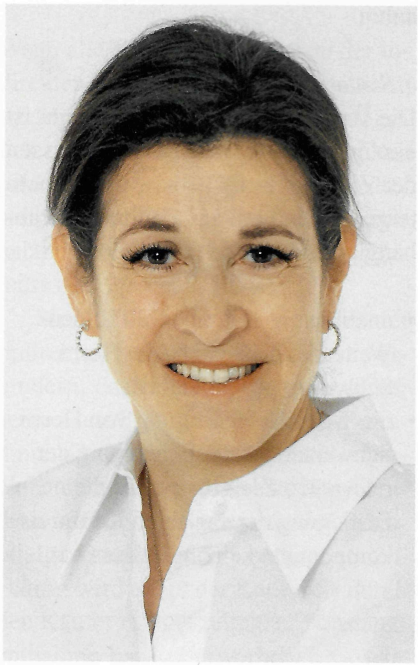
Grenzüberschreitende Datenübermittlungen als Normalität des Geschäftsbetriebs: Schaffen Sie Sicherheit!



Von Lara Elsayan
Rechtsanwältin
Co-Head Data Protection Practice
Lexperience AG

und Nadine Balkanyi-Nordmann
Rechtsanwältin, LL.M., FCIArb
CEO, Head Investigation Practice
Lexperience AG

In Zuge der Globalisierung und Digitalisierung ist Datenschutz – wie viele andere rechtliche Bereiche – schon lange keine rein nationale Angelegenheit mehr. Grenzüberschreitende Datenübermittlungen sind eine notwendige Realität: Es ist für eine funktionierende Wirtschaft und die Wettbewerbsfähigkeit auf dem internationalen Parkett von immanenter Bedeutung, dass Daten grenzüberschreitend bekanntgegeben werden können.

Im Anhang zur Schweizerischen Datenschutzverordnung sind diejenigen Länder publiziert, die gemäss Beschluss des Bundesrates über ein angemessenes Datenschutzniveau verfügen. Es handelt sich dabei vor allem um die Länder der EU und des EWR. Gleichzeitig hat die Europäische Kommission am 15. Januar 2024 die Angemessenheit des schweizerischen Datenschutzniveaus bestätigt. Auf dieser Basis ist der Austausch von Personendaten zwischen der Schweiz und der EU ohne zusätzliche Garantien möglich.

Weitergabe von Daten durch EU-Vertragspartner in die USA

Zu berücksichtigen ist in diesem Zusammenhang aber, dass es Divergenzen zwischen den Angemessenheitsbeschlüssen der EU und der Schweiz gibt. Während aus Sicht der EU – im Gegensatz zur Schweiz – auch die USA, Japan und Südkorea über ein angemessenes Datenschutzniveau verfügen, erachtet die Schweiz – im Gegensatz zur EU – das Datenschutzniveau von Gibraltar und Monaco als angemessen. Insbesondere die Sach- und Rechtslage mit Bezug auf die USA dürfte für viele Banken mit Schwierigkeiten verbunden sein, da mangels eines Angemessenheitsbeschlusses aus Schweizer Sicht eine Datenbekanntgabe in die USA mit Unsicherheiten und zusätzlichem Aufwand verbunden ist. Weiter besteht auch die Problematik, dass bei einer Datenbekanntgabe aus der Schweiz an einen Auftragsbearbeiter in der EU das Risiko einer Weiterleitung der Daten in die USA besteht. Auch wenn die weitere Bekanntgabe von Personendaten vertraglich ausgeschlossen wird, kann ein Restrisiko aufgrund ausländischer Gesetzgebung – und der operationellen Realitäten der europäischen Datenbearbeiter – verbleiben. Obwohl die Schweiz mit den USA schon seit Längerem in

Verhandlungen steht, besteht zurzeit noch kein neues Abkommen.

Neuigkeiten aus den USA

Angesichts der Bezeichnung der Schweiz als «qualifiying state» durch die USA am 7. Juni 2024 ist jedoch mit einem baldigen Inkrafttreten eines Datenschutz-Rahmenwerk zwischen diesen Ländern zu rechnen. Nichtdestotrotz ist es empfehlenswert, sich bei der Bekanntgabe von Personendaten ins Ausland nicht nur auf Angemessenheitsbeschlüsse abzustützen, sondern im Sinne eines «doppelten Bodens» weitere Sicherheitsgarantien zu schaffen. Dabei ist vor allem an die Einwilligung der betroffenen Person als auch an Standarddatenschutzklauseln zu denken.

Mit Bezug auf die Einwilligung der betroffenen Person ist zu berücksichtigen, dass diese bereits aus Beweisgründen in schriftlicher Form eingeholt werden sollte. Die meisten Banken integrieren den Hinweis auf die Datenbekanntgabe ins Ausland, die Möglichkeit des Zugriffs auf die Daten aufgrund ausländischer Gesetzgebungen und die Befreiung vom Bankkundengeheimnis in ihren AGB. Ein ausschliesslicher Hinweis in den AGB ist risikobehaftet und daher ist es empfehlenswert, im Vertrag mit den Kunden auf die entsprechende Regelung in den AGB hinzuweisen. Dies auch im Hinblick auf ausländische Gesetzgebungen.

Mit Bezug auf die Standarddatenschutzklauseln stehen grundsätzlich zwei Alternativen zur Verfügung: Eine Bank kann ihre eigenen Standarddatenschutzklauseln aufsetzen, die allerdings durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) vorgängig genehmigt werden müssen, oder es werden die vom EDÖB anerkannten Standarddatenschutzklauseln verwendet. Zurzeit anerkennt der EDÖB die Standardvertragsklauseln der EU-Kommission. Eigene Standarddatenschutzklauseln hat der EDÖB bis anhin keine erlassen. Bei der Verwendung von Standarddatenschutzklauseln, die der EDÖB anerkannt hat, ist gemäss dem neuen Datenschutzgesetz keine Mitteilung mehr an den EDÖB notwendig. Da es sich bei den vom EDÖB anerkannten Standardvertragsklauseln um solche der EU-Kommission handelt, sind zur Gewährleistung der Kompatibilität mit der schweizerischen Datenschutzgesetzgebung gewisse Anpassungen bzw. Ergänzungen vorzunehmen, wobei die materiellen Bestimmungen der Standardvertragsklauseln nicht verändert werden dürfen. Der EDÖB hat dazu auf seiner Webseite Informationen erlassen.

Zusammengefasst gilt, dass eine Kombination von verschiedenen Massnahmen den besten Schutz im Falle der Bekanntgabe von Daten ins Ausland bietet, wobei auch hier auf Verhältnismässigkeit zu achten und eine den Bedürfnissen angepasste Regelung zu finden ist. Im grossen Stil «Einwilligungen auf Vorrat» einzuholen, ist allerdings nicht empfehlenswert.

«Know your Data»

Ein wesentlicher Schritt für die Umsetzung der datenschutzrechtlichen Anforderungen ist die Übersicht und das Verständnis der Daten, im Hinblick auf das DSG der Personendaten, die bearbeitet werden. Vereinfacht gesagt geht es darum, sich unter anderem die Frage zu stellen, welche Daten wir zu welchem Zweck bearbeiten und wer alles in die Datenbearbeitung involviert ist. So wie im Geldwäschereibereich im Sinne der Sorgfaltspflichten von «Know your Client» gesprochen wird, könnte man hier von «Know your (personal) Data» sprechen.

Dem trägt die im Datenschutzgesetz verankerte Pflicht für Unternehmen mit mehr als 250 Mitarbeitenden, ein Datenbearbeitungsverzeichnis zu führen, Rechnung. Grundsätzlich ist ein Datenbearbeitungsverzeichnis, sofern es kostenmässig tragbar ist und genügend Ressourcen bestehen, auch für kleinere Institute zu empfehlen, auch wenn diese nur beschränkt dazu verpflichtet sind. Zu beachten ist, dass es sich beim Datenbearbeitungsverzeichnis nicht um ein statisches, sondern um ein dynamisches Verzeichnis handelt, das immer aktuell zu halten ist.

Datenschutz wird oft bei Compliance oder Legal angesiedelt. Diese sind aber nicht allein dafür verantwortlich, sondern das ganze Unternehmen ist miteinzubeziehen. Diejenigen, die das Datenbearbeitungsverzeichnis erstellen und führen sind auf die Informationen der Fachabteilungen angewiesen. Die Fachabteilungen wissen am besten, welche Informationen sie benötigen und bearbeiten und mit welchen anderen Parteien oder Gruppengesellschaften Verträge bestehen. Für ein vollständiges und aktuelles Datenbearbeitungsverzeichnis sollte somit ein Setup ins Leben gerufen und gepflegt werden, der den Fachabteilungen ermöglicht, die innerhalb der Bank designierte Stelle dynamisch und fortlaufend mit den entsprechenden Informationen / Verträgen zu bedienen. Dazu ist anzufügen, dass das Gesetz die Nennung der Kategorien von Datenempfängern im Datenbearbeitungsverzeichnis verlangt. Nicht notwendig ist aber eine genaue oder namentliche Bezeichnung der Empfänger. Auch wenn eine konkrete, namentliche Nennung nicht erforderlich ist, so ist es insbesondere für das Management der bestehenden Vertragsbeziehungen zu anderen Stellen – extern oder intern – empfehlenswert, diese namentlich zu erfassen. Ein aktuelles Vertragsmanagementsystem erleichtert die Wahrnehmung der datenschutzrechtlichen Pflichten, insbesondere auch wenn es zu gesetzlichen Änderungen kommt, die eine Anpassung des Vertragswerks erfordern.

Wir stellen bei unserer Beratungstätigkeit nach wie vor fest, dass Unternehmen nicht über eine aktuelle Liste von gültigen Drittparteienverträgen oder Service Level Agreements verfügen, so dass es mit einem enormen Aufwand verbunden ist, ex-post eine solche Übersicht zu schaffen. Dies wird oft durch personelle Wechsel verschärft, da das nötige Wissen nicht mehr rasch im Hause verfügbar ist.

Der Umgang mit Datenschutz ist ein weiteres Risiko, das man kennen, beurteilen und in die internen Prozesse integrieren muss. Wie aber bei anderen Risiken, müssen Unternehmen einen risikobasierten Ansatz erarbeiten, wobei den Grundprinzipien der Transparenz, der Verhältnismässigkeit von Datenbearbeitungen und der Gewährleistung der Datensicherheit Rechnung zu tragen ist.

elsayan@lexp.ch
balkanyi@lexp.ch
www.lexp.ch