Schrems II – Das Aus für die Datenübermittlung in die USA?

Der Europäische Gerichtshof das Privacy-Shield Abkommen mit den USA für ungültig erklärt. Dazu hat das European Data Protection Board Erläuterungen für die Zulässigkeit eines Datenexports in die USA und andere unsichere Drittländer herausgegeben. Damit ist die bisher übliche Praxis des Datenexports in vielen Fällen nicht mehr rechtens.

Was ist passiert.

Bisher war es gängige Praxis Dienstleister zur Verarbeitung personenbezogener Daten in den USA auf Grundlage des Privacy Shield Abkommens zu beauftragen und manchmal als doppelten Boden noch die Standardvertragsklauseln zu vereinbaren. Bei großen Anbietern konnten dazu noch verbindliche Unternehmensregeln bzw. Binding Corporate Rules (BCR) herangezogen werden. Wieder einmal hat der österreichische Jurist Maximilan Schrems gegen diese Praxis geklagt und wieder einmal hat er vor dem EuGH Recht bekommen. Mit dem Urteil Urteil C-362/18 ist das Privacy Shield Abkommen ungültig erklärt worden. Dazu kommt, wie das European Data Protection Board (EDPB) festgestellt hat, dass sowohl beim Datenexport in die USA als auch in andere unsichere Drittstaaten die Standardvertragsklauseln (Standard Contractual Clauses, SCC) und Verbindliche interne Datenschutzvorschriften (Binding Corporate Rules, BCR) genau geprüft werden müssen und, falls erforderlich, über andere Maßnahmen ein angemessenes Datenschutzniveau sichergestellt werden muss.

Datenübertragung in die USA

Die Gesetze der USA, im Besonderen Section 702 FISA und die Executive Order 12.333, erlauben es amerikanischen Behörden praktisch wahllos auf Daten von nicht-Amerikanern zuzugreifen ohne dass EU-Bürger die Möglichkeit haben ihre Rechte einzuklagen. An dieser Tatsache hat auch das Privacy Shield nichts geändert. Daher hat der EuGH es für ungültig erklärt. Auch eine Vereinbarung der SCC kann diesen Sachverhalt nicht ändern und der Europäische Datenschutzausschuss hat festgestellt, dass SCC nicht ohne Weiteres als Grundlage für einen Datenexport in die USA verwendet werden können. Gleiches gilt für die Rechtsgrundlage der BCR. Dazu möchte ich aus unser Kommunikation mit dem Bayerischen Landesamt für Datenschutzaufsicht zitieren:

> „Weder BCR noch SCC können daher "alleine", d.h. ohne zusätzliche Garantien, als Instrumente für Übermittlungen in die USA genutzt werden. Sondern das wäre nur dann möglich, wenn der Datenexporteur irgendwelche "zusätzliche Maßnahmen" finden kann, die dazu führen, dass die vom EuGH kritisierten zu weitgehenden Zugriffsrechte von US-Nachrichtendiensten nach FISA Section 702 und Executive Order 12.333 ausgeschlossen werden.

Welche „zusätzliche Maßnahmen“ dies sein können, ist jedoch uns, den Aufsichtsbehörden und vermutlich auch Ihnen unbekannt. Damit bleiben noch die Ausnahmen für bestimmte Fälle aus Art. 49 DSGVO. Diese sind jedoch Ausnahmeregeln und nicht unbedingt als Rechtfertigung für einen dauerhaften Datenaustausch geeignet. Verschiedene Organisationen haben trotzdem begonnen ihre Vereinbarungen auf diesen Art. 49 abzustellen. Sie sollten sich aber

bewusst sein, dass Sie sich bei solchen Vereinbarungen möglicherweise auf dünnem Eis bewegen.

Datenübertragung in andere unsichere Drittstaaten

Auch der Datenexport in andere unsichere Drittstaaten wurde in diesem Zusammenhang noch einmal beleuchtet. Auch hier ist es nicht alleine ausreichend sich auf die SCC oder BCR zu verlassen. Der EuGH hob hervor, dass es in der Verantwortung des Datenexporteurs und des Datenimporteurs liegt zu beurteilen, ob das vom EU-Recht geforderte Schutzniveau in dem betreffenden Drittland eingehalten wird. Ist dies nicht der Fall, sollten Sie prüfen, ob Sie zusätzliche Maßnahmen ergreifen können, um ein im Wesentlichen gleichwertiges Schutzniveau wie in der EU zu gewährleisten, und ob das Recht des Drittlandes diese zusätzlichen Maßnahmen nicht beeinträchtigt.

Was nun?

Mit dem EuGH Urteil ist es bis auf gewisse Ausnahmen oder bei ausdrücklicher Einwilligung der Betroffenen sehr schwierig geworden personenbezogene Daten in die USA zu übertragen. Die Ausnahmeregeln nach Art. 49 können in Einzelfällen geeignet sein. Wenn Sie sich auf diese Ausnahmeregeln abstützen wollen, sollten Sie dies mit Fachkundigen eingehend beleuchten und Ihre Überlegungen dazu umfassend dokumentieren. Nahezu alle wichtigen Anbieter von Cloud-Diensten haben jedoch mittlerweile Angebote, bei denen die Daten nur in der EU verarbeitet werden. Dies bietet Ihnen zumindest derzeit Rechtssicherheit – wenn auch zumeist zu einem gewissen Aufpreis. Es ist jedoch kein Geheimnis, dass die US Regierung auch auf Daten zugreifen möchte, die in Systemen von US Firmen die in der EU gespeichert sind. Ein erneuter Konflikt scheint hier vorprogrammiert.

Bei Datenübertragungen in andere unsichere Drittstaaten sollte in jedem Fall genau das Risiko für die Betroffenen bewertet und dokumentiert werden sowie geeignete Maßnahmen gegen diese Risiken getroffen werden. Die Vereinbarung von Standardvertragsklausen oder der Verlass auf Verbindliche interne Datenschutzvorschriften der US-Firmen ist alleine nicht ausreichend.

Sie haben noch Fragen? Gerne unterstütze ich und die Süd IT Sie bei offenen Fragen und helfen Ihnen Lösungen zu finden.

Weiterführende Informationen

1. EuGH C-362/18 - Der EuGH erklärt den Beschluss 2016/1250 über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes für ungültig. http://curia.europa.eu/juris/documents.jsf?num=C-311/18
2. FAQs des EDPB https://edpb.europa.eu/our-work-tools/our-documents/ovrigt/frequently-asked-questions-judgment-court-justice-european-union_en
3. Orientierungshilfe des LDI Baden-Württemberg: Was jetzt in Sachen internationaler Datentransfer? https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/08/Orientierungshilfe-Was-jetzt-in-Sachen-internationaler-Datentransfer.pdf

Kontakt

Falls Sie noch Fragen zu dem Thema haben freue ich mich auf Ihre Kontakt-aufnahme

Dr. Stefan Krempl
089 461 3505 12
krempl@sued-it.de

ISO/IEC 27001 Lead-Auditor, TÜV Rheinland u. Deutsche Auditoren eG, IT-Sicherheitskatalog Lead-Auditor & Fachexperte, TÜV Rheinland, Lead-Auditor für kritische Infrastrukturen gemäß §8a BSIG, ISO 22301 Lead Auditor, TÜV Rheinland, VdS-zertifizierter Berater für Cyber-Security, Datenschutzbeauftragter IHK, Datenschutzauditor ISO/IEC 27701