datenschutzpraxis.ch

Factsheet zum Datenschutz bereitgestellt von Daniel Kettiger

Ungültigkeit des EU-US Privacy Shield und Ungenügen des CH-US Privacy Shield

Gemäss einem Urteil des Europäischen Gerichtshofs (EuGH) ist das EU-US Privacy Shield ungültig. Damit entfällt eine wichtige Grundlage für die Übermittlung von Personendaten aus EU und EWR in die USA. Das CH-USPrivacy Shield bietet nach Auffassung des EDÖB kein adäquates Datenschutzniveau. US-amerikanische Dienste dürfen gestützt auf die Privacy Shield Regimes ab sofort nicht mehr zur Bearbeitung von Personendaten von EU-Unternehmen und Schweizer-Unternehmen eingesetzt werden.

I. Das EU-US Privacy Shield

Angemessenes Datenschutzniveau

Personendaten dürfen von Unternehmen im EU-Raum und im EWR-Raum nur in Drittländer übermittelt werden, wenn dort ein angemessener Datenschutz gewährleistet ist (Art. 44 ff. DSGVO). Solche Drittländer sind beispielsweise die Schweiz oder die USA.

Ob ein angemessener Datenschutz gewährleistet ist, kann die Europäische Kommission (EU-Kommission) mittels eines so genannten „Angemessenheitsbeschluss“ feststellen. Die EU-Kommission stellt darin fest, ob ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen ein angemessenes Mass an Schutz personenbezogener Daten gewährleistet. Ein solcher Beschluss hat zur Folge, dass personenbezogene Daten aus den 28 EU-Mitgliedstaaten und den drei EWR-Mitgliedstaaten Norwegen, Liechtenstein und Island ohne weitere Beschränkungen – wie innerhalb der EU bzw. des EWR – in das betreffende Drittland übermittelt werden dürfen.

Für die USA stellte die EU-Kommission einen angemessenen Datenschutz nur unter der Bedingung fest, dass sich die Verarbeiter von Personendaten dem EU-US Privacy Shield unterworfen hatten.

Das EU-US Privacy Shield (auch EU-US-Datenschutzschild) besteht aus einem Abkommen zwischen der EU und den USA, das im Februar 2016 zustande kam, sowie dem zugehörigen „Angemessenheitsbeschluss“ der EU-Kommission (Durchführungsbeschluss 2016/1250 vom 12. Juli 2016).

Vorgänger: Safe Harbour-Regelung

Bereits zuvor – noch vor dem Inkrafttreten der DSGVO – bestand ein ähnliches Rahmenabkommen, die Safe-Harbor-Regelung.

Der Europäische Gerichtshof (EuGH) hat in seiner Entscheidung (C-362/14) vom 6. Oktober 2015 den betreffenden Beschluss der EU-Kommission für unwirksam erklärt. Damit konnten ab diesem Zeitpunkt Übermittlungen personenbezogener Daten aus Europa an Unternehmen in den USA nicht mehr auf die die Safe-Harbor-Regelung gestützt werden.

Das EU-US Privacy Shield ist die Antwort auf die Forderungen, die der Gerichtshof in diesem Urteil gestellt hatte. Nach der neuen Regelung unterlagen Unternehmen in den USA strengeren Auflagen zum Schutz der personenbezogenen Daten europäischer Bürgerinnen und Bürger, und das US-amerikanische Handelsministerium sowie die Federal Trade Commission (FTC) waren zu intensiveren Kontroll- und Durchsetzungsmassnahmen verpflichtet, u.a. durch eine

verstärkte Zusammenarbeit mit den europäischen Datenschutzbehörden. Im Rahmen der neuen Regelung verpflichteten sich die USA ausserdem, ihren Behörden den Zugriff auf personenbezogene Daten, die nach der neuen Regelung übermittelt werden, nur unter rechtlich ganz klar festgelegten Bedingungen, strenger Aufsicht und in begrenztem Umfang zu ermöglichen.

Funktionsweise des Privacy Shield

Das EU-US Privacy Shield umfasst die Grundsätze zum Datenschutz, die von den amerikanischen Unternehmen einzuhalten sind. Die US-amerikanischen Unternehmen tragen sich, ähnlich wie schon zuvor bei der Safe-Harbor-Regelung, in eine entsprechende Liste ein und verpflichten sich selbst dazu, die diesbezüglichen Datenschutzregelungen einzuhalten. Das Privacy Shield beruht somit auf einer Selbstdeklaration.

Die USA haben sich verpflichtet, die Liste der Mitglieder des Datenschutzschilds stets auf dem neuesten Stand zu halten und Unternehmen, die nicht mehr teilnehmen, zu streichen. Zuletzt hatten sich rund 5'400 US-amerikanische Unternehmen bzw. Dienste am EU-US Privacy Shield beteiligt.

Den EU-Bürgerinnen und -Bürgern werden gegenüber den US-amerikanischen Unternehmen Ansprüche eingeräumt. Beschwerden müssten die Unternehmen innerhalb von 45 Tagen nachgehen. Im Streitfall gibt es ein Verfahren zur alternativen Streitbeilegung. Daneben können sich die Bürgerinnen und Bürger aber auch an ihre nationalen Datenschutzbehörden wenden, die gemeinsam mit der Federal Trade Commission Beschwerden nachgehen sollen.

II. Das CH-US Privacy Shield

Zwischen der Schweiz und den USA besteht ein annähernd gleiches, paralleles Regelungswerk, das Swiss-US Privacy Shield (CH-US Privacy Shield). An diesem sind rund 3'800 US-amerikanische Unternehmen bzw. Dienste beteiligt.

III. Das EuGH-Urteil

Inhalt und Bedeutung

Der EuGH hat in seinem Urteil (C-311/18) vom 16. Juli 2020 (Rechtssache Schrems II) den Beschluss 2016/1250 der EU-Kommission zur Übermittlung personenbezogener Daten in die USA (Privacy Shield) für unwirksam erklärt.

Zugleich hat der EuGH festgestellt, dass die Entscheidung 2010/87/EG der Kommission über Standardvertragsklauseln (Standard Contractual Clauses, SCC) grundsätzlich weiterhin gültig ist.

In seinem Urteil hielt der EuGH ausdrücklich fest, dass SCC in Bezug auf die USA wirksam sein können. Allerdings helfen SCC nur, wenn damit ein angemessener Datenschutz tatsächlich gewährleistet werden kann und nicht bloss pro forma vertraglich vereinbart wird.

Der EuGH begründete die Ungültigkeit des „Angemessenheitsbeschlusses" und damit des EU-US Privacy Shield mit den weitreichenden Überwachungsmöglichkeiten von US-amerikanischen Behörden bei gleichzeitig ungenügenden Rechtsbehelfen für betroffene Personen in der EU.

Im Gegensatz zu 2015, als die Safe-Harbor-Regelung für ungültig erklärt wurde, sollten betroffene Unternehmen nicht darauf hoffen, dass so schnell wieder eine Lösung gefunden wird wie damals.

Das Urteil des EuGH ist für die Schweiz nicht direkt anwendbar und hat keinen unmittelbaren Einfluss auf das CH-US Privacy Shield. Dieses gilt somit rechtlich betrachtet weiter.

Reaktionen anderer EU-Behörden

Der Europäische Datenschutzausschuss (EDSA) veröffentlichte am 23. July 2020 FAQ zum Schrems-II-Urteil des EuGH.

Der EDSA betont darin, dass die weitere Verwendung von Standardvertragsklauseln (SCC) nur dann. ausreichend ist, wenn der

Daten-Exporteur zuvor seine Hausaufgaben gemacht und die Datenschutzsituation auf der Grundlage der SCC sorgfältig analysiert hat.

Am 3. September 2020 tagte der EU-Ausschuss für bürgerliche Freiheiten, Justiz und Inneres unter anderem zur Frage, wie nach dem Schrems-II-Urteil weiter zu verfahren ist. Dabei nahmen der zuständige EU-Kommissär und die Vorsitzende des EDSA zum weiteren Vorgehen ihrer Behörden Stellung. Die EU-Kommission ist momentan daran, die Standardvertragsklauseln (SCC) zu überarbeiten und plant, nach erfolgtem Annahmeverfahren eine neue Fassung derselben bis Ende Jahr fertigzustellen. Der EDSA wird weitere Richtlinien und Arbeitshilfen (Guidelines) in Bezug auf Datenübermittlungen, die sich auch künftig auf die SCC stützen sollen, veröffentlichen, welche den Unternehmen als Orientierungshilfe zur Datenübermittlung in die USA dienen soll, damit diese im Einklang mit der DSGVO erfolgen.

IV. Die Evaluation des EDÖB

Vor dem Hintergrund seiner jährlichen Überprüfungen des CH-US Privacy Shield Regimes sowie der jüngsten Rechtsprechung des Europäischen Gerichtshofs (EuGH) zum Datenschutz evaluierte der Eidgenössische Datenschutz- und Öffentlichkeitbeauftragte (EDÖB) die Datenschutzkonformität des Privacy Shield Regimes neu. In seiner Stellungnahme vom 8. September 2020 kommt er zum Schluss, dass das Privacy Shield Regime trotz der Gewährung von besonderen Schutzrechten für Betroffene in der Schweiz kein adäquates Schutzniveau für Datenbekanntgaben von der Schweiz an die USA gemäss Bundesgesetz über den Datenschutz (DSG) bietet. Aufgrund dieser auf das schweizerische Recht gestützten Einschätzung hat der EDÖB in seiner permanenten Staatenliste den Verweis auf einen «angemessenen Datenschutz unter bestimmten Bedingungen» für die USA gestrichen.

Der EDÖB kommt – in Abweichung vom Urteil des EuGH – weiter zum Schluss, dass die auch in der Schweiz häufig verwendeten SCC der EU oder sog. «Binding Corporate Rules» den Zugriff auf Personendaten durch ausländische Behörden nicht zu verhindern vermögen, wenn – wie in den USA – das öffentliche Recht des Daten-Importstaates vorgeht und den behördlichen Zugriff auf die transferierten Personendaten ohne hinreichende Transparenz und Rechtsschutz der Betroffenen erlaubt. Dementsprechend muss davon ausgegangen werden, dass die SCC und vergleichbare Klauseln die Anforderungen an vertragliche Garantien nach Art. 6 Abs. 2 lit. a DSG für eine Datenübermittlung in die USA und andere nicht gelistete Staaten in vielen Fällen nicht erfüllen.

Die Beurteilung des EDÖB und die Streichung der USA von der Liste der Staaten mit adäquatem Datenschutz heben das CH-US Privacy Shield nicht auf. Das Abkommen wird dadurch nicht gekündigt. Die Beurteilung des EDÖB steht zudem unter dem Vorbehalt anderslautender Urteile von Schweizer Gerichten – diese sind nicht an die Einschätzung des EDÖB gebunden.

V. Auswirkungen auf Schweizer Unternehmen

CH-US-Privacy Shield gilt weiter

Das Urteil des EuGH ist für die Schweiz nicht direkt anwendbar und hat keinen unmittelbaren Einfluss auf das CH-US Privacy Shield. Dieses gilt somit rechtlich weiter.

Faktisch hat aber das EuGH-Urteil sehr wohl Auswirkungen auch auf das CH-US Privacy Shield. Die Argumentation des EuGH lässt sich weitgehend auch auf dieses Abkommen anwenden. Für Gerichte in der Schweiz würde es schwierig, in einem ähnlichen Fall wie jenem, der dem EuGH-Urteil zu Grunde lag, anders zu urteilen als das höchste europäische Gericht.

Die Beurteilung des EDÖB und die Streichung der USA von der Liste der Staaten mit

adäquatem Datenschutz heben – wie erwähnt – das CH-US Privacy Shield nicht auf. Unternehmen und betroffene Privatpersonen in der Schweiz können sich mithin gegenüber den US-amerikanischen Unternehmen immer noch auf das CH-US Privacy Shield berufen. Demgegenüber muss die Übermittlung von Personendaten durch Schweizer Unternehmen in die USA angesichts der Ungültigkeit des EU-US Privacy Shield und des Ungenügens des CH-US Privacy Shield von Grund auf neu beurteilt werden.

Auswirkungen auf Schweizer Unternehmen, die der DSGVO untersteht

Für Schweizer Unternehmen, die vollständig oder hinsichtlich bestimmter Aktivitäten der DSGVO unterstehen (Art. 3 Abs. 3 DSGVO), weil sie beispielsweise Endverbraucherinnen und -verbrauchern in der EU Waren oder Dienstleistungen anbieten oder im EU-Raum Marktbeobachtungen vornehmen, gilt das Datenschutzrecht der EU.

Für solche schweizerischen Unternehmen bedeutet das EuGH-Urteil folgendes:

- Die Übermittlung personenbezogener Daten in die USA auf der Grundlage des EU-US Privacy Shield ist unzulässig und muss unverzüglich eingestellt werden.
- Die meisten US-amerikanischen Internet-Dienste, die Daten von Personen im EU- bzw. EWR-Raum für europäische Unternehmen bearbeiten, beriefen sich bislang auf den EU-US Privacy Shield als Rechtsgrundlage bzw. als Rechtfertigungsgrund. Die Nutzung dieser Dienste ist rechtswidrig und muss eingestellt werden. Als Alternativen bieten sich allenfalls entsprechende Dienste europäischer Tochtergesellschaften mit Sitz und Servern im EU-Raum der US-Dienstleister an.
- Für eine Übermittlung personenbezogener Daten in die USA können die bestehenden Standardvertragsklauseln (SCC) der EU-Kommission zwar grundsätzlich weiter genutzt werden. Der EuGH betonte jedoch die Verantwortung des Verantwortlichen und des Empfängers, zu bewerten, ob die Rechte der betroffenen Personen im Drittland ein gleichwertiges Schutzniveau wie in der EU geniessen. Nur dann kann entschieden werden, ob die Garantien aus den SCC in der Praxis verwirklicht werden können.
- Die Wertungen des Urteils finden auch auf andere Garantien nach Art. 46 DSGVO Anwendung, wie verbindliche interne Datenschutzvorschriften („binding corporate rules“, BCR), auf deren Grundlage eine Übermittlung personenbezogener Daten in die USA erfolgt. Daher muss auch für Datenübermittlungen auf der Grundlage von BCR einer Prüfung unterzogen werden.
- Die Übermittlung von personenbezogenen Daten aus der EU in die USA nach Art. 49 DSGVO ist weiterhin zulässig, also beispielsweise gestützt auf eine ausdrückliche Einwilligung der betroffenen Person zur Übermittlung ihrer Daten oder weil die Übermittlung zur Vertragsabwicklung oder zur Durchsetzung von Rechtsansprüchen notwendig ist.

Verantwortliche, die weiterhin personenbezogene Daten in die USA übermitteln oder US-amerikanische Dienste nutzen möchten, müssen unverzüglich überprüfen, ob sie dies unter den genannten Bedingungen tun dürfen. Der EuGH hat keine Übergangs- bzw. Schonfrist eingeräumt.

In zahlreichen Informationen, die datenschutzrechtlich erforderlich sind, wird auf das EU-US Privacy Shield (als Rechtsgrundlage der Datenverarbeitung) hingewiesen. Beispiele dafür sind Datenschutzerklärungen und Auftragsverarbeitungsverträge. Hinweise auf das EU-US Privacy Shield sollten in Datenschutzerklärungen und Verträgen entfernt werden.

Auswirkungen auf Schweizer Unternehmen, die nicht der DSGVO unterstehen

Wie schon erwähnt, ist das CH-US Privacy Shield als Rechtsgrundlage bzw. Rechtfertigungsgrund für eine zulässige Übermittlung von Personendaten aus der Schweiz an einen Empfänger in den USA nicht mehr ausreichend. US-amerikanische Internet-Dienste, dürfen somit von Schweizer Unternehmen nicht mehr zur Verarbeitung von Personendaten verwendet werden, wenn sich der Datenaustausch bisher einzig auf das CH-US Privacy Shield abgestützt hat.

Die Standardvertragsklauseln werden zwar nicht aufgehoben, doch sind zusätzliche Massnahmen erforderlich. Der EDÖB empfiehlt den Schweizer Unternehmen, bei künftigen Übermittlungen von Personendaten in die USA oder andere nicht gelistete Staaten stets die geforderte Einzelfallprüfung mit besonderer Sorgfalt durchzuführen:

- Sollte sich die Datenbekanntgabe auf vertragliche Garantien wie die SCC in Verbindung mit Art. 6 Abs. 2 Bst. a DSG stützen, ist eine Risikoabschätzung vorzunehmen. Dabei prüft der Daten-Exporteur, ob die Klauseln die in dem nicht gelisteten Staat bestehen, die datenschutzrechtlichen Risiken abdecken. Gegebenenfalls sind die Klauseln zu ergänzen, wobei solche Ergänzungen im Falle eines derogatorischen Vorrangs des öffentlichen Rechts dieses Staates von beschränkter Wirkung sind, wie nachfolgend ausgeführt wird.
- Bei der Prüfung der datenschutzrechtlichen Risiken ist insbesondere relevant, ob die Daten an ein Unternehmen geliefert werden, das besonderen Zugriffen der dortigen Behörden unterworfen ist (z.B. US CLOUD Act; siehe dazu Factsheet Nr. 5). Weiter ist zu prüfen, ob die ausländische Empfängerpartei berechtigt und in der Lage ist, die zur Durchsetzung der schweizerischen Datenschutzgrundsätze nötige Mitwirkung zu leisten. Muss dies verneint werden, laufen die in den SCC vorgesehenen Mitwirkungspflichten ins Leere.
- Der schweizerische Daten-Exporteur muss in solchen Fällen technische Massnahmen prüfen, die den Behördenzugriff auf die übermittelten Personendaten im Zielland faktisch verhindern. Bei der Datenhaltung im Sinne eines reinen Cloud-Betriebs durch Dienstleister in den USA wäre z.B. eine Verschlüsselung denkbar, welche nach den Prinzipien BYOK (bring your own key) und BYOE (bring your own encryption) umgesetzt ist, so dass im Zielland keine Klardaten vorliegen und der Dienstleister keine Möglichkeit hat, die Daten selber aufzuschlüsseln. Bei über die reine Datenhaltung hinausgehenden Dienstleistungen im Zielland sind solche technischen Massnahmen weitgehend unmöglich. Soweit solche Massnahmen nicht möglich sind, empfiehlt der EDÖB auf die Übermittlung von Personendaten in die USA oder einen anderen nicht gelisteten Staat gestützt auf vertragliche Garantien zu verzichten.

VI. Fazit

Die Rechtslage für Unternehmen in der Schweiz kann hinsichtlich des Exports von Personendaten in die USA wie folgt zusammengefasst werden – unabhängig davon, ob das Unternehmen auch der DSGVO untersteht oder nicht:

- Das EU-US Privacy Shield ist ungültig und das CH-US Privacy Shield dient nicht mehr als Garantie im Sinne von 6 Abs. 2 DSG.
- Weiter muss davon ausgegangen werden, dass die SCC und vergleichbare Klauseln die Anforderungen an vertragliche Garantien nach Art. 6 Abs. 2 Bst. a DSG und nach EU-Recht für eine Datenübermittlung in die USA in den meisten Fällen nicht erfüllen, dies insbesondere wegen der Überwachungsgesetze der USA.
- Bei der Datenhaltung im Sinne eines reinen Cloud-Betriebs durch Dienstleister in den USA wäre als Massnahme, die

dem schweizerischen Datenschutzrecht und dem Datenschutzrecht der EU genügt, eine Verschlüsselung denkbar.

Wer auf Nummer sicher gehen möchte, verzichtet für die Verarbeitung von Personendaten auf die Nutzung von Internet-Diensten aus den USA. Konkret bedeute dies etwa den Verzicht

- auf das Führen von Telefongesprächen oder Videokonferenzen mit Skype, wenn Personendaten betroffen sind (z.B. Gespräche im medizinischen oder paramedizinischen Bereich oder im Personalwesen);
- auf Zoom-Videokonferenzen, wenn Personendaten betroffen sind (z.B. Gespräche im medizinischen oder paramedizinischen Bereich oder im Personalwesen);
- auf Mail-Chimp zur Versendung von Newslettern.