US-Cloud-Dienste nach Schrems II– Wie geht es weiter?

Der Europäische Gerichtshof hat das Privacy-Shield Abkommen mit den USA in dem sog. Schrems II Urteil für ungültig erklärt. Auch die Anwendung der EU-Standardvertragsklauseln oder von verbindlichen Unternehmensregeln hält das european data protecion board nicht für ausreichend. Die Aufsichtsbehörden gehen jetzt den nächsten Schritt und erwarten, dass auch Auftragsverarbeitungen durch Tochterfirmen von US-Unternehmen kritisch zu betrachten sind

Ausgangssituation

Die Situation, dass eine Übertragung personenbezogener Daten in die USA extrem schwierig bis nahezu unmöglich geworden ist, war Gegenstand unseres Newsletters von September[1]. Die meisten US-Cloud-Anbieter bieten daher Lösungen an, bei denen eine Verarbeitung ausschließlich in der EU zugesichert wird. So kann durch Abschluss geeigneter Verträge eine weitere Nutzung der Dienste von Google, Microsoft, Amazon, Salesforce, usw. zumindest formell auf eine rechtlich gültige Basis gestellt werden.

Schrems II – 2ter Akt

Nun kann es durchaus vorkommen, dass z.B. im Rahmen von Wartungsarbeiten personenbezogene Daten von der EU-Niederlassung in die USA übertragen werden. Auch Vertrags- oder Kundendaten könnten mit der US-Mutter ausgetauscht werden. Dazu ist zu befürchten, dass US-Behörden auf Daten zugreifen können, auch wenn diese in der EU gespeichert werden.

Die Datenschutzbehörden sind daher, nach eigener Kommunikation mit diesen, der Ansicht, dass verantwortliche Stellen ihre Auftragnehmer zu den Risiken befragen müssen, die sich aus der geschilderten Situation ergeben. Anderenfalls verstoßen sie gegen Ihre Pflichten Auftragnehmer angemessen zu prüfen (Art. 28 Abs. 1 DSGVO).

Sofern Sie Auftragsverarbeiter mit US-Mutterfirmen haben oder wenn die relevante Liste der Unterauftragnehmer solche Firmen enthält, sollten Sie diesen daher folgende Fragen stellen:

1) Ist es möglich, dass im Rahmen der Beauftragung personenbezogene Daten in Länder außerhalb der EU übertragen werden, für die keine Angemessenheitsbeschlusses nach Art. 45 DSGVO vorliegt (z.B. USA)?
2) Bestehen für Ihr Unternehmen Zusammenarbeitsverpflichtungen nach US Gesetzen wie Section 702 FISA oder Executive Order 12.333?
3) Falls eine solche Verpflichtung besteht, gab es in der Vergangenheit Anfragen von US Behörden auf Offenlegung personenbezogener Daten von EU Bürgern. Falls ja, wie häufig sind diese in der Vergangenheit erfolgt?
4) Haben Sie Sicherheitsmaßnahmen implementiert, mit deren Risiken für Betroffene reduziert werden? Dies kann sowohl Maßnahmen beinhalten, die einen unbemerkten Zugriff durch US-Behörden verhindern als auch Maßnahmen, die einen Zugriff gänzlich

[1] https://sued-it.de/unternehmen/news-presse/109-schrems-ii-das-aus-fuer-die-datenuebermittlung-in-die-usa

verhindern, wie z.B. End-to-End-Verschlüsselung oder Maßnahmen, die geeignet sind anderweitig das Risiko für Betroffene zu reduzieren.

Was nun?

Auf Grundlage der Antworten Ihrer Auftragnehmer oder Geschäftspartner müssen Sie dann die Risiken für Betroffene aufgrund des möglichen Zugriffs durch US-Behörden bewerten. Falls Sie die Aufsichtsbehörde fragt, wie und auf welcher Grundlage sie diese Risiken bewertet haben sollten dazu plausible Antworten vorliegen. Spätestens im kommenden Jahr ist zu erwarten, dass die Behörden ausgewählte Unternehmen dazu befragen werden.

Gerne unterstützen wir bei der Süd IT Sie bei der Bearbeitung der Fragen sowie der Durchführung einer Risikoanalyse.

Kontakt

Falls Sie noch Fragen zu dem Thema haben freue ich mich auf Ihre Kontaktaufnahme

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