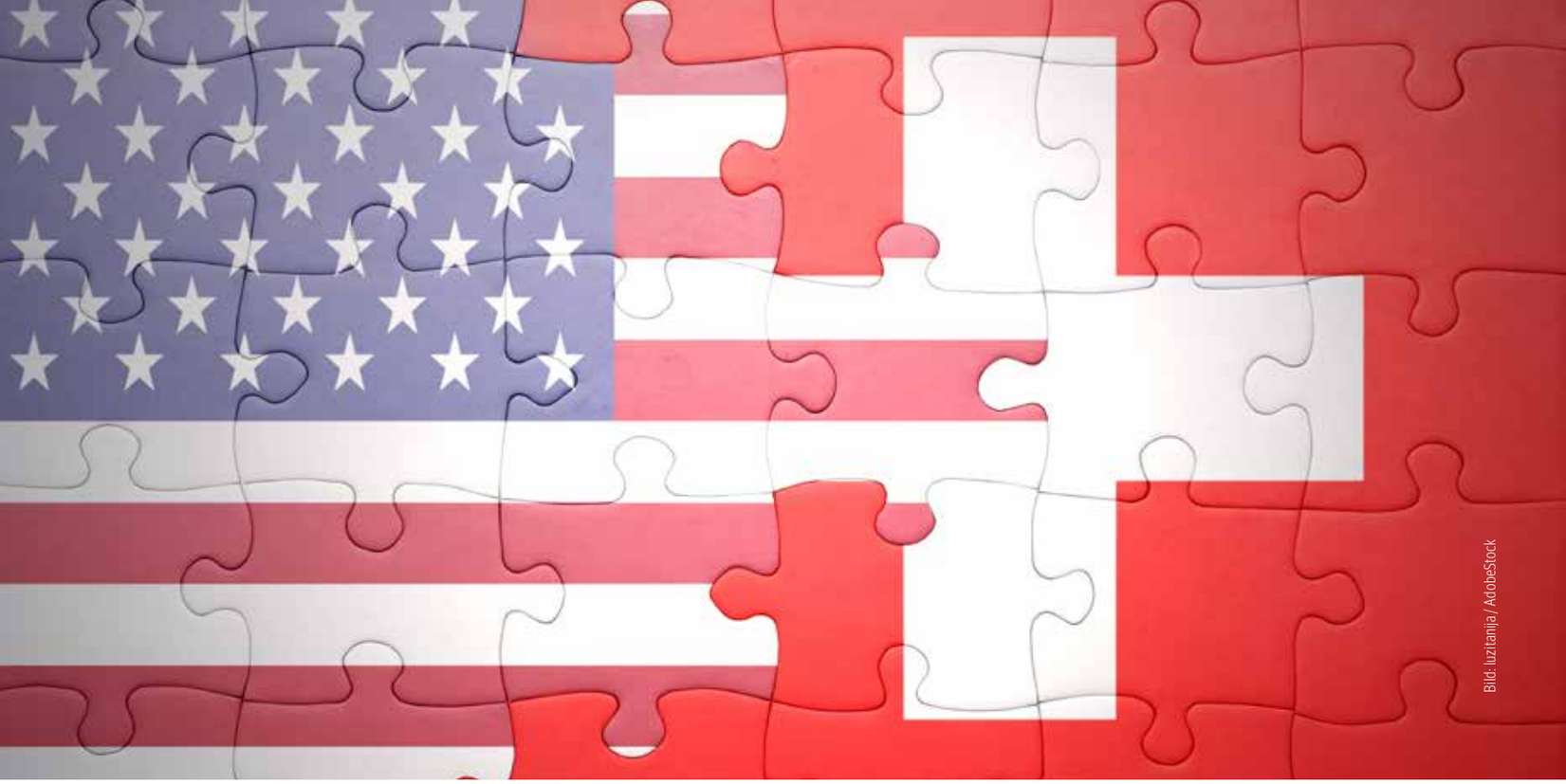

Bild: luzitanija / AdobeStock

Datenschutz-Gesetze und Zugriffe durch US-Behörden. Was betrifft mich das?

Der Durchblick bezüglich des Umgangs und Schützens von Personendaten ist komplex und schwierig. Eine Interpretation aus juristischer sowie aus Business-Sicht.

DIE AUTOREN

Andreas Dorta
Eigentümer Prewen

Clara-Ann Gordon
Rechtsanwältin für IT- und Datenschutz, Partnerin bei der Wirtschaftsanwaltskanzlei, Niederer Kraft Frey

Der Europäische Gerichtshof (EuGH) hat in seiner am 16. Juli 2020 veröffentlichten Entscheidung «Schrems II» die als Privacy Shield bekannte Rahmenvereinbarung zwischen den USA und der EU für ungültig erklärt. Dies bedeutet, dass das US-EU Privacy Shield keine genügende Rechtsgrundlage für einen Datentransfer in die USA darstellt. Das Privacy Shield ist ein US-Selbstzertifizierungsprogramm, bei dem US-Unternehmen öffentlich und verbindlich versprechen, sich an den Datenschutz nach europäischem beziehungsweise Schweizer Verständnis zu halten. Darüber hinaus äusserte der EuGH Zweifel daran, ob Standardvertragsklauseln (SCC) die Übermittlung personenbezogener Daten in die USA rechtfertigen können. Beide Mechanismen können einen Zugriff durch US-Behörden nicht verhindern.

Der EDÖB kam in seiner Stellungnahme vom 8. September 2020 im Hinblick auf das US-Swiss Privacy Shield zum gleichen Schluss und hat auf seiner Staatenliste den Verweis «angemessener Schutz unter bestimmten Voraussetzungen» für die USA gestrichen. Schweizer Unternehmen können daher ihre Datentransfers in die USA nicht mehr auf das US-Swiss Privacy Shield abstützen.

Entzug der Rechtsgrundlage

Die Hauptgründe für das als ungenügend erklärte Privacy Shield ist die Tatsache, dass personenbezogene Daten in den USA nicht ausreichend vor den US-Behörden geschützt sind und es keine hinreichenden Rechtsschutzmöglichkeiten für die betroffenen Personen gibt. Zum einen haben die US-Geheimdienste zu weitreichende Befugnisse, um auf Datenbestände zuzugreifen, insbesondere in Bezug auf Nicht-US-Bürger. Zum anderen können auch der beim US-Aussenministerium angesiedelte Ombudsmechanismus nicht als Rechtsschutz nach Massgabe der Europäischen Grundrechtecharta dienen. Schliesslich gibt es kein Datenschutzgesetz auf Bundesebene und die Behörden unterstehen daher nicht einem Datenschutzregime.

Konsequenzen für Firmen in der Schweiz

Unternehmen, die sich auf SCC und verbindliche unternehmensinterne Datenschutzvorschriften (sog. Binding Corporate Rules, BCR) stützen, sollten im Hinblick auf das Schrems-II-Urteil sowie die Stellungnahme des EDÖB prüfen, ob diese Mechanismen den Datenschutz ausreichend gewährleisten. Insbesondere bei Datenübermittlungen in die USA ist zu klären, ob die US-Behörden nach US-Recht ohne ausreichende Transparenz und ohne ausreichenden Rechtsschutz der Datensubjekte auf die übermittelten Daten zugreifen können. Sollte dies der Fall sein, bieten höchstwahrscheinlich weder die SCC noch die BCR eine gültige rechtliche Grundlage für die Datenübermitt-

lung. Grundsätzlich raten wir zur Umsetzung weiterer vertraglicher Verpflichtungen des Datenempfängers in den USA, das heisst durch eine Anpassung der geltenden SCC/BCR.

Nicht nur international tätige Firmen betroffen

Wichtig zu verstehen ist, dass es darauf ankommt, bei welchem Unternehmen die Daten gespeichert und verarbeitet werden. Immer mehr Unternehmen setzen auf eine Cloud-Strategie. Wir sprechen von tausenden Applikationen und Services wie beispielsweise Office 365 von Microsoft für die Office-Applikationen, Infrastruktur- und Plattform-Services von Amazon AWS, Microsoft Azure, Google. SaaS-Anwendungen (Software-as-a-Service oder Cloud-Applikationen) von Salesforce, Servicenow und viele, viele mehr. Die grosse Mehrheit dieser Applikationen wird durch US-Unternehmen betrieben. Somit sind Speicherung und Verarbeitung bei US-Unternehmen.

Technische Massnahmen, um lokale Gesetze zu erfüllen

Als Erstes sollten die Daten verschlüsselt werden. Datenzentrische Sicherheit ist ein Oberbegriff für verschiedene Methoden, welche die Daten in sich schützen. Bei diesen Methoden sind die Daten auch dann geschützt, wenn sie gestohlen wurden oder aus Versehen auf einem öffentlich zugänglichen System gespeichert werden. Zwei Lösungen für unterschiedliche Datentypen sind:

- Das Verschlüsseln, Anonymisieren, Pseudonymisieren oder Tokenisieren der Attribute in Applikationen und Datenbanken.
- Transparentes End-zu-End-Verschlüsseln von Dokumenten, E-Mails und Anhängen.

Der zweite Punkt ist das Schlüsselmanagement. Seine kostbaren Schätze im sichersten Tresor aufzubewahren ist gut. Aber was hilft es, wenn die Schlüssel nicht ebenfalls den bestmöglichen Schutz geniessen? Es empfiehlt sich, die Schlüssel in einem Hardware Security Modul (HSM) zu speichern. HSMs sind für die effiziente und sichere Ausführung kryptografischer Operationen oder Applikationen gebaut.

Eigene Verschlüsselungslösung als sicherste Lösung

Die sicherste Variante ist, die eigene Verschlüsselungslösung zu verwenden und auch die Schlüssel in einem eigenen HSM zu verwalten. Gleichzeitig gibt es Alternativen von Anbietern von Cloud-Services. Diese bieten integrierte Verschlüsselungslösungen an. Bildlich gesprochen steht der Safe dann beim Serviceprovider.

Die am wenigsten sichere Option ist, die Schlüssel beim Cloud-Service-Anbieter (z. B. Microsoft Azure) auf dessen Systemen zu erstellen und durch den Cloud-Service-Anbieter verwalten zu lassen. Wir empfehlen eine strikte Gewaltentrennung. Nie Schlüssel und Verschlüsselung vom selben Unternehmen zu verwenden. In diesem Fall wäre der Safe mit Daten beim Serviceprovider und gleichzeitig hat er auch den Schlüssel zum Safe.

Bild: hkama / AdobeStock

Bring your own Key (BYOK): Schlüssel werden in der eigenen Umgebung erstellt und danach in die Cloud-Service-Anbieter-Umgebung hochgeladen. Dazu sind zwei Dinge wichtig: Die Schlüssel sollen nur von der eigenen Tenant ID verwendet werden können. Es soll nicht mehr möglich sein, den Schlüssel aus dem HSM des Cloud-Service-Anbieter zu exportieren.

Hold your own Key (HYOK): HYOK ist die sicherste der drei Varianten. In diesem Fall werden die Schlüssel in eigenen HSM erstellt und verwaltet. Die Schlüssel sind zu keinem Zeitpunkt im Besitz oder Zugriff eines Cloud-Service-Anbieters. Hat der Kunde eine eigene IT-Infrastruktur, kann er die HSM selbst betreiben. Immer mehr Kunden wollen aber nichts mehr mit IT-Hardware zu tun haben, oder haben kein Know-how, wie HSMs implementiert oder betrieben werden. Managed HSM Provider bieten hier Alternativen.

Den vollständigen Artikel finden Sie online
www.netzwoche.ch

i MÖGLICHE LÖSUNGSANSÄTZE UND VORTEILE IM BEREICH BRING YOUR OWN ENCRYPTION (BYOE)

- Unternehmen, die sicherstellen wollen, dass auch Administratoren keine Einsicht auf Kundendaten in der eigenen Infrastruktur oder in IaaS und Paas haben.
- Lösungen, um Daten in Cloud-Applikationen zu schützen. Daten werden verschlüsselt, bevor sie im öffentlichen Netz sind. Diese Lösung eignet sich für KMUs. KMUs in der Schweiz sorgen sich in der Regel weniger um die Daten auf den eigenen Servern, verwenden aber immer mehr Cloud-Applikationen.
- Transparente Dokumentverschlüsselung für jede Art von Files. Dabei werden Document-Rights-Management-Lösung (DRM) verwendet. Bei Dokumenten geht es nicht nur um Zugriff, sondern auch ums Bearbeiten, Weiterleiten, Drucken oder anderweitiges Verwenden des Dokuments. DRM gibt es aber nicht für alle Arten von Dokumenten. Überwachung von Dokumenten ist aber möglich.
- Ende-zu-Ende-Verschlüsselung von E-Mails und den Anhängen jeglicher Grösse. Einfache Handhabung ist hier zentral. Auch das sichere Einreichen von Nachrichten und Dokumenten durch externe Personen, mit denen man noch Kontakt hatte, muss möglich sein.