PROBSTPARTNER

Newsletter Datenschutzrecht

Internationaler Datentransfer mit TIA und SCC – Wie schicke ich Daten legal in unsichere Drittländer wie die USA?

von Kaj Seidl-Nussbaumer

Februar 2022

Der internationale Transfer von Personendaten gestaltet sich zunehmend schwieriger. Ein häufiger Anwendungsfall für solche Bekanntgaben ist die Nutzung von Software-as-a-Service Angeboten aus den USA (wie z.B. Mailchimp, Salesforce, Workday, Microsoft 365). Daneben spielen auch konzerninterne Übertragungen an verbundene Gesellschaften in den USA oder anderen unsicheren Drittländern eine wichtige Rolle.

Während man sich früher für Übertragungen in die USA vor allem auf internationale Abkommen verliess (erst das Safe Harbor Abkommen, später das Privacy Shield), stellt aktuell meist der Abschluss von Standardvertragsklauseln die einzig gangbare Lösung dar. Doch auch diese genügen für sich alleine den heutigen strengen Anforderungen nicht mehr.

In diesem Newsletter erläutern wir, welche Voraussetzungen nach Schweizer Datenschutzrecht für die Übertragung von Personendaten ins Ausland gelten und zeigen auf, wie man entsprechende Transfers gesetzeskonform ausgestalten kann.

Bitte beachten Sie, dass wir vorliegend nicht auf die ähnliche, aber nicht in allen Details identische Situation in der EU bzw. nach DSGVO eingehen.

1. Transfers ins sichere Ausland

1.1 Grundsatz

Wer Personendaten ins Ausland transferieren möchte oder Services nutzt, bei denen Personen im Ausland Zugriff auf Personendaten haben können, muss zunächst folgende Fragen klären:

- In welches Land sollen die Daten übermittelt werden (beziehungsweise von welchem Land aus kann auf die Daten zugegriffen werden)?
- An welches Unternehmen sollen die Daten bekanntgegeben werden?

Transfers bzw. Bekanntgaben in Länder, die von der Schweiz als Länder mit angemessenem gesetzlichen Datenschutz anerkannt wurden, sind grundsätzlich ohne weitere Massnahmen möglich (Achtung aber auf die Ausnahme in Ziff. 1.2 unten!). Diese Anerkennung wird aktuell vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten ("**EDÖB**") vorgenommen, nach Einführung des neuen Schweizer Datenschutzgesetzes ("**nDSG**") dann durch den Bundesrat. Aktuell ist die sogenannte "Staatenliste" auf folgender Webseite des EDÖB abrufbar: https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland.html (Link "Staatenliste").

Länder mit angemessenem Datenschutz (in Bezug auf Personendaten natürlicher Personen) sind im Wesentlichen alle EU und EWR Staaten sowie UK, Kanada und noch einige weitere. Nicht angemessen ist der Schutz namentlich in den USA, Indien und China sowie den meisten anderen Staaten weltweit.

1.2 Ausnahme

Doch auch bei Bekanntgaben ins sichere Ausland, wie z.B. Deutschland oder Irland, können zusätzliche Massnahmen erforderlich sein. Das ist dann der Fall, wenn der Datenexporteur weiss oder annehmen muss, dass durch das empfangende Unternehmen ein Weitertransfer bzw. eine Bekanntgabe ins unsichere Ausland (vermutlich) vorgenommen werden wird, z.B. aufgrund von auf den Empfänger oder seine Muttergesellschaft anwendbaren Gesetzen in solchen Drittstatten.

Ein konkretes Beispiel: Übermittelt ein Schweizer Unternehmen Mitarbeiterdaten an eine irische Niederlassung eines US-Konzerns, muss der Empfänger z.B. aufgrund US-amerikanischer Gesetze in bestimmten Situationen Personendaten in die USA, also ein unsicheres Drittland, bekanntgeben.

Hat man Grund zur Annahme, dass eine solche Weiterübertragung (der EDÖB nennt das eine "mittelbare Weitergabe") vorkommen kann, so muss man auch bei Transfers in sichere Länder weitere Massnahmen implementieren, so als würde der Transfer direkt ins unsichere Drittland erfolgen (siehe dazu Ziff. 2 unten).

2. Transfers ins unsichere Ausland

2.1 Mögliche Grundlagen

Bei Bekanntgaben ins unsichere Ausland stehen gemäss Gesetz verschiedene Möglichkeiten zur Verfügung, den fehlenden Schutz der Personendaten zu kompensieren, insbesondere:

- Abschluss von Standardvertragsklauseln ("SCC")
- Internationale Abkommen
- Einwilligung des Betroffenen
- Verbindliche Konzernregeln (Binding Corporate Rules, "BCR")

Nachdem die einschlägigen internationalen Abkommen (zunächst Safe Harbor, danach Privacy Shield) durch die EU und im Anschluss auch durch den EDÖB für ungenügend erklärt wurden und die Einwilligung seit jeher eine schwierig zu verwaltende Grundlage darstellte, steht heute vor allem der Abschluss von Standardvertragsklauseln im Vordergrund.

Als Randnotiz sei hier angemerkt, dass sich die Einwilligung – zumindest für erst noch aufzunehmende Bearbeitungen ohne bisherige Datenbestände – zur valablen Alternative entwickelt, nachdem sich die Übertragung basierend auf Standardvertragsklauseln laufend komplizierter gestaltet.

2.2 Standardvertragsklauseln im Besonderen

Im Sommer 2021 hat die EU neue Standardvertragsklauseln (Standard Contractual Clauses, "**SCC**") eingeführt, welche die bisherigen ablösen. Diese SCC sind mittlerweile vom EDÖB für die Schweiz ebenfalls genehmigt worden, solange bei deren Implementierung gewisse zusätzliche Anforderungen für das Schweizer Recht berücksichtigt werden. Diese Schweizer Anforderungen können durch einen einfachen Anhang zu den SCC implementiert werden (mehr dazu im Merkblatt des EDÖB hier:

https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2021/Paper%20SCC%20def.%20D%2024082021.pdf.download.pdf/Paper%20SCC%20def.%20D%2024082021.pdf

Für Bekanntgaben, die noch auf den früheren SCC basieren, sind bis spätestens 1. Januar 2023 die neuen SCC (oder eine andere Grundlage) zu implementieren.

Die neuen SCC sind modular aufgebaut, so dass je nach Anwendungsbereich ein anderes Vertragswerk resultiert. Die vier Anwendungsbereiche sind:

- Modul 1: Controller to Controller
  d.h. Vertrag für Bekanntgaben von einem Verantwortlichen (Controller) in der Schweiz zu einem Verantwortlichen in einem unsicheren Land, also so, dass der Empfänger die Daten im Anschluss in eigener Verantwortung, nicht im Auftrag des Absenders verarbeitet.
- Modul 2: Controller to Processor
  d.h. Vertrag für Bekanntgaben von einem Verantwortlichen in der Schweiz zu einem Auftragsbearbeiter (Processors) in einem unsicheren Land, also so, dass der Empfänger die Daten im Anschluss nur im Auftrag des Absenders verarbeiten darf, wie das z.B. bei Software-as-a-Service in der Regel der Fall ist.

- Modul 3: Processor to Processor
  d.h. Vertrag für Bekanntgaben vom Auftragsbearbeiter in der Schweiz zu einem Subauftragsbearbeiter in einem unsicheren Land.
- Modul 4: Processor to Controller
  d.h. Vertrag für Bekanntgabe von einem Auftragsbearbeiter in der Schweiz zu einem Verantwortlichen in einem unsicheren Land.

Hat ein Schweizer Unternehmen nun also einen Auftragsbearbeiter (Processor) in einem unsicheren Drittland, so ist z.B. ein SCC nach Modul 2 mit dem Processor abzuschliessen – je nach Rechtslage im Drittland begleitet von weiteren Massnahmen (siehe dazu unten).

Für Intragroup Verhältnisse empfiehlt sich in der Regel die Erstellung eines umfassenderen Vertragswerkes, welches verschiedene dieser vier Module mitumfasst, um möglichst alle konzerninternen Datenübermittlungen abzudecken. Dieses Vertragswerk wird häufig als Intragroup Data Transfer Agreement (IGDTA oder IDTA) oder auch als Intragroup Data Processing Agreement (IGDPA) bezeichnet.

2.3 DTIA – Data Transfer Impact Assessment

Mit dem Abschluss von SCC alleine ist es aber heute nicht (mehr) getan. Die Bekanntgabe in ein unsicheres Drittland ist überdies im Rahmen eines formellen Berichtes, eines sogenannten Data Transfer Impact Assessments ("**DTIA**"), einerseits im Detail zu erfassen (Welche Daten? Betroffene? Auftragsbearbeiter? Subauftragsbearbeiter? Zweck? etc.). Anderseits ist in Anbetracht der Rechtslage im Drittland zu prüfen, ob die folgenden vier Garantien durch das Drittland gewährleistet werden bezüglich möglicher Zugriffe durch Behörden in diesem Drittland:

1. Besteht eine **klare Rechtsgrundlage** für solche Datenzugriffe?

2. Ist der Zugriff im Hinblick auf dessen Ziel **notwendig und verhältnismässig**?

3. Bestehen **wirksame Rechtsbehelfe** für die betroffenen Personen in der Schweiz zur Durchsetzung ihrer Rechte zum Schutz der Privatsphäre und informationellen Selbstbestimmung?

4. Besteht ein Zugang zu einem **unabhängigen und unparteiischen Gericht** zur Kontrolle von Eingriffen in die Privatsphäre und die informationelle Selbstbestimmung?

Sind diese Garantien gewährleistet, genügt grundsätzlich die Absicherung des Transfers mittels SCC. Sind sie nicht gewährleistet, was bei US-Clouddienstleistern regelmässig der Fall sein dürfte, sind zusätzliche Schutzmassnahmen (siehe Ziff. 2.4) zu prüfen und zu implementieren (siehe zum Ganzen auch das grafische Ablaufschema des EDÖB unter: https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2021/Anleitung%20f%C3%BCr%20die%20Pr%C3%BCfung%20von%20Daten%C3%BCbermittlungen%20mit%20Auslandbezug%20DE.pdf.download.pdf/Anleitung%20f%C3%BCr%20die%20Pr%C3%BCfung%20von%20Daten%C3%BCbermittlungen%20mit%20Auslandbezug%20DE.pdf)

2.4 Zusätzliche Schutzmassnahmen

Sind die vier Garantien nicht gewährleistet, kann versucht werden, sie durch zusätzliche Massnahmen zu kompensieren. Im Vordergrund stehen hier Verschlüsselungslösungen, bei denen der Schlüssel nicht durch den Auftragnehmer (z.B. US-Cloudanbieter) aufbewahrt wird, sondern durch den Auftraggeber selbst (Bring your own Key) oder einen von diesem beauftragten Dritten (Third Party Key oder Double Key Encryption). Damit wird dem Auftragnehmer bzw. den Behörden im Drittland der Zugriff auf die Daten faktisch verunmöglicht. Allerdings sind solche Verschlüsselungslösungen für die meisten komplexeren SaaS-Dienste keine Option, da der Auftragnehmer zur Erbringung seiner Dienstleistungen in der Regel zu irgendeinem Zeitpunkt Zugriff auf die Klardaten benötigt.

Kommt man zum Schluss, dass die Garantien zwar fehlen, aber durch die zusätzlichen Massnahmen angemessen kompensiert werden können, so ist der Transfer nach Implementierung der SCC und Zusatzmassnahmen möglich. Können die fehlenden Garantien nicht kompensiert werden, so ist der Transfer zu unterlassen bzw. einzustellen. Andernfalls drohen Non-Compliance Risiken, wie persönliche (!) Bussen in der Höhe von bis zu CHF 10'000.- bzw. CHF 250'000.- (nDSG), Unternehmensbussen von bis zu EUR 20 Millionen oder mehr (im Anwendungsbereich der DSGVO), Verlust des guten Leumunds (Strafregistereintrag), behördliche Verbote, Imageschäden etc.

3. Fazit

Datentransfers ins unsichere Ausland sind nicht unmöglich, müssen aber gut geplant und aufgegleist werden. Auch wenn man bereit ist, die verschiedenen Massnahmen durchzuführen und zu implementieren (wie DTIA, SCC und Zusatzmassnahmen), kann sich im Einzelfall ergeben, dass eine Übermittlung nicht rechtskonform möglich ist. In diesem Fall muss man sich schlussendlich entscheiden, ob der Transfer dennoch mit den bekannten Risiken vorgenommen oder eher ein anderer Weg gesucht wird (z.B. die Wahl eines in Europa angesiedelten Dienstleisters).

Weitere Informationen zum Datenschutz finden Sie unter http://swissdataprotectionlaw.ch/

* * * * *