Neue Bürden im internationalen Datentransfer

Heutzutage sind in der IT-Industrie eine globale Zusammenarbeit und die Nutzung von internationalen IT-Providern nicht mehr wegzudenken. Vielfach werden auch Personendaten ausgetauscht, wobei der rechtskonforme Austausch von Personendaten im Moment vielen Unternehmen Kopfschmerzen bereitet. Insbesondere seit dem Schrems-II-Urteil und dem Wegfall des EU-US Privacy Shields besteht allgemeine Rechtsunsicherheit bezüglich der notwendigen Massnahmen.

Yves Gogniat

Den Überblick über alle internationalen Datenflüsse zu behalten und gleichzeitig alle Rechtsvorschriften zu befolgen war bis anhin schon keine einfache Aufgabe. In Bezug auf die USA konnten sich die meisten Unternehmen zumindest auf den EU-US Privacy Shield verlassen und mussten lediglich prüfen, ob sich ein Provider korrekt registriert hatte. Nun aber sind weitere Schritte zum sicheren und rechtlich konformen Datenaustausch nötig.

Transfermechanismen

Neben internationalen Abkommen kennen sowohl die Datenschutzgrundverordnung (DSGVO) sowie auch das Schweizer Datenschutzgesetz (DSG) noch weitere Möglichkeiten, um einen internationalen Datentransfer datenschutzkonform umzusetzen. Diese Regelungen kommen jedoch nur zur Anwendung, wenn im Land des Datenimporteurs kein angemessenes Datenschutzniveau besteht. Die EU sowie auch die Schweiz halten das Datenschutzniveau des jeweils anderen für angemessen, daneben werden aber leider nur wenige Länder als gleichwertig angesehen. Besteht ein angemessenes Datenschutzniveau, sind keine zusätzlichen Massnahmen oder Prüfungen notwendig. Bei einem Datentransfer zwischen der EU und der Schweiz sind somit keine zusätzlichen Massnahmen notwendig. Der Empfänger der Personendaten wird wie ein lokaler Datenempfänger behandelt, d. h. die allgemeinen Datenschutzvorschriften gilt es weiterhin einzuhalten. Bei der Anwendbarkeit der DSGVO muss beispielsweise weiterhin ein Auftragsdatenverarbeitungsvertrag (ADV) nach DSGVO-Standards abgeschlossen werden.

Besteht kein angemessener Datenschutz im Zielland, so sehen beide Datenschutzgesetze ähnliche Massnahmen zur individuellen Sicherstellung des Datenschutzes vor. Das revidierte DSG rückt sogar nochmals näher zur DSGVO heran. Für Unternehmen sind vertragliche Garantien wie die Standardvertragsklauseln (SCC) oder der Mustervertrag für das Outsourcing von Datenbearbeitungen ins Ausland des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) sowie die verbindlichen internen Datenschutzvorschriften (sog. Binding Corporate Rules [BCR]) die einzig wirklich praktikablen Mechanismen. Gewisse Datenbearbeitungen lassen sich allenfalls unter der Ausnahmeregelung der Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags begründen. Diese Ausnahmeregelung ist aber immer mit

Rechtsunsicherheiten und Risiken verbunden. Daneben besteht auch die Möglichkeit, eine ausdrückliche Einwilligung bei der betroffenen Person einzuholen. Dies wird für Unternehmen ebenfalls nicht praktikabel sein, denn eine solche Einwilligung kann jederzeit widerrufen werden. Zudem ist bei einer Veränderung der Zielländer allenfalls wiederum eine neue Einwilligung einzuholen.

Schrems-II-Entscheide

Die aktuelle EU-Rechtsentwicklung hat den Privacy Shield als ungenügend beurteilt. Dieser Datentransfermechanismus entfällt somit. In einem weiteren Urteil wurde zudem der Datentransfermechanismus via SCC durch den EuGH unter die Lupe genommen. Der EuGH hat festgehalten, dass vertragliche Vereinbarungen – wie die SCC – einen behördlichen Zugriff auf die transferierten Personendaten nicht ausreichend verhindern können, wenn das öffentliche Recht des Importstaates einen entsprechenden Rechtsschutz ausschliesst. In einem solchen Fall bindet die vertragliche Vereinbarung lediglich die zivilrechtlichen Parteien, aber nicht das Zielland. Die SCC laufen damit ins Leere, da eine Durchsetzung im Widerspruch zum nationalen Recht steht und damit der Rechtsschutz der betroffenen Personen nicht gewährleistet ist. Der EuGH hat deshalb festgehalten, dass jeweils eine zusätzliche Prüfung und Risikoeinschätzung notwendig sei und, sofern der Datenexporteur den Rechtsschutz nicht für ausreichend hält, er zusätzliche vertragliche und technische Massnahmen zu treffen hat. Der EuGH hat sich allerdings nicht dazu geäussert, wie umfassend eine solche Prüfung sein muss und welche zusätzlichen Massnahmen notwendig sind. Klar ist jedoch, dass eine solche Prüfungspflicht sich nicht nur auf die USA bezieht, sondern für jeden Datentransfer in ein Drittland ohne angemessenen Datenschutz gilt. Der Entscheid des EuGH in Bezug auf die SCC stellt Unternehmen vor zusätzliche Herausforderungen, da nun auch beim Einsatz von SCC eine weitergehende Prüfung und allenfalls Zusatzmassnahmen notwendig werden.

Post Schrems II

Der Wegfall des Privacy Shield hat die Nutzung von vertraglichen Garantien bzw. die EU-SCC als nun wichtigsten Mechanismus für einen Datenaustausch in ein unsicheres Drittland ins Zentrum gerückt. Leider sind diese ebenfalls nicht mehr «Standard» und können daher nicht bedenkenlos als Zusatz zu einem Hauptvertrag übernommen werden. Es ist jeweils eine Zusatzprüfung notwendig. Diverse Aufsichtsbehörden inkl. Europäischer Datenschutzausschuss (EDSA) und EDÖB haben im Anschluss an die nicht durch den EuGH konkretisierte zusätzliche Prüfungspflicht entsprechende Guidelines veröffentlicht, teilweise mit etwas praxisfernen Anforderungen. Mittlerweile scheint zumindest darin Konsens zu bestehen, dass ein risikobasierter Ansatz ausreicht. Die Massnahmen müssen daher im Verhältnis zur entsprechenden Datenbearbeitung und im Verhältnis zum Risiko eines effektiven Zugriffs durch einen Drittstaat stehen. Erforderlich ist, dass man die unternehmensinternen Datenflüsse kennt («Know your transfers») und gestützt darauf jeweils ein Transfer Impact Assessment (TIA) durchführt. Ein solches Vorgehen von Risikoeinschätzung und allfälligen Zusatzmassnahmen bedeutet für ein Unternehmen einen potenziell grossen Mehraufwand. Es ist darauf zu hoffen, dass ausländische IT-Provider für ihre Standardanwendungen in Zukunft ein allgemeines TIA zur Verfügung stellen werden.

Neue EU-Standarddatenschutzklauseln

Als ob diese Zusatzanforderungen nach Schrems II nicht schon genug verwirrend wären, hat die EU-Kommission im Juni 2021 ein neues Set von SCC verabschiedet.
Die neuen SCC wurden nicht nur inhaltlich erneuert und an die DSGVO und die neuen Gegebenheiten angepasst, sie decken nun auch vier unterschiedliche Fallkonstellationen ab, welche alternativ oder parallel zum Einsatz kommen können. Die Module werden nach Transferszenario unterschieden:

- Modul 1:
  Verantwortlicher – Verantwortlicher
- Modul 2:
  Verantwortlicher – Auftragsverarbeiter
- Modul 3:
  Auftragsverarbeiter – Auftragsverarbeiter
- Modul 4:
  Auftragsverarbeiter – Verantwortlicher

Es muss daher jeweils zuerst geprüft werden, welches der Module zum Einsatz kommen. Die SCC können einzeln abgeschlossen oder in einen umfangreichen Vertrag aufgenommen werden. Eine Ergänzung der Klauseln ist zulässig, wenn diese nicht im Widerspruch zu den SCC steht oder die Grundrechte der betroffenen Personen beschneidet. Die neuen SCC können auch durch mehrere Parteien abgeschlossen werden oder eine Partei kann sich später einem Vertrag anschliessen. Die Nutzung der SCC im Rahmen einer konzernweiten Lösung ist daher möglich.
Aus Sicht der EU sind seit Oktober 2021 die neuen SCC zu verwenden. Verträge mit alten SCC gelten weiter, müssen aber bis Ende 2022 ersetzt werden.

Relevanz für die Schweiz

Die Entscheidungen des EuGHs (Schrems II) hat für die Schweiz als Nicht-EU-Mitglied keine direkte Wirkung. Indirekt hat sich die Schweiz aber der neuen Einschätzung angeschlossen. Mit Berufung auf das allgemeine Prinzip der Rechtsstaatlichkeit und das Bedürfnis nach Rechtssicherheit hat der EDÖB die Einschätzung bezüglich den USA ebenfalls angepasst und vertritt nun ebenfalls die Ansicht, dass der Privacy Shield nicht mehr einen angemessenen Datenschutz i.S. des Schweizer Datenschutzgesetzes bietet. Unabhängig davon müssen sich bereits heute aufgrund der extraterritorialen Wirkung der DSGVO viele Schweizer Unternehmen an die DSGVO halten. Der EDSA hat zudem in seiner neusten Guideline zum Datentransfer vom November 2021 festgehalten, dass sich Verantwortliche und Auftragsverarbeiter, welche nach Art. 3 Abs. 2 DSGVO die DSGVO einhalten müssen, die neuen SCC ebenfalls verwenden müssen.
Der EDÖB hat die neuen SCC Ende August 2021 grundsätzlich genehmigt, dies jedoch nicht vorbehaltlos. Die SCC seien so anzupassen, dass das Schweizer Datenschutzrecht ebenso darin reflektiert wird. Insbesondere sei der EDÖB als (parallel) zuständige Aufsichtsbehörde vorzusehen und die Schweiz als Mitgliedstaat i.S.d. SCC zu bezeichnen. Daneben sind auch in der Schweiz die alten SCC-Klauseln in den Verträgen bis Ende 2022 zu ersetzen.

Fazit

Die neuen SCC entbinden nicht von einer zusätzlichen Risikoprüfung und allfälligen Zusatzmassnahmen. Die neuen SCC stellen zwar Verbesserungen dar, aber reduzieren den zusätzlichen Compliance-Aufwand für Unternehmen nur bedingt. ■