

■ Datentransfer ohne Privacy

Über lange Zeit hielt er tapfer stand, der zurzeit so vielbesungene Privacy Shield. Als rechtliche Legitimation schützte er den Transfer personenbezogener Daten von der EU in die USA vor den hinterhältigen Angriffen überbesorgter Datenschutzorganisationen. So zumindest die Darstellung der für das Abkommen verantwortlichen Kommissionen und der Unternehmen dies- oder jenseits des Teichs, die lange davon profitierten. Unglücklicherweise zeigte sich die höchste juristische Instanz dieser Staatengemeinschaft ebenfalls nicht allzu überzeugt von der Sicherheit des Schutzschild: Am 16. Juli 2020 kippte der Europäische Gerichtshof nach einem jahrelangen Rechtsstreit den Privacy Shield.



Gab es zuvor noch eine gewisse Rechtsgrundlage zur Datenübertragung in die USA, wenn auch nur auf dem labilen Gebilde des amerikanischen Datenschutzes fußend, fischen viele Betriebe nun in trüben Gewässern. Schon mehr als zeitig machten laute Forderungen nach einem Ersatzabkommen die Runde – der Status quo solle wieder her, möglichst schon gestern. Dabei hat eine überhastete Reaktion beim Thema Datenschutzvereinbarung erst zu dieser verwirrenden Situation geführt, in der wir uns jetzt befinden.

Geschichte wiederholt sich

So wie Unternehmer und prominente Präsidenten verschiedenster Bundesverbände dem Privacy Shield nun nachtrauern, könnte der Laie ihn für einen Geniestreich des internationalen Datenschutzrechts halten. In Wahrheit handelte es sich beim Schutzschild bereits um den zweiten Versuch, einen personenbezogenen Datenfluss von der EU in die USA allgemeingültig zu legitimieren und eine Rechtsgrundlage für alle Unternehmen zu schaffen, die dies praktizieren. Unter dem Namen Safe Harbor ging bereits im Jahr 2000 sein Vorgänger an den Start. Es waren die Enthüllungen des ehemaligen CIA-Mitarbeiters Edward Snowden, die den angeblich sicheren Hafen zum Einsturz brachten.

Der Whistleblower deckte einen weitreichenden Überwachungsskandal auf und bewies damit die

beträchtliche Machtposition der US-amerikanischen Geheimdienste – inklusive der Möglichkeit eines Einblicks in Unmengen privater Daten. Schon der Safe Harbor hielt damals vor diesem Hintergrund keiner genaueren Rechtsprüfung stand und der EuGH erklärte das Abkommen im Jahr 2015 folgerichtig für nichtig.

Getrieben von den gleichen Sorgen wie heute, präsentierten die Datenschutzkommissionen beider Lager innerhalb eines Jahres den Ersatz unter dem klingvollen Namen Privacy Shield. Doch schon 2016 stand das neue Abkommen in der Kritik: Datenschützer bemängelten die immer noch zu großen qualitativen Differenzen zwischen der EU-DSGVO und dem Datenschutz der USA – der Privacy Shield übertünche nur die vielen Probleme, löse sie aber nicht.

Neues Abkommen, neues Glück

Nun besteht wieder einmal die Chance, aus der Geschichte zu lernen und es zukünftig besser zu machen. Mit einer erneut schnellen, aber dafür zu wenig durchdachten Präsentation eines Ersatzabkommens dürften wir uns spätestens in fünf Jahren wieder an der gleichen Diskussion erfreuen. Datenschutz vollumfänglich und konsequent durchzusetzen, erweist sich schon im Normalfall als komplexe Aufgabe – zusätzliche Komplikationen entstehen dann noch durch unterschiedliche Rechtsprechung auf den Gebieten der Ko-

Shield: So funktioniert`s!

operationspartner. Deshalb sollten sich die EU-Kommissionen dieses Mal genügend Zeit lassen und ein Abkommen erarbeiten, welches dem europäischen Datenschutzanspruch genügt. Um jeden Preis gilt es, einen weiteren Rechtsstreit und die damit einhergehende Unklarheit für alle Beteiligten zu vermeiden. Auch wenn dies für viele international operierende Unternehmen auf unbestimmte Zeit einige Unwegsamkeiten bedeuten kann und sie deshalb auf weniger komfortable Alternativen zurückgreifen müssen, hilft ein weiteres Debakel ähnlich dem des Privacy Shields vor allem auf lange Sicht niemandem weiter.

Altbewährtes aus der Schublade ziehen

Bis sich die rechtliche Lage wieder final aufklärt und der Transfer personenbezogener Daten so einfach vorstättengeht wie in der sorglosen Zeit vor dem EuGH-Urteil, müssen sich Unternehmen theoretisch jede Übermittlung einzeln bestätigen lassen. Ohne die Erlaubnis des Kunden und der zuständigen Datenschutzbehörde machen sie sich aufgrund mangelnder juristischer Legitimation strafbar. Schnelle Lösungen liefert in diesem Fall eine altbewährte Methode: Standardvertragsklauseln – seit jeher ohnehin die meistgenutzte Rechtsgrundlage bei Datentransfers in Drittländer – haben den strengen Blick des EuGH überlebt. Jedoch auch nur mit dem Zusatz einer genauen Prüfung der jeweiligen Behörden des Absenderlandes, weshalb die Luxemburger Richter eine Pflicht zur Vorlage der jeweiligen Klausel verhängten. Dies erfordert in der Praxis eine Neubewertung bereits im Einsatz befindlicher internationaler Datenflüsse. Es emp-

fehlt sich ein reger Kontakt mit diesen Institutionen, um Unklarheiten aus der Welt zu schaffen und anfallende Fragen direkt von den Profis beantworten zu lassen.

Auf der sicheren Seite

Ob ein rechtlich einwandfreier Datentransfer aus der EU in die USA jemals möglich sein wird, lässt sich nicht voraussagen – zu groß erscheinen die Unterschiede in Gesetzgebung und allgemeinem Datenschutzniveau. Die einfachste Methode erweist sich aber wie so oft als die beste: Zentralisierung. Mit einer Serverkonzentration gesamtheitlich auf deutschem, beziehungsweise europäischem, Boden umgehen Unternehmen nicht nur eine Abhängigkeit von der internationalen Rechtsprechung, sondern schützen die Daten ihrer Kunden auch vor unausgereiften Regelungen in potenziellen Drittländern. Denn seit Einführung der DSGVO stellt sich die EU im Bereich Datenschutz besser auf als alle vergleichbaren Rechtsgemeinschaften.

Als großer Schritt in Richtung einer solchen Unabhängigkeit von den USA könnte sich das Projekt Gaia-X erweisen. Dieser Aufbau einer sicheren und vertrauenswürdigen Dateninfrastruktur soll eine nie dagewesene Souveränität und Innovationsunabhängigkeit von Großkonzernen aus den USA und China garantieren. Ob Safe Harbor oder Privacy Shield – beide Abkommen sorgten zwar für eine deutliche Vereinfachung von interkontinentalen Geschäftsabläufen, aber waren datenschutzrechtlich nie wirklich tragbar. Nun besteht erneut die Möglichkeit, es besser zu machen.



Der Autor:



(C) cobra GmbH

Seit 2009 ist Jürgen Litz Geschäftsführer des Herstellers für Kundenmanagement-Software cobra GmbH mit Sitz in Konstanz. Basierend auf seinen langjährigen Erfahrungen im Bereich Kundenmanagement setzt er sich hier im Hinblick auf die EU-Datenschutz-Grundverordnung für ein positives Verständnis von Datenschutz und Datenchancen ein. Litz war zuvor acht Jahre lang Geschäftsführer Vertrieb und Marketing beim Markenartikler ADO-Goldkante. Nach seinem BWL-Studium in Köln begann er seine Karriere beim Computer-Händler comtech/escom.

✉ litz@wissensmanagement.net