LEGAL REVOLUTIONary
Recht in der digitalen Wirtschaft

Die Schrems II Entscheidung

Düstere Aussichten für internationale Datentransfers

Dennis Schmidt LL.M | Associate | Orrick, Herrington & Sutcliffe LLP

Johanna Klingen | Assessorin iur.

22. Dezember 2020

LR 2020, Seiten 329 bis 336 (insgesamt 8 Seiten)

Der Europäische Gerichtshof ("**EuGH**") hat am 16. Juli 2020 in seinem viel beachteten Urteil in der Rechtssache „Schrems II" (C-311/18) einmal mehr das Spannungsverhältnis zwischen dem datenschutzrechtlichem Grundrechtschutz auf der einen und dem wirtschaftlichen Interesse an einem freien Datenfluss auf der anderen Seite deutlich aufgezeigt. 1

Nachdem im Nachgang des Urteils zunächst nur wenig konkrete Handlungsempfehlungen verfügbar waren, bestand für die meisten Unternehmen eine erhebliche Unsicherheit. Der Europäische Datenschutzausschuss ("**EDSA**") hat hierzu kürzlich zwei Handlungsempfehlungen veröffentlicht, wodurch sich mittlerweile klare Vorgaben herausbilden lassen. Die Anforderungen stellen jedoch eine hohe Hürde für internationale Datentransfers dar. Dies ist problematisch, da die Nutzung vieler Services ohne internationale Datentransfers nicht vorstellbar ist und europäische Alternativen in der Regel nicht existieren. Vor diesem Hintergrund ist die Frage berechtigt, ob das der erste Schritt in Richtung einer europäischen Datenlokalisierung ist.

Dieser Artikel befasst sich mit den Anforderungen, die der EDSA in seinen Handlungsempfehlungen aufgestellt hat und wie Unternehmen diesen Herausforderungen begegnen können, um die Anforderungen zu erfüllen oder jedenfalls das Bußgeldrisiko zu minimieren.

I. Hintergrund – Schrems II

Das Schrems II Urteil des EuGHs war ein datenschutzrechtlicher Paukenschlag für internationale Datentransfers. Das Urteil hat seine Wurzeln in einem bereits im Jahre 2013 von Maximilian Schrems angestoßenen Verfahren bei der irischen Datenschutzaufsicht. Dieses Verfahren fand seinen vorläufigen Höhepunkt in der EuGH Entscheidung vom 06. Oktober 2015 (C-362/14), auch „Schrems I" genannt. In diesem Urteil erklärte der EuGH das sog. „Safe Harbor Abkommen" für unwirksam. Dieses Abkommen ermöglichte zu dem damaligen Zeitpunkt Datentransfers in die USA. 2

Als Reaktion auf dieses Urteil stellten viele Unternehmen ihre Datentransfers auf die Standardvertragsklauseln der Europäischen Kommission ("**SCC**") oder auf das damals neue EU-US Privacy Shield um, welches als Nachfolgeabkommen von Safe Harbor und als Form eines Angemessenheitsbeschlusses den Datentransfer aus der Europäischen Union ("**EU**")/dem Europäischen Wirtschaftsraum ("**EWR**") in die USA rechtlich legitimierte.

In der Folge stellte Maximilian Schrems auch die Rechtmäßigkeit von internationalen Datentransfers auf diesen Grundlagen infrage, sodass der Irish High Court sich gezwungen sah, dem EuGH mehrere Fragen zur Datenübermittlung auf Basis der SCC und des Privacy Shields vorzulegen. Diese Vorlagefragen waren die Grundlage für die Schrems II Entscheidung. Der EuGH entschied, dass das EU-US Privacy Shield unwirksam ist. Mangels einer Umsetzungsfrist sind Datentransfers auf dieser Grundlage nicht mehr zulässig. 3

Internationale Datentransfers auf Grundlage der SCC oder anderer Garantien nach Art. 46 Abs. 2 Datenschutzgrundverordnung ("**DSGVO**") sind auch künftig grundsätzlich möglich. Soll ein Datentransfer jedoch weiterhin auf Basis der geeigneten Garantien erfolgen, muss der Datenexporteur[1] prüfen, ob zusätzliche Schutzmaßnahmen getroffenen werden müssen, um ein angemessenes Schutzniveau im Umgang mit personenbezogenen Daten zu erreichen, dass dem in der EU gleicht. Für die SCC bedeutet dies, dass stets eine Risikobewertung im Einzelfall durchzuführen ist. Bedauerlicherweise nennt der EuGH in seiner Entscheidung weder konkrete Kriterien, anhand denen eine solche Risikobewertung durchzuführen ist noch ergänzende Maßnahmen, mit denen ein angemessenes Schutzniveau hergestellt werden kann.

Dieser Grundsatz gilt nicht nur in Bezug auf den Datentransfer in die USA, sondern in jedes Drittland[2], für das kein Angemessenheitsbeschluss nach Art. 45 Abs. 3 DSGVO besteht, also beispielsweise auch für Datentransfers nach Indien oder China.

II. Rechtliche Grundlagen für internationale Datentransfers

Um die Auswirkungen des Schrems II Urteils gänzlich verstehen zu können, ist es sinnvoll, einen Schritt zurückzugehen und sich die Anforderungen an internationale Datentransfers unter der DSGVO zu vergegenwärtigen. 4

Die Übermittlung personenbezogener Daten an Drittländer ist als zwingendes Recht in Kapitel V der DSGVO, genauer in den Art. 44 – 50 DSGVO geregelt. Insgesamt bietet die DSGVO drei Transfermechanismen, um personenbezogene Daten rechtmäßig aus der EU/dem EWR in ein Drittland zu übertragen.

- **Angemessenheitsbeschluss – Art. 45 Abs. 3 DSGVO:** Die Datenübermittlung kann auf Grundlage eines sog. Angemessenheitsbeschlusses der Europäischen

[1] Datenexporteuer sind Verantwortliche oder Auftragsdatenverarbeiten, die personenbezogene Daten aus der EU/dem EWR in ein Drittland übermitteln.
[2] Als Drittländer werden solche Länder bezeichnet, die nicht zu der EU/dem EWR gehören.

Kommission, in der diese festlegt, dass in einem Drittland ein angemessenes Schutzniveau für die Verarbeitung personenbezogener Daten gewährleistet ist, beruhen. Ein Datentransfer kann hier ohne weitere Anforderungen in das entsprechende Drittland erfolgen Angemessenheitsbeschlüsse bestehen beispielsweise für die Schweiz, Japan und Neuseeland.[3]

- **Geeignete Garantien – Art. 46 DSGVO:** Existiert kein Angemessenheitsbeschluss, so können geeignete Garantien nach Art. 46 DSGVO als Transfermechanismus dienen. Die bekannteste Garantie stellen die SCC, Art. 46 Abs. 2 lit. c DSGVO, dar, aber auch die sog. Binding Corporate Rules ("**BCR**") nach Art. 46 Abs. 2 lit. b DSGVO dürften nicht unbekannt sein. Die geeigneten Garantien dienen dem Zweck, das fehlende Schutzniveau für die Verarbeitung personenbezogener Daten in einem Drittland aufzufangen und so einen Datentransfer zu ermöglichen.

- **Ausnahmen für bestimmte Verarbeitungssituationen – Art. 49 DSGVO:** Kann eine Datenübermittlung nicht auf einem Angemessenheitsbeschluss oder einer geeigneten Garantie gestützt werden, normiert Art. 49 DSGVO als letzten Notanker für Datenexporteure einen abschließenden Ausnahmekatalog. Der EDSA legt in einer Stellungnahme jedoch ein sehr enges Verständnis der Ausnahmen nach Art. 49 DSGVO nahe, wodurch der praktische Anwendungsbereich dieser Vorschriften stark einschränkt wird.[4]

Da sich für Großbritannien angesichts des im Januar 2021 bevorstehenden Brexits bislang noch keine Angemessenheitsentscheidung abzeichnet, ist zu befürchten, dass Großbritannien ab diesem Zeitpunkt auch ein unsicheres Drittland im Sinne der DSGVO ist.

III. Handlungsempfehlungen des EDSA

Im November 2020 veröffentlichte der EDSA zwei Handlungsempfehlungen[5] [6] zum Umgang mit internationalen Datentransfers im Lichte der Schrems II Entscheidung. 5

Der EDSA ist eine unabhängige europäische Einrichtung, die zur einheitlichen Anwendung der datenschutzrechtlichen Vorschriften in der gesamten EU beiträgt und die Zusammenarbeit zwischen den Datenschutzbehörden der Mitgliedsstaaten fördert. Es ist

[3] Die von der Europäische Kommission ergangenen Angemessenheitsbeschlüsse können unter dem Link https://bit.ly/3qemlpw abgerufen werden.
[4] EDSA, Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679, 25.05.2018, https://bit.ly/36nAYUX (besucht am 30.11.2020).
[5] EDSA, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data – version for public consultation, 10.11.2020, https://bit.ly/3fQoiJn (besucht am 30.11.2020), im Folgenden: "**Handlungsempfehlung 1**".
[6] EDSA, Recommendations 02/20 on the European Essential Guarantees for surveillance measures, 10.11.2020, https://bit.ly/37qnnM5 (besucht am 30.11.2020), im Folgenden: "**Handlungsempfehlung 2**".

jedoch zu bedenken, dass die Handlungsempfehlung 1 sich bis zum 21. Dezember 2020 noch in der Konsultationsphase befindet und daher noch Änderungen möglich sind.

Der EDSA betonte in seinen Handlungsempfehlungen nochmals, dass bei der Übermittlung von personenbezogenen Daten das hohe Schutzniveau im EWR mit den übermittelten Daten „mitreist". Mit anderen Worten darf die Übermittlung von Daten in ein Drittland nicht dazu genutzt werden, um die Erfüllung der hohen Anforderungen des europäischen Datenschutzrechts zu umgehen.[7] Auch der EuGH stellte in seiner Entscheidung klar, dass Datenexporteure stets im Einzelfall das Schutzniveau in dem Drittland überprüfen müssen.

Und genau hier setzen die Handlungsempfehlungen der EDSA an. Sie sollen Datenexporteuren Schritte aufzeigen, anhand derer eine Prüfung des Schutzniveaus in einem Drittland erfolgen kann und nennt exemplarisch verschiedene Maßnahmen, die potenziell dabei helfen können, ein angemessenes Schutzniveau herzustellen. Hierzu hat der EDSA einen sechsstufigen Test entwickelt:

Schritt 1: Kenntnis der eigenen Datenübermittlungen[8]

Als ersten Schritt muss der Datenexporteur einen Überblick über jegliche bestehende und beabsichtigte Datentransfer erlangen. Dies kann bestenfalls durch ein aktuelles Verarbeitungsverzeichnis nach Art. 30 DSGVO erfolgen. Hierbei dürfen auch Weiterübermittlungen in ein (weiteres) Drittland nicht vergessen werden. Bei Weiterübermittlungen handelt es sich um Datenübermittlungen, die nicht der Datenexporteur originär vornimmt, sondern von dem Datenempfänger beabsichtigt werden. Dies ist beispielsweise der Fall, wenn ein Auftragsverarbeiter einen Unterauftragsverarbeiter beauftragt und personenbezogenen Daten zu diesem Zweck an den Unterauftragsverarbeiter übermittelt. Der EDSA stellt zudem klar, dass auch Fernzugriffe unter den Begriff des Datentransfers fallen. 6

Schritt 2: Identifikation der Rechtsgrundlage[9]

In einem zweiten Schritt hat sich der Datenexporteur darüber zu vergewissern, auf welcher Rechtsgrundlage die Datenübermittlung in ein Drittland erfolgen kann. 7

Basiert die Datenübermittlung auf einem Angemessenheitsbeschluss oder einer Ausnahme nach Art. 49 DSGVO, bedarf es keiner weiteren Schritte, außer der Dokumentation nach Schritt 1. Andernfalls muss der Datenexporteur mit der Prüfung des Schritts 3 fortfahren.

Unternehmen, die sich bislang aktiv um die Umsetzung der Vorgaben der DSGVO gekümmert haben, sollten die erforderlichen Informationen für Schritt 1 und 2 dem Verarbeitungsverzeichnis nach Art. 30 DSGVO entnehmen können. Alle anderen

[7] Handlungsempfehlung 1, Executive Summary.
[8] ebd., Rn. 8 - 13.
[9] ebd., Rn. 14 - 27.

Unternehmen sollten dieses Urteil als Gelegenheit verstehen, sich einen Überblick über die eigenen Datenverarbeitungen zu verschaffen.

Schritt 3: Bewertung des Schutzniveaus im Zielstaat[10]

Schritt 3 betrifft die Bewertung des datenschutzrechtlichen Schutzniveaus im Zielstaat. 8

Der EDSA stellt Datenexporteure mit diesem Schritt vor die undankbare Aufgabe, selbst die Rechtslage in dem Drittland überprüfen zu müssen. Denn die Praxis oder das Recht eines Drittlandes können einen derartigen Einfluss auf einen Datenverarbeitungsvorgang und die geeignete Garantie haben, dass der Datenempfänger ein angemessenes Schutzniveau nicht mehr gewährleistet kann. Im Fokus stehen dabei solche Gesetze, die öffentlichen Behörden unter bestimmten Voraussetzungen die Befugnis verleihen, die Offenlegung von oder den Zugang zu personenbezogenen Daten zu verlangen.

Mehr zu diesem anspruchsvollen Bewertungsschritt folgt in einem separaten Aufsatz, der weitere Handlungsempfehlungen zur Prüfung des Schutzniveaus im Zielstaat enthalten wird.

Schritt 4: Implementierung zusätzlicher Schutzmaßnahmen[11]

Zeigt Schritt 3, dass die geeignete Garantie, auf der der Datentransfer rechtlich basieren soll, kein angemessenes Schutzniveau bietet, folgt für den Datenexporteur Schritt 4. Hier muss der Datenexporteur evaluieren, welche zusätzlichen Schutzmaßnahmen implementiert werden können, um für den geplanten Datentransfer ein angemessenes Schutzniveau zu erreichen. 9

Die zusätzlichen Schutzmaßnahmen können organisatorischer, technischer oder vertraglicher Natur sein. Der Fokus sollte hierbei auf den technischen Maßnahmen liegen. Hierzu stellt der EDSA im Annex der Handlungsempfehlung 1 für sieben Use Cases detaillierte Anforderungen dar. Der EDSA betont, dass organisatorische und vertragliche Schutzmaßnahmen in der Regel nicht ausreichen, um einen Zugang der Behörden zu den personenbezogenen Daten zu unterbinden. In der Konsequenz sind zusätzliche technische Maßnahmen notwendig, um das Sicherheitsniveau auf ein angemessenes Level zu heben.

Der EDSA legt aus technischer Sicht einen besonderen Fokus auf den Einsatz von Verschlüsselungstechniken sowie einer Pseudonymisierung oder gar Anonymisierung, soweit dies in Bezug auf den genutzten Service umsetzbar ist. Die Beschreibung dieser technischen Schutzmaßnahmen ist das Herzstück der Handlungsempfehlung 1 der EDSA.

[10] ebd., Rn. 28 - 44.
[11] ebd., Rn. 45 - 54.

1. Technische Maßnahmen[12]

- **Verschlüsselung**: Der EDSA verlangt insb. die Nutzung eines hohen technischen Verschlüsselungsstandards, einschließlich einer starken Verschlüsselung vor der Übermittlung der Daten (d. h. Verschlüsselung im Transit und im Ruhezustand), die Verwendung belastbarer Verschlüsselungsmechanismen, die als robust gegenüber einer Kryptoanalyse durch öffentliche Behörden angesehen werden können, sowie einer "fehlerfreien" Implementierung und zuverlässigen Verwaltung des Verschlüsselungsalgorithmus. 10

In diesem Zusammenhang wird interessant zu beobachten sein, wie sich dieser Fokus auf die Verschlüsselung mit den europäischen Bestrebungen zum Verbot von Ende zu Ende Verschlüsselungen für Datentransfers in Einklang bringen lässt.[13]

- **Pseudonymisierung**: Als mögliche technische Maßnahme nennt der EDSA die Pseudonymisierung. Bei einer Pseudonymisierung können personenbezogene Daten nicht mehr einer bestimmten Person zugeordnet oder die betroffene Person aus einer größeren Gruppe herausgefiltert werden, ohne dafür weitere Zusatzinformationen zu benötigen.

- **Mehrparteienverarbeitung:** Im Falle einer Mehrparteienverarbeitung, die in den Augen des EDSA eine geeignete technische Maßnahme ist, soll der Datenexporteur sicherstellen, dass für den jeweiligen Datenempfänger die empfangenen Daten nicht ohne Zusatzinformationen einer natürlichen Person zuordenbar sind.

Überdies haben die dargestellten technischen Maßnahmen gemein, dass die jeweiligen kryptografischen Schlüssel bzw. die Zusatzinformationen außerhalb der Reichweite des Datenempfängers aufbewahrt werden müssen - d. h. ausschließlich beim Datenexporteur oder anderen Stellen in einem sicheren Drittland. 11

Führt die Zusammenwirkung der SCC oder BCR und der Implementierung zusätzlicher Schutzmaßnahmen zu einem angemessenen Schutzniveau, kann ein Datentransfer erfolgen. Andernfalls müssen (geplante) Datentransfers ausgesetzt oder beendet werden und übermittelte Daten zurückgegeben oder gelöscht werden.

Sofern der der Datentransfer für Datenexporteur nichtsdestotrotz erforderlich ist, muss sich dieser an die zuständige Datenschutzaufsichtsbehörde wenden. Diese wird sodann das Schutzniveau selbst beurteilen und dem Datenexporteur eine entsprechende Anordnung geben. In der Regel wird der Datentransfer dann nicht erfolgen dürfen.

Grund zur Beunruhigung geben insb. die Use Cases, für die der EDSA angibt, noch keine wirksamen (technischen) Schutzmaßnahmen gefunden zu haben. Zu diesen Fallbeispielen

[12] ebd., Rn. 72 - 91.
[13] Daniel AJ Sokolov, EU-Regierungen planen Verbot sicherer Verschlüsselung, 09.11.2020, https://bit.ly/39vRGnb (besucht am 02.12.2020).

zählen die Verarbeitung unverschlüsselter Daten durch Cloud Anbieter oder der Fernzugriff und die damit verbundene Verarbeitung unverschlüsselter Daten für geschäftliche Zwecke, beispielsweise die Verarbeitung von personenbezogenen Daten im Drittland zu HR-Zwecken.

2. Vertragliche Maßnahmen[14]

Zusätzliche vertragliche Maßnahmen müssen per Definition über den bestehenden Schutz durch die Regelungen der SCC bzw. der BCR hinausgehen. Der EDSA stellt jedoch fest, dass vertragliche Maßnahmen insgesamt nur einen geringen zusätzlichen Schutz bieten können, da solche Regelungen keine Bindungswirkung in Bezug auf die Sicherheitsbehörden im Drittland entfalten können. Die vom EDSA vorgeschlagenen Maßnahmen umfassen bspw.: 12

Eine vertragliche Verpflichtung des Datenempfängers zur Anwendung spezifischer technischer Maßnahmen, zusätzliche Transparenzverpflichtungen, z.B. die regelmäßige Veröffentlichung von sog. Transparenzberichten, in denen der Datenempfänger die Anzahl der Datenanfragen von staatlichen Stellen sowie die jeweilige Reaktion darstellt. Weitere vertragliche Regelungen können eine Garantie dahingehend sein, dass keine „back-doors" in die fragliche Software implementiert wurden oder die Verpflichtung, jegliche Anfragen von staatlichen Stellen kritisch zu prüfen und juristisch dagegen vorzugehen.

3. Organisatorische Maßnahmen[15]

Ebenso wie die zusätzlichen vertraglichen Maßnahmen können auch organisatorische Maßnahmen für sich genommen nur in den wenigstens Fällen ein angemessenes Schutzniveau herbeiführen. Der EDSA nennt insb. die Einführung interner Richtlinien zur Festlegung interner Kommunikationswege im Falle von staatlichen Zugriffsanfragen und die entsprechende Dokumentation sowie regelmäßige Mitarbeiterschulungen als mögliche organisatorische Maßnahmen. 13

Schritt 5: Formale Schritte[16]

Soweit erforderlich sind im fünften Schritt die erforderlichen formalen Schritte zur Umsetzung der im Rahmen von Schritt 3 und 4 getroffenen Maßnahmen einzuleiten. Dies können bspw. die Korrespondenz und Abstimmung mit einer Aufsichtsbehörde sein. 14

Schritt 6: Erneute Bewertung[17]

Im Einklang mit der in der DSGVO normierten Rechtschaffenheitspflicht erfordert Schritt 6 die stetige Kontrolle über die Lage in einem Drittland. Bei Veränderungen im Drittland folgt die Überprüfung der Effektivität der geeigneten Garantie und der zusätzlichen Schutzmaßnahmen. 15

[14] ebd. 92 - 121.
[15] ebd., Rn. 122 - 137.
[16] ebd., Rn. 55 - 61.
[17] ebd., Rn. 62 - 63.

Wichtig dabei ist, dass der Datenexporteur Maßnahmen trifft, mit denen der Datentransfer unverzüglich gestoppt werden kann, sofern es rechtliche Entwicklungen in dem Drittland erfordern oder der Datenempfänger die Einhaltung vertraglicher Regelungen oder zusätzlicher Schutzmaßnahmen nicht gewährleisten kann bzw. gegen sie verstößt.

IV. Fazit

Die Nachbeben des Schrems II Urteils sind bis heute deutlich zu spüren. Noch immer besteht eine erhebliche Unsicherheit in Bezug auf die Anforderungen an die internationalen Datentransfers. Die Empfehlungen des EDSA schlagen nun zwar zum ersten Mal konkrete Maßnahmen vor, die zum Erreichen eines angemessenen Sicherheitsniveaus herangezogen werden können. Diese Maßnahmen erscheinen aktuell sehr restriktiv. Es bleibt zu hoffen, dass am Ende der Konsultationsphase eine abgeschwächte Handlungsempfehlung veröffentlicht wird, die leichter umsetzbare Vorschläge enthält. 16

Am 12. November, nur wenige Tage nach Veröffentlichung dieser Handlungsempfehlungen, veröffentlichte die Europäische Kommission Entwürfe für neue SCC. Der EDSA und die Kommission scheinen die jeweiligen Veröffentlichungen nicht miteinander abgestimmt zu haben. Beide folgen in Teilen unterschiedlichen Ansätzen. Denn der Entwurf der SCC hat zwar in großen Teilen die Handlungsempfehlungen des EDSA berücksichtigt, jedoch scheinen die neuen SCC eine Risikobewertung unter Berücksichtigung u. a. der betroffenen Datenkategorien und der Zugriffanträge der Strafverfolgungsbehörden des Drittlandes zu ermöglichen (siehe Klausel 2 lit. b). Dies führt zu der spannenden Frage, ob zukünftig Datentransfers auf Grundlage der neuen SCC möglich sein werden, ohne das zusätzliche technische Maßnahmen getroffen werden. Zudem bleibt aufmerksam zu beobachten, wie sich die Gespräche zwischen der US-Regierung und der EU-Kommission zu einem neuen „Privacy Shield" entwickeln.[18] Ein wirksames neues „Privacy Shield", welches auch den Schutz der Grundrechte der EU-Bürger ausreichend berücksichtigt, wäre ein Silberstreif am Himmel für die Zukunft der internationalen Datentransfers.

[18] Holger Bleib, EU-Kommission verhandelt zu neuem Privacy Shield, 31.08.2020, https://bit.ly/36rqHaw (besucht am 01.12.2020).