gemeinsamen Verantwortlichen.

Weil die SCC die Verantwortlichkeiten zwischen den Parteien in allen für den Datenschutz relevanten Bereichen regeln, können sie unseres Erachtens den Anforderungen an eine Vereinbarung nach Art. 26 DSGVO genügen, wenn ihr Regelungsgehalt (zufällig) für die betreffende Situation passt. Tut sie dies nicht, so muss es unseres Erachtens zulässig sein, nebst den SCC eine zusätzliche Verantwortlichkeitsordnung zu schaffen, die der einen oder anderen Partei zusätzliche Pflichten auferlegt. Dies mag formal den Regelungen der SCC auf den ersten Blick widersprechen, doch wird dies zulässig sein, soweit der Schutzzweck der SCC erreicht wird.

Kommt es beispielsweise zu einer Verletzung der Datensicherheit, ist nach den SCC der Importeur verpflichtet, diese Verletzung der zuständigen Aufsichtsbehörde zu melden (Modul 1, Clause 8.5(e)). Hier muss es unseres Erachtens im Falle einer gemeinsamen Datenbearbeitung zulässig sein zu vereinbaren, dass diese Data-Breach-Meldung stattdessen vom Exporteur im Namen aller Verantwortlicher vorgenommen wird, was in der Praxis wohl ohnehin sinnvoller ist, da er näher an der Aufsichtsbehörde dran ist. Wer ganz vorsichtig sein wird, wird in der Zusatzvereinbarung zwischen den gemeinsamen Verantwortlichen nicht nur festhalten, dass der Exporteur zur Meldung verpflichtet ist, sondern ebenso, dass er sie auch im Namen des Importeurs vornimmt. So kann später argumentiert werden, dass der Importeur trotz allem seiner Pflicht nach Modul 1, Clause 8.5(e) der SCC nachgekommen ist. In solchen Fällen wird es für die Zwecke von Art. 26 DSGVO nötig sein, eine zusätzlich Regelung zu treffen.

29. Welche Besonderheiten sind bei einem Controller-Processor-Transfer (Modul 2) unter den neuen SCC zu beachten?

Die Konstellation kommt in der Praxis besonders häufig vor und wird auch am meisten zu reden geben. Für den Auftragsbearbeiter sind die neuen SCC vergleichsweise nachteilig. Während in einem Verhältnis zu einem Auftragsbearbeiter innerhalb des EWR oder eines sicheren Drittlands nur die Vorgaben von Art. 28(3) DSGVO zu beachten sind oder die noch weniger weitgehenden Vorgaben des DSG, so stellen die SCC detailliertere und strengere Regeln auf, die nicht verändert werden

dürfen. Immerhin gibt es eine Möglichkeit, diese Nachteile teilweise zu vermeiden (Ziff. 31).

Hervorzuheben sind insbesondere folgende Punkte:

- Während Art. 28(3)(a) DSGVO nur verlangt, dass der Auftragsbearbeiter Daten nur auf "dokumentierte Weisungen des Verantwortlichen" hin bearbeiten darf, verlangen die SCC zusätzlich, dass sie jederzeit während der Vertragslaufzeit geändert werden können. Das wird für Anbieter standardisierte Services eine Herausforderung sein, da sie in der Regel mit dem Kunden vereinbaren, dass der Vertrag und die Konfiguration der Dienste des Kunden die "abschliessenden und finalen" Instruktionen des Kunden sind. Dies steht der neuen Regel auf den ersten Blick entgegen. Es kann allerdings vertreten werden, dass die Möglichkeit zur Anpassung der Konfiguration der Services der erforderlichen Anpassungsmöglichkeit der SCC genügen muss, da es sich von selbst versteht, dass Instruktionen nur soweit befolgt werden müssen, als sie im Rahmen der Services erfolgen. Werden die Weisungen nicht befolgt, hat der Verantwortliche qua der neuen SCC im Ergebnis ein ausserordentliches Kündigungsrecht auch des Hauptvertrags. Es bleibt abzuwarten, inwiefern dies als jederzeitiges Kündigungsrecht ohne Grund genutzt werden kann, indem der Verantwortliche dem Auftragsbearbeiter eine Instruktion erteilt, die dieser nicht bereit ist umzusetzen und danach gestützt auf Clause 16(a)-(c) der Vertrag beendet wird.
- Zusätzlich zur Pflicht zur weisungsgemässen Datenbearbeitung untersagen die SCC dem Auftragsbearbeiter die Bearbeitung der Daten für andere Zwecke als im Annex I.B. des Appendix festgehalten. Hier ist in der Praxis darauf zu achten, dass falls der Auftragsbearbeiter Personendaten auch für eigene Zwecke (als Verantwortlicher) bearbeiten können will (z.B. zwecks Anonymisierung zur Verwendung für eigene Zwecke oder zwecks Offenlegung in behördlichen oder gerichtlichen Verfahren), dass dies im Annex I.B. ebenfalls festgehalten wird.
- Der Auftragsbearbeiter wird verpflichtet, den Verantwortlichen darüber zu informieren, wenn ihm bekannt werden sollte, dass die von ihm bearbeiteten Personendaten falsch oder veraltet sind. Diese Pflicht geht über die Pflichten eines Auftragsbearbeiters nach Art. 28 DSGVO hinaus. Immerhin hat der Auftragsbearbeiter keine Pflicht, nach falschen oder veralteten Daten zu suchen. Er wird somit mit Vorteil eine "Vogel-Strauss"-Taktik verfolgen.
- Weniger weit als die DSGVO geht die Pflicht zur Rückgabe von Personendaten. Nach Art. 28(3)(g) DSGVO muss ein Auftragsbearbeiter nach Auftragsende Daten nur soweit nicht zurückgeben, als ihm das Recht des EWR oder eines Mitgliedsstaates dies untersagt; in Modul 2, Clause 8.5 kann sich der Auftragsbearbeiter

auf sein Heimatrecht berufen – was in der Praxis allerdings schon bisher Standard war. Richtigerweise wird zusätzlich festgehalten, dass solange eine Löschung nicht erfolgt ist, die Daten weiterhin zu schützen sind. Diese Regel fehlt heute in vielen ADVs.

- Bezüglich der Massnahmen der Datensicherheit (TOMS) wird dem Auftragsbearbeiter die Pflicht auferlegt, diese regelmässig auf ihre Angemessenheit zu prüfen (Modul 2, Clause 8.6(a)). Diese Pflicht wollen viele Auftragsbearbeiter ihrem Kunden übertragen mit dem Argument, dass nur dieser seine Daten kennt und beurteilen kann, wie weit der Schutz zu gehen hat. Es kann unseres Erachtens weiterhin so verfahren werden, dass der Auftragsbearbeiter dem Kunden seine Massnahmen (d.h. die TOMS) vorlegt und dieser im Hauptvertrag bestätigen muss, dass diese angesichts seiner Personendaten und Bearbeitungsaktivitäten hinreichend sind. Dies ist während der Vertragslaufzeit zu wiederholen, da es an sich dem Auftragsbearbeiter obliegt, ihre Angemessenheit zu überprüfen.
- Zu den TOMS ist ferner zu bemerken, dass diese nicht mehr nur Massnahmen zur Datensicherheit enthalten müssen, sondern auch Massnahmen zur Einhaltung der Betroffenenrechte und der weiteren Bearbeitungsgrundsätze (Modul 2, Clause 10(b)). Das war bisher nicht so. Sie müssen daher ergänzt werden (Ziff. 18). Auch müssen sie möglicherweise detaillierter ausfallen als bisher.
- Selbstverständlich ist der Auftragsbearbeiter zur Meldung von Verletzungen der Datensicherheit verpflichtet (Modul 2, Clause 8.6(c)). Hier fällt allerdings auf, dass keine zeitliche Maximalfrist vorgesehen ist (nur "without undue delay", "unverzüglich").
- Die SCC sehen zwar eine allgemeine Unterstützungspflicht des Auftragsbearbeiters gegenüber dem Verantwortlichen vor (Modul 2, Clause 8.6(d)), aber diese ist weniger konkret formuliert als von Art. 28(3) DSGVO verlangt. Da die SCC jedoch auch als genehmigte ADV-Klauseln nach Art. 28(7) DSGVO gelten (siehe dazu Ziff. 47), spielt dies keine Rolle.
- Anders als bisher regeln die neuen SCC auch die Weiterleitung an Dritte. Soweit es sich um Unterauftragsbearbeiter (Subprocessors) handelt oder ein behördliches oder gerichtliches Verfahren des Auftragsbearbeiters, erscheint dies unproblematisch. Eine Stolperfalle ist jedoch der Fall der vom Verantwortlichen verlangten Weiterleitung, d.h. wo z.B. der Kunde von seinem Provider verlangt, die Daten irgendwelchen Dritten bekanntzugeben. Gemäss Modul 2, Clause 8.8 genügt die Instruktion in diesem Falle nicht. Es muss zusätzlich einer der vier Fälle gemäss Modul 2, Clause 8.8 erfüllt sein. Dabei wird nicht klar, ob es der Verantwortliche ist, der dies sicherzustellen hat oder der Auftragsbear-

beiter. Vermutlich wird es letzterer sein, der den Ball wiederum an den Verantwortlichen zurückspielen wird, indem er von ihm im Hauptvertrag verlangt, die Weitergabe von Personendaten nur und erst anzuordnen, wenn die Voraussetzungen von Modul 2, Clause 8.8 gegeben sind (die SCC auferlegen dem Verantwortlichen aber nicht die Pflicht, nur gemäss SCC zulässige Instruktionen zu erteilen).

- Der Auftragsbearbeiter muss seine Auftragsbearbeitung in angemessener Weise für den Verantwortlichen "dokumentieren" (Modul 2, Clause 8.9(b)). Was dies genau bedeutet, ist unklar. Die Pflicht geht weiter als Art. 28(3)(h) DSGVO, wonach ein Auftragsbearbeiter nur dokumentieren können muss, dass er die Vorgaben von Art. 28 DSGVO (und den ADV) einhält. Letztere Pflicht ist separat enthalten (Modul 2, Clause 8.9(c)).
- Das Audit-Recht wird ebenfalls etwas näher ausgeführt als in Art. 28(3)(h) DSGVO vorgesehen. Die vollständige Delegation des Audit-Rechts an einen vom Auftragsbearbeiter beauftragten Dritten (wie es Cloud-Provider heute regelmässig vorsehen) ist nicht vorgesehen; es wird lediglich zugunsten des Verantwortlichen festgehalten, dass dieser sich auch auf "certifications" solcher Dritter stützen darf in seinem Entscheid, einen Audit durchzuführen (Modul 2, Clause 8.9(c)). Aus dieser Formulierung ergibt sich im Umkehrschluss, dass auf das eigene Audit-Recht nicht vollumfänglich verzichtet werden darf. Hingegen hält Modul 2, Clause 8.9(d) fest, dass es dem Verantwortlichen erlaubt ist, einen unabhängigen Prüfer beizuziehen. Es wird somit erlaubt sein, dass ein Auftragsbearbeiter verlangt, dass sein Kunde seine Prüfrechte zunächst anhand bestehender Audit-Berichte (bzw. Zertifizierungen, was nicht dasselbe ist) ausübt und, wenn dies nicht genügt, einen unabhängigen (aber vom Auftragsbearbeiter vorgegebenen) Dritten mit der Prüfung mandatiert (d.h. der Kunde nie selbst vor Ort eine Prüfung durchführt).
- Der Beizug von Unterauftragsbearbeitern (Subprocessors) ist analog der nach Art. 28 DSGVO vorgesehenen Regelung möglich; sie lässt dem Auftragsbearbeiter erstaunlich viele Freiheiten:
  - Die SCC sehen sowohl das Verfahren der Einzelgenehmigung wie auch der Pauschalgenehmigung mit Widerspruchsrecht vor. Eine Ankündigungsfrist geben die SCC nicht vor; sie dürfte je nach Fallkonstellation zwischen 10 und 180 Tagen liegen.
  - Was die SCC nicht regeln sind die Folgen eines Widerspruchs, d.h. ob der Verantwortliche kündigen muss, der Auftragsbearbeiter kündigen darf oder ihm schlicht der Beizug des neuen Subprocessors verboten ist. Aus der Regel, dass die SCC DSGVO-konform auszulegen sind, ergibt sich,

dass ein Beizug trotz Widerspruch ohne (praktikable) Exit-Möglichkeit des Verantwortlichen nicht zulässig ist.

- Die SCC geben eine sequenzielle Verpflichtung des Subprocessors vor, d.h. er hat einen Vertrag nur mit dem Auftragsbearbeiter, nicht mit dem Verantwortlichen. Diesem muss allerdings der Vertrag zwischen Auftragsbearbeiter und Subprocessor auf Verlangen vorgelegt werden (Geschäftsgeheimnisse dürfen geschwärzt werden) (Clause 9(c)). Den einzigen Anspruch, der dem Verantwortlichen gegen den Subprocessor direkt eingeräumt werden muss, ist das Recht, die Unterauftragsbearbeitung (d.h. den Vertrag zwischen Auftragsbearbeiter und Subprocessor) zu beenden und die Rückgabe oder Löschung der Daten zu verlangen – falls der (zwischengeschaltete) Auftragsbearbeiter pleite geht oder nicht mehr handlungsfähig ist (Clause 9(e)). Dies ist eine etwas merkwürdige Regelung, denn naheliegend wäre gewesen, dass dem Verantwortlichen ein Eintrittsrecht in den Vertrag eingeräumt wird, aber die Regelung ist besser als nichts.
- Nach ganz nachvollziehbar ist die Regelung in Clause 9(d), wonach der Auftragsbearbeiter zwar dafür einstehen muss, dass der Subprocessor seinen Vertrag mit dem Auftragsbearbeiter einhält, aber nicht für dessen Verhalten generell, was an sich üblich wäre. Schliesst der Auftragsbearbeiter mit seinem Subprocessor einen ungünstigen Vertrag, schränkt er damit seine eigene Haftung ein. Dabei ist der Auftragsbearbeiter ausdrücklich nicht verpflichtet, mit dem Subprocessor die SCC abzuschliessen; es genügt, dass es ein Vertrag ist, der in der Substanz dieselben Datenschutzpflichten vorsieht (Clause 9(b)).
- Will ein Verantwortlicher den Subprocessor direkt verpflichten, muss er ihn zum direkten Auftragsbearbeiter machen, was zulässig aber nicht erforderlich ist.

Anders als unter Art. 13 f. DSGVO praktiziert, genügt es unter den neuen SCC nicht mehr, den betroffenen Personen in der eigenen Datenschutzerklärung einen Link auf die SCC anzubieten. Sie haben neu Anspruch auf Einsicht in die konkret vereinbarten SCC inklusive Appendix (Modul 2, Clause 8.3). Dies dürfte jedenfalls bei kommerziellen Auftragsbearbeitern kein Problem darstellen, da ihre SCC in der Regel ohnehin allgemein verfügbar sind. Immerhin kann aus der Pflicht zur Offenlegung der SCC auch eine Pflicht zur Offenlegung der Namen der von einem Unternehmen beauftragten Auftragsbearbeiter in unsicheren Drittländern abgeleitet werden. Eine betroffene Person kann von einem Unternehmen im Grunde verlangen, dass ihm alle SCC mit Auftragsbearbeitern in unsicheren Drittstaaten vorgelegt werden und diesen Anspruch auch einklagen (soweit die neuen SCC vereinbart wurden).

Zur Frage der Durchsetzung und Haftung vgl. Ziff. 40 und Ziff. 41. Zu neuen Informationspflichten vgl. Ziff. 38. Zur Herausgabe an Behörden vgl. Ziff. 43.

30. Wie ist vorzugehen, wenn wir eine Service-Provider sowohl für uns selbst als auch für andere Konzerngesellschaften unter Vertrag nehmen?

Handelt es sich beim Service-Provider um einen Auftragsbearbeiter und befindet er sich in einem unsicheren Drittland, werden mit ihm die SCC abgeschlossen werden müssen, und zwar gleich mit zwei Modulen. Denn wer die Dienstleistungen eines Auftragsbearbeiters für sich selbst benutzt, ist Verantwortlicher, doch wer dies im Auftrag seiner Konzerngesellschaften tut, wird in aller Regel selbst Auftragsbearbeiter sein (es sei denn, er schliesst den Vertrag mit dem Service-Provider im Namen aller Konzerngesellschaften ab, was ein Service-Provider aber normalerweise nicht möchte). Für den ersten Fall kommt Modul 2 zur Anwendung, für den zweiten Fall Modul 3.

Sollte der Service-Provider gewisse Daten für eigene Zwecke bzw. als Verantwortlicher bearbeiten wollen (z.B. Benutzerdaten), so wird sogar Modul 1 abgeschlossen werden müssen.

31. Wie kann sich ein Auftragsbearbeiter vor den Nachteilen der neuen SCC mindestens im Verhältnis zum Kunden schützen?

Der "Schutzbedarf" entsteht, weil viele der neuen Bestimmungen der SCC für den Auftragsbearbeiter nicht nur nachteilig sind (Ziff. 29), sondern er sie auch nicht ändern kann, weil die SCC nicht angepasst werden dürfen.

Um sich dennoch zu schützen, empfehlen wir die Zwischenschaltung eines Vertragspartners im EWR oder einem sicheren Drittland wie der Schweiz. Der Verantwortliche (z.B. Kunde des Cloud-Providers) schliesst seinen Vertrag mit dem "lokalen" Auftragsbearbeiter ab und ist daher nicht gezwungen, die SCC zu vereinbaren. Er kann sich auf einen weniger weitgehenden Vertrag über die Auftragsbearbeitung (ADV) einigen. Die SCC kommen zwar zum Einsatz, jedoch erst in zweiter Stufe, wenn der lokale Auftragsbearbeiter die Personendaten des Kunden an seine ausländischen Gruppengesellschaften zur Bearbeitung weitergibt. Diese sind dann Unterauftragsbearbeiter (Subprocessor) und es sind die SCC mit dem Modul 3 (Processor-Processor)" abzuschliessen.

Es ist nach der DSGVO (und nach dem DSG) nicht erforderlich, dass der Verantwortliche einen direkten Vertrag mit dem Subprocessor abschliesst; auch die SCC sehen solche direkten Vertragsverhältnisse nicht vor, sondern lediglich ein Eintrittsrecht im Falle eines Ausfalls des Auftragsbearbeiters (Modul 3, Clause 9(e) des Moduls "Processor-Processor").

Wir erwarten, dass viele Service-Provider diesen Weg wählen werden um sich besser zu schützen. Obwohl ihre Kunden dadurch nicht mehr verantwortlich dafür sind, die SCC abzuschliessen, bleiben sie natürlich für Datenbearbeitung an sich verantwortlich. Darum werden sie trotzdem sicherstellen wollen, dass ihr Service-Provider die SCC einsetzt und sich auch an diese hält.

32. Welche Besonderheiten sind zu beachten, wenn ein Auftragsbearbeiter einen Subprocessor in einem unsicheren Drittland einsetzen will?

Hierbei ist unterscheiden, ob der Auftragsbearbeiter in der Schweiz ist oder der DSGVO untersteht:

- Ist das eine oder andere erfüllt, dann wird er die SCC einsetzen, weil die Transferbeschränkungen nach Art. 44 ff. DSGVO und Art. 6 DSG ebenso gelten wie für einen Verantwortlichen (mit Ausnahme, dass ihn unter Art. 6 Abs. 3 DSG in der Regel keine Meldepflicht beim EDÖB trifft, wenn er nicht Inhaber der Datensammlung ist).
- Befindet sich der Auftragsbearbeiter in einem unsicheren Drittland und unterliegt er nicht der DSGVO (was unklar sein kann: Ziff. 8), so muss er die SCC für den Beizug eines Subprocessors weder nach DSG noch nach DSGVO verwenden, darf es aber tun. Hat er selbst die SCC unterzeichnet, gelten für den Beizug eines Subprocessors die weniger strengen Voraussetzungen von Clause 9, wonach sein Vertrag mit dem Subprocessor nur (aber immerhin) dasselbe Schutzniveau wie die SCC sicherstellen muss, hierzu aber nicht mehr die SCC verwendet werden müssen (siehe dazu Ziff. 32). In der Praxis dürften trotzdem meist die SCC zum Einsatz kommen, oder ein Derivat davon.
- Von beiden Fällen abzugrenzen ist schliesslich der Fall, wo ein Auftragsbearbeiter eines Verantwortlichen irgendwelche Daten einem anderen Auftragsbearbeiter eines Verantwortlichen übermittelt. Dieser Fall ist von Modul 3 nicht gedeckt, denn Modul 3 geht von einem Subordinationsverhältnis zwischen Exporteur und Importeur aus, d.h. letzterer ist der Unterauftragsbearbeiter des ersten. Für diesen Sonderfall wird zwischen den beiden Auftragsbearbeitern gar nichts zu vereinbaren sein, soweit der Verantwortliche mit beiden Auftragsbearbeitern die SCC je separat abgeschlossen hat (nach Modul 2).

Den ersten Fall regeln die SCC mit dem dritten Modul 3 (Processor-Processor). Hier ist darauf zu achten, wie die SCC die "Befehlskette" regelt. Auch hier kommt die sequenzielle Methode zum Einsatz, d.h. die Instruktionen und Kommunikation läuft über Auftragsbearbeiter, welcher den Verantwortlichen vertritt (bisher wurden für diese Fälle die Controller-Processor-SCC analog verwendet). Es wird dem Auftragsbe-

arbeiter das Recht eingeräumt, dem Subprocessor zusätzliche Weisungen zu erteilen (Modul 3, Clause 8.1(b)), doch muss der Auftragsbearbeiter dem Subprocessor versichern, dass er ihm dieselben Pflichten auferlegt hat, wie ihm bereits der Verantwortliche auferlegt hat (Modul 3, Clause 8.1(d)).[20] Praktisch ist das höchstens dann relevant, wenn der Subprocessor belangt werden sollte, weil der Auftragsbearbeiter ihm gegenüber die "Zügel" zu locker liess.

Kommen die SCC mit dem dritten Modul 3 (Processor-Processor) zum Einsatz, gelten die Ausführungen für das zweite Modul 2 (Controller-Processor) analog (Ziff. 29). Abweichend ist der Fall der Verletzung der Datensicherheit zu erwähnen, in welchem Fall der Subprocessor nicht nur seinen direkten Vertragspartner, den Auftragsbearbeiter, zu informieren hat, sondern "where appropriate and feasible" auch den Verantwortlichen (Modul 3, Clause 8.6(c)). Kooperationspflichten hat der Subprocessor jedoch nur gegenüber dem Auftragsbearbeiter. Eine direkte Meldung des Subprocessors an den Verantwortlichen dürfte nur ausnahmsweise angezeigt sein; dies hat eine Auswirkung darauf, wie schnell der Verantwortliche von einem Data Breach erfährt. Immerhin ist der Subprocessor auch dem Verantwortlichen gegenüber zur angemessenen Behandlung seiner etwaigen Anfragen verpflichtet (Modul 3, Clause 8.9(a)). Ein direktes Audit-Recht ist jedoch nicht vorgesehen; dieses steht dem Auftragsbearbeiter zu.

Unklar geregelt ist der Beizug weiterer Subprocessors durch den Subprocessor (Clause 9). Eine solche Kette von Auftragsbearbeitungen ist unter den SCC vorgesehen, aber die Freigabe muss gemäss den SCC vom Verantwortlichen kommen und nicht vom Auftragsbearbeiter. Diese Regelung ist zwar nachvollziehbar, aber praxisfremd ausgestaltet. Zunächst ist klar, dass es letztlich der Verantwortliche sein muss, der über den Beizug von Auftrags- oder Unterauftragsbearbeitern entscheidet. Das ergibt sich bereits aus Art. 28 DSGVO: Der Verantwortliche soll und muss eine gewisse Kontrolle darüber haben, wer seine Daten bearbeitet – ob dieser Bearbeiter formal im ersten oder nur im zweiten oder dritten Glied ist. Praxisfremd ist, dass der Subprocessor – also der Vertragspartner des Auftragsbearbeiters – den Verantwortlichen (also den Kunden des Auftragsbearbeiters) direkt kontaktieren und darüber informieren muss, dass er als Subprocessor einen weiteren Unterakkordanten beizieht. Die SCC verlangen also eine Umgehung des Dienstwegs. Da es am Ende nur darum gehen kann, dass der Verantwortliche vom Beizug einer weiteren Person erfährt und ihr zustimmt bzw. nicht widerspricht, wird der Auftragsbearbeiter mit seinem Subprocessor sinnvollerweise vereinbaren, dass die Information des

---

20 An dieser Formulierung wird auch bereits klar, dass die Autoren des SCC nur an den Fall gedacht haben, dass es *einen* Auftragsbearbeiter im EWR oder in einem sicheren Drittland ist und die Auftragsbearbeitungs-"Kette" spätestens ab dem ersten Subprocessor in einem unsicheren Drittland weitergeführt wird. Das muss natürlich nicht sein, ist aber in der Praxis wohl irrelevant.

Verantwortlichen in den von den SCC vorgeschriebenen Fällen an den Auftragsbearbeiter (als direkten Vertragspartner des Kunden) delegiert wird.

Diese Fragen sind durchaus von praktischer Relevanz. Nehmen wir das Beispiel eines europäischen SaaS-Providers, der wiederum eine Cloud-Instanz von Microsoft oder Amazon für seinen Service verwendet. Die Kunden des SaaS-Providers werden mit diesem einen ADV nach Art. 28 DSGVO abschliessen, dieser wiederum einen ADV mit Microsoft oder Amazon. Die europäischen Microsoft- und Amazon-Gesellschaften werden – als Auftragsbearbeiter – die SCC mit Modul 3 (Processor-Processor) mit ihren US-Konzerngesellschaften abschliessen. Bei Microsoft wird das Microsoft Corp. sein, die wiederum weitere Microsoft-Gesellschaften als Subprocessors beizieht. Letzteres muss gemäss den SCC von den Subunternehmern von Microsoft Corp. korrekterweise dem Kunden des SaaS-Providers zur Genehmigung vorgelegt werden. Microsoft geht damit heute schon so um, dass sie bloss eine Liste mit allen beteiligten Gesellschaften liefert, die sie im Internet abrufbar macht. Der SaaS-Provider wird korrekterweise von seinem Kunden nicht nur den Beizug von Microsoft oder Amazon genehmigen lassen, sondern auch deren Liste an Unterauftragsbearbeitern qua Verweis auf die Liste. Damit sollte den SCC Genüge getan sein.

33. Muss ein Auftragsbearbeiter in der Schweiz oder im EWR die SCC mit seinen Kunden in unsicheren Drittländern ebenfalls abschliessen?

Ja, es sei denn, der (Re-)Export der Personendaten kann anders abgesichert oder gerechtfertigt werden. Dieser Fall wurde bisher in der Praxis in den meisten Fällen kurzerhand ignoriert. Beispiel ist ein Hosting-Provider in der Schweiz, der einen Kunden in den USA bedient. Diese Fälle kommen vor allem im Konzernverbund häufig vor, wenn ein europäischer Konzern die IT-Infrastruktur in Europa auch für aussereuropäische Konzerngesellschaften betreibt.

Rechtlich wurde in diesen Fällen – wenn überhaupt – immer so argumentiert, dass die betroffenen Personen in diesen Fällen der Bearbeitung im Land des Verantwortlichen zugestimmt hätten und damit ein Re-Export in dieses Land von ihrer Einwilligung gedeckt ist (z.B. Art. 49(1)(a) DSGVO). Dies macht auch Sinn: Wer sich als Arbeitnehmer einer US-Gesellschaft von einer solchen anstellen lässt, geht davon aus, dass die HR-Daten in den USA bearbeitet werden und ist damit auch einverstanden. Es gibt keinen Grund, warum diese Personendaten, sollten sie nun zufälligerweise auf einem Server in Europa statt in den USA gespeichert sein, nicht wieder in die USA zurückübermittelt werden dürfen. Die Problematik bei dieser Argumentation ist, dass eine Einwilligung im Einzelfall erforderlich ist (unter dem DSG) die ausdrücklich sein muss (unter der DSGVO und bei besonders schützenswerten Personendaten auch unter dem DSG), eine solche aber je nach

Situation nicht vorliegt. Über diesen Umstand wurde hinweggesehen, weil die Rechte der betroffenen Personen nicht gefährdet sind und es unter der DSGVO für diesen Fall keine genehmigten SCC gab. Stattdessen wurden teilweise die Controller-Controller-SCC benutzt.

Die neuen SCC decken diesen Fall mit Modul 4 nun ebenfalls ab, was bedeutet, dass diese in den betreffenden Fällen nun konsequenterweise zu vereinbaren sind, falls ein Auftragsbearbeiter Rechtssicherheit sucht. Das gilt insbesondere für konzerninterne IGDTA, wo solche Datenflüsse regelmässig vorkommen.

Die Regelungen der neuen SCC zu dieser Fallkonstellation gehen nicht sehr weit. Im Wesentlichen verpflichtet sich die Stelle im unsicheren Drittland gegenüber ihrem Auftragsbearbeiter, (i) diesen nicht an der Einhaltung der DSGVO zu hindern, (ii) mit ihm für eine angemessene Datensicherheit zu sorgen, und (iii) ihn bei der Erfüllung von Anfragen im Rahmen der DSGVO zu unterstützen. Dies sind vergleichsweise harmlose Pflichten.

Wesentlich gewichtiger sind die Rechte zugunsten betroffener Personen, welche der Abschluss der SCC konstituiert: Sie dürften vermutlich gegen den Kunden des Auftragsbearbeiters vorgehen können, wenn dieser vom Kunden beauftragt wird, eine nach DSGVO unzulässige Datenbearbeitung vorzunehmen und damit selbst gegen die DSGVO zu verstossen. Der Kunde haftet gegenüber den betroffenen Personen in diesen Fällen auch unbeschränkt (Ziff. 39).

Solange also der Kunde eines Auftragsbearbeiters, der im EWR oder in der Schweiz ist oder sonst unter der DSGVO steht, diesem erlaubt, für eine angemessene Datensicherheit zu sorgen und von ihm keine unzulässigen Datenbearbeitungen verlangt, wird der Abschluss der SCC nicht besonders problematisch sein. Er erhält sogar selbst weitergehende vertragliche Haftungsansprüche gegenüber seinem Auftragsbearbeiter, die er ohne SCC nicht hätte. Will der Kunde den Auftragsbearbeiter hingegen für nach DSGVO (oder DSG) unzulässige Datenbearbeitungen nutzen, so exponieren ihn die SCC in beträchtlicher Weise: In diesen Fällen hat nicht nur der Auftragsbearbeiter einen Haftungsanspruch gegenüber seinem Kunden, sollte dessen Verhalten ihn als Auftragsbearbeiter in Schwierigkeiten bringen (eine solche Regelung sehen viele Provider-Verträge heute schon vor). Die SCC geben auch betroffenen Personen einen Rechtstitel, um direkt gegen den Kunden vorzugehen (Ziff. 39). Das war bisher nicht der Fall und dürfte einen erheblichen Wettbewerbsnachteil für europäische Provider darstellen.

Ein kleiner Vorteil bietet Modul 4 aber gegenüber den anderen Modulen: In der hier diskutierten Konstellation sind die Parteien frei in der Rechtswahl und in der Vereinbarung des Gerichtsstands, solange das gewählte Recht von Dritten einklagbare Ansprüche zulässt (Ziff. 20; Clause 17 und Clause 18). Es können also das Heimatrecht und die Heimatgerichte des Kunden gewählt werden.

In der Praxis zeichnet sich freilich bereits ab, dass Service-Provider in Europa mit Kunden in unsicheren Drittstaaten trotz Modul 4 weiterhin keine SCC zum Einsatz bringen werden. Neben den Haftungsrisiken und sonstigen Regelungen von Modul 4 hat dies auch praktische Gründe. Für die Anhänge zu den SCC müssten beispielsweise Zusatzangaben erhoben werden, die im Vertragsprozess oft nicht vorliegen. Es müsste für jeden Kunden in einem unsicheren Drittland zudem ein TIA durchgeführt werden: Bevor der Provider die SCC mit dem Kunden überhaupt abschliessen könnte, müsste er von seinem Kunden also detaillierte Angaben über die Möglichkeit staatlicher Zugriffe auf diesen erheben und sie analysieren. Abgesehen von den damit verbundenen Zusatzkosten sind dies Umstände, die kaum ein Kunde auf sich nehmen wird, wenn er nicht unbedingt auf den betreffenden Provider angewiesen ist. Europäische Provider haben mit Modul 4 der SCC somit einen gewichtigen Wettbewerbsnachteil.

Ihnen ist als Alternative zu Modul 4 zu empfehlen, ihre Geschäfte mit Kunden in unsicheren Drittstaaten über eine Tochtergesellschaft in einem unsicheren Drittstaat abzuwickeln. Der grenzüberschreitende Datenfluss kann dann innerhalb der Gruppe des Providers mit einem IGDTA durchgeführt werden.

Eine weitere Alternative ist es, auf die vorstehend erwähnte Ausnahme der Einwilligung der betroffenen Person abzustellen, soweit keine offenkundigen Gründe dagegen sprechen. Der Provider kann sich im Vertrag mit dem Kunden hierzu von diesem bestätigen lassen, dass er die nach dem anwendbaren Recht nötige Einwilligung der betroffenen Personen zur Bearbeitung der Personendaten durch, und zur Übermittlung an, den Kunden hat. Willigt die betroffene Person der Bearbeitung ihrer Daten am Standort des Kunden zu, akzeptiert sie damit auch den dort fehlenden gesetzlichen Datenschutz. Ist ihr der Standort des Kunden bekannt und übermittelt sie ihm ihre Daten, kann mit guten Gründen vertreten werden, dass sie damit ausdrücklich und im Einzelfall eingewilligt hat, dass ihre Daten eben dort bearbeitet werden – und damit auch dorthin (zurück)übermittelt werden dürfen. Vorbehalten bleiben können die von Modul 4 ebenfalls abgedeckten Fälle der Datenerhebung in Europa.

Der Auftragsbearbeiter wird sich möglicherweise auch noch auf eine andere Ausnahme stützen können: Handelt es sich bei der betroffenen Person um einen Vertragspartner des Kunden (z.B. um dessen Arbeitnehmer), wird die Übermittlung der Personendaten an den Kunden letztlich oft auch für die Abwicklung seines Vertrags mit der betroffenen Person (Art. 49(1)(b) DSGVO) oder für diese (Art. 49(1)(c) DSGVO) erforderlich sein, was ebenfalls einen Verzicht auf Modul 4 rechtfertigt.

Verzichtet ein Auftragsbearbeiter auf den Einsatz von Modul 4, verbleibt für ihn freilich ein gewisses Restrisiko, dass ihm eine Verletzung der DSGVO bzw. des CH DSG vorgeworfen wird. DSGVO bzw. des CH

DSG. Eine solche dürfte allerdings in den hier diskutierten Konstellationen weit unten auf der Prioritätenliste der Aufsichtsbehörden sein, zumal in solchen Fällen der Schutz der betroffenen Personen nicht wirklich untergraben wird – aber nur darum geht es nach Art. 44 GDPR.

34. Liegt auch dann eine Übermittlung in ein unsicheres Drittland vor, wenn der Auftragsbearbeiter oder Verantwortliche seinen Sitz zwar in einem solchen hat, die Daten aber im EWR bleiben?

Die Antwort auf diese Frage ist unklar. Auch der Europäische Datenschutzausschuss (**EDSA**) geht in seiner Stellungnahme zum Anwendungsbereich von Kapitel V der DSGVO nicht auf diese (seltene) Konstellation ein.[21] Der EDSA stellt ohne nähere Ausführung pauschal darauf ab, wo sich der Verantwortliche oder Auftragsbearbeiter befindet und nicht auf den Ort der Daten.

Auf den ersten Blick liesse sich vertreten, dass in diesen Fällen in der Tat keine Übermittlung vorliegt, wenn sichergestellt ist, dass aus einem unsicheren Drittland nicht einmal ein Fernzugriff möglich ist. Bei näherer Betrachtung zeigt sich allerdings, dass der Schutz der Daten nicht davon abhängt, wo die Daten sich physisch befinden, sondern davon, wer ihre Bearbeitung steuert – selbst wenn er sie selbst nicht einsehen kann. Befindet sich diese Person in einer Rechtsordnung ohne angemessenen Datenschutz, kann sie auch nicht zur Verantwortung gezogen werden, wenn sie beispielsweise entscheidet, dass die Daten länger als erforderlich aufbewahrt werden oder dass Weisungen des Verantwortlichen nicht beachtet werden sollen. Auf den Standort der Daten kommt es daher nicht an.

Daraus ergibt sich, dass mit einem Auftragsbearbeiter oder Verantwortlichen in einem unsicheren Drittland die SCC auch dann zu vereinbaren sind, wenn die Personendaten selbst den EWR nie verlassen. Anders wäre es nur, wenn der Auftragsbearbeiter oder Verantwortliche sich gegenüber dem Exporteur verpflichten würde, die Personendaten nicht zu bearbeiten oder die Parameter ihrer Bearbeitung nicht zu bestimmen. Dann aber wäre die betreffende Partei auch keine Auftragsbearbeiterin oder Verantwortliche mehr und der Einsatz der SCC wäre hinfällig, weil es gar keine Übermittlung mehr gäbe. Es wäre aber auch nicht mehr zulässig, dieser Partei Daten zu übermitteln, da deren Bearbeitung nicht mehr kontrolliert wäre.

---

[21] European Data Protection Board (EDPB), Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, 18. November 2021 (Version for public consultation, https://bit.ly/3mDiWWx).

35. Was ist zu tun, wenn ein Subprocessor in Europa ist, der Auftragsbearbeiter jedoch in einem unsicheren Drittland?

An diesen Fall hat die Europäischen Kommission nicht gedacht, obwohl er in der Praxis durchaus vorkommen kann – etwa wenn ein Provider in den USA von Tochtergesellschaften in Europa Rechenzentren betreibt, seine Kundenverträge aber selbst abschliesst. Die Kunden müssen nicht der DSGVO unterliegen.

Streng genommen können die neuen SCC in diesen Fällen nicht im Rahmen von Art. 46(2)(c) DSGVO verwendet werden, da keines der Module auf diese Konstellation passt. Eine Lösung wären BCR, aber wo diese nicht vorliegen muss entweder auf dafür gesorgt werden, dass seitens des Auftragsbearbeiters keine Zugriffe auf die Daten aus einem unsicheren Drittland möglich sind (und es so zu keiner nach Kapitel V der DSGVO relevanten Übermittlung kommt) oder aber die SCC werden – im Sinne eines risikobasierten Ansatzes – analog zur Anwendung gebracht.

Für letzteren Fall empfehlen wir den Abschluss von Modul 4, allerdings nicht mit dem Verantwortlichen, sondern dem Auftragsbearbeiter als dessen *indirekter* Stellvertreter: Formal schliesst der Auftragsbearbeiter den Vertrag mit seinem Subprocessor ab, aber er vertritt dabei materiell seinen Kunden – den Verantwortlichen – indem er letztlich dessen Weisungen und dessen Datenbearbeitung ausführt. Es entspricht dies der Praxis unter den alten SCC, wonach für Processor-Subprocessor-Transfers die SCC für Controller-Processor-Transfers analog zum Einsatz gekommen sind. Auch dies war gemeinhin akzeptiert: Der Auftragsbearbeiter tritt auf als wäre er der Verantwortliche und der Subprocessor sein Auftragsbearbeiter.

Anders verfahren werden muss allerdings dort, wo der Auftragsbearbeiter im unsicheren Drittland seinerseits einen der DSGVO unterstehenden Verantwortlichen und daher mit ihm die SCC nach Modul 2 abgeschlossen hat. In diesem Fall greift die Subprocessor-Regelung nach Clause 9 und der Auftragsbearbeiter wird mit seinem Subprocessor die SCC nach Modul 3 abschliessen oder einen anderen Back-to-Back-Vertrag, der im Wesentlichen dem Modul 2 entspricht. Der Grund: In diesem Fall ist der Auftragsbearbeiter bereits über seinen Vertrag mit dem Kunden (d.h. die SCC nach Modul 2) zur Einhaltung des Datenschutzes verpflichtet; der Einsatz von Modul 4 erübrigt sich und wäre – in Anbetracht von Clause 9 – auch nicht genügend. Ungenügend ist – wiederum wegen Clause 9 – ein gewöhnlicher ADV nach Art. 28(3) DSGVO, obwohl sich der Subprocessor im EWR oder einem sicheren Drittland befindet. Diese Konstellation hat die Kommission ebenfalls nicht bedacht.

36. Müssen wir auch firmeninterne Übermittlungen in unsichere Drittländer absichern?

Ja, allerdings ist dies ein blinder Fleck der DSGVO und des DSG und wurde in der Literatur über lange Zeit so gut wie nicht thematisiert. Gemeint sind Transfers von Personendaten innerhalb derselben Rechtseinheit in Länder ohne angemessenen Datenschutz (z.B. an eine dortige Zweigniederlassung oder an einen Mitarbeiter im Home Office oder in den Ferien).

Rechtlich kann in diesen Fällen argumentiert werden, dass wenn der Verantwortliche oder Auftragsbearbeiter selbst der DSGVO oder dem DSG untersteht (weil sein Mutterhaus im EWR oder der Schweiz ist), dies auch für jene Betriebsteile gilt, die sich in einem unsicheren Drittland befinden. Dies bedeutet, dass er sich auch dort an die Vorgaben der DSGVO und des DSG halten muss. Um dies sicherzustellen, muss er geeignete technische und organisatorische Massnahmen (**TOMS**) treffen. Zu den letzteren gehören entsprechende Weisungen, Schulungen und Kontrollen in Bezug auf die Mitarbeiter, welche für ihn die Personendaten in den unsicheren Drittländern bearbeiten. Dies ergibt sich unter der DSGVO aus Art. 25, 29 und 32 DSGVO. Im DSG ergibt sich dies aus Art. 7 DSG und künftig aus Art. 7 und 8 revDSG. Die Problematik des ausländischen Behördenzugriffs stellt sich hier natürlich im selben Ausmass wie im Falle von Transfers an Dritte, und erfordert letztlich auch dieselben Abklärungen und Massnahmen (Ziff. 43).

Die SCC müssen jedoch nicht abgeschlossen werden. Rechtlich wäre dies auch gar nicht möglich, denn eine Gesellschaft kann keine Verträge mit sich selbst vereinbaren.

Im Falle eines IGDTA hat es sich in der Praxis jedoch bewährt, die SCC analog auch den Zweigniederlassungen in unsicheren Drittländern zu überbinden – nicht als Vertrag, sondern als interne Weisung. Zweigniederlassungen können somit wie eigenständige Parteien in ein solches IGDTA aufgenommen werden, wobei in einer Klausel klargestellt werden sollte, wie die Bestimmungen des IGDTA in ihrem Falle gelten sollen.

Im Anwendungsbereich des DSG kann beim Fernzugriff durch eigene Mitarbeiter (aus dem Home Office oder auf Reisen) ferner vertreten werden, dass gar keine "Bekanntgabe" im Sinne von Art. 6 DSG bzw. Art. 16 revDSG vorliegt, weil eine solche voraussetzt, dass Personendaten einer Person mitgeteilt werden, die noch nicht über sie verfügt. Greift ein Mitarbeiter jedoch auf jene Daten zu, über die er in der Schweiz bereits verfügt, können ihm die Daten begriffslogisch nicht mehr bekanntgegeben werden – und Art. 6 DSG bzw. Art. 16 revDSG kommen nicht mehr zum Tragen.

Unter der DSGVO ist dieselbe Argumentation schwieriger, da sie an eine "Übermittlung" anknüpft (Art. 45 DSGVO), welche nach dem reinen Wortverständnis auch dann vorliegt, wenn eine *Bekanntgabe* dieser

Personendaten nicht mehr möglich ist, weil der Empfänger über die Information bereits verfügt und somit kennt. Allerdings kann mit guten Gründen vertreten werden, dass die Übermittlung von Personendaten an die eigenen Mitarbeiter grundsätzlich nicht in den Anwendungsbereich von Kapitel V der DSGVO fällt. Zu dieser Sichtweise hat sich inzwischen auch der Europäische Datenschutzausschuss entschlossen (dazu Ziff. 37).

37. Was gilt für die Übermittlung an beigezogene Dritte, die nicht als Auftragsbearbeiter gelten?

Wie schon die firmeninterne Übermittlung von Personendaten ins Ausland (Ziff. 33) ist auch dies ein blinder Fleck der DSGVO und des DSG und wurde lange Zeit ebenfalls kaum thematisiert.

Gemeint ist der Beizug von Dritten, die nicht Auftragsbearbeiter sind, sondern Personen "unter der Aufsicht" des Verantwortlichen oder Auftragsbearbeiters nach Art. 29 DSGVO (im DSG gibt es dazu kein Equivalent). Dies können nicht nur die eigenen Arbeitnehmer sein, sondern auch andere Dritte, die in die eigene Organisation integriert sind und Daten ausschliesslich nach der Instruktion des betreffenden Verantwortlichen oder Auftragsbearbeiters bearbeiten (z.B. Leiharbeiter, Einzelauftragnehmer). Die Europäische Kommission hat den Abschluss der SCC jedoch nur im Verhältnis zwischen Auftragsbearbeitern und Verantwortlichen genehmigt, d.h. nicht für diesen Fall. Vom Text der SCC her wäre eine Anwendung auf den vorliegenden Fall möglich, aber der Abschluss der SCC zwischen einem Verantwortlichen oder Auftragsbearbeiter und einzelnen, im Ausland beigezogenen Personen erscheint übertrieben.

Lösen liesse sich das Problem, indem die Übermittlung an solche Personen nicht als Übermittlung im Sinne von Art. 45 DSGVO bzw. nicht als Bekanntgabe im Sinne von Art. 6 DSG bzw. Art. 16 revDSG qualifiziert wird. Dies wäre jedoch systemwidrig, denn in dieser Konstellation befinden sich die Personendaten tatsächlich im unsicheren Drittland und diejenigen, die sie dort bearbeiten, unterliegen dort keinem angemessenen Datenschutz. Auch ein Behördenzugriff ist jedenfalls theoretisch möglich. Dem liesse sich jedoch entgegenhalten, dass das Konzept von Art. 45 DSGVO sich nur auf Übermittlungen beschränkt, welche zwischen Verantwortlichen bzw. Auftragsbearbeitern erfolgen, was daraus ersichtlich sei, dass sowohl die geeigneten Garantien nach Art. 46 DSGVO als auch die verbindlichen internen Datenschutzvorschriften nach Art. 47 DSGVO konzeptionell davon ausgehen, dass sie nur die Verantwortlichen bzw. Auftragsbearbeiter selbst binden, nicht die von ihnen beigezogenen Mitarbeiter und externen Einzelpersonen. Aus demselben Grund verpflichten auch die SCC den Importeur in einem unsicheren Drittland nach herrschender Auffassung nicht, mit jedem seiner Mitarbeiter einen Vertrag ähnlich der SCC abzuschliessen, bevor er ihm oder ihr Zugang zu den von ihm erhaltenen Personendaten ge-

währt. Daraus kann geschlossen werden, dass Übermittlungen an Mitarbeiter vom Kapitel V der DSGVO grundsätzlich nicht erfasst sind und daher auch nicht mittels der SCC abgesichert werden müssen.

Es ist daher richtig, dass in solchen Fällen in der Praxis keine anderen Vorkehrungen getroffen, als wenn sich die Person am Sitz des Verantwortlichen oder Auftragsbearbeiters befinden würde: Er oder sie wird zur Vertraulichkeit verpflichtet und es wird vereinbart, dass er oder sie Personendaten ausschliesslich auf und nach den Weisungen des Verantwortlichen oder Auftragsbearbeiters bearbeiten darf.

Wir empfehlen, dass zusätzlich eine "defend your data"-Klausel vereinbart wird (d.h. die Pflicht, behördliche Zugriffsversuche zu melden und mit den möglichen rechtlichen Mitteln abzuwehren) und angemessene technische und organisatorische Massnahmen zur Datensicherheit (z.B. Verschlüsselung von Übermittlungen) ebenfalls vertraglich vereinbart sind, soweit diese nicht ohnehin vollständig in der Hand des Verantwortlichen oder Auftragsbearbeiters liegen. Auch ist zu prüfen, ob ein relevantes Risiko unerlaubter Zugriffe ausländischer Behörden besteht. Dies ergibt sich aber nicht aus Kapitel V der DSGVO (das hier nicht greift), sondern aus der allgemeinen Pflicht, für eine angemessene Datensicherheit zu sorgen.

In technischer Hinsicht ist in solchen Konstellationen ferner der Einsatz von Remote-Access-Techniken zu empfehlen, d.h. den Personen im unsicheren Drittland lediglich einen Fernzugriff auf einen virtuellen Computer am Sitz des Verantwortlichen oder Auftragsbearbeiters anzubieten, so dass sich nach Beendigung einer Benutzersitzung keine Personendaten im unsicheren Drittland befinden. Dies reduziert das Risiko eines Zugriffs ausländischer Behörden zusätzlich.

Der Europäische Datenschutzausschuss (**EDSA**) hat das Problem inzwischen erkannt und im vorstehenden Sinne gelöst. In einer Stellungnahme kommt er zum Schluss, dass eine Übermittlung im Sinne des Kapitels V der DSGVO nur und erst vorliegt, wenn Personendaten von einer Partei (der Verantwortlicher oder Auftragsbearbeiter sein muss) an eine *andere* Partei (der *ebenfalls* Verantwortlicher oder Auftragsbearbeiter sein muss) übermittelt wird.[22] Eine Übermittlung von Personendaten innerhalb derselben Rechtseinheit (Zentrale an Zweigniederlassung oder umgekehrt), an einen eigenen Mitarbeiter im ausländischen Home Office oder an einen nach Art. 29 DSGVO beigezogenen Dritten gilt gemäss EDSA *nicht* als Übermittlung im Sinne von Kapitel V der DSGVO, weshalb auch der Abschluss der SCC nicht nötig ist. Die Schutzlücke löst der EDSA wie vorne und unter Ziff. 36 dargelegt: Er betont, dass für die Daten im unsicheren Drittland auch in diesen Fäl-

---

22 European Data Protection Board (EDPB), Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, 18. November 2021 (Version for public consultation, https://bit.ly/3mDiWWx), Rz. 11 ff.

len eine angemessene Datensicherheit sichergestellt sein muss, diese Pflicht sich in diesen Fällen aber aus Art. 32 DSGVO ableitet.[23] Sie hat auch den Schutz vor einem (unzulässigen) Behördenzugriff zu umfassen. Kann die Datensicherheit nicht gewährleistet werden, dürfen die Daten nicht ins betreffende Land gehen. Diese Konstruktion über Art. 32 DSGVO hat einen Vorteil und einen Nachteil: Der Vorteil besteht darin, dass die formalen Vorgaben und die Beschränkungen des Kapitel V der DSGVO hier nicht gelten; wie der Verantwortliche oder Auftragsbearbeiter für einen angemessenen Datenschutz (nicht nur Datensicherheit) sorgt, ist ihm überlassen. Der Nachteil ist, dass die Ausnahmen von Art. 49 DSGVO nicht direkt angerufen werden können, sondern ggf. indirekt herzuleiten sind.

38. Gibt es unter den neuen SCC neue Informationspflichten gegenüber den betroffenen Personen?

Ja, und zwar zweierlei:

- Für Verantwortliche in unsicheren Drittstaaten sehen die SCC eine gegenüber Art. 13 ff. DSGVO reduzierte Informationspflicht gegenüber den betroffenen Personen vor.
- Von *allen* Importeuren – auch von Auftragsbearbeitern und deren Subprocessors – verlangen die neuen SCC eine Information auf ihrer Website oder direkt gegenüber den betroffenen Personen die Angabe einer Kontaktadresse für Beschwerden (und verpflichten sie, diese beförderlich zu bearbeiten) (Clause 11). Dies geht über die DSGVO hinaus, denn dort obliegt nur dem Verantwortlichen eine Informationspflicht gegenüber den betroffenen Personen.

Ferner sehen die neuen SCC gewisse Meldepflichten gegenüber den betroffenen Personen vor. Dies ist einerseits eine Pflicht zur Meldung von Verletzungen der Datensicherheit, soweit diese ein hohes Risiko nachteiliger Auswirkungen für die betroffene Person mit sich bringt (z.B. Modul 1, Clause 8.5(f)) und andererseits eine Meldepflicht, falls eine ausländische Behörde auf die Personendaten der betreffenden Person zugreift oder dies versucht (Clause 15.1).

39. Wo exponieren uns die neuen SCC gegenüber betroffenen Personen und Organisationen wie NOYB?

Alle Bestimmungen der neuen SCC sind auch den betroffenen Personen direkt einklagbar, soweit sie nicht im Ausnahmekatalog von Clause 3 aufgelistet sind. Dieser Katalog ist relativ kurz.

Bei den betreffenden Bestimmungen liegt somit ein echter Vertrag zugunsten Dritter vor, was unter Schweizer Recht durchsetzbar ist (auch

---

[23] Ebd., Rz. 17.

wenn das DSG solche Rechte zugunsten Dritter in einem Vertrag nach Art. 6 Abs. 2 Bst. a DSG an sich nicht verlangt). Das ist allerdings nicht überall so. So lässt irisches Recht Ansprüche zugunsten Dritter praktisch nicht zu (Irland hat in seinem Recht inzwischen allerdings klargestellt, dass solche Rechte zugunsten Dritter für die Zwecke der SCC durchsetzbar sind).

Für die Parteien der SCC bedeuten die Ansprüche zugunsten betroffener Personen zweierlei:

- Alle Bestimmungen, die ein Verhalten zugunsten der betroffenen Person vorschreiben (z.B. Erteilung einer Auskunft, Vornahme einer bestimmten Schutzmassnahme), können von dieser gerichtlich durchgesetzt werden. Unter Schweizer Recht sind solche Ansprüche auf Realerfüllung einklagbar. In anderen Rechtsordnungen kann mitunter nur Schadenersatz geltend gemacht werden. Ob die Wahl eine solchen Vertragsstatuts zulässig ist, ist fraglich, da die SCC klarerweise die Realerfüllung bezwecken. Die Autoren der SCC haben dies übersehen, da sie die Durchsetzbarkeit solcher Ansprüche bei der Rechtswahl nicht vorsehen.
- Jede Verletzung der SCC (mit Ausnahme der in Clause 3 aufgeführten Bestimmungen), der der betroffenen Person einen Schaden verursacht, führt zur unbeschränkten vertraglichen Haftung gegenüber dieser betroffenen Person. In Frage kommen dabei sowohl verletzte Verhaltensnormen (also Bestimmungen, die dem Exporteur, Importeur oder allen Parteien ein bestimmtes Verhalten auferlegen) wie auch verletzte Gewährleistungen (wie z.B. Clause 14(a)). Dieser Schadenersatzanspruch richtet sich zwar nur gegen die verantwortliche Partei. Doch bereits eine Mitverantwortung genügt zur solidarischen Haftung (Clause 12(c)). Unter Schweizer Recht muss die betreffende Partei zwar ein Verschulden treffen, aber es würde vermutet werden.

Schon die bisherigen SCC sahen vor, dass betroffene Personen Ansprüche geltend machen konnten. Dies spielte in der Praxis allerdings so gut wie keine Rolle, da ein Vorgehen mit erheblichen Prozessrisiken verbunden ist. Die zivilprozessualen Erleichterungen, die für Datenschutzprozesse teilweise vorgesehen sind, gelten hier nicht, da es letztlich um normale Vertragsansprüche geht.

Zu beachten ist allerdings, dass betroffene Personen auch eine Non-Profit-Organisation wie NOYB mit der Durchsetzung ihrer Ansprüche betrauen kann. Für diese eröffnen die neuen SCC somit ein neues, breites Spielfeld.

40. Wie funktioniert die Durchsetzung der neuen SCC? Was passiert, wenn wir uns nicht an die Vorgaben in den SCC halten?

Die Durchsetzung erfolgt auf drei Ebenen:

- Durch die Vertragsparteien: Die SCC begründen vertragliche Pflichten für die Parteien. Hält eine Partei ihrer Pflicht nicht ein, kann die andere Partei sie auf dem Klageweg in Form von Schadenersatz oder – wo das anwendbare Recht dies zulässt – in Form einer Realerfüllung durchsetzen. Dies ist die schwächste Form der Durchsetzung. Zwar wird insbesondere der Exporteur ein Interesse an einer Durchsetzung haben, weil er sich nur auf sie für den Transfer von Personendaten in unsichere Drittstaaten stützen kann, wenn er sie nicht nur abschliesst, sondern auch gegenüber dem Importeur auch durchsetzt. Trotzdem zeigt die Erfahrung der Vergangenheit, dass Exporteure kaum je Ansprüche aus SCC geltend machen, obwohl es das Instrument schon seit mittlerweile 20 Jahren gibt. Hinzu kommt, dass einige Pflichten so formuliert sind, dass eine Durchsetzung durch die eine Partei gegen die andere nicht ohne weiteres möglich ist, etwa, weil sie den Parteien gemeinsam auferlegt sind (z.B. Modul 4, Clause 8.2(a) oder Clause 14(a)). Das ist eine schlechte Vertragsredaktion.

  Kommt es zu einer wesentlichen oder anhaltenden Verletzung der SCC, steht dem Exporteur selbstverständlich ein Kündigungsrecht zu (Clause 16(c)). Weniger selbstverständlich ist, dass er sehr genau prüfen wird, ob er tatsächlich kündigen will. Denn tut er dies, muss er dies der Aufsichtsbehörde mitteilen und exponiert sich damit möglicherweise auch selbst (Clause 16(c)). Allerdings ist fraglich, ob die Verletzung dieser Pflicht überhaupt sanktioniert werden kann. Sie erscheint jedenfalls nicht zu Ende gedacht. Die Kündigungsklausel ist auch in anderer Hinsicht mangelhaft (Ziff. 45).

- Durch die Aufsichtsbehörde: Die SCC sehen an manchen Stellen die Pflicht vor, etwas zugunsten der Aufsichtsbehörde zu tun (z.B. ihr einen Data Breach zu melden in Modul 1, Clause 8.5(b) oder ihr die Dokumentation der eigenen Bearbeitungsaktivitäten herauszugeben in Modul 1, Clause 8.9(b)). Die SCC sehen jedoch kein vertragliches Recht der Aufsichtsbehörde vor, diese Pflichten zu ihren Gunsten auch gerichtlich durchzusetzen, obwohl dies vertraglich möglich gewesen wäre. Ansprüche zugunsten Dritter sieht Clause 3 nur für die betroffene Person vor; daraus muss jedenfalls für den Fall des Schweizer Rechts geschlossen werden, dass die Aufsichtsbehörde keine solche (vertraglichen) Ansprüchen hat, was letztlich eine verpasste Chance zur Durchsetzung ist.

  Stattdessen sieht Clause 13(b) vor, dass sich der Importeur (der naturgemäss *nicht* der DSGVO untersteht) freiwillig der Zuständigkeit der von den Parteien bezeichneten Aufsichtsbehörde "unterwirft" und sich verpflichtet sich, mit ihr zu kooperieren. Wir haben jedoch erhebliche Zweifel an der Rechtmässigkeit dieser

Konstruktion. Beantwortet werden kann dies letztlich nur nach dem Recht der jeweiligen Aufsichtsbehörde, doch in der Schweiz wäre eine solche "gewillkürte" Zuständigkeit der Behörde wohl unwirksam, weil sich die Zuständigkeit einer Behörde abschliessend nach dem auf sie anwendbaren Recht ergibt und nicht nach einer privatrechtlichen Verpflichtung eines Rechtsunterworfenen. Auch nach der DSGVO ergibt sich die Zuständigkeit einer Aufsichtsbehörde ausschliesslich aus Art. 50(1) DSGVO und damit nach dem Territorialitätsprinzip. Sie setzt zudem die Anwendbarkeit der DSGVO nach Art. 3 DSGVO voraus. Beides wird in manchen Fällen der hier relevanten Fälle nicht erfüllt sein – nicht einmal nach den liberalen Vorgaben der Erwägung 122 der DSGVO.[24]

Anders verhält es sich beim Exporteur, der je nach Fallkonstellation unabhängig von den SCC der Zuständigkeit einer (aber nicht notwendigerweise der in Clause 13 gewählten) Aufsichtsbehörde untersteht. Auf diese Weise können die SCC immerhin indirekt gegen den Importeur durchgesetzt werden: Setzt der Exporteur die SCC nicht gegen den Importeur durch oder hält er sich selbst nicht daran, muss er damit rechnen, dass ihm die Aufsichtsbehörde einen Datentransfer unter Verletzung von Art. 46 DSGVO vorwirft. Diese Bestimmung verlangt die Einhaltung und Durchsetzung der SCC zwar nicht ausdrücklich, aber wäre dies mitgemeint, wären die SCC nutzlos. Die Nichteinhaltung der SCC setzt also vor allem den Exporteur einem Sanktionsrisiko aus.

Das Schweizer Recht gilt ähnliches, allerdings mit gewissen Differenzierungen:

- Hält sich eine Partei nicht an die SCC, muss zunächst geprüft werden, ob es dadurch am erforderlichen Datenschutzniveau fehlt. Das ist nicht notwendigerweise der Fall. Wird beispielsweise eine Pflicht verletzt, die über die DSGVO oder das DSG hinausgeht (z.B. im Bereich der Dokumentationspflichten), dann kann nicht vernünftigerweise vertreten werden, dass der Datenschutz verletzt ist. Selbst der künftige Art. 16 Abs. 2 revDSG verlangt nur, dass ein "geeigneter" Datenschutz gewährleistet ist – aber nicht ein identischer und schon gar nicht ein besserer Datenschutz als nach dem DSG in der Schweiz bestehen würde (einige Bestimmungen der SCC gehen aber über diesen hinaus). Fehlt es am geeigneten Datenschutz, weil der Importeur sich nicht an seine Pflichten hält, kann der EDÖB einschreiten und beispielsweise eine weitere Übermittlung der Daten

[24] Demnach besteht eine Zuständigkeit für Verantwortliche oder Auftragsbearbeiter schon dann, wenn sie Verarbeitungstätigkeiten vornehmen, die auf betroffene Personen in ihrem Hoheitsgebiet der Behörde "ausgerichtet" sind.

untersagen (Art. 51 Abs. 2 revDSG). Was er nicht tun kann, weil Art. 51 revDSG dies nicht vorsieht, ist vom Exporteur die vertragliche Durchsetzung der SCC verlangen. Kann der EDÖB den Importeur aufsichtsrechtlich nicht selbst belangen, hat er gegen ihn keine Handhabe. Die vorstehend für die DSGVO diskutierte "gewillkürte" Unterstellung dürfte in der Schweiz nicht durchsetzbar sein.

- Parallel dazu kann die Strafbestimmung von Art. 61 Bst. a revDSG greifen, wenn der Exporteur weiterhin Personendaten ins Ausland bekanntgibt, obwohl er weiss, dass der Importeur trotz Vertrag keinen geeigneten Datenschutz sicherstellt, weil er sich nicht an den Vertrag hält oder halten kann. Die Vertragsverletzung selbst kann hingegen nicht gebüsst werden; dazu ist der Wortlaut von Art. 61 Bst. a revDSG zu einschränkend. Unter dem heutigen Recht ist jedenfalls gestützt auf das DSG keine Busse für eine Verletzung von Art. 6 Abs. 2 DSG möglich. Nicht gebüsst werden kann der Importeur, da nur die Bekanntgabe von Personendaten tatbestandsmässig ist – nicht deren Entgegennahme oder vertrags- oder datenschutzwidrige Verwendung.

  Pro memoria: Eine ausländische Datenschutz-Aufsichtsbehörde kann in der Schweiz weder Anordnungen noch Bussen zwangsweise durchsetzen, weil sie damit sich und die mitwirkende Schweizer Partei strafbar machen würde (Art. 271 StGB).

- Durch die betroffene Partei oder einen Vertreter: Vgl. hierzu Ziff. 39.

In der Praxis spielte die Durchsetzung bzw. Einhaltung der SCC bisher eine eher untergeordnete Rolle. Mit "Schrems II" hat sich dies immerhin mit Bezug auf die für deinen Datentransfer zu treffenden Schutzmassnahmen verändert: Hier haben gewisse Aufsichtsbehörden im EWR begonnen, den Exporteuren Fragen zu stellen. Es ist davon auszugehen, dass diese Aufsichtstätigkeit zunimmt.[25]

41. Wie verhält es sich mit der Haftung unter den neuen SCC?

Unter den neuen SCC haften die Parteien nicht nur gegenüber den betroffenen Personen für Verstösse gegen die SCC, sondern auch einander (Clause 12).

Die bisherigen SCC sahen zwar zwingend eine Haftung zugunsten betroffener Personen vor (was bisher kaum relevant war in der Praxis), aber eine gegenseitige Haftung der Vertragsparteien war optional. Die von der Europäischen Kommission in den bisherigen SCC vorgeschlagene Klausel wurde in der Praxis so gut wie nie eingesetzt.

---

[25] Vgl. hierzu https://www.lda.bayern.de/de/thema_schrems2_pruefung.html.

Neu ist die gegenseitige Haftung der Vertragsparteien eine zwingende Bestimmung, die weder direkt noch indirekt geändert oder eingeschränkt werden darf. So jedenfalls ist unser Verständnis. Die SCC gehen damit über die Anforderungen der DSGVO hinaus, dies selbst für Auftragsbearbeitungen weder für den Auftragsbearbeiter noch den Verantwortlichen eine unbeschränkte Haftung vorschreibt. In der Praxis wird sie auch selten vereinbart; immer wieder anzutreffen ist allerdings ein sog. "Super-Cap", d.h. eine gegenüber dem restlichen Vertrag erhöhte maximale Haftungssumme – soweit die Haftung unter dem anwendbaren Vertragsrecht beschränkt oder wegbedungen werden kann.

Es ist zwar weiterhin möglich, dass ein Kunde und ein Provider in einem Servicevertrag eine Haftungsbegrenzung vereinbaren, aber soweit die SCC zur Anwendung kommen und die Regelung des Servicevertrags damit im Widerspruch steht, geht die Regelung der SCC vor (Clause 5) und muss dies auch, damit die SCC als solche ihre Gültigkeit behalten (Clause 2(a)). Somit stellt sich die Frage, ob eine Haftungsbegrenzung im Servicevertrag ein Widerspruch zur Haftungsregelung in den SCC darstellt. Ist dies der Fall, kommt erstere nicht zur Anwendung, soweit ein Haftungsanspruch auf Clause 12 abgestützt werden kann. Sie sieht sogar vor, dass ein Importeur sich nicht exkulpieren, wenn nicht er, sondern sein Auftragsbearbeiter oder Subprocessor für den Schaden verantwortlich ist. Damit ist sie strenger als Art. 84(3) DSGVO, wonach sich ein Verantwortlicher von der Haftung befreien kann, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

In der Praxis stellen sich verschiedene Fragen, die zugleich Ansätze bieten, wie die Parteien von SCC ihr gegenseitiges Haftungsrisiko möglicherweise begrenzen können:

- Steht Clause 12(a) tatsächlich im Widerspruch zu einer vertraglichen Haftungsbeschränkung? Hier lässt der Wortlaut je nach Sprachfassung der SCC Spielraum offen. In der englischsprachigen Version besagt Clause 12(a), dass eine Partei der anderen Partei "for any damages" haftet, also für "jeden" Schaden. Die deutschsprachige Fassung ist weniger absolut. Sie besagt nur, dass jede Partei den anderen Parteien "für Schäden" haftet, welche sie verursacht. Diese Formulierung lässt Argumentationsspielraum offen, wonach Clause 12(a) lediglich den Haftungsgrundsatz festhält, aber Raum für weitere Klauseln zur Beschränkung der Haftung lässt. In Tat und Wahrheit enthalten viele kommerzielle Verträge Formulierungen, die einerseits festhalten, dass Parteien einander für Schäden haften, diese Haftung in einer nächsten Klausel aber in bestimmten Fällen ausschliessen oder einschränken. Dies gesagt würde eine Haftungsbeschränkung in einem Servicevertrag kein Widerspruch zu Clause 12(a) darstellen. Immerhin besteht das Risiko, dass eine Datenschutzbehörde

sich auf den Standpunkt stellt, Clause 12(a) sei dem Sinn und Zweck nach als abschliessende Regelung zu interpretieren, weil sie auf diese Weise einen maximalen Anreiz zur Einhaltung der SCC schafft, was wiederum im Sinne der DSGVO sei und daher für die Auslegung massgeblich sei (Clause 4(b)). Auch würde sonst Clause 12(a) geschwächt, was Clause 2(a) widerspreche.

- Eine weitere relevante Frage wird sein, *welche* Schäden eine Partei des SCC im Rahmen von Clause 12(a) geltend machen kann. Das gilt insbesondere für Auftragsbearbeitungen, wo die Datenbearbeitung eine vertragliche Leistung der einen Partei darstellt, welche die sie typischerweise nie ohne weitgehende Haftungsbeschränkungen und -ausschlüsse anzubieten bereit ist.

  Die Antwort ist letztlich eine Frage des anwendbaren Vertragsrechts, nicht der DSGVO. Ein Ansatzpunkt ist der Vertragszweck, der sich aus Clause 1(a) ergibt, nämlich die Einhaltung der DSGVO bei der Bearbeitung von Personendaten. Daraus lässt sich das Argument ableiten, dass auch die Haftungsklausel nur Schäden im Visier hat, vor denen die DSGVO schützen will: Wer wegen einer Verletzung der Datensicherheit Datenschutzverletzung seinen Online-Shop für drei Tage ausser Betrieb nehmen muss und dadurch einen Gewinnausfall erleidet, hat keinen solchen Schaden. Anders würde es sich wohl verhalten, wenn aufgrund mangelhafter Datensicherheit eines Providers seitens des Kunden Aufwendungen zur Wiederherstellung von verlorener Personendaten entstehen – es ist dies der Aufwand, um den Zustand einer ordnungsgemässen Bearbeitung von Personendaten wiederherzustellen.

  Das Schweizer Recht lässt eine solche Betrachtung zu. Sie basiert auf der sog. Schutzzwecktheorie, welche eine zunehmende Anzahl schweizerischer Autoren auch bei Ansprüchen nach Art. 97 Obligationenrecht (**OR**), um die es hier geht, im Rahmen der Adäquanzbetrachtung zulassen will. Auch das Bundesgericht hat in jüngeren Entscheiden den Zweck der konkret infrage stehenden Haftungsnorm in die Adäquanzbeurteilung einbezogen.[26] Für den Fall eines Schadens im Zusammenhang mit den SCC könnte also argumentiert werden, dass die Schutzzwecktheorie hier vollends (oder zumindest teilweise) Anwendung findet und daher Clause 12(a) nur den Ersatz von "Datenschutzschäden" will und erlaubt, d.h. für alle anderen Schäden die Haftungsregelung im Hauptvertrag der Parteien zur Anwendung käme. Dort könnte zur Vermeidung von Widersprüchen festgehalten werden, dass die Haftungsbeschränkung im Hauptvertrag nicht für "Datenschutz-

---

[26] BGE 123 III 110 E. 3a S. 112 f, BGer 4C.422/2004 vom 12. September 2005 E. 5.2.2.1, BGer 4C.103/2005 vom 1. Juni 2005 E. 5.1 und BGer 4A_87/2019 vom 2. September 2019 E. 4.3.1 ff.

schäden" gelte, die nach Clause 12(a) der SCC gefordert werden können. Was solche Datenschutzschäden genau sind, ist eine andere Frage. Entgangenen Gewinn und dergleichen dürften sie nicht umfassen.

Wir erwarten, dass es zur Tragweite der Haftungsklausel und der Möglichkeit der Vermeidung einer weitgehenden Haftung noch einige Diskussionen geben wird.

Zu Schadenersatzansprüchen von betroffenen Personen siehe Ziff. 39.

42. Welche rechtliche Bedeutung haben die Zusicherungen, die abgegeben werden?

Diese Frage entscheidet sich nach dem anwendbaren Vertragsrecht.

Im Schweizer Recht führt die Verletzung einer der (wenigen) Zusicherungen (im Englisch: "warranties") in den SCC zu einem Schadenersatzanspruch aus Vertragsverletzung. Der Gewährleistungsfall muss zum Zeitpunkt des Inkrafttretens des Vertrags vorliegen. Im Fall von Clause 14(a) müssen die Parteien also bereits zum Zeitpunkt des Zustandekommens des Vertrags Grund zur Annahme haben, dass das nationale Recht des Importeurs seine Einhaltung der SCC verhindern wird. Ist dies der Fall, kann sich in diesem Fall eine betroffene Person bei gegebenen Voraussetzungen den entstandenen Schaden ersetzen lassen, der durch einen Vorfall verursacht wurde, betreffend welchem die Parteien (oder eine der Parteien) Anlass hatten zu anzunehmen, dass er geschehen könne. Mussten sie nicht damit rechnen, weil er so unwahrscheinlich war, haften sie jedenfalls unter Schweizer Recht nicht.

43. Was müssen wir tun, um die Anforderungen von Schrems II zu erfüllen? Genügen die neuen SCC?

Nein, die neuen SCC genügen nicht. Die Parteien müssen sich zusätzlich (i) vergewissern, dass sie die SCC ungeachtet des nationalen Rechts des Importeurs auch einhalten können und (ii) sie müssen ihre diesbezügliche Einschätzung dokumentieren. Durchzuführen ist mit anderen Worten ein sog. *Transfer Impact Assessment* (**TIA**) und Daten dürfen nur transferiert werden, wenn dieses TIA zufriedenstellend ausfällt. Zur Durchführung des TIA vgl. Ziff. 44.

Der Fokus eines TIA liegt auf der Frage, ob der Importeur (und weitere Empfänger in der Kette) nach seinem Recht von einer lokalen Behörde zur Herausgabe von Personendaten gezwungen kann *und* dieser Zugriff nicht Standards des EU-Rechts entspricht. Dieser letzte Teilsatz ist wichtig: Ordnet ein US-Gericht im Zusammenhang mit einem Zivil- oder Strafverfahren gegenüber einem US-Provider die Herausgabe von Personendaten seines europäischen Kunden an, so steht dies im Prinzip nicht im Widerspruch mit EU-Recht. Auch der US CLOUD Act steht nicht im Widerspruch mit europäischem Recht – ganz im Gegenteil, er

setzt Art. 18 der Cybercrime-Konvention des Europarats um. Solche Zugriffe sind auch innerhalb Europas jederzeit und immer möglich.

Mit den Standards des EU-Rechts hingegen nicht vereinbar ist eine Herausgabepflicht, die *keiner* gerichtlichen Überprüfung unterliegt. Nur darum ging es in Schrems II.[27]

Im Rahmen eines TIA ist somit zu überprüfen, ob der Importeur zur Herausgabe von Personendaten gezwungen werden kann, ohne dass er bzw. die betroffenen Personen sich dagegen gerichtlich zur Wehr setzen können und ob gewisse weitere Garantien erfüllt sind.[28] Darüber hinaus soll ein behördlicher Zugriff nur zu den in Art. 23(1) DSGVO aufgeführten Zwecken erfolgen.

Bei welchem Ergebnis eines TIA eine Übermittlung von Personendaten gestützt auf die SCC zulässig sein soll, darüber herrschte zunächst Uneinigkeit. In einer ersten Stellungnahme haben diverse EU-Datenschutzbehörden und der Europäischen Datenschutzausschusses (**EDSA**) die Ansicht vertreten, das Risiko eines solchen Zugriffs ohne Rechtsweggarantie (und gewisse weitere Garantien) muss null sein. Dies wurde an breiter Front kritisiert. Inzwischen hat der EDSA seine Haltung revidiert und akzeptiert in Version 2.0 seiner Empfehlung 01/2020 vom 18. Juni 2021[29] ein Restrisiko. An die Adresse der Exporteure hält der EDSA fest: Personendaten "dürfen Sie" auch ohne zusätzliche Massnahmen (nebst den SCC) in ein unsicheres Drittland übermitteln, wenn "Sie der Ansicht sind und nachweisen und dokumentieren können, dass Sie keinen Grund zu der Annahme haben, dass relevante und problematische Rechtsvorschriften in der Praxis so ausge-

---

27 Konkret ging es zwei Bestimmungen des US-Rechts, in welchen US-Nachrichtendienste unter gewissen, speziellen Konstellationen auf europäische Daten zugreifen dürfen, ohne, dass dies einer Rechtsweggarantie unterliegt. Der US COUD Act war nicht Gegenstand von Schrems II. Vgl. auch https://www.vischer.com/know-how/blog/schrems-ii-was-er-fuer-unternehmen-in-der-schweiz-bedeutet-38295/.

28 Im Wesentlichen sind es vier Anforderungen (Quelle: EDÖB): (1) Legalitätsprinzip: Klare, präzise und zugängliche Regeln, d.h. hinreichend bestimmte und klare Rechtsgrundlage betreffend Zwecke sowie Verfahren und materiellrechtliche Voraussetzungen des behördlichen Datenzugriffs und Befugnisse der Behörden. (2) Verhältnismässigkeit der Befugnisse und Massnahmen im Hinblick auf die verfolgten Regelungsziele, d.h. die Befugnisse und Massnahmen der Behörden müssen geeignet und erforderlich sein, um die gesetzlichen Zwecke der behördlichen Zugriffe zu erfüllen. Zudem müssen sie für die Betroffenen zumutbar sein. (3) Dem Einzelnen müssen wirksame Rechtsmittel zur Verfügung stehen, d.h. Betroffene müssen wirksame gesetzlich verankerte Rechtsbehelfe für die Durchsetzung ihrer Rechte zum Schutz der Privatsphäre und informationellen Selbstbestimmung (z.B. Auskunft-, Berichtigungs- und Löschungsrecht) haben. (4) Rechtsweggarantie und Zugang zu einem unabhängigen und unparteiischen Gericht, d.h. Eingriffe in die Privatsphäre und informationelle Selbstbestimmung müssen einem wirksamen, unabhängigen und unparteiischen Kontrollsystem unterliegen (Gericht oder andere unabhängige Stelle, z.B. Verwaltungsbehörde oder parlamentarisches Gremium); neben vorheriger (gerichtlichen) Genehmigung von Überwachungsmassnahmen (Schutz vor Willkür) muss auch die tatsächliche Funktionsweise des Überwachungssystems überprüft werden können.

29 https://edpb.europa.eu/news/news/2021/edpb-adopts-final-version-recommendations-supplementary-measures-letter-eu_en.

legt und/oder angewendet werden, dass sie Ihre übermittelten Daten und den Importeur erfassen."[30]

Nach unserer Erfahrung aus der Praxis kommt eine vernünftige TIA mit Bezug auf die USA, aber auch punkto mancher anderer "unsicherer" Drittländer in fast allen Anwendungsfällen zum Schluss, dass kein relevantes Risiko eines Behördenzugriffs ohne Rechtweggarantie vorliegt und daher einer Übermittlung von Personendaten unter den SCC in ein unsicheres Drittland zulässig sein muss. Durchzuführen und zu dokumentieren ist die TIA gemäss EDSA und den SCC trotzdem.

Der gemäss den EU-Datenschutzbehörden hierfür zu betreibende Aufwand wird von vielen Experten (richtigerweise) als unverhältnismässig beurteilt. Mit ihren ersten extremen, praxisfernen und vor allem kopflos anmutenden Reaktionen auf das EuGH-Urteil zu "Schrems II" positionierte sich der EDSA und viele Einzelbehörden in eine Ecke, aus welcher sie nun ohne Gesichtsverlust nur schwer wieder herauskommen. Um zu begründen, dass Datentransfers in die USA auch ohne Vollverschlüsselung nun doch wieder möglich sein sollen, weil die Gefahr der Behördenzugriffe ohne Rechtsweggarantie (und gewisse weitere Garantien) bei Lichte betrachtet in den meisten Fällen nicht so gross wie befürchtet ist, werden die Anforderungen an ein die belegende TIA nun entsprechend hochgeschraubt. So verlangt der EDSA selbst für Standardsituationen einen für den konkreten Einzelfall verfassten "detaillierten" Bericht[31], mit Belegen aus öffentlich zugänglichen, dokumentierten Quellen[32]. Wir gehen davon aus, dass diese Anforderungen in der Praxis häufig nicht befolgt werden wird und in den kommenden Jahren langsam abgebaut werden.

Hier wird sich wohl mancher denken, dass es den betroffenen Personen mehr dienen würde, wenn die dafür vom Exporteur hierfür aufzuwendenden Ressourcen stattdessen in die Überprüfung der Datensicherheit investiert würde. So wären beispielsweise *Audits* der Datensicherheit nach unserer Praxiserfahrung viel wichtiger und wirksamer für den Schutz der betroffenen Personen als ein TIA, da heute Personendaten durch mangelnde Datensicherheit wesentlich stärker bedroht sind als durch ausländische Behördenzugriffe ohne Rechtsweggarantie (und gewisse weitere Garantien). Solche Audits kommen allerdings selten vor.

Wir sind der Ansicht, dass die Durchführung eines Transfers auch ohne Durchführung eines detaillierten und formalisierten TIA vertretbar ist,

---

30 EDSA, Recommendation 01/2020, Executive Summary und Rz. 43.3.

31 EDSA, Recommendation 01/2020, Fussnote 54 (übersetzt): "Die von Ihnen zu erstellenden Berichte müssen umfassende Informationen über die rechtliche Bewertung der Rechtsvorschriften und Praktiken sowie deren Anwendung auf die spezifischen Datenübermittlung, das interne Verfahren zur Erstellung der Bewertung (einschliesslich Informationen über die an der Bewertung beteiligten Akteure – z.B. Anwaltskanzleien, Berater oder interne Abteilungen) und das Datum der Prüfung enthalten. Die Berichte sollten vom gesetzlichen Vertreter des Exporteurs abgezeichnet werden."

32 EDSA, Recommendation 01/2020, Annex 3.

wenn es höchstwahrscheinlich zu keinem ausländischen Behördenzugriffs ohne Rechtsweggarantie und gewissen weiteren Garantien kommt. Nach Schweizer Recht ist dies unseres Erachtens ohne Weiteres zulässig. Dasselbe muss für die DSGVO gelten, auch wenn hier wie erwähnt Konflikte mit EU-Datenschutzbehörden denkbar sind. In der Praxis haben wir mit dieser Position jedoch gute Erfahrungen gemacht, wenn einer Datenschutzbehörde gezeigt werden kann, dass ein Exporteur sich einerseits mit der Frage entsprechend eingehend auseinandergesetzt hat und seine Haltung auch unter ausländischem Recht begründen kann und andererseits auch Massnahmen getroffen hat, um das Risiko eines solchen Behördenzugriffs entsprechend zu reduzieren. Wir haben hierzu eine (frei verfügbares) statistische Methode entwickelt, wie die Eintrittswahrscheinlichkeit eines ausländischen Behördenzugriffs im Sinne eines prädiktiven Urteils für die Zwecke eines Risikoentscheids nachvollziehbar und konkret berechnet werden kann.[33] Diese hat sich in der Praxis bewährt und wird in der Schweiz für heiklere Fälle inzwischen regelmässig eingesetzt, so etwa um die Wahrscheinlichkeit eines unerwünschten Zugriffs auf Berufsgeheimnisdaten zu ermitteln. Was für das Bankgeheimnis genügt, muss auch für die Zwecke des Datenschutzes genügen. Wir haben daher frei verfügbare TIA Formulare basierend auf unserer statistischen Methode entwickelt (siehe Ziff. 44 am Ende).

Auch die grossen Cloud-Provider haben inzwischen damit begonnen, ihren Kunden Information und Vorlagen für TIAs zu liefern, um diesen Prozess soweit wie möglich zu standardisieren. Die Qualität dieser Unterlagen schwankt allerdings stark. In vielen Fällen handelt es sich einfach nur um eine allgemein gehaltene Abhandlung des lokalen Rechts zum Thema Behördenzugriffe. Eine eigentliche Risikobeurteilung fehlt. Auch werden in der Regel keine genauen Zahlen betreffend Behördenzugriffe offengelegt, sondern mit nichtssagenden Zahlen wie "0-499" gearbeitet.

Die neuen SCC verfolgen ebenfalls den risikobasierten Ansatz. Die Parteien müssen nicht zusichern, dass kein ausländischer Behördenzugriff ohne Rechtsweggarantie (und gewisse weitere Garantien) geschehen kann, sondern nur, dass sie "keinen Grund zu der Annahme" ("no reason to believe") haben, dass es in ihrem Fall zu solchen Zugriffen kommen wird. Damit bewegen wir uns – um es mit einem Terminus des Schweizer Rechts auszudrücken – im Bereich des Eventualvorsatzes: Der Erfolgseintritt wird für möglich gehalten und er wird zwar nicht angestrebt, aber letztlich in Kauf genommen, d.h. akzeptiert. Die "bewusste Fahrlässigkeit" genügt nicht: Sie läge vor, wenn der Exporteur den Zugriff zwar für möglich hält, aber darauf vertraut ("annehmen", im Englisch "believe"), dass es nicht dazu kommt. Dies ist auch

---

[33] https://www.rosenthal.ch/downloads/Rosenthal_Cloud_Lawful_Access_Risk_Assessment.xlsx und der wissenschaftliche Beitrag dazu unter https://www.rosenthal.ch/downloads/Rosenthal-CloudLawfulAccess.pdf.

nach der Lehre des Eventualvorsatzes natürlich nicht bei beliebig hoher Eintrittswahrscheinlichkeit möglich – überschreitet die Wahrscheinlichkeit des Erfolgseintritts ein gewisses Mass, so wird angenommen, dass die betreffende Person mit dem Erfolgseintritt gerechnet haben muss.

In der Praxis werden diese Überlegungen überflüssig sein, denn in den allermeisten Fällen von Datenübermittlungen im unternehmerischen Alltag wird die Eintrittswahrscheinlichkeit so gering sein, dass nicht einmal der Vorwurf der Fahrlässigkeit begründet werden könnte. Wird der von den neuen SCC verlangte Standard als das Mass der Dinge genommen, wäre eine Übermittlung somit unproblematisch und die Zusicherung von Clause 14(a) nicht verletzt.

Dies alles gilt auch für Übermittlungen aus der Schweiz. Der EDÖB hat hierzu am 18. Juni 2021 eine Anleitung für die Prüfung der Zulässigkeit von Datenübermittlungen mit Auslandsbezug nach Art. 6 Abs. 2 Bst. a DSG publiziert.[34] Auch diese verlangt eine Prüfung der Rechtslage im Zielland, unter Einbezug der geltenden Rechtsvorschriften im Zielland, der Praxis der Verwaltungs- und Gerichtsbehörden und der Rechtsprechung. In der ursprünglichen Fassung der Anleitung war noch der Satz enthalten: "Subjektive Faktoren wie z.B. die Wahrscheinlichkeit eines Zugriffs können im Regelfall nicht berücksichtig werden." Dieser wurde in der Folge (richtigerweise) gestrichen, denn er ist schlicht falsch: Die Wahrscheinlichkeit eines Zugriffs ist kein subjektiver Faktor, sondern letztlich das Ergebnis der Analyse. Auch für die Schweiz gilt: Die Wahrscheinlichkeit eines ausländischen Behördenzugriffs ohne Rechtsweggarantie (und gewisse weitere Garantien) muss nicht Null sein. Auch Rechtsgutachten liefern nie Gewissheit; ihre Aussagen sind in der Regel sehr viel ungenauer und mit mehr Rauschen, Verzerrungen und Vorbehalten befrachtet als das Fachurteil auf Basis der bereits erwähnten statistischen Methode. Richtig ist aber, dass es nicht einfach auf das "Gefühl" ankommen kann, ob ein ausländischer Behördenzugriff ohne Rechtsweggarantie (und gewisse weitere Garantien) ankommt.

Die neuen SCC regeln nicht nur, unter welchen Voraussetzungen (nach Ansicht der Europäischen Kommission) übermittelt werden darf, sondern auch, was im Falle eines drohenden Behördenzugriffs zu tun ist. Dies ist kein Widerspruch zur Zusicherung, dass die Parteien nicht mit einem Zugriff ohne Rechtsweggarantie (und gewisse weitere Garantien) rechnen, denn die betreffende Clause 15 deckt alle Formen von Herausgabebefehlen oder Zugriffen durch ausländische Behörden ab, auch solche, die einer gerichtlichen Überprüfung unterliegen. Für diese Fälle sehen die SCC neu einerseits in Clause 15.2 eine Pflicht zur "Verteidigung" der Daten auf dem Rechtsweg vor (d.h. eine "Defend your data"-Klausel, die ein rechtliches Vorgehen gegen den Herausgabebefehl bzw. den Zugriff verlangt) und andererseits in Clause 15.1 eine Meldepflicht.

---

[34] https://bit.ly/3kMnc5j.

Diese Meldepflicht hat es in sich, denn sie verlangt nicht nur die Information des Exporteurs, sondern auch der betroffenen Personen (Clause 15.1(a)). Wenn also eine Bank ihre Daten in die Cloud eines europäischen Providers auslagert und dieser einen Subprocessor in den USA beizieht, über welchen eine US-Behörde an Kundendaten der Bank herankommen will, dann müsste der Subprocessor in den USA nach dem Wortlaut der SCC die Kunden der Bank anschreiben, und die Bank muss ihm letztlich die dazu erforderlichen Angaben liefern. Das ist nicht nur praxisfern, sondern widerspricht über dem Datenschutz, da in diesem Falle dem Subprocessor unter dem Vorwand des Datenschutzes noch mehr Personendaten gegeben werden müssen, als er schon hat. In solchen Fällen ist den Parteien zu empfehlen, die Meldung an die betroffene Person an den Verantwortlichen zu delegieren, was unseres Erachtens zulässig sein muss (Clause 4(c): Die SCC sind datenschutzkonform zu interpretieren).

44. Wie wird ein Transfer Impact Assessment (TIA) unter den neuen SCC gemacht?

Das *Transfer Impact Assessment* (**TIA**) ist in Clause 14(b) geregelt, jedenfalls teilweise. Es wird benötigt, wenn Personendaten in ein unsicheres Drittland gestützt auf die SCC übermittelt werden sollen (dazu Ziff. 43).

An sich beantwortet ein TIA die Frage, welche möglichen negativen Auswirkungen die Übermittlung der Personendaten in das Zielland für die betroffenen Personen vernünftigerweise haben kann, und wie wahrscheinlich dies ist. Das können irgendwelche negativen Auswirkungen sein. Herrscht im Zielland beispielsweise ein Ausnahmezustand, so kann sich das auf die Datensicherheit oder sonst die Zuverlässigkeit der datenschutzkonformen Bearbeitung der Daten auswirken. Selbstverständlich muss ein Exporteur sich vor jeder Übermittlung von Personendaten an einen Dritten überlegen, ob damit den Personendaten (und damit auch den betroffenen Personen) irgendwelches Ungemach droht.

Im Kontext von Clause 14(b) wird das TIA allerdings viel enger verstanden. Für die Zwecke von Clause 14 muss das TIA die Frage beantworten, wie wahrscheinlich es ist, dass aufgrund der Übermittlung der Daten in das Zielland es ist, dass dort die Behörden auf die Personendaten zugreifen oder sie herausverlangen könne, ohne dass dieser Vorgang einer unabhängigen gerichtlichen Überprüfung unterliegt (oder anderweitig den Kern der Grundrechte und -freiheiten nicht respektiert oder über das hinausgeht, was in einer demokratischen Gesellschaft notwendig und verhältnismässig ist, um eines der in Art. 23 Abs. 1 DSGVO aufgeführten Ziele zu schützen). Für die USA hat der Europäische Gerichtshof in seiner Entscheidung "Schrems II" festgestellt, dass dies bei Section 702 FISA und EO 12.333 der Fall ist.

Für andere Länder, für die kein Angemessenheitsbeschluss besteht, muss in der Regel eine Abklärung einer Anwaltskanzlei vor Ort stattfinden, die darlegt, inwiefern das lokale Recht im Bereich behördlicher Zugriffe die Vorgaben der DSGVO und des DSG respektiert. Hierzu haben wir einen kostenlosen Fragebogen entwickelt und bereitgestellt, mit welchem die erforderlichen Informationen gezielt erhoben werden können.[35] Wir haben leider die Erfahrung gemacht, dass viele Anwaltskanzleien ohne genaue Vorgaben dieser Art mit der Aufgabenstellung überfordert sind und unbrauchbare Ergebnisse liefern. Was sich viele nicht bewusst sind: Der Umstand, dass eine Rechtsordnung keinen angemessenen gesetzlichen Datenschutz aufweist, bedeutet noch nicht, dass die dort möglichen Behördenzugriffe die von der DSGVO und dem DSG verlangten Garantien verletzen und problematisch sind. Auch in den USA sind es nur sehr spezifische Behördenzugriffe, die den europäischen Standards nicht genügen; andere wiederum stellen kein Problem aus Sicht des Datenschutzes dar. Ein TIA für den Einzelfall ist daher nur und erst nötig, wenn es sich um eine Rechtsordnung handelt, welche Behördenzugriffe erlaubt, die nicht den Vorgaben der DSGVO und des DSG entsprechen. Nur in Bezug auf diese muss in einem zweiten Schritt abgeklärt werden, ob ein relevantes Risiko vorliegt, dass es zu einem solchen Zugriff kommt. Mit dem von uns entwickelten Fragebogen ist es möglich, die nötigen Rechtsgrundlagen zu erheben. Er dient zugleich der Dokumentation für die Zwecke von Clause 14 der SCC.

Ist klar, dass es Behördenzugriffe geben kann, die den Anforderungen der DSGVO und des DSG nicht entsprechen, muss diesbezüglich eine Prüfung des Zugriffsrisikos im Einzelfall erfolgen. Clause 14(b) der SCC legt hierzu fest, dass alle Umstände des Einzelfalls zu betrachten sind, einschliesslich der Natur der Daten, der Datenbearbeitung und des Datenbearbeiters, den bisherigen Erfahrungen mit Behördenzugriffen in der betreffenden Konstellation und den getroffenen Massnahmen zum Schutz vor Behördenzugriffen. Dies bedeutet mit anderen Worten, dass eine Risikoeinschätzung vorzunehmen ist und es – jedenfalls nach Ansicht der Europäischen Kommission – nicht erforderlich ist, dass in technischer Hinsicht der Zugriff durch eine ausländische Behörde z.B. mittels Vollverschlüsselung vollständig verhindert wird. Solche technischen Massnahmen sind nach Clause 14(b) nur ein von mehreren, im TIA zu beachtenden Faktoren. Datenschutzbehörden haben jedoch betont, dass es nicht genügt darauf abzustellen, dass die Art der Daten in einem konkreten Fall für die ausländischen Behörden "nicht interessant" sind. Damit muss gemeint sein, ob die Daten eines bestimmten Unternehmens für die Behörden interessant sind oder nicht; dies kann in der Tat keine Rolle spielen. Hingegen darf berücksichtigt werden, welche Kategorien von Daten erfahrungsgemäss Gegenstand der behördlichen Zugriffe sind. Eine Analyse des ausländischen Rechts und

---

35 https://www.rosenthal.ch/downloads/Rosenthal_Assessing_Lawful_Access_Laws.xlsx.

der Art und Weise, wie es angewandt wird, ist erforderlich falls technische Massnahmen den verpönten Behördenzugriff nicht verhindern können.

Von Gesetzes wegen ist es der Exporteur, der das TIA durchführen muss. Werden die SCC jedoch unterzeichnet, wird damit zumindest vertraglich auch der Importeur in die Pflicht genommen, der sogar ausdrücklich zusichern muss, dem Exporteur nach bestem Wissen und Gewissen alle für die TIA erforderlichen Informationen geliefert zu haben (Clause 14(c)). Sollte sich ein TIA also als fehlerhaft oder lückenhaft herausstellen und dem Exporteur daraus einen Schaden entstehen (z.B. weil er seinen Vertrag nach der Intervention einer Datenschutzbehörde nicht wie geplant durchführen kann), riskiert der Importeur Ersatzansprüche des Exporteurs, falls er diesen nicht, nicht korrekt oder nicht vollständig über die Zugriffsrisiken unter seinem Heimatrecht aufgeklärt hat. Dasselbe gilt, wenn er ihn nicht über Anpassungen des Heimatrechts (einschliesslich der Gerichtspraxis) informiert (Clause 14(e)). Dies gilt für die gesamte Kette an Unterauftragsbearbeitern.

Ziff. 7 enthält eine Übersicht derjenigen, die für die Durchführung einer TIA in erster Linie verantwortlich sind.

Service-Provider in unsicheren Drittstaaten ist somit zu empfehlen, von sich aus ihre Kunden in Europa über Zugriffsrisiken und Zugriffsfälle zu informieren, damit diese ihr TIA durchführen und sie nötigenfalls anpassen können. Kunden in Europa ist wiederum zu empfehlen, sich bei ihren Service-Providern nach diesen Informationen zu erkundigen. Eine Regelung zur Kostentragung enthalten die SCC nicht. Wir gehen aber davon aus, dass sich für bestimmte Standard-Anwendungsfälle auch Standard-TIAs herausbilden werden, mit denen die Parteien ihren Pflichten nachkommen können und nicht mehr für jede Datenübermittlung jeweils aufwändig entsprechende Rechtsgutachten einzuholen sind. Der EDSA geht in seiner Empfehlung 01/2020[36] allerdings noch von letzterem Modell aus. Er verlangt selbst für Standardsituationen einen für den konkreten Einzelfall verfassten, "detaillierten" Bericht.[37] Dieser muss sich auf öffentlich verfügbare Quellen stützen und die Anwendung der einem verpönten Behördenzugriff entgegenstehende Bestimmungen des ausländischen Rechts für den betroffenen Branchensektor aufzeigen (zur Einordnung vgl. auch Ziff. 43). Immerhin akzeptiert der EDSA, dass nicht nur der nackte Buchstabe des Gesetz-

---

36 https://edpb.europa.eu/news/news/2021/edpb-adopts-final-version-recommendations-supplementary-measures-letter-eu_en.

37 EDSA, Recommendation 01/2020, Fussnote 54 (übersetzt): "Die von Ihnen zu erstellenden Berichte müssen umfassende Informationen über die rechtliche Bewertung der Rechtsvorschriften und Praktiken sowie deren Anwendung auf die spezifischen Datenübermittlung, das interne Verfahren zur Erstellung der Bewertung (einschliesslich Informationen über die an der Bewertung beteiligten Akteure – z.B. Anwaltskanzleien, Berater oder interne Abteilungen) und das Datum der Prüfung enthalten. Die Berichte sollten vom gesetzlichen Vertreter des Exporteurs abgezeichnet werden."

gebers relevant ist, sondern auch die konkrete Anwendung der Bestimmungen in der Praxis.

Wir haben ein einfaches, Excel-basiertes Formular zur Durchführung eines TIA entwickelt, das für die meisten Fälle in der Praxis für die Zwecke der EU-SCC verwendet werden kann. Es basiert auf einer statistischen Methode zur Bewertung ausländischer behördlicher Zugriffsrisiken, die wir 2019 für eine grosse Schweizer Bank entwickelt haben, um die Wahrscheinlichkeit eines ausländischen behördlichen Zugriff auf Bankkundendaten im Rahmen der Nutzung von Cloud-Diensten objektiver zu bewerten.[38] Die Methode wurde 2020 veröffentlicht und wird heute in der Schweiz für solche Zwecke regelmässig verwendet. Unser TIA nutzt jene Teile dieser Methode, die unter dem EU SCC relevant sind, und kombiniert sie mit einer automatisierten Bewertung des Risikos der gemäss DSGVO (und DSG) verbotenen ausländischen Behördenzugriffe. Das Spezielle an unserem TIA ist, dass es in den einzelnen Bewertungsschritten vom Benutzer keine Gewissheit verlangt; er kann mit sehr groben Einschätzungen arbeiten. Die Methode ist auch unabhängig davon, ob der Benutzer die Bedenken bezüglich Behördenzugriffen teilt oder nicht oder ob er bestimmte rechtliche Argumente gegen solche Zugriffe für überzeugend hält oder nicht. Ausserdem ist die Vorgehensweise so strukturiert, dass sie Zufallsstreuungen und Verzerrungen reduziert, um eine bessere Einschätzung zu erzielen. Wir sind der Meinung, dass diese Methode klare Vorteile gegenüber dem klassischen Ansatz hat, lediglich ein Rechtsgutachten einzuholen. Ein Rechtsgutachten kann zwar im Einzelfall weiterhin nötig sein, aber mit unserer Methode sind sehr viel klarere und Einzelfall-bezogenere Aussagen möglich, welche die Unsicherheiten, die jedes Rechtsgutachten mit sich bringt, einkalkulieren. Dies erreichen wir mittels Wahrscheinlichkeitsberechnungen und einem strukturierten Ansatz, der sowohl rechtliche als auch technische und faktische Elemente kombiniert.In der Praxis hat sich dieser Ansatz bewährt. Inzwischen hat auch die *International Association of Privacy Professionals* (**IAPP**) unser TIA übernommen und bietet es unter ihrem eigenen Namen an.[39]

Unser TIA steht als Download mit einer kostenlosen Lizenz zur Verfügung; es enthält verschiedene Fallbeispiele zur Veranschaulichung der Anwendung und eine Anleitung.[40] Wir bieten es kostenlos an, weil wir glauben, dass jeder es nutzen und zu seiner Verbesserung beitragen können sollte. Die erste Fassung des TIAs war für Übermittlungen in die USA (als in der Praxis häufigster Fall) erstellt worden; inzwischen gibt es auch Fassungen für Übermittlungen in andere unsichere Drittländer wie Russland und Indien.

---

38 https://www.rosenthal.ch/downloads/Rosenthal_Cloud_Lawful_Access_Risk_Assessment.xlsx und der wissenschaftliche Beitrag dazu unter https://www.rosenthal.ch/downloads/Rosenthal-CloudLawfulAccess.pdf.

39 https://iapp.org/resources/article/transfer-impact-assessment-templates/.

40 https://www.rosenthal.ch/downloads/Rosenthal_EU-SCC-TIA.xlsx.

Illustrativ zur Dokumentation einer TIA sind hier auch die vom BayLDA, der Bayerischen Datenschutzbehörde, für verschiedene Anwendungen entwickelten Fragebögen.[41] Hilfreich in Bezug auf die USA kann auch das Formular von NOYB sein, mit welchem US-Importeure um Auskunft über ihr eigenes Zugriffsrisiko gebeten werden können;[42] es dürfte den Anforderungen des EDSA allerdings nicht genügen, da es keine Nachweise enthält und auch sonst zuwenig in die Tiefe geht – was insofern paradox ist, als es faktisch NOYB war, welche "Schrems II" überhaupt erst auslöste. Es bleibt zu hoffen, dass sich auch diesbezüglich die Gemüter etwas beruhigen und die Anforderungen an ein TIA für offenkundig harmlose Standardsituationen (wie z.B. die Übermittlung von HR-Daten an eine Konzernmutter in den USA) auf ein vernünftiges Mass reduziert werden, zumal mit guten Gründen vertreten werden kann, dass die befürchteten US-Geheimdienstzugriffe in solchen Fällen schon aufgrund der Tatsache ausgeschlossen sind, dass in solchen Fällen Datenübermittlungen an US-Personen erfolgen – spannend ist hierzu der Aufsatz von Alan Charles Raul, der aufzeigt, warum ausgerechnet der Abschluss der SCC die übermittelten Daten auch rechtlich vor dem Zugriff nach Section 702 FISA und EO 12.333 schützt.[43]

In der Praxis haben wir leider auch ungenügende und unbrauchbare TIAs gesehen. Hierzu gehören juristische Ausführungen, die zwar das lokale Recht zum Behördenzugriff erörtern, dies jedoch entweder nur exemplarisch oder oberflächlich tun (und somit unbrauchbar sind), keine Aussagen über das konkrete Risiko eines ausländischen Behördenzugriffs tätigen wo sie es sollten (und damit ebenfalls wertlos sind), das lokale Recht nicht den Anforderungen der DSGVO und des DSG gegenüberstellen (und somit regelmässig zu streng sind) oder aber pauschal ein "hohes" Risiko verorten, obwohl eine Einzelfallbetrachtung zu einem völlig anderen Ergebnis kommt.

Zum Schluss hier noch ein Flussdiagramm, welches die Prüfschritte im Falle einer internationalen Datenübermittlung nach DSGVO zeigt:[44]

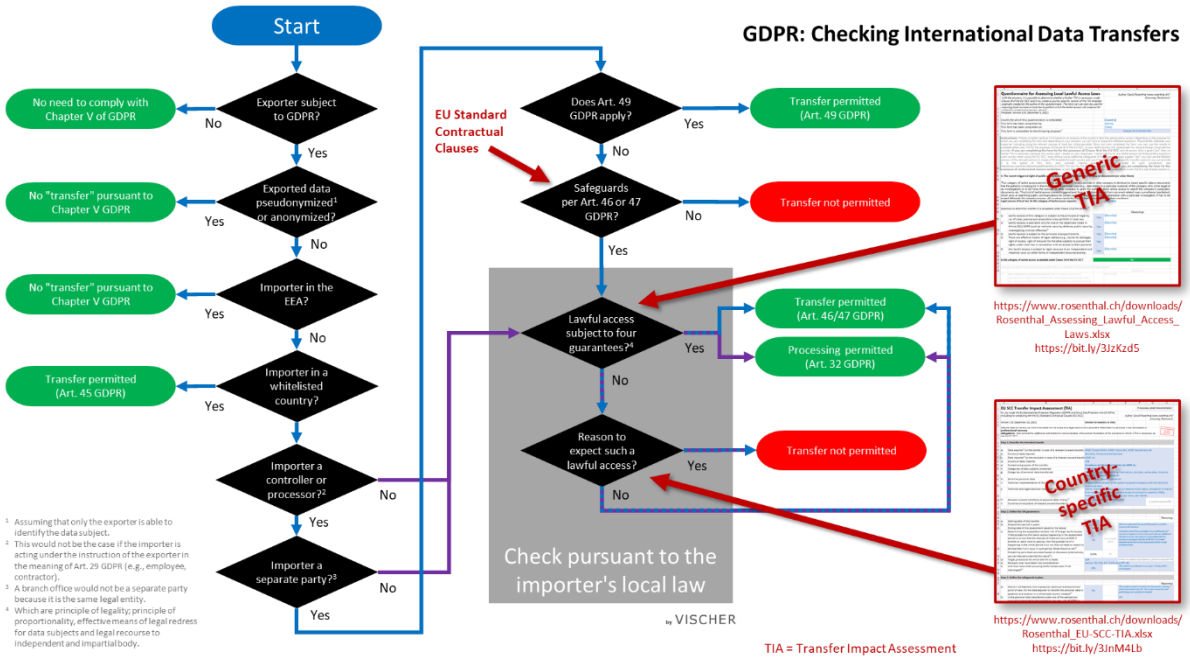
---

41 https://www.lda.bayern.de/de/thema_schrems2_pruefung.html.

42 https://noyb.eu/files/CJEU/EU-US_form_v3_nc.pdf.

43 Alan Charles Raul (Sidley), Schrems II Concerns Regarding U.S. National Security Surveillance Do Not Apply to Most Companies Transferring Personal Data to the U.S. Under Standard Contractual Clauses (https://bit.ly/3cWsyXB); siehe auch die Fortsetzung https://bit.ly/3l12oHZ.

44 https://www.rosenthal.ch/downloads/Rosenthal_International_Transfers_Charts.pdf.



45. Auf welche handwerklichen Mängel in den neuen SCC müssen wir achten?

Die neuen SCC sind in einigen Punkten nicht zu Ende gedacht oder formuliert. Hier eine Auswahl von handwerklichen Mängeln und eine Umgehungslösung:

- Clause 7: Es fehlt eine Regelung, wie die Zustimmung der bestehenden Parteien zum Vertragsbeitritt einer neuen Partei sichergestellt wird. Lösung: Clause 7 weglassen, separat regeln.
- Modul 3, Clause 8.1: Es wird fälschlicherweise angenommen, dass in einer Kette mehrerer Auftragsbearbeiter höchstens das erste Glied sich im EWR oder einem sicheren Drittland befindet. Lösung: Ignorieren.
- Modul 2, Clause 8.8: Es ist nicht klar, wem es obliegt, die Einhaltung der Voraussetzungen einer Weiterleitung von Daten zu gewährleisten. Lösung: Der Auftragsbearbeiter verpflichtet den Verantwortlichen dazu, nur dann die Weiterleitung anzuweisen, wenn die Anforderungen gemäss Clause 8.8 erfüllt sind.
- Onward Transfer-Bestimmungen: Es fehlt ein Vorbehalt betr. die Veröffentlichung von Personendaten, soweit eine solche an sich zulässig ist. Eine solche gilt grundsätzlich nicht als Transfer von Personendaten in ein Drittland. Lösung: Den Mangel ignorieren.
- Clause 9: Es ist zwar vorgesehen, dass ein Subprocessor abgelehnt werden kann, aber es fehlt eine Regelung, was in diesem Fall geschieht. Dass dieser Subprocessor nicht eingesetzt werden kann, ergibt sich immerhin aus einer Auslegung nach dem Sinn und Zweck der Regelung. Lösung: Separat regeln, z.B. mittels ei-

nes Kündigungsrechts, falls die Ankündigungsfrist hinreichend lang ist.

- Clause 9: Es fehlt eine Subprocessor-Regelung für den Fall, dass der Auftragsbearbeiter im EWR ist, aber der Verantwortliche nicht. Auch in diesen Fällen ist der Einsatz von Subprocessors denkbar, und ihr Einsatz müsste im Grunde nach Art. 28 DSGVO geregelt werden. Lösung: Separat regeln.
- Es fehlt ein Modul für den Fall, dass der Subprocessor der DSGVO untersteht, sein Auftragsbearbeiter aber in einem unsicheren Drittland ist. Lösung: Modul 4 verwenden (wenn der Verantwortliche nicht der DSGVO unterliegt) oder Modul 3 (in den anderen Fällen).
- Clause 9(b): Ein Unterauftragsbearbeiter in einem unsicheren Drittland muss einen eigenen Subprocessor nicht nach den SCC verpflichten, selbst wenn sich dieser in einem unsicheren Drittland befindet. Dies obwohl der Unterauftragsbearbeiter für ihn grundsätzlich nur insoweit einstehen muss, als dieser sich nicht an seinen Vertrag mit dem Unterauftragsbearbeiter hält. Die SCC sehen nicht vor, dass der Unterauftragsbearbeiter generell für das Verhalten seines Subprocessors verantwortlich ist. Dies führt zu einer Regelungslücke. Lösung: Verlangen, dass ein Subprocessor ebenfalls die SCC abschliesst.
- Clause 13: Es fehlt eine Regelung für den Fall, dass zwar ein Vertreter nach Art. 27 DSGVO bestellt werden muss, aber nicht bestellt wurde. Lösung: Die dritte Option verwenden.
- Clause 13: Die "vertragliche" Begründung der Zuständigkeit der gewählten EWR-Aufsichtsbehörde über den Importeur ist mutmasslich nicht durchsetzbar, weil sich die Zuständigkeit der EWR-Aufsichtsbehörde abschliessend aus der DSGVO ergibt, die eine solche für einen ausländischen Importeur, der naturgemäss nicht der DSGVO unterliegt, nicht vorsieht. Lösung: Den Mangel ignorieren.
- Clause 15.1: Die Pflicht jedes Importeurs, im Falle eines ausländischen Behördenzugriffs oder Versuch desselbigen die betroffene Person direkt zu informieren wird in vielen Fällen deren Datenschutzrechte nicht schützen, sondern verletzten, weil dem betreffenden Importeur sogar noch mehr Angaben über die betroffenen Personen geliefert werden müssen. Lösung: Die Notifikation der betroffenen Person ist an den Verantwortlichen zu delegieren.
- Clause 16: Es ist in Bst. (c) die Rede davon, dass der Exporteur bei einer Verletzung der SCC den "Vertrag" beenden kann, "soweit" er die Bearbeitung von Personendaten betrifft. Erstens ist nicht klar, worauf sich "Vertrag" ("contract") bezieht (wohl nicht nur auf die SCC, sondern auf den Hauptvertrag, dem die SCC dienen, siehe aber nachstehend), und zweitens führt eine solche

Bestimmung zu unkontrollierbaren Ergebnissen, da sie der kündigenden Partei nur (aber immerhin) die Teilkündigung des Hauptvertrags erlaubt. Lösung: Diese Kündigungsmöglichkeit sollte durch den Hauptvertrag abgefangen werden. Die Klausel besagt zudem in keiner Weise, wie die Kündigung zu erfolgen hat und in welchen Fristen. Notabene: Zeigt der Importeur an, dass er die SCC nicht mehr einhalten kann, ist eine Kündigung erst nach Ansetzen einer Frist möglich (vgl. Clause 16(c)(i)).

Die Verweise auf den Hauptvertrag bleiben freilich handwerklich problematisch, da dieser Hauptvertrag nicht unbedingt zwischen der Partei besteht, welche die SCC abgeschlossen hat. Im bisherigen Standardvertrag mit Microsoft schliessen europäische Kunden ihren Hauptvertrag beispielsweise mit der irischen Gesellschaft von Microsoft ab, die SCC jedoch mit Microsoft Corp. Da es Verträge zulasten Dritter nicht gibt, läuft das in den SCC statuierte Kündigungsrecht des Hauptvertrags ins Leere. Die naheliegende Lösung ist in solchen Fällen, die SCC nicht mit einem Unterauftragsbearbeiter abzuschliessen (Ziff. 31), doch kann ein solcher direkter Vertragsschluss der SCC für den Kunden natürlich auch Vorteile mit sich bringen, da er ihm zusätzliche Ansprüche einbringt.

Und noch einen Mangel weist diese Bestimmung auf: Kündigt der Exporteur gestützt auf Clause 16(c) wegen Nichteinhaltung der SCC, ist er nach derselben Klausel verpflichtet, dies der Aufsichtsbehörde zu melden. Auch wenn nicht klar ist, wie diese Bestimmung durchzusetzen ist, ist diese Pflicht besonders geeignet, den Exporteur von einer Kündigung abzuhalten – was sicherlich nicht Sinn der Sache ist.

- Clause 18: Der Gerichtsstand verweist auf das Land, nicht die Stadt bzw. den Gerichtsbezirk. Damit ist die Zuständigkeit nicht klar bzw. nach innerstaatlicher Zuständigkeitsordnung zu klären. Lösung: Ort angeben, nicht bloss das Land.

Ein ganz grundsätzlicher Mangel nicht der neuen SCC selbst sondern deren Erlass ist die Einschränkung der Europäischen Kommission auf Übermittlungen an Importeure, die selbst nicht der DSGVO unterstehen, was keinen Sinn macht (Ziff. 8). Wir glauben aber, dass das letzte Wort hier noch nicht gesprochen ist. Lösung: Ignorieren.

46. Wir arbeiten für ein Behörden- oder Gerichtsverfahren mit Anwälten in den USA zusammen. Welchen Teil der SCC setzen wir ein? Funktioniert dies noch?

Ja, die neuen SCC können hier eingesetzt werden und bringen eine Verbesserung mit sich. Es gilt allerdings zu unterscheiden zwischen zwei Situationen:

- Die Bekanntgabe von Personendaten an die eigenen Anwälte und Konzerngesellschaften im Ausland zur Durchführung eines ausländischen Behörden- oder Gerichtsverfahrens. Hier kommen die SCC weiterhin zum Einsatz.
- Die Bekanntgabe von Personendaten an die Gegenseite (namentlich im Falle einer *pre-trial-discovery*) oder ausländische Behörden oder Gerichte. Hier kommen nicht die SCC zum Einsatz, sondern die Ausnahmeregelung von Art. 49(1)(e) DSGVO, wobei dafür zu sorgen ist, dass die offengelegten Daten nur für die Zwecke des betreffenden Behörden- oder Gerichtsverfahrens verwendet werden (z.B. mit einer *Protective Order*).

Kommen die SCC zum Einsatz, so kann sowohl Modul 1 (Controller-Controller) als auch Modul 2 (Controller-Processor) angezeigt sein, je nach Fallkonstellation. In der Vergangenheit kamen meist die Controller-Processor-SCC zum Einsatz, weil die Controller-Controller-SCC eine Weitergabe der Personendaten in den ausländischen Behörden- oder Gerichtsverfahren aufgrund ihrer restriktiven Formulierung faktisch unterbunden haben: Die Daten konnten zwar den US-Anwälten für ein US-Verfahren mitgeteilt werden, aber sie durften sie nicht im Prozess einsetzen. Die Controller-Processor-SCC regelten die Weitergabe nicht in dieser Form; sie war Sache der Instruktion des Verantwortlichen.

Die neuen SCC lösen das Problem dadurch elegant, dass sowohl in Modul 1 (Clause 8.7(iv)) wie auch Modul 2 (Clause 8.8(iii)) eine Weitergabe durch den Importeur zulässig ist, wenn dies zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen in aufsichtsrechtlichen, regulatorischen oder gerichtlichen Verfahren im Ausland nötig ist. Damit ist das Problem gelöst. Mit den eigenen Anwälten im Ausland können also auch die neuen SCC also auch im Modul 1 vereinbart werden.

47. Brauchen wir noch einen ADV, wenn wir die neuen SCC einsetzen?

Nein, aus rein rechtlicher Sicht nicht, denn im Gegensatz zu den bisherigen SCC erfüllen die neuen SCC nach Ansicht der Europäischen Kommission alle Voraussetzungen von Art. 28(3) DSGVO. Sie gelten als genehmigte Standardklauseln für Auftragsbearbeitungen im Sinne von Art. 28(7) DSGVO (Clause 2(a)).

In der Praxis wird in vielen Fällen trotzdem das Bedürfnis für weitere Absprachen bestehen, so namentlich zur Art und Weise der Instruktionserteilung, zur Kostentragung und zur Füllung der Lücken der in den SCC enthaltenen Regelungen (z.B. zu den Folgen einer Ablehnung eines Unterauftragsbearbeiters). Dies kann z.B. in einem Service-Provider-Vertrag so umgesetzt werden, dass im Hauptvertrag eine datenschutzrechtliche Rumpfvereinbarung mit den nötigen Präzisierungen und Ergänzungen enthalten ist, welche dann entweder die nötigen Mo-

dule und Optionen der vollen SCC zum Vertragsbestandteil erklärt und in einem Anhang die individuellen Angaben enthält oder auf einen Anhang verweist, der eine auf den konkreten Anwendungsfall bereits reduzierte, ausgefüllte Variante der SCC enthält.

Anders beurteilt sich die Situation, wo ein ADV zwischen zwei Parteien abzuschliessen ist, die beide entweder im EWR oder einem sicheren Drittland sind. Hier sind die SCC an sich nicht erforderlich und es muss damit gerechnet werden, dass die Genehmigung der SCC als ADV im Sinne von Art. 28(7) DSGVO für diesen Fall nicht gilt, weil die Europäische Kommission den Einsatz der SCC in dieser Situation nicht vorgesehen hat. Allerdings heisst dies nicht, dass die SCC nicht auch in diesen Fällen eingesetzt werden *dürfen*. Nach unserer Ansicht ist dies zulässig (Ziff. 9). Es muss demnach möglich sein, die SCC als ADV auch zwischen einem Verantwortlichen und einem Auftragsbearbeiter (oder zwischen zwei Auftragsbearbeitern) einzusetzen, die *beide* im EWR oder einem sicheren Drittland sind. Die Formulierung der SCC entspricht zwar formal gesehen nicht ganz den Vorgaben von Art. 28(3),[45] aber die Abweichungen liegen innerhalb der in der Praxis üblichen Grundrauschens.

In der Praxis werden die meisten Parteien kein Interesse haben, die SCC freiwillig einzusetzen, da sie recht weit gehen. Es ist daher nicht zu erwarten, dass die SCC öfters als Vorlage für ADVs für Auftragsbearbeitungen im EWR und in sicheren Drittstaaten zum Einsatz kommen werden. Das gilt erst recht für Auftragsbearbeitungen nach Schweizer Recht, wo die Anforderungen noch geringer sind. Hinzu kommt, dass die Europäische Kommission für diesen Fall eigene Standardvertragsklauseln (d.h. die SCC-ADV) vorgelegt hat, die allerdings aus denselben Gründen nicht sehr attraktiv sind, zumal sie nicht verändert werden dürfen, falls sie kraft Art. 28(7) DSGVO zum Einsatz kommen sollen.

Im Falle von IGDTA kann der Einsatz der SCC als ADV jedoch sinnvoll sein. Denn ein IGDTA regelt regelmässig nicht nur den Transfer von Personendaten in unsichere Drittstaaten, sondern auch Auftragsbearbeitungen innerhalb des EWR und im Verkehr mit Drittstaaten. In einer solchen Konstellation macht es mitunter wenig Sinn, im IGDTA für diese Fälle eine andere Regelung vorzusehen als jene, die nach den SCC gilt. Im Gegenteil kann es sogar angezeigt sein, für den gesamten Konzern dieselben Regeln vorzusehen, wenn es zu einer internen Auftragsbearbeitung kommt – ob in einem Land mit oder ohne angemessenen Datenschutz.

---

[45] Die Unterstützungspflicht des Auftragsbearbeiters nimmt nicht Bezug auf die Pflichten von Art. 32 bis 36 DSGVO (Art. 28(3)(f) DSGVO) und lässt sich daher mit Bezug auf die Erstellung von Datenschutz-Folgenabschätzungen nur indirekt begründen. Auch das Äquivalent zu Art. 28(3)(a) und (g) DSGVO ist in den SCC etwas liberaler formuliert, indem die SCC einen Vorbehalt zugunsten des Heimatrechts des Auftragsbearbeiters vorsehen, während die DSGVO einen solchen Vorbehalt nur für das Recht des EWR und seiner Mitgliedstaaten zulässt.

Trotzdem rechnen wir damit, dass es immer wieder auch IGDTA geben wird, in welchen auch die neuen SCC-ADV zum Einsatz kommen, etwa bei IGDTA im rein europäischen Kontext oder wo die Autoren "auf Nummer sicher" gehen wollen, auch wenn dies auf Kosten der Lesbarkeit und Einheit der Vertragswerke geht.

Die SCC-ADV dürften allerdings für viele umständlicher und weniger attraktiv wirken als die individuellen ADV, die sich in der Praxis durchgesetzt haben. Sie weisen überdies ähnliche Schwächen wie die SCC auf (sind mit diesen aber nicht identisch):

- Sie regeln nicht die Folgen eines Widerspruchs gegen den Beizug eines neuen Unterauftragsbearbeiters (Clause 7.7). Diesen handwerklichen Mangel weisen auch die neuen SCC.
- Sie enthalten eine unnötig komplizierte Regelung betreffend die Meldung von Verletzungen der Datensicherheit, indem sie zwischen Verletzungen seitens des Verantwortlichen unterscheiden (in welchen Fällen dieser vom Auftragsbearbeiter zu unterstützen ist) und solchen seitens des Auftragsbearbeiters (Clause 9). Wann genau welche der Bestimmungen zur Anwendung kommt bleibt unklar.
- Wie schon die SCC gehen sie über die DSGVO hinaus (z.B. Information über unkorrekte Daten, Offenlegung von Unterlagen gegenüber den Datenschutzbehörden, Umfang der TOMS).
- Sie enthalten keine Regelungen zur Kostentragung.

Einzelne Parteien werden die SCC-ADV in Vertragsverhandlungen allerdings immer wieder einbringen oder bei der Aushandlung individueller ADVs auf die Musterregelung der SCC-ADV verweisen, z.B. wenn es zu Differenz betreffend die Frist zur Meldung einer Verletzung der Datensicherheit kommt (welche weder die SCC noch die SCC-ADV kennen).

48. Was sollten wir jetzt konkret tun als Unternehmen?

Für ein europäisches Unternehmen, welches selbst nicht primär als Auftragsbearbeiter tätig ist, ist eine typische Vorgehensweise die folgende:

- Es wird das bestehende Intra-Group Data Transfer Agreement (**IGDTA**), also die vertragliche Regelung des gruppeninternen Datenaustausches (dazu Ziff. 49), bis zum 27. September 2021 angepasst – jedenfalls soweit im Konzern Daten auch in unsichere Drittländer fliessen. Achtung: Soweit das IGDTA auch Datenflüsse aus Drittländern mit eigenen Datenschutzgesetzen regelt, sind auch diese zu beachten. Für die Schweiz vgl. Ziff. 10, für das Vereinigte Königreich vgl. Ziff. 22.
- Die eigenen Datenschutzerklärungen sind entsprechend anzupassen. Sie müssen bekanntlich die nach Art. 46 DSGVO verwendeten Garantie ausdrücklich erwähnen und darauf hinweisen, wo

diese verfügbar oder eine Kopie erhältlich ist (Art. 13(1)(f) DSGVO, Art. 14(1)(f) DSGVO; Art. 19 Abs. 4 revDSG).

- Es wird ein Überblick darüber verschafft, in welchen anderen Fällen Personendaten in unsichere Drittländer kommuniziert werden. Optimalerweise sind diese Daten dem Verzeichnis der Bearbeitungstätigkeiten zu entnehmen.
- Die Einträge in dieser Liste wird in drei Gruppen unterteilt:
  - Die erste Gruppe umfasst jene Fälle, in denen Kundenverträge betroffen sind. Diese Fälle sind prioritär zu behandeln: Befindet sich der Kunde in einem unsicheren Drittland, wird es für das Unternehmen möglicherweise nicht sehr einfach sein, diesen zur Vertragsanpassung zu bewegen. Allenfalls muss eine "Massenlösung" ausgearbeitet werden, wenn viele Verträge betroffen sind. Dies braucht Zeit. Befindet sich das Unternehmen selbst in einem unsicheren Drittland, muss es damit rechnen, dass es sehr bald von Kunden kontaktiert wird, die eine Lösung für die Einführung der neuen SCC erwarten sowie Unterstützung bei der Durchführung der *Transfer Impact Assessments* (**TIA**) (Ziff. 44). Hier muss sich das Unternehmen frühzeitig vorbereiten.
  - Die zweite Gruppe umfasst jene Fälle, in denen Dienstleistungen von einem der grossen bekannten Provider bezogen wird, der standardisierte Verträge einsetzt (Beispiel: Cloud-Provider wie Microsoft, Amazon, Salesforce.com). Hier ist es in der Regel am einfachsten auf einen Vorgehensvorschlag des Providers zu warten. Tut sich hier nichts, sollte nachgefragt werden. Die meisten Provider werden eine Standardvorgehensweise entwickeln; anders lässt sich die Flut der Anpassungen nicht bewältigen.
  - Die dritte Gruppe von Fällen wird nach Risiko sortiert. Gemeint ist das mit den Daten und der Datenbearbeitung verbundene Risiko (aufgrund der Art, des Umfangs oder des Zwecks der Bearbeitung). Datenexporte in die USA haben tendenziell eine höhere Priorität als Datenexporte in andere unsichere Drittländer wie z.B. Indien.[46] Auftragsbearbeiter erhalten eine höhere Priorität als andere Verantwortliche.[47]
- Die Einträge der dritten Gruppe werden nach ihrer Priorität abgearbeitet und es wird geprüft, ob diese die neuen SCC benötigen (weil sie sich schon bisherig auf die SCC stützten oder die bisherige Rechtsgrundlage wie etwa "Privacy Shield" weggefallen ist).

---

46 Weil EU-Datenschutzbehörden den US-Rechtsraum aus welchen Gründen auch immer als besonders gefährlich betrachten.

47 Sie sind in den USA tendenziell eher von den Gesetzen erfasst, welche einen Behördenzugriff ohne Rechtsweggarantie vorsehen.

- Werden die neuen SCC benötigt, so wird der Importeur (z.B. der Service-Provider) angeschrieben und um zwei Dinge gebeten:
  - Eine Auskunft betr. das Risiko eines behördlichen Zugriffs ohne Rechtsweggarantie (und gewisse weitere Garantien) (vgl. Ziff. 43). Er sollte zugleich um Vorschläge gebeten werden, dieses Risiko durch weitere Massnahmen zu reduzieren. Es ist davon auszugehen, dass insbesondere Service-Provider mit vielen Kunden sehr viele Anfragen erhalten und sich weigern werden, Fragebögen auszufüllen. Sie werden stattdessen auf Standardantworten mit den erforderlichen Angaben verweisen.
  - Unterzeichnung eines Vertragsdokuments, welches die bisherigen SCC mit den neuen SCC ersetzt, wobei dieses wahlweise bereits ausgefüllt sein kann mit den für den Appendix erforderlichen Angaben oder dies dem Importeur überlassen wird.
- Basierend auf der Auskunft betr. das Risiko eines behördlichen Zugriffs ohne Rechtsweggarantie (und gewisse weitere Garantien) wird mittels eines TIA geprüft (Ziff. 44), ob das Risiko vertretbar ist. In diesem Falle wird unterzeichnet. Sind weitere Massnahmen möglich, werden diese evaluiert und ggf. vereinbart. Dieser Prozess muss abgeschlossen sein bis zum Zeitpunkt, an welchem die Datenbearbeitung verändert wird (z.B. Bestellung weiterer Services, Abdeckung weiterer Standorte), spätestens aber bis zum 27. Dezember 2022.
- Im Hinblick auf die Zeit nach dem 27. September 2021 werden die eigenen Vertragsvorlagen angepasst, um Verweise bzw. den Einsatz der bisherigen SCC zu ersetzen. Das gilt auch für eigene Standardverträge, welche auf die SCC verweisen.
- Soweit die Übermittlung von Daten aus der Schweiz betroffen ist, wird auch der Einsatz der neuen SCC dem EDÖB gemeldet werden müssen, wobei die vereinfachte Meldung erfolgen kann (Art. 6 Abs. 3 VDSG), sofern die SCC wie vom EDÖB verlangt angepasst worden sind für die Zwecke des DSG. Die Meldung kann mit einem einfachen Brief erfolgen.

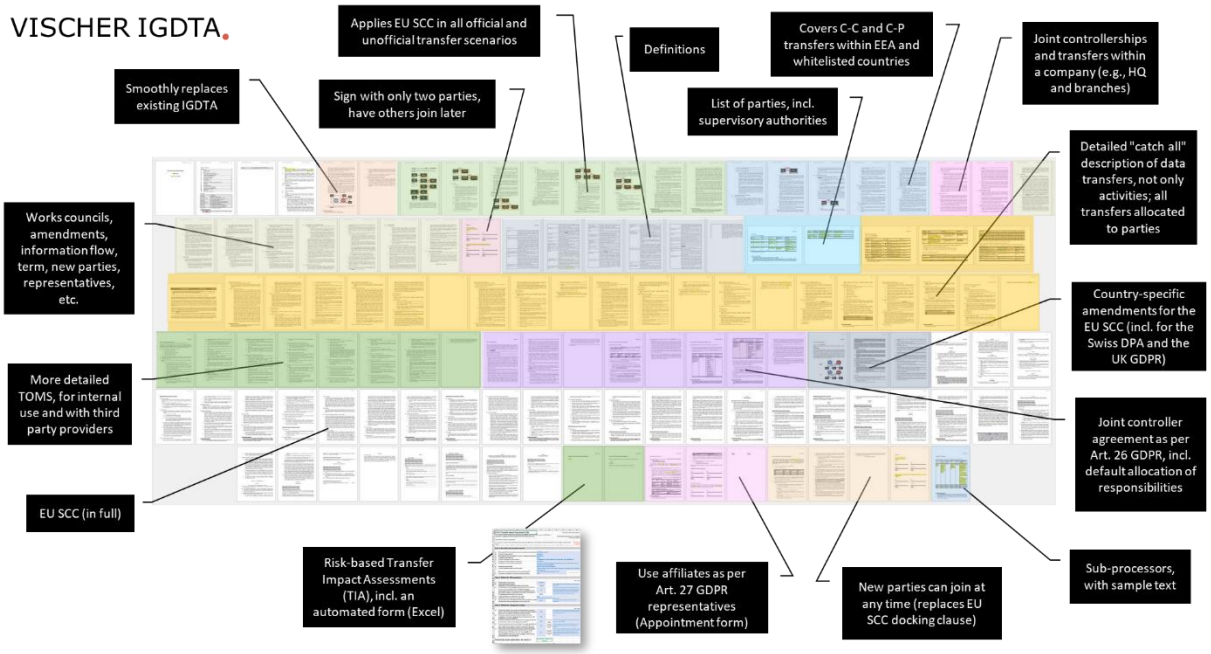
49. Was müssen wir bei der Erstellung oder Prüfung eines IGDTA beachten?

Ein IGDTA ist ein vom Konzept her allseitiger Vertrag, den ein Teil oder alle Unternehmen einer Unternehmensgruppe miteinander abschliessen, um die Datenflüsse in dieser Gruppe datenschutzkonform zu regeln.

In der Praxis sehen wir IGDTA sehr unterschiedlichen Umfangs und auch unterschiedlicher Qualität. Die ersten IGDTAs regelten nur inter-

nationale Datenübermittlungen in unsichere Drittstaaten, indem die SCC allseitig vereinbart wurden. Heutzutage regeln IGDTA in der Regel auch die Auftragsbearbeitung im Konzern.

Die IGDTAs, die wir für unsere Klienten erstellt haben, decken zudem die Anforderungen von Art. 26 DSGVO (gemeinsame Verantwortlichkeiten) ab, sehen eine gruppeninterne Vertretung (nach Art. 27 DSGVO und UK GDPR) vor und regeln die Nachführung und Verwaltung des IGDTA. Sie decken auch den Umstand ab, dass im Vereinigten Königreich die neuen SCC noch nicht akzeptiert sind und regeln die Ablösung bestehender IGDTA. Die Verträge sind oft auf den ersten Blick komplex, die aber den Vorteil haben, viele der geltenden Anforderungen in einem Vertragswerk und einheitlichen Regelungen abzudecken.



Unser IGDTA ist vom EDÖB geprüft und zur Verwendung freigegeben worden.

Einige Punkte, auf die Sie IGDTA hin prüfen sollten:

- Sind neben Datentransfers in unsichere Drittstaaten auch gruppeninterne Auftragsbearbeitungen geregelt?
- Ist der Spezialfall der Schweiz und das Vereinigte Königreich abgedeckt?
- Sind nebst den Datentransfers vom EWR und sicheren Drittstaaten in unsichere Drittstaaten auch Weiterübermittlungen (sog. onward transfers) von unsicheren Drittstaaten angemessen geregelt?

- Sind die Lücken, welche die SCC aufweisen, angemessen gefüllt?
- Sind Datentransfers aus nicht-europäischen Ländern mit Datenschutzgesetzen durch das IGDTA ebenfalls abgedeckt?
- Sind länderspezifische Anpassungen möglich und wo nötig gemacht? Möglich sein sollten auch Anpassungen für Länder, welche zwar Garantien benötigen, aber die SCC der EU nicht anerkennen
- Sind Regelungen für jene Datentransfers getroffen, welche beim Erlass der SCC vergessen oder nicht beachtet wurden?
- Finden die SCC auch dort Anwendung, wo ein Exporteur nicht im EWR oder einem sicheren Drittstaat ist, aber das Datenschutzrecht (wie etwa die DSGVO) eine Exportregelung vorschreibt?
- Erlaubt das IGDTA eine Übermittlung in einen unsicheren Drittstaat auch auf der Basis der Ausnahmetatbestände (z.B. Art. 49 DSGVO) vor?
- Sind Controller-Controller-Übermittlungen innerhalb des EWR und sicherer Drittstaaten abgedeckt?
- Funktioniert das IGDTA auch, wenn Übermittlungen durch ein anderes Datenschutzrecht als die DSGVO geregelt sind?
- Sind die nötigen gruppeninternen Delegationen (z.B. der Information betroffener Personen) geregelt?
- Ist der Beizug von externen Service-Providern geregelt? Gelten für diese eigene Anforderungen an die Datensicherheit? Sind sie aufgeführt?
- Sind Datentransfers innerhalb des EWR und sicherer Drittstaaten geregelt?
- Sind grenzüberschreitende Datentransfers innerhalb einer Rechtseinheit (z.B. vom Mutterhaus in eine Zweigniederlassung und umgekehrt) in unsichere Drittstaaten abgedeckt?
- Ist eine fliessende Ablösung von bestehenden IGDTAs vorgesehen und angemessen geregelt? Ist die Fortgeltung der bisherigen SCC in den Ländern, in denen die neuen SCC noch nicht anerkannt sind, sichergestellt?
- Sind Regelung zu Betriebsvereinbarungen und Betriebsräten vorhanden (wichtig für Deutschland)?
- Bestehen hinreichende Regelungen für gemeinsame Verantwortlichkeiten (Art. 26 DSGVO)?
- Bestehen Regelungen für die konzerninterne Vertretung für die Zwecke von Art. 27 DSGVO (und vergleichbaren Bestimmungen in anderen Datenschutzgesetzen)?

- Kann das IGDTA einfach ohne neue Unterschriften angepasst werden?
- Ist die Information der Parteien über Entwicklungen im Rahmen des IGDTA praktikabel geregelt?
- Ist das anwendbare Recht und der Gerichtsstand angemessen und DSGVO-konform geregelt – und zwar sowohl im IGDTA wie auch in den SCC?
- Ist klar, wer für die Verwaltung des IGDTA verantwortlich ist?
- Ist ein Bei- und Austritt von Parteien jederzeit einfach möglich?
- Sind die Parteien mit den gemäss den neuen SCC erforderlichen zusätzlichen Angaben versehen?
- Ist festgehalten, für welche Partei welche Aufsichtsbehörde zuständig ist – auch wo die DSGVO nicht gilt?
- Sind die Datentransfers ausreichend detailliert dargestellt? Sind alle Datentransfers abgedeckt?
- Ist klar, welche Gesellschaften an welchen Datentransfers in welcher Rolle beteiligt sind?
- Sind die technischen und organisatorischen Massnahmen der Datensicherheit mehr als nur generisch beschrieben, wie das in der Vergangenheit oft der Fall war? Decken sie mehr als nur die Datensicherheit ab, sondern z.B. auch die Bearbeitungsgrundsätze und Betroffenenrechte?
- Regelt das IGDTA die Erstellung von Transfer Impact Assessments (und bietet es hierzu die nötigen Vorlagen)?

Existiert bereits ein IGDTA, so empfehlen wir eine schrittweise Ablösung. Leider ist es aber nicht möglich, im bestehenden IGDTA in den Anhängen mit den bisherigen SCC die alten SCC mit den neuen SCC auszutauschen. Damit die neuen SCC richtig funktionieren, sind tiefgreifendere Anpassungen nötig. Auch die Anhänge müssen erfahrungsgemäss oftmals deutlich ausgebaut werden.