

„Schrems II“-Compliance – What’s next

Die letzte war eine der arbeitsreichsten Wochen für Datenschutzpraktiker seit In-Kraft-Treten der EU-Datenschutzgrundverordnung. Am Dienstag, 10. November, hat der Europäische Datenschutzausschuss (EDSA) seine Empfehlungen verabschiedet, wie zusätzliche Schutzmaßnahmen bei der Übermittlung von Daten in Drittländer ohne angemessenes Datenschutzniveau auf Basis der Standardvertragsklauseln in der Praxis aussehen können. Am Donnerstag, den 12. November, veröffentlichte die Europäische Kommission den seit langem angekündigten Entwurf für neue Standardvertragsklauseln.



In Kürze:

- Die erste europäische Auslegungshilfe nach dem Schrems II-Urteil ist veröffentlicht.
- Die Übermittlung von unverschlüsselten Daten u.a. an Cloud-Dienstleister steht im besonderen Fokus des EDSA und der nationalen Aufsichtsbehörden.
- Neue Standardvertragsklauseln liegen im Entwurf vor und werden für Anfang 2021 erwartet.
- Es gibt eine Jahresfrist zur Umstellung auf die neuen Standardvertragsklauseln.

Was geschah bisher?

Im Juli hat der Europäische Gerichtshof in der Schrems II-Entscheidung (C-311/18) (i) das sog. Privacy Shield-Abkommen zwischen der EU und den USA für ungültig erklärt und (ii) entschieden, dass sich Organisationen unter bestimmten Umständen immer noch auf die Standardvertragsklauseln (SCCs) verlassen können, um personenbezogene Daten aus dem Europäischen Wirtschaftsraum (EWR) in die USA oder in ein anderes Land zu übermitteln, das nach Ansicht der EU über kein angemessenes Datenschutzniveau verfügt. Um sich bei solchen Übermittlungen jedoch auf die SCCs verlassen zu können, muss das die Daten übermittelnde Unterneh-

men eine Einzelfallprüfung vornehmen, ob die Gesetze des Drittlandes ein „im Wesentlichen gleichwertiges“ Schutzniveau für die personenbezogenen Daten bieten, und erforderlichenfalls „ergänzende Maßnahmen“ zur Gewährleistung dieses Schutzes ergreifen. Die Datenschutzaufsichtsbehörden in den verschiedenen EU-Ländern haben unterschiedliche Ankündigungen in Bezug auf die Durchsetzung dieser Entscheidung veröffentlicht. Vor diesem Hintergrund hatten wir ein vorläufiges Maßnahmenpaket entwickelt, um Datentransfers zu evaluieren, Risiken zu identifizieren und zu adressieren, das die Empfehlungen des EDSA teilweise bereits vorweg genommen hat.

Was ist neu?

Mit den Empfehlungen des EDSA liegt die europäische Auslegungshilfe für Datenübermittlungen nach der Schrems II-Entscheidung vor. Gleichzeitig hat die EU-Kommission einen Entwurf der neuen Standardvertragsklauseln vorgelegt. Diese neuen SCCs unterscheiden sich erheblich von den bisher geltenden SCCs. Die vielleicht aufregendste Entwicklung ist, dass die SCC-Entwürfe in einem „modularen“ Format strukturiert sind, das Übermittlungen in allen denkbaren Konstellationen, neuerdings auch zwischen zwei Auftragsverarbeitern, abdeckt. Das „Modul“ zur Übermittlung vom für die Verarbeitung Verantwortlichen zum Auftragsverarbeiter erfüllt die Anforderungen von Artikel 28 DSGVO, was bedeutet, dass kein separater Auftragsverarbeitungsvertrag mehr nötig ist.

Unternehmen sind nun mit verschiedenen Herausforderungen konfrontiert.

- Bereits abgeschlossene oder derzeit abzuschließende SCCs müssen nach den Empfehlungen des EDSA um zusätzliche Maßnahmen ergänzt werden, wenn die gesetzlichen Regelungen oder eine sonstige Praxis im Drittland die Wirksamkeit der angemessenen Garantien, wie sie die SCCs darstellen, beeinträchtigen können. Kommt das Unternehmen bei dieser Prüfung zu dem Schluss, dass die Gesetzgebung im Drittland Überwachungsmaßnahmen zulässt, die die Wirksamkeit der SCCs beeinträchtigt, sind zusätzliche Maßnahmen zu ergreifen. In der Praxis gestalten sich insbesondere die Ermittlungen schwierig, ob die im Einzelfall übermittelten Daten von der Überwachungs-gesetzgebung betroffen sind.

Der EDSA identifiziert verschiedene Konstellationen von Übermittlungen und beschreibt beispielhaft welche zusätz-

lichen technischen und/oder vertraglichen Maßnahmen vereinbart werden können. Die Fallgruppe 6 beschreibt die Leistungen eines Cloud-Diensteanbieters, der Zugang zu unverschlüsselten Daten benötigt, um die Leistungen erbringen zu können. Hier sieht der EDSA keine Möglichkeit, diese Übermittlung rechtskonform zu ermöglichen, wenn das Ergebnis der Analyse der Situation im Drittland ist, dass ein vergleichbarer Datenschutzstandard nicht gewährleistet werden kann. Entsprechendes gilt für den Zugriff in einer Unternehmensgruppe, wenn ein Gruppenunternehmen in einem Land mit nicht angemessenem Datenschutzniveau Zugriff auf personenbezogene Daten im Klartext erhalten soll. Für diese Fallgruppen sind die Empfehlungen wohl dahingehend zu verstehen, dass eine Übermittlung unzulässig bleibt. Eine starke Verschlüsselung und Pseudonymisierung als ausreichende Maßnahme zur Gewährleistung einer konformen Übermittlung kann danach nur funktionieren, solange die Daten durchgehend verschlüsselt und pseudonymisiert bleiben.

- Die Empfehlungen des EDSA vom 10. November 2020, die technischen und vertraglichen Maßnahmen in Ergänzung zu den derzeit geltenden SCCs zu vereinbaren, sind nun vor dem Hintergrund des Entwurfs der neuen SCCs vom 12. November 2020 zu bewerten. Die derzeit gültigen SCCs werden nach Wirksamwerden des Kommissionsbeschlusses zu den neuen SCCs – wenn auch nach Ablauf einer derzeit geplanten einjährigen Karenzfrist – ungültig. Die Kommission ist zum Erlass von Standardvertragsklauseln als sog. Durchführungsrechtsakt ermächtigt (sog. Prüfverfahren nach Art. 5 (EU) Nr. 182/2011). Dabei muss die Kommission den von ihr vorgeschlagenen Entwurf für einen Durchführungsrechtsakt mit einem Ausschuss abstimmen, der aus Vertretern der einzelnen EU-Länder besteht. Der Vorschlag muss von einer qualifizierten Mehrheit des Ausschusses unterstützt werden. Der Entwurf der neuen SCCs ist bis zum 10. Dezember 2020 zur Kommentierung freigegeben und würde dann – vorbehaltlich weiterer Änderungen – voraussichtlich im neuen Jahr in Kraft treten können.
- Teilweise greifen die neuen Standardvertragsklauseln die Empfehlungen des EDSA auf. Dies betrifft insbesondere die Frage der Transparenz von Zugriffen auf die übermittelten Daten durch Regierungsbehörden, die Vorgabe, Rechtsmittel gegen den Zugriff auszuschöpfen und Statistiken über derartige Zugriffe zu führen. Zum Teil berücksichtigen die neuen SCCs aber weitergehend als die Forderungen des EDSA die Interessen des Importeurs und die rechtlichen

Vorgaben, denen dieser in seinem Land unterliegt. Während die vertraglichen Sicherungsmechanismen in den neuen SCCs ausformuliert sind, enthalten diese keine konkreten Vorgaben zu technischen Sicherungsmaßnahmen. Insoweit bleiben die Empfehlungen des EDSA relevant. Die Empfehlungen zu den ergänzenden Transfermaßnahmen stehen bis zum 30. November zur Konsultation.

Was ist zu tun?

Die relevanten Drittstaatenübermittlungen sollten identifiziert werden, soweit dies noch nicht erfolgt ist. Der EDSA verlangt nun insbesondere, die Angemessenheit des Datenschutzniveaus im Land des Datenempfängers zu überprüfen. Dann sind zunächst technische Sicherungsmaßnahmen anhand der vom EDSA ermittelten Fallgestaltungen daraufhin zu überprüfen, ob sie in der vorliegenden Konstellation zum Einsatz kommen können. Erst wenn sich solche technischen Sicherungen als grundsätzlich geeignet erweisen, kann über zusätzliche vertragliche Maßnahmen nachgedacht werden. Hierbei kann einerseits auf die Beispiele in den Empfehlungen des EDSA abgestellt werden; andererseits können diese durchaus im Lichte der neuen Standardvertragsklauseln ausgelegt werden. Hier zeigt sich, dass die Überlegungen des EDSA zwar in gewissem Maße in den Neu-Entwurf der SCCs eingeflossen sind, die Abstimmung zwischen EDSA und Kommission aber nicht so nahtlos war, dass die vom EDSA geforderten vertraglichen Sicherungen nun eins zu eins in die Standardvertragsklauseln übernommen wurden. Vor diesem Hintergrund stellt sich dann zu Recht die Frage, ob auch in die neuen Standardvertragsklauseln weitreichende Sicherungen zusätzlich aufzunehmen wären und ob die Formulierung der neuen SCCs zu staatlichen Zugriffen einen bereits jetzt schon gangbaren Weg aufzeigen. Nicht wirklich zu erwarten ist,

dass der EDSA seine Forderungen nach Abschluss der Kommentierungsphase zurücknimmt und die Empfehlungen diesbezüglich überarbeitet.

So sollten Unternehmen aktuell die derzeit geltenden SCCs unter Berücksichtigung dieser Anforderungen ergänzen und gleichzeitig eine Öffnungsklausel aufnehmen, die nach Erscheinen der neuen SCCs eine erleichterte Vertragsanpassung und -umstellung ermöglicht. Die Arbeiten zu den technischen Sicherungsmaßnahmen sowie die Erarbeitung überprüfbarer Freigabeprozesse sollten insoweit Vorarbeiten sein, die auch unter Geltung der neuen SCC Bestand haben. Diese Arbeiten werden jedoch ein Provisorium bleiben, auf die die entsprechenden vertraglichen Umstellungsarbeiten dann zu folgen haben.

Empfohlene Schritte:

- Internationale Datentransfers identifizieren;
- Technisch-organisatorische Maßnahmen an EDSA-Empfehlungen ausrichten; prüfen, ob ein Zugriff auf unverschlüsselte Daten im Drittland zwingend erforderlich ist;
- Wenn unverschlüsselte Daten verarbeitet werden, Anwendbarkeit von Überwachungsgesetzgebung auf den Dienstleister und die betroffene Dienstleistung verifizieren;
- Bestehende SCCs anhand der EDSA-Empfehlungen und den neuen SCCs ergänzen sowie Öffnungsklausel in den SCCs zur Umstellung auf neue SCCs in 2021 aufnehmen; und
- Projektplanung für die Umstellung auf SCCs in 2021 beginnen.

Timeline



Ihre Ansprechpartner:



Dr. Jörg Alshut

Berlin

T +49 30 52133 21890

joerg.alshut@luther-lawfirm.com



Silvia C. Bauer

Köln

T +49 221 9937 25789

silvia.c.bauer@luther-lawfirm.com



Dr. Maximilian Dorndorf

Essen

T +49 201 9220 24027

maximilian.dorndorf@luther-lawfirm.com



Dr. Stefanie Hellmich, LL.M.

Frankfurt a.M.

T +49 69 27229 24118

stefanie.hellmich@luther-lawfirm.com



Dr. Kay Oelschlägel

Hamburg

T +49 40 18067 12175

kay.oelschlaegel@luther-lawfirm.com



Christian Kuß, LL.M.

Köln

T +49 221 9937 25686

christian.kuss@luther-lawfirm.com



Dr. Michael Rath

Köln

T +49 221 9937 25795

michael.rath@luther-lawfirm.com



Carsten Andreas Senze

Stuttgart

T +49 711 9338 25222

carsten.a.senze@luther-lawfirm.com



Dr. Wulff-Axel Schmidt

Frankfurt a.M.

T +49 69 27229 27078

wulff-axel.schmidt@luther-lawfirm.com

