integratio

Der zerbrochene Schild und die Schweiz

Ist die Übermittlung von Personendaten in die USA noch erlaubt?

Was Schweizer Unternehmen nach dem Privacy-Shield-Urteil beachten müssen

von *Henriette Baumann*

Am 16. Juli 2020 gab der Europäische Gerichtshof dem österreichischen Juristen Max Schrems Recht und kippte das Privacy-Shield-Datenschutzabkommen zwischen der EU und den USA. Der EU-US Privacy Shield bildete eine Rechtsgrundlage für Datenübermittlungen aus der EU[1] in die USA und wurde mit diesem Urteil mit sofortiger Wirkung für ungültig erklärt. Begründet hat der Europäische Gerichtshof das Urteil mit den weitreichenden Überwachungsmöglichkeiten von US-amerikanischen Behörden bei gleichzeitig ungenügenden Rechtsbehelfen für betroffene Personen in der EU. Gemessen an der EU-Grundrechte-Charta wurden die staatlichen Überwachungsmassnahmen der USA als unverhältnismässig eingestuft.

Ein annähernd gleiches Abkommen besteht zwischen der Schweiz und den USA: der Swiss-US Privacy Shield. Der Swiss-US Privacy Shield gilt nach wie vor. Jedoch hat der EDÖB (Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragter) mit Mitteilung vom 8. September 2020 erklärt, dass der Swiss-US Privacy Shield kein angemessenes Datenschutzniveau bietet. In der Argumentation lehnt sich der EDÖB an die Begründung des EuGH an.

Für den Schutz der persönlichen Daten und der digitalen Souveränität jedes einzelnen Bürgers wurde damit ein Erfolg erzielt. Aber welche Konsequenzen hat das Urteil für Schweizer Unternehmen?

1 Die Ausführungen gelten gleichermassen für die EWR-Staaten Norwegen, Island und Liechtenstein.

integratio

Hintergrund

Personendaten dürfen nur dann ins Ausland übermittelt werden, wenn dort ein angemessener Schutz dieser Daten sichergestellt werden kann. Ob in einem Staat ein angemessener Datenschutz gewährleistet ist, stellen staatliche Behörden oder Institutionen anhand von Angemessenheitsbeschlüssen fest. In der Schweiz führt der EDÖB eine Liste der Staaten, deren Gesetzgebung nach seiner Einschätzung einen angemessenen Datenschutz i.S. des Schweizer Datenschutzgesetzes (DSG) gewährleistet[2]. Für die EU stellt die EU-Kommission die Angemessenheit des Datenschutzniveaus eines Drittstaates fest[3].

Solche Länder mit angemessenem Datenschutzniveau sowohl aus Sicht der Schweiz wie auch aus Sicht der EU sind etwa Andorra, Argentinien, Kanada, die Färöer-Inseln, Guernsey, Israel, die Isle of Man, Jersey, Neuseeland und Uruguay.

Die USA fehlen jedoch auf den Listen der Schweiz und der EU. Für die Vereinigten Staaten erstellte die EU-Kommission deshalb im Jahr 2016 das "EU-US Privacy Shield"-Abkommen als Folge des vom Europäischen Gerichtshof im Jahr 2015 für unwirksam erklärten Safe-Harbor-Abkommen, das ebenfalls auf dem Klageweg durch Max Schrems gestürzt wurde. Im Jahr 2017 hat die Schweiz mit einem annähernd gleichen Abkommen, dem Swiss-US Privacy Shield, nachgezogen.

Sowohl der Swiss-US Privacy Shield wie auch der EU-US Privacy Shield definieren einen angemessenen Datenschutz in den USA nur dann als gegeben, wenn sich die amerikanischen Verarbeiter von Personendaten per Selbstdeklaration dem Abkommen unterwerfen. Privacy Shield beinhaltet Datenschutzgrundsätze, zu denen sich US-amerikanische Unternehmen verpflichten konnten, indem sie sich auf der Website des US-Handelsministeriums in eine Liste eintragen ließen (https://www.privacyshield.gov/list).

Bis zum Urteil des Europäischen Gerichtshofs (EuGH) vom 16. Juli 2020 war mit diesen Regeln ein Datentransfer von der EU in die USA wie innerhalb der EU möglich. Das EU-US Privacy Shield bildete die Rechts-

Glossar: FISA
Foreign Intelligence Surveillance Act

Section 702 des US-Geheimdienstgesetzes FISA erlaubt Geheimdiensten wie der NSA, ohne konkreten Verdacht und ohne Gerichtsbeschluss weitreichende Zugriffe auf Daten von Ausländern ("non-US persons"), die von US-amerikanischen Unternehmen wie beispielsweise Google und Telekom-munikationsanbietern erhoben wurden, auszuwerten. Danach dürfte die gesamte elektronische Kommunikation von und zur Zielperson sowie über die Zielperson abgefangen werden. Voraussetzung ist die Relevanz für Ermittlungen zur Terrorismusabwehr. Es erfolgt keine Einschränkung der Art der Daten.

Unter dieses Massenüberwachungsgesetz fallen US-amerikanische (Zitat in Originalsprache):

"electronic communication service provider:

A) telecommunications carrier
B) provider of electronic communication service
C) provider of a remote computing service
D) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored
E) an officer, employee, or agent of an entity described in A), B), C) or D)"

Damit fallen US-amerikanische Anbieter elektronischer Kommunikations- und Cloud-Dienste wie zum Beispiel Amazon AWS, Apple, AT&T, Dropbox, Microsoft, Facebook, Google, Yahoo und Verizon unter FISA 702. Ob ein US-Anbieter unter FISA 702 fällt, kann man direkt beim Anbieter erfragen.

2 "Staatenliste" des EDÖB: https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland.html

3 https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

grundlage für Datenübermittlungen aus der EU in die USA, doch das Urteil hat den EU-US Privacy Shield für unwirksam erklärt.

Begründet hat der EuGH das Urteil mit den weitreichenden Überwachungsmöglichkeiten von US-amerikanischen Behörden bei gleichzeitig ungenügenden Rechtsbehelfen für betroffene Personen in der EU. Gemessen an der EU-Grundrechte Charta wurden die staatlichen Überwachungsmassnahmen der USA als unverhältnismässig eingestuft.

Das EuGH-Urteil ist für die Schweiz rechtlich nicht verbindlich. Der Swiss-US Privacy Shield ist daher weiterhin gültig. Aufgrund der Beurteilung des EDÖB, der in seiner Mitteilung vom 8. September 2020 erklärte, dass der Swiss-US Privacy Shield kein angemessenes Datenschutzniveau mehr bietet und die USA von der Liste der Staaten mit angemessenem Datenschutz gestrichen hat, sollten Datenübermittlungen aus der Schweiz in die USA allein auf Basis des Swiss-US Privacy Shield im Regelfall nicht mehr durchgeführt werden. In seiner Argumentation lehnt sich der EDÖB an die Begründung des EuGH an. Die Einschätzung des EDÖB steht unter dem Vorbehalt einer abweichenden Rechtssprechung schweizerischer Gerichte.

Mit dem Urteil des Europäischen Gerichtshofes und der Beurteilung des EDÖB fällt die USA zurück in den Status eines Landes ohne Angemessenheitsbeschluss wie beispielsweise Indien, China oder Russland. Betrachtet man die engen Verflechtungen zwischen der Schweiz bzw. der EU und den USA und die stetig ansteigenden Datenübermittlungen nicht nur aber auch in US-Cloud-Dienste, Google oder Facebook, handelt es sich also um sehr weitreichende Entscheidungen.

Der Privacy Shield bildet jedoch nicht die einzige Rechtsgrundlage für Datenübertragung in die USA, sowohl das DSG wie auch die DSGVO bieten weitere Möglichkeiten für einen rechtskonformen Datentransfer in Länder ohne Angemessenheitsbeschluss. Für die Datenübermittlung in die USA bedeutet das, dass jede Übertragung daraufhin geprüft werden muss, ob eine andere gültige Rechtsgrundlage als der Privacy Shield vorliegt, so wie dies für alle anderen Länder ohne Angemessenheitsbeschluss auch vor dem Urteil erforderlich war und ist.

Auswirkungen auf Schweizer Unternehmen

Schweizer Unternehmen, die nicht der DSGVO unterliegen und Personendaten aus der Schweiz in die USA übermitteln, unterliegen ausschliesslich Schweizer Regelungen. Wie bereits ausgeführt ist das Swiss-US Privacy Shield noch gültig, aber als Rechtfertigungsgrund nicht mehr ausreichend.

Für Schweizer Unternehmen, die der DSGVO unterliegen, gelten zudem die Regelungen der EU. D.h. die Übermittlung von Personendaten, deren Verarbeitungen der DSGVO unterliegen, in die USA ist auf Grundlage des EU-US Privacy Shields nicht mehr zulässig.

In beiden Fällen müssen Massnahmen ergriffen werden, soll eine Übermittlung personenbezogener Daten in die USA durch- oder weitergeführt werden. Da sich der EDÖB mit seinen Empfehlungen stark an den Empfehlungen des EuGH und dem Europäischen Datenschutz-Ausschuss orientiert, kann weitgehend gleichförmig agiert werden. Die rechtlichen Hintergründe und Regelungen und die Sanktionen bei Verstössen weichen zwar voneinander ab, die de facto umzusetzenden Massnahmen jedoch unterscheiden sich nicht wesentlich. Die folgenden Ausführungen sind daher für beide Fälle anwendbar, soweit nicht explizit auf Abweichungen hingewiesen wird.

Betrachtet man den in der Praxis häufig auftretende Fall des EU-Auftragsverarbeiters eines Schweizer Unternehmens oder umgekehrt, kann man ersehen, dass die Parallelität der Massnahmen von erheblichem praktischen Nutzen sein kann.

integratio

Welche Daten sind in welcher Form betroffen?

Täglich werden heute riesige Mengen personenbezogener Daten aus der Schweiz und der EU an die USA übermittelt, nicht nur in multinationalen Konzernen. Auch kleinere Unternehmen speichern immer häufiger Daten in der Cloud, setzen Software US-amerikanischer Anbieter ein und bei der Kommunikation auf die großen Anbieter von sozialen Netzwerken. Webkonferenzsysteme wie Zoom oder Microsoft Teams, Sprachdienste von Amazon und Apple oder auch die Cookies und Tracker der Dienste zur Webseitenanalyse wie Google Analytics finden sich allerortens. Mit den Konsequenzen des Urteils beschäftigen muss sich deshalb jedes in der Schweiz und der EU ansässige Unternehmen, das personenbezogene Daten von Kunden, Partnern, Mitarbeitern, Lieferanten, Websitebesuchern oder sonstigen Personen in Länder ohne adäquaten Datenschutz übermittelt.

Die Verarbeitung personenbezogener Daten umfasst alle Vorgänge wie das Erheben, Erfassen, Ordnen, Speichern, Anpassen, Verändern, Auslesen, Abfragen, Offenlegen durch Übermittlung, Verbreitung, Abgleich, Verknüpfung, Einschränkung, Löschung oder Vernichtung. Es spielt also nicht nur eine Rolle, wo die Daten gespeichert sind, sondern auch, wo weitere Verarbeitungen stattfinden.

Die Datenübermittlung umfasst nicht nur den physischen „Export" der Daten. Auch jede Zugriffsmöglichkeit beispielsweise über Schnittstellen, Abrufmöglichkeiten oder Fernwartungszugänge sind ebenfalls als Datenübermittlung zu sehen.

Unternehmen, die aufgrund des Privacy-Shield-Urteils eine Bestandsaufnahme ihrer Datenübermittlungen durchführen, müssen also nicht nur ihre Datenbestände analysieren, sondern auch alle stattfindenden Verarbeitungen und Zugriffsmöglichkeiten.

Betroffen sind auch die Auslagerung von Datenverarbeitungen an ein US-Unternehmen, der konzerninterne Datentransfer an eine US-Muttergesellschaft, der Zugriff von US-Mutterkonzernen auf Daten von Konzerngesellschaften in der Schweiz oder der EU oder die Nutzung von US-Cloud-Diensten wie Amazon AWS oder Google Cloud.

Auch Cloud-Services von US-Anbietern, die personenbezogene Daten auf Servern ihrer Tochtergesellschaften in der Schweiz oder der EU speichern, müssen genau analysiert werden. Häufig finden spezifische Verarbeitungen trotzdem in den USA statt und die Daten werden dafür von der Tochtergesellschaft an die US-Muttergesellschaft in den USA übermittelt. Zudem können meist Zugriffe der US-Mutter- oder US-Konzerngesellschaft auf die in der Schweiz oder der EU befindlichen Daten bei den Tochtergesellschaften erfolgen. Diese Zugriffs- und Übermittlungsmöglichkeiten müssen vertraglich ausgeschlossen werden, was derzeit die meisten US-Konzerne nicht zusichern wollen oder können.

Auch Betriebsgeheimnisse wollen geschützt sein

Nicht zu unterschätzen sind Verarbeitungen sensibler Daten und Betriebsgeheimnisse wie Techniken, Rezepturen, Patente, Marktstrategien, Finanzdaten, Entwicklungs- und Forschungsdaten.

Diese Inhalte fallen zwar – sofern nicht personenbezogen – nicht unter das Datenschutzgesetz und sind daher nicht vom EuGH-Urteil und der Einschätzung des EDÖB betroffen. Je nach Wirtschaftszweig und Unternehmenstätigkeit sollte ein Unternehmen diese Datenbestände in die Analysen mit einbeziehen und das Risiko bewerten, inwieweit ein nicht ausreichendes Datenschutzniveau und weitreichende Überwachungs- und Zugriffsmöglichkeiten im Zielland dem Unternehmen schädlich werden können.

Auch Betreiber kritischer Infra-strukturen sehen sich hier grösseren Herausforderungen ausgesetzt.

integratio

Was ist zu tun?

Weil weder der EDÖB noch der Europäische Gerichtshof eine Übergangs- oder Schonfrist eingeräumt haben, müssen Unternehmen möglichst zeitnah mit ersten Massnahmen beginnen und diese Aktivitäten nachweisen können. In jedem Fall müssen Datenübermittlungen in die USA identifiziert und jede Datenübermittlung muss überprüft werden.

Analyse der Datenübermittlungen

Im ersten Schritt sollte ein Überblick über alle Datenströme, die personenbezogene Daten beinhalten, und die Betriebsstandorte der Datenverarbeitung verschafft werden. Das ist nicht nur für den Datenschutz relevant, sondern auch für die IT-Sicherheit, die Betriebssicherheit sowie Wartung und Support. Dabei muss die gesamte Software- und Service-Lieferkette nachvollzogen werden können.

Auf dieser Basis sollten alle Datenflüsse in die USA und weitere Länder ohne angemessenes Datenschutzniveau geprüft werden. Als verantwortliches Unternehmen ist man in der Pflicht, die Situation bei Dienstleistern bzw. Subunternehmen aufzunehmen.[4] Das umfasst auch Zugriffsmöglichkeiten durch Dritte, Verarbeitungen bei Auftragnehmern und deren Weitergabe von Daten an Dritte. Transparenz ist das oberste Gebot. Auch Dienstleister und Subunternehmen in der Schweiz und der EU müssen überprüft werden. Schweizer und europäische Anbieter können wiederum US-amerikanische Dienstleister als Subunternehmen in ihr Angebot einbinden oder personenbezogene Daten an Dritte in den USA übermitteln.

Dabei ist man darauf angewiesen, dass Dienstleister, Hersteller und Subunternehmen ihrer Informationspflicht vollumfänglich nachkommen und sämtliche Verarbeitungen offenlegen. Eine Überprüfung ist bei proprietären Closed Source[5]-Anbietern im Regelfall nicht vollumfänglich möglich.

Eine vollumfängliche Kontrollmöglichkeit bieten Open Source Lösungen durch den offengelegten Quellcode. Es lässt sich prüfen und sicherstellen - ggf. durch spezialisierte Experten - , dass keine rechtswidrigen Datenabflüsse erfolgen und die Daten nur für die zulässigen Zwecke verarbeitet werden. Aufsichtsbehörden empfehlen daher immer häufiger Open-Source-Lösungen als Alternative.

Nach dieser Bestandsaufnahme sollte für jede Datenübermittlung die Rechtsgrundlage bestimmt werden. Im folgenden zeigen wir die für Unternehmen wesentlichen Rechtsgrundlagen, Garantien und Massnahmen auf.

Gelegentliche notwendige Datenübermittlung

Datenübermittlungen, die in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags stehen, können auch weiterhin stattfinden. Diese und weitere zulässige Datenübermittlungen wie beispielsweise zur Wahrung des öffentlichen Interesses oder zur Ausübung von Rechtsansprüchen sind in Art. 6 DSG aufgeführt. Ebenso hat der EuGH in seinem Urteil ausdrücklich betont, dass durch die Aufhebung des EU-US Privacy Shield kein Rechtsvakuum entsteht, da unbedingt notwendige, gelegentliche Datenübermittlungen zur Erfüllung vertraglicher Leistungspflichten weiterhin stattfinden können. Diese Ausnahmen sind unter Art. 49 Abs. 1 DSGVO aufgeführt.

Damit können Datenübermittlungen wie Reisebuchungen, Kauf von Waren bei einem US-Unternehmen oder die Ausführung eines Zahlungsauftrags weiterhin durchgeführt werden. Erlaubt sind mit dieser Rechtsgrundlage Datenübermittlungen in jedes Land der Welt.

4 Die Non-Profit-Organisation NOYB (Europäisches Zentrum für digitale Rechte, www.noyb.eu) hat dafür Musterfragebögen zur Verfügung gestellt.

5 Closed Source Software: Der Quellcode der Software wird vom Hersteller nicht herausgegeben.

Nicht zur Anwendung kann diese Regelung kommen, wenn ein Unternehmen aus betrieblichen Gründen beispielsweise die gesamte Kundendatenverwaltung oder Schulungsplattformen in die USA auslagert, da es keinen unmittelbaren und objektiven Zusammenhang zwischen der Erfüllung des Kundenvertrags und einer solchen Übermittlung gibt.

Für Datenübermittlungen in die USA, die nicht unter diese Regelungen fallen, stehen mehrere Instrumente zur Verfügung, um die Datenübermittlungen rechtskonform zu gestalten. Diese sind im Folgenden aufgeführt.

Einholen einer Einwilligung

Grundsätzlich besteht die Möglichkeit, eine Einwilligung derjenigen Personen einzuholen, deren Daten in die USA übermittelt werden. Diese Option wird von den meisten Unternehmen erst dann eingesetzt, wenn sich keine andere Rechtsgrundlage eignet. Dafür gibt es zwei Gründe: Die Einwilligung des Betroffenen muss in Kenntnis der Sachlage erfolgen und nicht jedes Unternehmen möchte seine Kunden, Mitarbeiter oder Partner umfassend darüber informieren, dass deren Daten in einem Land verarbeitet werden, in dem kein adäquater Datenschutz gewährleistet werden kann. Zudem kann eine solche Einwilligung jederzeit widerrufen werden, was dann letztlich bedeuten würde, dass das Unternehmen den Datentransfer derjenigen Personen, die ihre Einwilligung widerrufen, sofort stoppen müsste. Das kann mit dem Verlust von Kunden einhergehen.

Anonymisierung

Die Anonymisierung der Personendaten vor der Datenübermittlung in die USA ist eine weitere Möglichkeit der rechtskonformen Übermittlung. Durch die Anonymisierung ist eine Identifikation von Personen durch den Empfänger nicht mehr möglich, die Persönlichkeitsrechte werden gewahrt und die Datenübermittlung unterliegt nicht mehr den Datenschutzgesetzen.

Das Fehlen des Personenbezugs kann Funktionalitäten einschränken und ist daher nicht in jedem Fall möglich. Das Anonymisierungsverfahren muss eine Re-Identifizierung ausschliessen.

Anwendung von Standarddatenschutzklauseln[6]

Nach Feststellung des Europäischen Gerichtshofes und des EDÖB sind Standarddatenschutzklauseln für die USA und alle weiteren Länder ohne angemessenes Datenschutzniveau nur noch bedingt verwendbar. Mit Standarddatenschutzklauseln lassen sich Vertragspartner vertraglich verpflichten, das Datenschutzniveau der Schweiz bzw. der EU sicherzustellen.

Allerdings nur, wenn es im Zielland kein kollidierendes Recht gibt. Folgerichtig ist in einer Einzelprüfung vom verantwortlichen Unternehmen in der Schweiz (Datenexporteur) zu überprüfen, ob die in den Standarddatenschutzklauseln enthaltenen vertraglichen Verpflichtungen für die Datenübermittlung tatsächlich umgesetzt werden können. Für die meisten Unternehmen in den USA ist dies gemäss der Feststellung des EuGH und des EDÖB nicht der Fall, denn US-Anbieter elektronischer Kommunikationsdienste und die meisten US-Clouds wie Apple, Google, Amazon AWS, Dropbox, Facebook, Microsoft fallen unter das US Geheimdienstgesetz Foreign Intelligence Surveillance Act (FISA 702 – siehe Kasten).

Selbst wenn US-Anbieter Serverstandorte in der Schweiz und der EU anbieten, muss in einer Einzelfallprüfung belegt werden, dass aus den USA keine Zugriffsmöglichkeiten auf die Daten bestehen. Da diese Beschränkung die US-Unternehmen in ihrem Geschäftsmodell beschneidet und technisch häufig

6 Oftmals auch als «Standardvertragsklauseln» bezeichnet.

nicht umgesetzt ist, kann man nicht von einer Rechtskonformität bei Schweizer oder EU-Tochtergesellschaften von US-Unternehmen ohne Einzelfallprüfung ausgehen.

Solche Einzelfallprüfungen sind aufwändig müssen regelmässig wiederholt werden, um das Ergebnis zu verifizieren. Es sind Kenntnisse über das Rechtssystem und die Zugriffsmöglichkeiten der Behörden im Zielland erforderlich. Zudem sind detaillierte Angaben und Zusicherungen des Datenimporteurs im Zielland erforderlich über dessen Verarbeitungen, IT-Systeme und Massnahmen, die nicht in jedem Fall herausgegeben werden und auch nicht in jedem Fall überprüft werden können. Hier empfiehlt es sich, Experten hinzuzuziehen.

Ergibt die Einzelfallprüfung, dass die Standarddatenschutzklauseln keine ausreichende Garantie darstellen, um ein angemessenes Datenschutzniveau zu gewährleisten, muss das verantwortliche Unternehmen zusätzliche Garantien bieten.

Zusätzliche Garantie: Verschlüsselung

Eine mögliche und sowohl vom EDÖB wie auch von EU-Aufsichtsbehörden empfohlene Massnahme wäre die Verschlüsselung der Personendaten, welche nach den Prinzipien BYOK (bring your own key) und BYOE (bring your own encryption) umgesetzt ist, sodass der Dienstleister oder andere Akteure keine Möglichkeit haben, die Daten zu entschlüsseln. Allerdings sind viele US-Dienste mit verschlüsselten Daten in ihrer Funktion nur eingeschränkt nutzbar, etwa bei Suchalgorithmen oder Analysefunktionen.

Zusätzliche Garantie:
Ergänzende vertragliche Bestimmungen

Eine alternative Massnahme sind ergänzende vertragliche Bestimmungen, die zusätzlich zu den Standarddatenschutzklauseln den Datenimporteur in den USA noch strenger zur Einhaltung des Datenschutzes verpflichten. Solch individuellen Bestimmungen benötigen meist eine Vorlaufzeit wegen der Genehmigungsvorgabe und unterliegen den gleichen Anforderungen an die Einzelfallprüfung wie die Standarddatenschutzklauseln. Deshalb stellen sie für kleine und mittlere Unternehmen meist keine Alternative dar.

Zudem können ergänzende vertragliche Regelungen zwischen Datenexporteur und US-Datenimporteur US-Behörden genau wie die Standardvertragsklauseln nicht binden, d.h. der Zugriff durch ausländische Behörden kann nicht verhindert werden, wenn das öffentliche Recht des Ziellandes vorgeht und den behördlichen Zugriff auf die übermittelten Personendaten ohne hinreichende Transparenz und Rechtsschutz der Betroffenen erlaubt.

Glossar: Standarddatenschutzklauseln

EU-Standarddatenschutzklauseln sind von der EU-Kommission genehmigte Vertragsklauseln, die unverändert in das Vertragswerk der Vertragspartner (Datenexporteur in der Schweiz bzw. in der EU/EWR und Datenimporteur in einem Drittland ohne angemessenen Datenschutz) eingebunden werden. Mit ihnen verpflichtet sich der Datenimporteur, ein Schutzniveau sicherzu-stellen, das dem der EU entspricht.

Auch nach dem EuGH-Urteil und der Einschätzung des EDÖB sind Standarddatenschutzklauseln grundsätzlich eine zulässige Grundlage für die Datenübermittlung in Drittländer. Der EuGH hat in seinem Urteil jedoch darauf hingewiesen, dass der Verantwortliche im Einzelfall prüfen muss, ob mit den vertraglichen Regelungen unter Nutzung der EU-Standarddatenschutzklauseln tatsächlich sichergestellt werden kann, dass das Schutzniveau für personenbezogene Daten tatsächlich dem in der Schweiz bzw. in der EU entspricht.

Der EDÖB anerkennt EU-Standarddatenschutzklauseln grundsätzlich als hinreichende Garantie, weist allerdings auch darauf hin, dass in Ländern wie den USA davon ausgegangen werden muss, dass EU-Standarddatenschutzklauseln und vergleichbare Klauseln die Anforderungen an vertragliche Garantien in vielen Fällen nicht erfüllen.

Es reicht also nicht mehr aus, diese Vertragsklauseln einfach in einen Dienstleistungsvertrag hinein zu kopieren. Vielmehr hat der Verantwortliche im Einzelfall das tatsächliche Datenschutzniveau zu prüfen und ggf. zusätzliche Massnahmen zu ergreifen.

Binding Corporate Rules

Bei Binding Corporate Rules (BCR) handelt es sich um verbindliche, unternehmensinterne Datenschutzvorschriften, die für alle Mitglieder einer Unternehmensgruppe gelten und nachweisbar durchgesetzt werden. Mit Binding Corporate Rules können sich Unternehmensgruppen zur Sicherstellung eines dem EU-Niveau entsprechenden Datenschutzes verpflichten. Gemäss DSGVO müssen Binding Corporate Rules von der zuständigen EU-Aufsichtsbehörde genehmigt werden. Gemäss Schweizer DSG müssen Binding Corporate Rules dem EDÖB zur Prüfung vorgelegt werden.

Die Möglichkeit geeigneter Garantien durch Bindung Corporate Rules steht nur Unternehmensgruppen oder einer Gruppe von Unternehmen offen. Abgedeckt sind dabei Datenübermittlungen zwischen den Unternehmen der Gruppe. Für Datenübermittlungen an gruppenfremde Dritte bilden Binding Corporate Rules keine geeignete Garantie.

Binding Corporate Rules unterliegen einer Einzelfallprüfung analog der Standarddatenschutzklauseln. D.h. es muss überprüft werden, ob mit den Binding Corporate Rules das geforderte Datenschutzniveau tatsächlich sichergestellt werden kann, was im Falle der USA - wie bereits ausgeführt - in vielen Fällen nicht erfüllt werden kann.

Alternativen

Kann keine der geeigneten Garantien und Massnahmen angewendet werden, empfiehlt der EDÖB, auf die Datenübermittlung in die USA zu verzichten.

Für Unternehmen in der Schweiz, die der DSGVO unterliegen, ist die Datenübermittlung in die USA unzulässig. Gemäß der Leitlinien der EU-Aufsichtsbehörden muss die Datenübermittlung mit sofortiger Wirkung gestoppt werden. Werden Auftragsverarbeiter eingesetzt, so müssen diese angewiesen werden, die Übermittlung personenbezogener Daten mit sofortiger Wirkung auszusetzen. Wird beabsichtigt, die Datenübermittlungen weiterhin durchzuführen, muss das Unternehmen dies der zuständigen EU-Aufsichtsbehörde mitteilen.

Zu beachten ist hierbei, dass ein EU-Auftragsverarbeiter eines Schweizer Verantwortlichen von der EU-Aufsichtsbehörde ein sofortiges Verbot zur Übermittlung von Daten in die USA auferlegt bekommen kann. Das Schweizer Unternehmen kann im schlimmsten Fall handlungsunfähig werden.

Prüfen: Ist eine Datenübermittlung in die USA zwingend notwendig?

Datenübermittlungen in die USA und insbesondere Datenverarbeitungen von Diensten aus den USA sollten grundsätzlich dahingehend untersucht werden, ob sie notwendig sind und tatsächlich in Anspruch genommen werden müssen. In vielen Fällen haben Unternehmen US-Anbieter gewählt, ohne die Auswirkungen zu berücksichtigen und ohne gleichwertige datenschutzkonforme Alternativanbieter in die Evaluation einzubeziehen.

Zurückholen der Daten

Das Zurückholen der Daten in die Schweiz, die EU oder ein Land mit angemessenem Datenschutz ist ein sicherer und nachhaltiger Weg, die zeitaufwändigen Massnahmen für die rechtskonforme Verarbeitung in Ländern ohne angemessenen Datenschutz zu vermeiden. Wer auf der sicheren Seite sein will, und Stabilität in seine Datenübermittlungen und Verarbeitungen bekommen möchte, sollte das Zurückholen der Daten in Erwägung ziehen. Die Berliner Beauftragte für den Datenschutz fordert die Unternehmen auf, zu Dienstleistern in der EU oder in einem Land mit angemessenem Datenschutzniveau zu wechseln.

integratio

Keine gute Idee: Das Urteil ignorieren

Wie bereits erwähnt haben der EDÖB wie auch der Europäische Gerichtshof keine Übergangs- bzw. Schonfrist eingeräumt.

Die EU-Datenschutzbehörden wurden vom EuGH ausdrücklich in die Pflicht genommen, Datenübermittlungen auszusetzen oder zu verbieten, sollte eine gültige Rechtsgrundlage fehlen. Gemeinnützige Organisationen, Betriebsräte und auch Nutzer können Beschwerden oder Klagen einreichen und Schadenersatz für unzulässige Datenexporte verlangen, was auch immaterielle Schäden umfassen kann.

Die DSGVO sieht Bussgelder vor, sollten weiterhin Daten ohne ein gültiges Rechtsinstrument übermittelt werden (Art. 83 Abs. 5 lit. c DSGVO). Aufsichtsbehörden können einen Datentransfer mit sofortiger Wirkung untersagen.

Der Landesdatenschutzbeauftragte in Baden-Württemberg hat publiziert, dass seine Behörde einen Datentransfer nicht untersagt, wenn belegt werden kann, dass der genutzte US-Dienstleister bzw. Vertragspartner kurz- und mittelfristig unersetzlich ist durch einen Dienstleister bzw. Vertragspartner ohne Datentransferproblematik, also beispielsweise aus der EU oder einem Drittland mit Angemessenheitsbeschluss. Im Zentrum dieser Beurteilung steht also die Frage, ob das verantwortliche Unternehmen zumutbare rechtskonforme Alternativangebote gehabt hätte. Hier ist anzumerken, dass der Landesdatenschutzbeauftragte Baden-Württemberg seine Position laufend überprüft und daher zu einem späteren Zeitpunkt zu einer anderen Einschätzung kommen kann.

Mit Inkrafttreten des revidierten Schweizer Datenschutzgesetzes - man geht aktuell von 2022 aus - werden auch in der Schweiz Bussgelder verhängt werden können und der EDÖB kann Datenübermittlungen ins Ausland untersagen.

Geht man nach einer Einzelfallprüfung und zusätzlich getroffenen Massnahmen davon aus, dass kein angemessener Datenschutz gewährleistet werden kann und will die Datenübermittlung fortführen, sollte eine Risikoabwägung vorgenommen werden. Ist eine Datenübermittlung für das Unternehmen wichtig und das Risiko von Sanktionen oder Klagen erscheint geringer? Wie sensibel sind die übermittelten Daten? Jedes Unternehmen muss seine Risiken im Einzelfall identifizieren und abwägen und in eigener Verantwortung entscheiden.

Glossar: CLOUD Act

Der CLOUD Act (Clarifying Lawful Overseas Use of Data Act) von 2018 hat entgegen seines Namens nicht zwingend etwas mit Clouds zu tun. Er betrifft anders gelagerte Sachverhalte als FISA. Im Gegensatz zu nachrichtendienstlicher Überwachung (FISA) wird die Erhebung von elektronischen Beweismitteln für Strafverfahren geregelt. Darauf gestützt werden können strafverfahrensrechtliche Durchsuchungs- und Beschlagnahmungsbeschlüsse einer US-Behörde zur Herausgabe von Daten als Beweismittel, auch wenn diese außerhalb des US-Territoriums gespeichert sind.

Der CLOUD Act verpflichtet US-Unternehmen selbst dann zur Datenherausgabe, wenn lokale Gesetze am Ort des Datenspeichers dies verbieten. Der übliche Weg eines Rechtshilfeersuchens auf Basis von Rechtshilfeabkommen ist aus US-Sicht nach dem CLOUD Act nicht mehr erforderlich - was im Konflikt mit dem Recht der EU und ihrer Mitgliedsstaaten steht.

integratio

Die wichtigsten Dos und Dont's

Don't:

- ✖ Keine Auslagerung von Verarbeitungen, Nutzung von Cloud-Services oder sonstigem Outsourcing ohne "Durchblick" – immer auf Klarheit, Transparenz und Nachvollziehbarkeit achten.
- ✖ Kein Einsatz von IT-Services, Cloud-Services etc. ohne vorherige Prüfung des Dienstleisters, wozu transparente Informationen über den Dienstleister und dessen Leistungen zwingend notwendig sind.
- ✖ Kein Einsatz von IT-Services und Cloud-Services von Anbietern aus Drittländern ohne vorherige Prüfung der Rechtsgrundlagen und zusätzlich erforderlichen Massnahmen.
- ✖ Kein Einkauf von Software-Services, Cloud-Leistungen etc. ohne vertragliche Verpflichtung der Auftragnehmer zur Einhaltung des erforderlichen Datenschutzniveaus.

Do:

- ✔ Überblick über alle Datenströme und die Betriebsstandorte der Datenverarbeitung verschaffen. Das ist nicht nur für den Datenschutz relevant, sondern auch für die IT-Sicherheit, die Betriebssicherheit sowie Wartung und Support.
- ✔ Schweizer und EU-Unternehmen müssen sich über die Rechtslage des Dienstleisters in einem Land ohne angemessenes Datenschutzniveau informieren. Die Non-Profit-Organisation NOYB (Europäisches Zentrum für digitale Rechte, www.noyb.eu) stellt dafür Musterfragebögen zur Verfügung.
- ✔ Für jede Datenübermittlung in ein Land ohne angemessenes Datenschutzniveau: Rechtsgrundlage, Garantien und Massnahmen bestimmen.
- ✔ Subunternehmen ebenfalls prüfen – und durch vertragliche oder andere Massnahmen verpflichten.
- ✔ Bei der Auswahl neuer IT-Services und Software auf grösstmögliche Transparenz und Prüfbarkeit achten, damit keine rechtswidrigen Datenabflüsse erfolgt und die Daten nur für die zulässigen Zwecke verarbeitet werden.
- ✔ Bei jedem Entwicklungsprozess frühzeitig einen Experten aus den Bereichen Datenschutz und IT-Sicherheit hinzuziehen. Der Aufwand dafür ist vergleichsweise gering im Vergleich zu Massnahmen, die bei Fehlentwicklungen ergriffen werden müssen.
- ✔ Die Berliner Beauftragte für den Datenschutz fordert die Unternehmen auf, zu Dienstleistern in der EU oder in ein Land mit angemessenem Datenschutzniveau zu wechseln.

integratio

Informationen zum Whitepaper

Zur Autorin

Henriette Baumann ist Diplom-Betriebswirtin (DH), Informatikerin und zertifizierte Datenschutz-Expertin. Sie ist Partnerin beim Beratungsunternehmen integratio GmbH und Datenschutzbeauftragte verschiedener länderübergreifend tätiger Unternehmen. Seit 2009 ist Henriette Baumann im Vorstand der OSB Alliance[7] vertreten, seit 2020 als zweite stellvertretende Vorstandsvorsitzende.

Quellen

- European Data Protection Board, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Adopted on 10 November 2020
- European Data Protection Board, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, Adopted on 10 November 2020
- Urteil des Europäischen Gerichtshofs vom 16. Juli 2020 in der Rechtssache C-311/18. https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:62018CJ0311&qid=1606948270244&from=DE
- Wissenschaftlicher Dienst des Deutschen Bundestages, Dokumentation US-Datenrecht, Zugriff US-amerikanischer Behörden auf Daten, WD 3 - 3000 - 181/20 vom 3. August 2020
- Stellungnahme zur Übermittlung von Personendaten in die USA und weitere Staaten ohne angemessenes Datenschutzniveau i.S.v. Art. 6 Abs. 1 DSG, Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB, 8. September 2020.

Über integratio

Als herstellerunabhängiges IT-Beratungsunternehmen mit Standorten in Zürich und Böblingen (Deutschland) verfügt integratio über länderübergreifendes Datenschutz-Know-How und fundiertes technisches und juristisches Fachwissen mit zertifizierten Datenschutz- und IT-Sicherheitsexperten, erfahrenen Juristen und Branchenexpertise. Zum Kundenkreis gehören international agierende Konzerne wie auch kleinere und mittelständische Unternehmen verschiedener Branchen.

Kontakt

integratio GmbH
Börsenstr. 18
8001 Zürich

Tel. +41 (0)44 431 72 00
E-Mail: info@integratio.com

7 Open Source Business Alliance - Bundesverband für digitale Souveränität e.V., http://www.osb-alliance.com