Alert

Breaking News
von
Blum&Grob
RECHTSANWÄLTE

Zürich, September 2020

"Privacy Shield" als ungenügende Rechtsgrundlage für Datentransfers in die USA

Am 16. Juli 2020 hat der Europäische Gerichtshof (EuGH) den EU-US "Privacy Shield" zu Fall gebracht. Nach dem "Safe Harbor"-Datenschutzabkommen ist nun auch der Privacy Shield aufgrund eines Urteils des EuGH für die EU ungültig. Damit hat der EuGH für viele Unternehmen eine wesentliche Grundlage für Datentransfers zwischen der EU und den USA für unwirksam erklärt. Auch der Schweizer Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) hat sich nun diese Woche zur Sache geäussert: Er hält den Privacy Shield ebenfalls für ungenügend.

Hintergrund

Im Oktober 2015 hatte der EuGH auf Klage des österreichischen Aktivisten Max Schrems den Entscheid der EU-Kommission aufgehoben, welcher das Safe Harbor Abkommen als Grundlage für einen genügenden Datenschutz in den USA bezeichnet hatte (wir berichteten im November 2015 dazu). Der EuGH kam damals zum Schluss, die US-Gesetze würden vor einem unberechtigten Zugriff oder Missbrauch von Daten nicht genügend schützen, was auch durch das Abkommen nicht verhindert werde. In der Folge hatten sich der EDÖB und darauf der Bundesrat dieser Meinung angeschlossen. Im Sommer 2016 (EU) bzw. Frühjahr 2017 (CH) ersetzte dann ein neuer Rahmenvertrag das Safe Harbor Abkommen, nämlich der sog. Privacy Shield (wir berichteten im April 2017). Er sollte wesentliche Verbesserungen gegenüber dem Safe Harbor Abkommen bringen.

EuGH-Urteil

Am 16. Juli 2020 hat allerdings der EuGH – wiederum auf Klage von Max Schrems – auch den EU-US Privacy Shield zu Fall gebracht. Dies aufgrund der weitreichenden Zugriffsmöglichkeiten von US-Behörden auf die Daten der Europäer (bzw. Nicht-US-Bürgern), (auch) ohne gerichtlichen Beschluss. Der EuGH legt dar, die amerikanische Überwachungspraxis sei nicht auf das zwingend erforderliche Mass begrenzt und Betroffene könnten ihre vorgesehenen Rechte nicht gerichtlich durchsetzen. Die Ungültigkeit des Privacy Shield in der EU wirkt ab sofort.

Stellungnahme des EDÖB

Laut dem EDÖB ist das EuGH-Urteil für die Schweiz nicht direkt anwendbar. Trotzdem hat es auch Auswirkungen für die Schweiz. Der EDÖB weist in seiner Stellungnahme vom 8. September 2020 darauf hin, dass der Privacy Shield auch aus schweizerischer Sicht Kritikpunkte aufweise, was er auch wiederholt betont habe. Aus diesem Grund ist er der Ansicht, dass der Privacy Shield die Anforderungen an den Datenschutz nicht erfüllt. Natürlich haben die Gerichte das letzte Wort, wobei allerdings damit zu rechnen ist, dass die Gerichte wohl zum gleichen Schluss kämen.

Folgen & Risiko

Mit diesem Entscheid kann man sich bei Transfers von Personendaten an Empfänger in den USA nicht mehr ohne Risiko auf den Privacy Shield abstützen. Es können (zumindest in der EU) Massnahmen von Datenschutzbehörden drohen, inkl. Bussgelder unter der EU-Datenschutzgrundverordnung (DSGVO), bis zu 4% des weltweit erzielten Jahresumsatzes, oder auch Abmahnungen von Betroffenen und von Mitbewerbern oder Datenschutzorganisationen. Dies ist von Unternehmen in der Schweiz, auf welche die DSGVO Anwendung findet, zu berücksichtigen (wir haben im November 2017 dazu berichtet).
In der Schweiz drohen aktuell v.a. vertragliche Risiken (Vertragsverletzung). Wer amerikanische Dienste einsetzt, riskiert z.B. ein Vorgehen von Vertragspartnern, wenn er nicht in der Lage ist, einen angemessenen Datenschutz zu gewährleisten.

Alternative 1: Standardvertragsklauseln?

Abgesehen vom Privacy Shield gibt es noch andere Möglichkeiten für den rechtmässigen Datenaustausch mit Unternehmen in sog. unsichere Drittstaaten (z.B. USA) – etwa die sog. Standardvertragsklauseln. Diese helfen aber nur, wenn damit ein angemessenes Datenschutzniveau tatsächlich gewährleistet werden kann. Sie können also verwendet werden, müssen aber hinsichtlich der Einhaltung im Empfängerland bzw. des Aspektes der behördlichen Zugriffsrechte im Zielland überprüft werden. Wenn das Recht des Importstaates den behördlichen Zugriff auf die transferierten Personendaten ohne hinreichende Transparenz und Rechtsschutz der Betroffenen erlaubt,

genügen die Standardvertragsklauseln nicht – meint auch der EDÖB.

Alternative 2: Verschlüsselung
Laufen die Standardvertragsklauseln ins Leere, muss der schweizerische Datenexporteur technische Massnahmen prüfen, die den Behördenzugriff auf die übermittelten Personendaten im Zielland faktisch verhindern. Bei der Datenhaltung im Sinne eines Cloud-Betriebs durch Dienstleister in einem datenschutzrechtlich unsicheren Drittstaat wäre gemäss EDÖB z.B. eine Verschlüsselung denkbar, welche nach den Prinzipien BYOK (bring your own key) und BYOE (bring your own encryption) umgesetzt ist. So liegen im Zielland keine Personendaten vor und der Dienstleister hat keine Möglichkeit, die Daten selber aufzuschlüsseln. Allerdings gestaltet sich der Einsatz solcher technischen Massnahmen bei über die reine Datenhaltung hinausgehenden Dienstleistungen im Zielland als anspruchsvoll. Soweit solche Massnahmen nicht möglich sind, empfiehlt der EDÖB auf die Übermittlung von Personendaten in unsichere Drittstaaten (wie bspw. die USA) einzig gestützt auf vertragliche Garantien zu verzichten.

Alternative 3: Einwilligung
Eine weitere Alternative wäre das Einholen von Einwilligungen der betroffenen Personen, wobei die Hürde für eine rechtswirksame Einwilligung hoch ist. Die Betroffenen müssen transparent auf den Einsatz von US-Dienstleistern und die konkreten Risiken, namentlich nicht adäquates Datenschutzniveau, hingewiesen werden. Diese "Alternative" dürfte in vielen Fällen mit grossem Aufwand verbunden sein. Zu beachten ist, dass eine Einwilligung auch jederzeit widerrufen werden kann.

Alternative 4: CH oder EU-Server
Gewisse US-Anbieter, wie z. B. Amazon Web Services (AWS), Microsoft oder Google, bieten die Möglichkeit an, Personendaten auf EU-Servern zu speichern. Ob eine solche Speicherung in Europa oder in der Schweiz genügt, wenn ein Dienst aus den USA genutzt wird, ist jedoch umstritten.

Handlungsbedarf
Verträge und Datenschutzerklärungen sollten angepasst und allfällige Hinweise auf den Privacy Shield entfernt werden. Unternehmen, die Datentransfers in die USA gestützt auf den Privacy Shield tätigen, sollten die Übermittlungen so rasch als möglich auf eine andere rechtliche Grundlage stellen. Allein die Standardvertragsklauseln bilden in der Regelkeine genügende Grundlage mehr; vielmehr wäre deren Einsatz mit technischen Massnahmen wie die Verschlüsselung zu kombinieren. Sobald die Datenbearbeitung im unsicheren Drittland allerdings über die reine Datenhaltung hinausgeht, sprich die Personendaten vor Ort unverschlüsselt bearbeitet werden, müssen die Datentransfers ganz grundsätzlich überdacht werden.

Gerne unterstützen wir Sie bei einer Umsetzung und stehen Ihnen bei Fragen beratend zur Verfügung.

David Schwaninger, lic. iur., d.schwaninger@blumgrob.ch
Dr. André Wahrenberger, lic. iur., a.wahrenberger@blumgrob.ch
Stephanie Bruderer, M.A. HSG in Law, s.bruderer@blumgrob.ch
Michelle Merz, MLaw, m.merz@blumgrob.ch