Das SchremsII-Urteil des EuGH: Folgen für die Praxis des Einsatzes von Standarddatenschutzklauseln

Dr. Carlo Piltz, 20.7.2020

Inhalt

Was sind die Konsequenzen des Schrems II-Urteils des EuGH (C-311/18)? Was ist bei Datentransfers in die USA und auch andere Drittländer zu beachten? Diese Fragen stellen sich aktuell natürlich viele Unternehmen und allgemein datenverarbeitende Stellen. Ich habe nicht den Anspruch, hierauf abschließende Antworten zu geben.

Gerne möchte ich aber in diesem Beitrag versuchen, das Urteil zum einen systematisch einzuordnen und etwas „aufzudröseln“. Zum anderen auch mögliche (!) praktische Konsequenzen für datenverarbeitende Stellen abzuleiten. Im Blick sollen hierbei die Standardvertragsklauseln (jetzt: Standarddatenschutzklauseln, „SDK“) stehen. Das andere Interpretation des Urteils sicherlich ebenso vertretbar sind, versteht sich meines Erachtens von selbst.

Ich verzichte hier bewusst auf eine Darstellung, was Hintergrund des Verfahrens war und auch auf Erläuterungen, was das EU US Privacy Shield oder die SDK sind.

A. Systematik des Urteils

Meines Erachtens bietet sich zunächst an, den Prüfaufbau des EuGH in den Blick zu nehmen. Dies ist, gerade aufgrund der Länge des Urteils relevant. Denn man kann sich gut in der Begründung verlieren, nur um dann die Frage zu stellen, was denn eigentlich gerade geprüft wird. Hierzu habe ich eine kleine Gliederung erstellt:

1. Das erforderliche Schutzniveau nach Art. 46 Abs. 1 und Art. 46 Abs. 2 lit. c DSGVO, wenn Daten auf der Grundlage von Standarddatenschutzklauseln in ein Drittland übermittelt werden? (ab Rz. 90)

2. Aussetzungspflicht der Datenschutzbehörde, wenn die Klauseln in diesem Drittland nicht eingehalten werden oder nicht eingehalten werden können? (ab Rz. 106)

3. Gültigkeit des Standarddatenschutzklausel-Beschlusses im Hinblick auf die Art. 7, 8 und 47 der Charta („angemessenes Schutzniveau“)? (ab Rz. 122)

4. Ob und inwieweit eine Datenschutzbehörde („DSB“) eines Mitgliedstaats an die Feststellungen im Privacy Shield-Beschluss gebunden ist // ob die auf die Standarddatenschutzklauseln gestützte Übermittlung personenbezogener Daten in die USA die durch die Art. 7, 8 und 47 der Charta verbürgten Rechte verletzt? (ab Rz. 150)

a. Zum Inhalt des Privacy Shield-Beschlusses (ab Rz. 163)

b. Zur Feststellung eines angemessenen Schutzniveaus (ab Rz. 168)

B. Einheitliches Schutzniveau für Kapitel V der DSGVO

Aus der Gliederung wird bereits deutlich, dass der EuGH in dem Urteil zunächst prüft, was denn überhaupt für ein Schutzniveau zu erreichen ist, wenn Daten auf der Grundlage von Art. 46 DSGVO übermittelt werden. In der Prüfung im ersten Abschnitt befasst sich der EuGH ganz allgemein mit der Frage, welches Schutzniveau „geeignete Garantien“ erreichen müssen.

Also ganz abstrakt: gibt es einen Unterschied des zu erreichenden Schutzniveaus bei den Transfermechanismen nach Kapitel V DSGVO?

Nein. Nach dem EuGH gilt für die ganze DSGVO und damit auch Kapitel V ein einheitliches Schutzniveau. Das bedeutet, dass die in Art. 46 Abs. 1 DSGVO genannten „geeigneten Garantien“ so beschaffen sein müssen, dass sie für Personen, deren personenbezogene Daten auf der Grundlage von SDK in ein Drittland übermittelt werden – wie im Rahmen einer auf einen Angemessenheitsbeschluss gestützten Übermittlung – ein Schutzniveau gewährleisten, das dem in der Union garantierten Schutzniveau der **Sache nach gleichwertig** ist (Rz. 96).

In den Rz. 90-105 geht es noch gar nicht spezifisch um die aktuell geltenden SDK, sondern allgemein um dieses Transferinstrument an sich. Das Gericht betrachtet den allgemeinen Prüfungsmaßstab, der an Datentransfers nach Art. 46 DSGVO zu stellen ist. Die SDK stellen dabei ein Beispiel dar.

C. Anforderungen an Datentransfers ohne Angemessenheitsbeschluss

Nach dem EuGH (und der Vorgaben in Art. 46 Abs. 1 DSGVO) dürfen, bei fehlendem Angemessenheitsbeschluss, personenbezogene Daten an ein Drittland übermitteln werden, wenn der Exporteur folgende drei Ziele erreicht:

- er „**geeignete Garantien**“ vorgesehen hat (diese können u.a. in den SDK bestehen)
- den betroffenen Personen „**durchsetzbare Rechte**“ und
- „**wirksame Rechtsbehelfe**“ zur Verfügung stehen (Rz. 91)

Dies sind, für Art. 46 DSGVO, die maßgeblichen drei Kriterien des angemessenen Schutzniveaus.

Wichtig: im Rahmen des Art. 46 DSGVO (und damit auch der SDK) muss aber nicht das Zielland und die dortige Rechtsordnung ein der Sache nach gleichwertiges Schutzniveau aufweisen. Sondern die „geeigneten Garantien“ selbst, also zB die SDK, sollen für Personen ein Schutzniveau gewährleisten, das dem in der Union garantierten Schutzniveau der Sache nach gleichwertig (Rz. 96).

Das bedeutet dann auch, dass der Prüfungsmaßstab für das Schutzniveau inhaltlich ein anderer ist, als im Fall des Angemessenheitsbeschlusses nach Art. 45 DSGVO (vgl. auch Rz. 129 und 130). Das zu erreichende Ziel (Gleichwertigkeit) ist aber dasselbe.

Meine verbildlichte Darstellung: im Fall des Angemessenheitsbeschlusses ist das ganze Drittland eine schöne grüne Datenschutzwiese. Im Fall des Art. 46 DGSVO (also etwa des Einsatzes von SDK) ist das

Drittland aber eine böse Vulkanlandschaft, in der Daten nicht sicher sind und mit den SDK wollen wir nun einen Tunnel zu einem bestimmten Empfänger schaffen. Es existiert also, quasi als Voraussetzung, ein Mangel an Datenschutz, der durch den Tunnel für eine Übermittlung ausgeglichen werden muss (Rz. 95). Dieser Tunnel muss die Daten entsprechend den Anforderungen des Art. 46 DSGVO gegen die Vulkanlandschaft schützen.

D. Schutzniveau beim Einsatz von SDK

Das vorlegende Gericht wollte vom EuGH auch wissen, welche Gesichtspunkte denn konkret zu berücksichtigen sind, um festzustellen, ob ein angemessenes Schutzniveau besteht, wenn personenbezogene Daten auf der Grundlage der SDK übermittelt werden (Rz. 102).

Die Antwort des EuGH hierauf ist wenig spezifisch und praxistauglich. Er orientiert sich natürlich an dem oben aufgestellten Schutzniveau für Art. 46 DSGVO. Hinsichtlich seiner bereits zuvor herausgestellten drei Kriterien, erläutert er aber in Rz. 104 zusätzlich, dass in Bezug auf eine Übermittlung auf Grundlage der SDK folgende Punkte zu berücksichtigen sind:

- insbesondere die **vertraglichen Regelungen,** die zwischen dem in der Union ansässigen Verantwortlichen und dem im betreffenden Drittland ansässigen Empfänger der Übermittlung vereinbart wurden, sowie,
- was einen etwaigen **Zugriff der Behörden** dieses Drittlands auf die übermittelten personenbezogenen Daten betrifft, die **maßgeblichen Elemente der Rechtsordnung** dieses Landes.

Und hier vollzieht der EuGH einen wichtigen vergleichenden Schwenk zu den Voraussetzungen für einen Angemessenheitsbeschluss: hinsichtlich des Zugriffs von Behörden des Drittlands auf die übermittelten personenbezogenen Daten entsprechen die Elemente, die im Kontext von Art. 46 DSGVO zu berücksichtigen sind, jenen, die in Art. 45 Abs. 2 DSGVO in nicht abschließender Weise aufgezählt werden.

E. Bewertung der aktuell geltenden SDK (2010/87/EU)

Erfüllen die aktuell geltenden SDK diese Anforderungen? Und was ist konkret bei ihrem Einsatz zu beachten? Mit den aktuell geltenden SDK (bzw. genauer, mit dem zugrundliegenden Beschluss der Kommission) befasst sich der EuGH ab Rz. 122.

Die erste wichtig Feststellung des EuGH ist, dass es Situationen geben kann, in denen die SDK unverändert genutzt werden können, da sie selbst das angemessene Schutzniveau schaffen. Der EuGH unterscheidet zwei Szenarien (Rz. 126):

- Szenario 1: Der Empfänger einer Übermittlung kann, in Anbetracht der Rechtslage und der Praxis im betreffenden Drittland, den erforderlichen Datenschutz **allein** auf der **Grundlage der SDK garantieren** kann.
- Szenario 2: Situationen, in denen die in den SDK enthaltenen Regelungen möglicherweise **kein ausreichendes Mittel** darstellen, um in der Praxis den effektiven Schutz der in das betreffende Drittland übermittelten personenbezogenen Daten zu gewährleisten.

Zu Szenario 2 nennt das Gericht ein Beispiel: wenn das Recht dieses Drittlands dessen Behörden bezüglicher dieser Daten **Eingriffe in die Rechte der betroffenen Personen erlaubt**.

Achtung: nur weil Eingriffe in die Rechte der Betroffenen möglich und durch die nicht angepasste Form der SDK nicht ausgeschlossen werden können, sind die SDK aber nicht untauglich. Das ist meines Erachtens wichtig zu erkennen.

Denn Art. 46 Abs. 2 DSGVO verlangt laut dem EuGH nicht, dass sämtliche Garantien zwangsläufig in einem Beschluss der Kommission wie dem SDK-Beschluss vorgesehen sind (Rz. 128). Dies ist auch gar nicht möglich, denn die SDK sind nur allgemein erstellt und gelten für alle Drittländer (Rz. 130, 133).

Ab Rz. 137 befasst sich der EuGH dann mit dem Beschluss der Kommission zu den aktuell geltenden SDK. Die Ausführungen sind also eher abstrakt wertender Natur. Jedoch geht der EuGH in seiner Prüfung der Gültigkeit des Beschlusses auch auf Pflichten ein, die für Verantwortliche gelten und er erläutert, wie diese auszuüben sind.

F. Pflichten des Verantwortlichen (Exporteur) und des Auftragsverarbeiters (Importeur)

Und nun nähern wir uns auch praktischen Vorgaben. Nach dem EuGH kann es, aufgrund dieses allgemeinen Charakters der SDK, in dem oben erwähnten Szenario 2, je nach der in einem bestimmten Drittland gegebenen Lage erforderlich sein, dass der Verantwortliche **zusätzliche Maßnahmen ergreift**, um die Einhaltung **des Schutzniveaus der SDK** zu gewährleisten (Rz. 133).

Noch einmal zur Erinnerung: Schutzniveau der SDK ist nach EuGH ein der Sache nach gleichwertiges Schutzniveau wie in der EU.

Und der EuGH geht noch weiter: es obliege vor allem Verantwortlichen, **in jedem Einzelfall** – gegebenenfalls in Zusammenarbeit mit dem Empfänger der Übermittlung – **zu prüfen**, ob das Recht des Bestimmungsdrittlands **nach Maßgabe des Unionsrechts einen angemessenen Schutz** der auf der Grundlage von SDK übermittelten personenbezogenen Daten gewährleistet, und **erforderlichenfalls mehr Garantien** als die durch diese Klauseln gebotenen zu gewähren (Rz. 134).

Achtung: das bedeutet, dass der exportierende Verantwortliche zumindest vor der Übermittlung validieren muss, ob die unveränderte Form der SDK zum Einsatz kommen kann, um das Schutzniveau (das sie per se schaffen) zu halten. Es geht bei dieser Prüfung nicht um das komplette Recht des Drittlandes. Der EuGH verweist klar auf die konkret übermittelten Daten: „*einen angemessenen Schutz **der auf der Grundlage von Standarddatenschutzklauseln übermittelten personenbezogenen Daten** gewährleistet*“ (Rz. 134). Zudem wäre eine Prüfung der gesamten Rechtsordnung nicht mit der vorherigen Begründung des EuGH zu dem Unterschied zwischen Angemessenheitsbeschluss und SDK vereinbar.

Kann der Exporteur oder der Empfänger der Daten keine zusätzlichen Maßnahmen ergreifen, um den Standard der SCC zu halten, ist er verpflichtet, die Übermittlung personenbezogener Daten in das betreffende Drittland auszusetzen oder zu beenden (Rz. 135). Der EuGH nennt auch ein Beispiel: wenn das Recht des Drittlands dem Empfänger Verpflichtungen auferlegt, die den SDK widersprechen und daher geeignet sind, die vertragliche Garantie zu untergraben.

1. Umfang der Prüfpflicht des Verantwortlichen

Und es stellt sich dann natürlich die Frage, was konkret der Verantwortliche vor der Übermittlung zu prüfen hat? Reicht der Nachweis durch den Importeur, dass er sich an die SDK halten kann? Muss der Verantwortliche eigene Untersuchungen anstellen?

Die Antwort hierauf ergibt sich nach dem EuGH (Rz. 141) aus den Klauseln der SDK, konkret Klausel 4 Buchst. a sowie Klausel 5 Buchst. a und b. Diese verpflichten den in der Union ansässigen Verantwortlichen und den Empfänger, sich **vor der Übermittlung personenbezogener Daten in ein Drittland zu vergewissern**, dass das Recht des Bestimmungsdrittlands es dem Empfänger erlaubt, die **SDK einzuhalten**.

Das bedeutet, dass die Prüfungsfrage hier auf erster Stufe lautet: kann der Empfänger die SDK auf Basis des für ihn geltenden Rechts einhalten?

Daraus ergeben sich direkt einige wertvolle Erkenntnisse:

- Es geht immer um die in den SDK festgelegte Übermittlung; nicht generell um Übermittlungen in das Drittland.
- Das bedeutet, die Einhaltung der SDK ist grundsätzlich vertragsspezifisch zu prüfen.
- Die Einhaltung der SDK im Hinblick auf das Recht im Drittland, muss daher wohl auch konkret anhand der zu übermittelnden Daten und des spezifischen Empfängers geprüft werden (und nicht allgemein).
- Sowohl der Verantwortliche als auch der Empfänger sind verpflichtet, sich entsprechend zu vergewissern (natürlich insbesondere in Form der Zusammenarbeit).

2. Inhalt der Prüfpflicht

Und der EuGH gibt zudem noch einen Hinweis darauf, was die Vertragsparteien bei dieser Prüfung als Bewertungskriterien zu berücksichtigen haben, wovon sie sich also „vergewissern“ müssen.

In der Fußnote zu Klausel 5 der SDK wird klargestellt, dass zwingende Erfordernisse des Rechts im Drittland, die nicht über das hinausgehen, was in einer demokratischen Gesellschaft zur Gewährleistung u. a. der Sicherheit des Staates, der Landesverteidigung und der öffentlichen Sicherheit erforderlich ist, nicht den Standarddatenschutzklauseln widersprechen.

Das heißt: ein angemessenes Schutzniveau kann auf Basis der SDK auch dann bestehen, wenn Behörden des Drittlandes Zugriff auf die übermittelnden Daten nehmen. Das ist eine wichtige Klarstellung des EuGH, die auch in der Praxis Relevanz hat.

Nur muss dieser Zugriff legislativ so ausgestaltet sein, dass er den Anforderungen des vormaligen Art. 13 Abs. 1 RL 95/46/EG genügt. Dort wurden Ziele aufgeführt, die einschränkende Gesetzesmaßnahmen verfolgen müssen, damit sie zulässig sind.

Art. 13 RL 95/46/EG existiert jedoch nicht mehr. Da nach Art. 94 Abs. 2 DSGVO Verweise auf die RL 95/46/EG als Verweise auf die DSGVO zu verstehen sind, muss man hier meines Erachtens an die Stelle des Art. 13 Abs. 1 RL 95/46/EG nun Art. 23 Abs. 1 DSGVO und die dort benannten Ziele setzen (die jenen des Art. 13 Abs. 1 RL 95/46/EG sehr ähnlich sind. Hierzu gehören:

- die nationale Sicherheit;
- die Landesverteidigung;
- die öffentliche Sicherheit;
- die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit;
- den Schutz der Unabhängigkeit der Justiz und den Schutz von Gerichtsverfahren;
- den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen;
- die Durchsetzung zivilrechtlicher Ansprüche.

Aber: es reicht nicht, dass das Recht des Drittlandes bei dem Zugriff auf die Daten ein solches Ziel verfolgt. Der Zugriff muss auch zur Verfolgung dieses Ziels erforderlich sein. Verlangt wird also eine Verhältnismäßigkeitsprüfung. Und hier wird es meines Erachtens für europäische Unternehmen alleine sehr schwer, diese Prüfung valide vornehmen zu können. Insbesondere sollten hierbei daher die Empfänger im Drittland unterstützen.

Der EuGH stellt klar, dass es als Verstoß gegen die SDK anzusehen ist, wenn einer aus dem Recht des Bestimmungsdrittlands folgenden Verpflichtung nachgekommen wird, die über das hinausgeht, was für Zwecke wie die oben genannten erforderlich ist.

3. Umsetzung in der Praxis?

In der Praxis könnte der Verantwortliche etwa über einen vorgefertigten Fragenkatalog an den Empfänger validieren, ob Zugriffe möglich sind und wenn ja, zu welchem Zweck. Sind Zugriffe auf die Daten möglich, so muss dieser Zugriff auf seine Erforderlichkeit hin geprüft werden. Meines Erachtens ergibt sich aus dem Urteil nicht, dass der Verantwortliche selbst diese Prüfung vorzunehmen hat. Es dürfte auch in Ordnung sein, wenn der Importeur (etwa über ein rechtliches Gutachten) dem Verantwortlichen nachweisen kann, dass die Zugriffe durch Behörden die europäischen Anforderungen erfüllen.

Die Prüfung erfolgt also grob wie folgt:

Stufe 1: Einsatz der unveränderten SDK. Kann der Empfänger alle SDK Pflichten einhalten?

- Verantwortlicher muss sich hiervon „vergewissern“ (ggfs. in Zusammenarbeit mit dem Empfänger).
- „Vergewissern“ umfasst die Prüfung, ob Zugriffe von Behörden auf die Daten möglich sind.
- Wenn ja, dann muss geprüft werden, ob die Zugriffe erforderlich sind, um einem in Art. 23 Abs. 1 DSGVO erwähnten Ziel zu dienen und erforderlich sind.

Stufe 2: Pflichten der SDK reichen allein nicht aus. Zusätzliche Maßnahmen sind umzusetzen (Rz. 146).

- Diese Maßnahmen können sowohl vertraglicher als auch technischer Natur sein.
- Achtung: Risiko für den Importeur, gegen nationales Recht zu verstoßen.

Meines Erachtens ist noch einmal wichtig klarzustellen, dass die fehlende Möglichkeit, die SDK Pflichten einzuhalten, nach Ansicht des EuGH nicht direkt zur Unzulässigkeit der Übermittlung führt. Nur wenn dann auch zusätzliche Mittel bzw. Garantien nicht helfen, muss die Aufsichtsbehörde den Transfer untersagen bzw. vorher schon der Exporteur. Dies ergibt sich aus Rz. 146: „…,dass die Klauseln in diesem Drittland nicht eingehalten werden oder nicht eingehalten werden können und dass der nach dem Unionsrecht erforderliche Schutz der übermittelten Daten **nicht mit anderen Mitteln gewährleistet werden kann“.**

Der EuGH endet dann in Rz. 149 mit der Feststellung, dass die SDK in ihrer aktuellen Fassung und durch die dort enthaltenen Garantien grundsätzlich das erforderliche Schutzniveau (Rz. 96, „gleichwertig“) bieten. Ist die Einhaltung der SDK nicht möglich, müsste man mit der oben genannten Stufe 2 der Prüfung und Umsetzung weiterer Garantien fortfahren.