FAQ

Das Ende des Privacy Shields

Der Europäische Gerichtshof hat den Datenschutzbeschluss EU-US Privacy Shield für nichtig erklärt. Gibt es jetzt noch eine Rechtsgrundlage, um personenbezogene Daten legal in die USA zu transferieren?

Von Holger Bleich

Privacy Shield erklärt

Was genau war dieses Privacy Shield, das vom Europäischen Gerichtshof (EuGH) am 16. Juli 2020 für nichtig erklärt wurde?

Nicht erst, seitdem die EU-Datenschutz-Grundverordnung (DSGVO) im Mai 2016 in Kraft getreten ist, bedarf der Transfer von personenbezogenen Daten aus der EU in Drittstaaten einer Rechtsgrundlage. Der „Verantwortliche“, also in der Regel das transferierende Unternehmen, muss sicherstellen, dass die Daten am Ziel nach europäischen Datenschutzstandards gelagert und verarbeitet werden. Um dies in der Praxis möglich zu machen, prüft die EU-Kommission Staaten und erklärt jeweils mit einem „Angemessenheitsbeschluss“, dass sie diese Kriterien erfüllen. Derzeit gehören Andorra, Argentinien, Kanada, die Färöer-Inseln, Guernsey, Israel, die Isle of Man, Jersey, Neuseeland, die Schweiz, Uruguay und Japan zu diesen sogenannten sicheren Drittstaaten. In diese ist die Datenübermittlung daher ohne weiteres gestattet.

Die Vereinigten Staaten gehören nicht dazu, denn dort gewährt der Staat per Gesetz Ermittlungsbehörden und Geheimdiensten kaum zu kontrollierenden Zugriff auf personenbezogene Daten von EU-Bürgern sowie auf solche Daten, die in europäischen Rechenzentren von US-Konzernen gespeichert sind. Damit Daten trotzdem problemlos in die USA und an US-amerikanische Unternehmen fließen konnten, beschloss die EU-Kommission passende Regelungen im „Safe Harbour“-Abkommen. Bereits 2015 kassierte der EuGH im Urteil „Schrems I“ diesen Beschluss, weil er – wie sich herausstellte – ohne Faktengrundlage ein angemessenes Schutzniveau postuliert hatte.

Angetrieben von verunsicherten Konzernen entwickelte die EU eilig einen neuen Angemessenheitsbeschluss, damit die Daten weiterhin rechtens in die USA fließen konnten. Auf der Basis informeller Zusicherungen der Vereinigten Staaten entstand so das „EU-US Privacy Shield“. US-Konzerne wie Microsoft oder Google konnten sich selbst „zertifizieren“, also über einen Eintrag in eine Datenbank angeben, diese Zusicherungen einhalten zu wollen. Die Rechtslage in den USA hat sich seit den Snowden-Enthüllungen allerdings kaum verändert, sodass die Daten von EU-Bürgern genauso exponiert in den US-Rechenzentren lagen wie zuvor. Das Privacy Shield stand deshalb seit seinem Start Mitte 2016 auf tönernen Füßen.

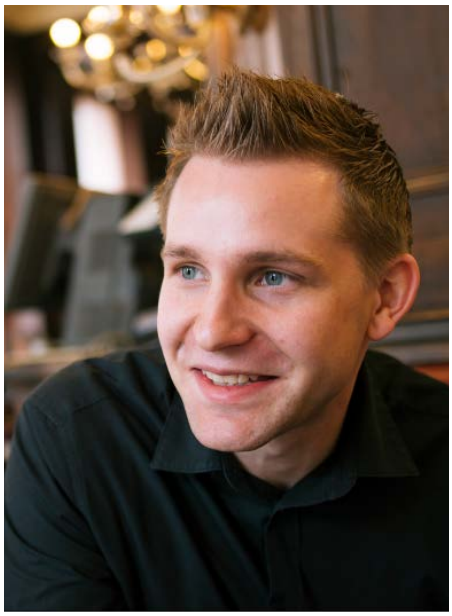


Foto: noyb.eu

Eine Auseinandersetzung des Datenschutzaktivisten Max Schrems (Bild) mit der irischen Datenschutzbehörde gipfelte im „Schrems-II-Urteil“ des EuGH.

Entscheidung mit Folgen

Was hat der EuGH entschieden? Es ist oft die Rede davon, dass es ja „Standardvertragsklauseln“ gibt, die nun das Privacy Shield ersetzen. Stimmt das?

Der EuGH hatte im sogenannten Schrems-II-Urteil eigentlich gar nicht über das Privacy Shield zu entscheiden. Im konkreten Fall ging es um Transfers personenbezogener Daten von europäischen Facebook-Kunden in die USA. Facebook sicherte diese Transfers aber nicht unter Berufung auf das Privacy Shield, sondern über EU-Standardvertragsklauseln ab. Dennoch hat sich der EuGH mit dem Privacy Shield beschäftigt und diesen Beschluss für europarechtswidrig und damit nichtig erklärt.

Nun kommt es also auf die von der EU-Kommission vorformulierten Standardschutzklauseln (SCC) an, die der EuGH im selben Urteil nicht grundsätzlich ablehnt. Gemäß Art. 46 DSGVO können diese oft in Verträgen zwischen EU-Dependance und US-Zentrale genutzten Zusatzklauseln in Betracht kommen.

Allerdings gibt es ein großes „Aber“: Der EuGH hat betont, dass es in der Verantwortung des Datenexporteurs liegt, zu prüfen, ob die Rechte der betroffenen Personen im Drittland ein gleichwertiges Schutzniveau wie in der EU genießen. Im Einzelfall müssen gegebenenfalls zusätzliche Maßnahmen sicherstellen, dass das garantierte Schutzniveau dem der EU im Wesentlichen gleichwertig ist.

Doch da die US-Regierung in ersten Konsultationen nach dem Urteil kaum den Willen zeigt, das Schutzniveau von EU-Bürgern in den USA zu erhöhen, könnten auch Anpassungen der SCC ins Leere laufen. De facto ist derzeit auf Basis der SCC ein DSGVO-konformer Datentransfer in

© Copyright by Heise Medien.
Persönliches PDF für alle Leser der c't aus 30625 Hannover

die USA kaum möglich. Änderungen könnten sich eventuell nach der US-Präsidentschaftswahl am 3. November ergeben. Zumindest bis dahin ist die Situation festgefahren und höchst brisant.

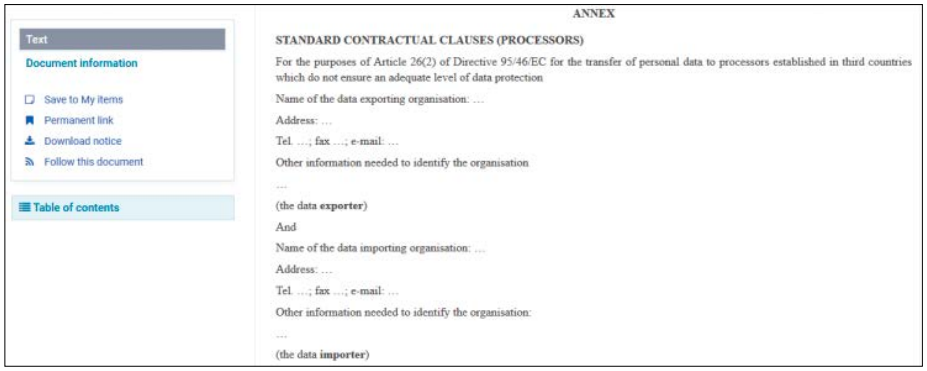
Standardschutzklauseln schwer anwendbar

Welche praktischen Konsequenzen ergeben sich aus dem Wegfall des Privacy Shields für Unternehmen, die personenbezogene Daten in die USA transferieren?

Sollten sie sich für den Datentransfer noch auf das Privacy Shield als Rechtsgrundlage berufen, müssen sie ihn sofort stoppen und ihre Datenschutzerklärungen anpassen. Auch der Einsatz der Standardschutzklauseln steht infrage. Maßgeblich ist, wie es die fürs Unternehmen zuständige Aufsichtsbehörde sieht. In Deutschland sind das in der Regel die Landesdatenschutzbehörden. Einige der Behörden haben bereits klargestellt, dass sie das Urteil restriktiv auslegen und danach handeln werden.

Beispielsweise teilte der Landesdatenschutzbeauftragte Baden-Württembergs mit: „Eine Übermittlung auf Grundlage von Standardvertragsklauseln ist zwar denkbar, wird die Anforderungen, die der EuGH an ein wirksames Schutzniveau gestellt hat, jedoch nur in seltenen Fällen erfüllen.“ Der Europäische Datenschutzausschuss EDSA hatte sich bereits kurz nach Verkündung des Urteils ähnlich geäußert: Nur wenn ein ausreichendes Schutzniveau garantiert werden kann, ist eine Berufung auf die SCC möglich. Dies könnte beispielsweise sein, wenn alle Daten vor dem Transfer so verschlüsselt werden, dass sie dem Zugriff von US-Behörden wirksam entzogen sind.

Facebook hat bereits zu spüren bekommen, was die Auslegung der Datenschutzbehörden in der Praxis bedeutet: Per einstweiliger Anordnung hat die irische Datenschutzbehörde (DPC) der europäischen Niederlassung des US-Konzerns am 10. September untersagt, Daten von EU-Bürgern in die USA zu transferieren, solange sie sich dabei auf die Standardschutzklauseln beruft. Postwendend stützt sich Facebook nun auf eine angebliche „Notwendigkeit“ der Datenübertragung gemäß Artikel 49 DSGVO. Rechtlich dürfte diese Argumentation kaum haltbar sein, der Konzern verschafft sich damit aber Zeit.



Die Standardschutzklauseln (SCC) lassen sich per Cut & Paste aus dem EU-Dokument 2010/593 in den eigenen Auftragsverarbeitungsvertrag kopieren. Doch nach dem Schrems-II-Urteil ist unklar, ob das noch ausreicht.

Hohe Bußgelder drohen

Welche Strafen drohen Unternehmen, die sich nicht an das EuGH-Urteil halten und verhängte Transferverbote der Aufsichtsbehörden unterlaufen?

Die EU-Aufsichtsbehörden sind nach Art. 83 DSGVO gehalten, in solchen Fällen verhältnismäßige und abschreckende Bußgelder zu verhängen. Dies können bis zu 20 Millionen Euro oder im Fall eines Unternehmens bis zu 4 Prozent des gesamten weltweit erzielten Jahresumsatzes des Mutterkonzerns im vorangegangenen Geschäftsjahr sein.

Verträge prüfen

Was sollten Unternehmen jetzt tun?

Sie sollten alle Verarbeitungsprozesse daraufhin abklopfen, ob dabei Daten in die USA gelangen, etwa zu Auftragsverarbeitern. Die entsprechenden Auftragsverarbeitungsverträge sollten Sie nach der neuen Rechtslage juristisch prüfen und anpassen lassen. Sollte kein rechtskonformer Datentransfer möglich sein, ist er sofort zu stoppen.

Für Unternehmen, die Verträge mit Dependancen von US-Unternehmen innerhalb der EU geschlossen haben, ist die Lage nicht ganz so dringlich, sofern sie Daten nur zu Servern dieses Unternehmens innerhalb der EU transferieren. Nach derzeitigem Stand ist man nicht dafür verantwortlich zu machen, dass ein Dienstleister seinerseits die Daten in die USA transferiert. Das betrifft beispielsweise die Cloud- und Kommunikationsdienste von Microsoft.

Beschwerde einlegen

Ich beobachte, dass mein Lieblings-Newsportal weiterhin Google Analytics einsetzt, YouTube-Videos einbindet und Facebooks Social-Plug-ins nutzt. Alle diese externen Services übertragen doch personenbezogene Daten in die USA. Wie kann ich mich wehren?

Sie sollten sich an den Betreiber wenden und fragen, auf welcher Rechtsgrundlage er diese Services einsetzt. Genügt Ihnen die Antwort nicht, können Sie Beschwerde bei der für Sie zuständigen Datenschutzbehörde einlegen.

Privat ist erlaubt

Sollte ich nun auch privat US-Dienstleister meiden?

Der Transfer der eigenen persönlichen Daten in die USA ist von dem Urteil nicht betroffen. Er geschieht aus Ihrem Willen und in „informationeller Selbstbestimmung“. Allerdings bleibt es meist nicht bei der Speicherung der eigenen Daten. Nutzen Sie beispielsweise Google Mail, speichert der US-Dienst auch die Daten Ihrer Korrespondenzpartner. Ähnlich verhält es sich mit Messengern oder Videokonferenzen. Besser ist es also, auf europäische Dienste zurückzugreifen. *(hob@ct.de)*

© Copyright by Heise Medien.
Persönliches PDF für alle Leser der c't aus 30625 Hannover