datenschutz-berater.de

44. Jahrgang

DSB 09/2020

DATENSCHUTZ-BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

ISSN 0170-7256

dfv Mediengruppe

Felix Meurer

Aktuelle Anforderungen an Drittlandübermittlungen EDSA veröffentlicht FAQ zu „Schrems II“-Urteil

Der Europäische Datenschutzausschuss (EDSA) hat sich in seiner Sitzung am 23. Juli 2020 mit dem kurz zuvor ergangenen Urteil des EuGH zum EU-US Privacy Shield und der Gültigkeit der Standarddatenschutzklauseln (Beschluss 2010/87/EU) sowie den sich daraus ergebenden Konsequenzen für Datenübermittlungen in Drittländer befasst. Nachfolgend veröffentlichte der EDSA einige Antworten auf häufig gestellte Fragen („FAQ“). Diese FAQ bieten Verantwortlichen eine erste Hilfestellung. Dennoch bleiben Fragen offen, die in den kommenden Monaten – auch durch die Aufsichtsbehörden und den EDSA – beantwortet werden müssen.

Datenexporteure in der Verantwortung

Der EDSA greift in seinen FAQ die zentralen Aussagen der EuGH-Entscheidung „Schrems II“ (Rechtssache C-311/18) auf: Der Beschluss 2010/87/EU, mit dem die EU-Kommission Standarddatenschutzklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern erlassen hat, sei gültig. Die Gültigkeit der Standarddatenschutzklauseln hänge im jeweiligen Einzelfall jedoch davon ab, dass diese tatsächlich geeignete Garantien enthielten, die es ermöglichten, ein dem der EU angemessenes Schutzniveau für die übermittelten personenbezogenen Daten auch in dem Drittland zu gewährleisten. Es müsse gesichert sein, dass Datenübermittlungen auf Grundlage von Standarddatenschutzklauseln ausgesetzt oder beendet werden, sofern einzelne Klauseln nicht eingehalten und das Datenschutzniveau nicht mehr gewährleistet werden könne.

Der EDSA betont die bereits durch den EuGH hervorgehobene Verantwortung des jeweiligen Datenexporteurs, die in dem jeweiligen Drittland bestehenden Umstände und die Rechtslage im Hinblick auf das Schutzniveau der übermittelten Daten vor einer jeden Datenübermittlung zu prüfen. Diese Prüfpflicht stellt verantwortliche Stellen vor eine große Herausforderung. Weitere Hilfestellungen seitens der Aufsichtsbehörden wären diesbezüglich begrüßenswert.

Datenimporteure seien verpflichtet, den Datenexporteur über jedes Unvermögen bezüglich der Einhaltung der Klauseln oder etwaiger zusätzlicher Maßnahmen zu informieren. In diesem Fall bestehe für Datenexporteure die Pflicht, Datenübermittlungen auszusetzen und zu beenden.

Zudem betont der EDSA, dass Datenübermittlungen in die USA umgehend nicht mehr auf den EU-US Privacy Shield gestützt werden könnten. Der EuGH habe diesen mangels eines hinreichenden Datenschutzniveaus, insbesondere im Hinblick auf das Nichtbestehen einklagbarer Rechte betroffener Personen aus der EU, für ungültig erklärt. Diese Entscheidung gelte unmittelbar.

Hohe Anforderungen gelten für sämtliche Garantien

Die EuGH-Entscheidung und die sich daraus ergebenden Anforderungen für Drittlandübermittlungen gelten nicht allein für Datenübermittlungen auf Grundlage des Privacy Shields, so der EDSA. Implikationen ergeben sich für sämtliche Garantien im Sinne des Art. 46 DSGVO.

Datenexporteure, die Daten bisher auf Grundlage des Privacy Shields übermittelt hätten, müssten nun umgehend anderweitige Garantien im Sinne des Art. 46 DSGVO vorsehen. Auch für diese ergeben sich Implikationen aus der EuGH-Entscheidung. Anders als nach der Safe Harbor-Entscheidung gebe es keine Karenzzeit. Erforderliche Maßnahmen müssten unmittelbar ergriffen werden.

Auch Datenübermittlungen auf Grundlage der Standarddatenschutzklauseln an Datenimporteure in den USA seien fortan nicht ohne Weiteres zulässig. Die Entscheidung, ob eine Datenübermittlung in die USA auf Grundlage der Standarddatenschutzklauseln weiterhin rechtmäßig erfolgen könne, sei von der Überprüfung der Rechtslage des Drittlandes, die der Datenexporteur im jeweiligen Einzelfall vorzunehmen habe, abhängig. Gegebenenfalls könne es erforderlich sein, zusätzliche Maßnahmen vorzusehen. Durch diese müsse sichergestellt werden, dass US-Recht das durch die Standarddatenschutzklauseln garantierte angemessene Schutzniveau nicht beeinträchtige.

Auch diese Anforderung stellt Datenexporteure vor Herausforderungen. Es ist fraglich, ob einzelne Datenexporteure in der Lage sind, im Einzelfall geeignete zusätzliche Garantien zu schaffen, die ein angemessenes Schutzniveau gewährleisten. Dies gilt besonders vor dem Hintergrund, dass ein solches Niveau weder durch „Safe Harbor“ noch durch „Privacy Shield“ gegenüber den USA geschaffen werden konnte.

Die dargestellten Anforderungen gelten auch bei der Verwendung verbindlicher interner Datenschutzvorschriften („BCR", Art. 47 DSGVO). Datenexporteure, die Datenübermittlungen bislang auf diese Grundlage gestützt haben, müssten nunmehr ebenfalls überprüfen, ob ein angemessenes Datenschutzniveau gewährleistet werde. Dies gelte insbesondere im Hinblick auf die USA, da die US-Gesetze, die der EuGH bei der Beurteilung des US-Datenschutzniveaus berücksichtigt hat, ebenfalls gegenüber den BCR vorrangig seien. Somit könnte es trotz Verwendung entsprechender Datenschutzvorschriften zu einer Absenkung des Schutzniveaus kommen.

Welche zusätzlichen Maßnahmen Datenexporteure konkret ergreifen müssten, sei eine Frage des Einzelfalls, so der EDSA. Auch diesbezüglich müsse insbesondere die Rechtslage des jeweiligen Drittlandes berücksichtigt werden. In diesem Punkt bleiben die FAQ des EDSA lückenhaft und helfen Datenexporteuren nicht konkret weiter. Der EDSA kündigt jedoch an, das EuGH-Urteil weiter analysieren und ermitteln zu wollen, welche rechtlichen, technischen und organisatorischen Maßnahmen zusätzlich zu Standarddatenschutzklauseln oder BCR ergriffen werden könnten, um ein angemessenes Datenschutzniveau zu gewährleisten.

Falls die Überprüfung der Rechtslage des Drittlandes durch den Datenexporteur jedoch ergebe, dass ein angemessenes Datenschutzniveau trotz etwaiger zusätzlicher Maßnahmen nicht gewährleistet werden könne, sei der Datenexporteur verpflichtet, die Datenübermittlung auszusetzen. Falls eine Datenübermittlung dennoch fortgesetzt werden soll, müsse unmittelbar eine Mitteilung an die zuständige Aufsichtsbehörde erfolgen.

Sämtliche in Art. 46 DSGVO vorgesehenen Garantien müssten im Licht des Art. 44 DSGVO gesehen werden und somit den durch den EuGH konkretisierten Anforderungen entsprechen. Der EDSA will die Konsequenzen des EuGH-Urteils auf die weiteren Garantien überprüfen. Daher ist es Datenexporteuren zu empfehlen, weitere Veröffentlichungen aufmerksam zu verfolgen.

Zudem ergeben sich Konsequenzen nicht nur für Datenübermittlungen in die USA. Auch Datenübermittlungen in andere Drittländer unterliegen den dargestellten Anforderungen. Auch insoweit obliege den Datenexporteuren die Verantwortung, für ein angemessenes Datenschutzniveau zu sorgen und die erforderlichen Maßnahmen zu ergreifen, so der EDSA.

Art. 49 DSGVO: Übermittlungen in Ausnahmefällen

Eine Übermittlung personenbezogener Daten in die USA oder andere Drittländer auf Grundlage der Ausnahmevorschriften des Art. 49 DSGVO sei auch weiterhin grundsätzlich möglich. Eine Hilfestellung für Datenexporteure könnten insoweit die vom EDSA veröffentlichten Leitlinien (2/2018) zu Art. 49 DSGVO bieten.

Sofern Datenübermittlungen auf die Einwilligung der betroffenen Personen gestützt würden (Art. 49 Abs. 1 lit. a DSGVO), müssten Datenexporteure insbesondere beachten, dass es sich um eine „ausdrückliche" Einwilligung handeln müsse. Diese sei spezifisch auf eine bestimmte Datenübermittlung zu beziehen. Datenexporteure müssten daher sicherstellen, dass vor der Übermittlung eine spezifische Einwilligung der Betroffenen eingeholt werde, auch wenn die jeweiligen Daten bereits zuvor erhoben wurden. Zudem müssten die betroffenen Personen insbesondere über die mit der Datenübermittlung möglicherweise einhergehenden Risiken informiert werden („Informierte Einwilligung", vgl. Art. 49 Abs. 1 lit. a DSGVO).

Datenübermittlungen auf Grundlage eines zwischen dem Datenexporteur und der betroffenen Person bestehenden Vertrages (Art. 49 Abs. 1 lit. b DSGVO) dürften nur „gelegentlich" erfolgen, nicht jedoch dauerhaft. Ob sich eine Datenübermittlung als „gelegentlich" darstellt oder nicht, sei eine Frage des jeweiligen Einzelfalls. Jedenfalls seien Datenübermittlungen insoweit jedoch ohnehin nur zulässig, sofern diese für die Erfüllung eines Vertrages oder die Durchführung vorvertraglicher Maßnahmen objektiv erforderlich sind. Insoweit ergibt sich eine Parallele zu den Anforderungen der Rechtsgrundlage des Art. 6 Abs. 1 lit. b DSGVO.

Im Hinblick auf Datenübermittlungen aus wichtigen Gründen des öffentlichen Interesses (Art. 49 Abs. 1 lit. d DSGVO) stellt der EDSA fest, dass das jeweilige öffentliche Interesse im Unionsrecht oder dem Recht des Mitgliedstaates, dem der Verantwortliche unterliegt, anerkannt sein müsse. Wesentliche Voraussetzung für die Anwendbarkeit dieser Ausnahmeregelung sei die Feststellung eines wichtigen öffentlichen Interesses, nicht die Art der jeweiligen Organisation. Datenübermittlungen auf dieser Grundlage seien zwar nicht auf gelegentliche Übermittlungen beschränkt. Dennoch könnten insoweit keine Übermittlungen in größerem Umfang oder in systematischer Weise erfolgen. Art. 49 DSGVO statuiere Ausnahmevorschriften. Es sei daher eine restriktive Handhabung erforderlich. Dies müsse durch jeden Datenexporteur gewährleistet werden.

Vereinbarungen zur Auftragsverarbeitung

Verantwortliche müssten außerdem bestehende Vereinbarungen zur Auftragsverarbeitung im Hinblick auf Drittlandübermittlungen überprüfen. Vereinbarungen mit Auftragsverarbeitern müssten in Übereinstimmung mit den Anforderungen des Art. 28 Abs. 3 DSGVO zumindest Regelungen enthalten, ob eine Übermittlung der verarbeiteten Daten in Drittländer erlaubt ist oder nicht. Dies gelte auch bezüglich der Beauftragung von Unterauftragsverarbei-

tern. Der EDSA betont, dass insbesondere IT-Lösungen oftmals die Übermittlung personenbezogener Daten in Drittländer implizierten und Verantwortliche insoweit besonders aufmerksam agieren müssten. Entsprechende Risiken ergeben sich dabei oftmals bei Produkten von Anbietern außerhalb der USA (z. B. Microsoft, Amazon, Google).

Sofern bestehende Vereinbarungen zur Auftragsverarbeitung Drittlandübermittlungen erlaubten und weder durch zusätzliche Maßnahmen ein angemessenes Datenschutzniveau gewährleistet werden könne noch eine der Ausnahmevorschriften des Art. 49 DSGVO einschlägig sei, hätten Datenexporteure allein die Möglichkeit, mit dem Auftragsverarbeiter eine ergänzende Vereinbarung zu treffen, um unzulässige Datenübermittlungen zu verhindern. Dies gelte sowohl mit Blick auf die USA als auch Datenübermittlungen in andere Drittländer. Anderenfalls dürfe eine Übermittlung der betreffenden personenbezogenen Daten nicht erfolgen.

Fazit

Die FAQ des EDSA bieten eine erste Hilfestellung für Datenexporteure. Dennoch liegt die Hauptverantwortung nun bei den Datenexporteuren selbst. Diese sollten bei Verwendung von Standarddatenschutzklauseln und BCR soweit möglich weitere technische und organisatorische Maßnahmen vorsehen, beispielsweise bestimmte Verschlüsselungen der übermittelten Daten. Bezüglich der Ausnahmevorschriften des Art. 49 DSGVO sollte eine restriktive Handhabung erfolgen, um nicht das Risiko der Unzulässigkeit von Datenübermittlung einzugehen.

Im Hinblick auf die Förderung einer einheitlichen Anwendung der DSGVO, insbesondere bezogen auf die Übermittlung personenbezogener Daten in Drittländer, obliegt es nun vor allem dem EDSA, für ein kohärentes Vorgehen aller Datenschutzbehörden zu sorgen. Dazu müssen weitergehende Fragen in Bezug auf die Anforderungen an Standarddatenschutzklauseln und verbindliche interne Datenschutzvorschriften sowie die Ausnahmevorschriften des Art. 49 DSGVO beantwortet werden. Bis zur Klärung dieser Fragen bestehen für verantwortliche Stellen gewisse Unsicherheiten im Umgang mit Datenübermittlungen. Es ist zu erwarten, dass die Datenschutzbehörden und der EDSA zu diesem Zweck zeitnahe weitere Stellungnahmen und Leitlinien veröffentlichen werden.

Autor: **Felix Meurer (Ass. iur.) ist wissenschaftlicher Mitarbeiter bei Orth Kluth Rechtsanwälte in Düsseldorf in der Praxisgruppe IT/IP/Datenschutz.**