Die datenschutzrechtliche Rolle von Konzerngesellschaften

Seit dem 1. September 2023 gelten in der Schweiz das revidierte Datenschutzgesetz (DSG) sowie die dazugehörige Datenschutzverordnung (DSV). In diesem Beitrag wird insbesondere der Frage nachgegangen, wie bei Datenbearbeitungen von Personendaten im Konzern korrekt umzugehen ist. In Bezug auf die konzerninternen Datenbearbeitungen bzw. Datenübermittlungen zwischen einzelnen Tochtergesellschaften innerhalb eines Konzerns ist die korrekte Qualifizierung dieser Zusammenarbeit von entscheidender Bedeutung, um die Compliance mit dem DSG zu gewährleisten. Denn es gilt im DSG (und auch in der DSGVO) kein sogenanntes datenschutzrechtliches Konzernprivileg. Das heisst, dass jeder Datenaustausch zwischen Gruppengesellschaften eines Konzerns gesondert betrachtet und auch entsprechend qualifiziert werden muss. Zentral ist dabei die Frage, in welcher Rolle die beteiligten Unternehmen beim jeweiligen Datenaustausch auftreten. Einerseits ist ein Auftragsbearbeitungsverhältnis zwischen einem Auftragsbearbeiter und einem Verantwortlichen und andererseits eine Bearbeitung von gemeinsamen Verantwortlichen als sogenannte Joint-Controller möglich.

Von Lukas Lezzi

Verantwortlicher

Ein Verantwortlicher gemäss Art. 5 Bst. j DSG ist (i) jede Person, welche (ii) allein oder zusammen mit anderen (iii) über den Zweck und die Mittel der (iv) Datenbearbeitung entscheidet. Wenn diese vier Kriterien erfüllt sind, ist die Rolle als Verantwortlicher gegeben.

Natürliche Personen, die innerhalb einer juristischen Person für die Datenbearbeitung verantwortlich sind (z. B. in verschiedenen Abteilungen innerhalb derselben AG), werden nicht als Verantwortliche im Sinne des DSG qualifiziert. Ihre Tätigkeit wird in diesem Zusammenhang der juristischen Person, für welche sie tätig sind, zugerechnet. Der Verantwortliche ist also anders ausgedrückt der «Herr der Daten».

Auftragsbearbeiter

Gemäss Art. 5 Bst. k DSG wird eine Person als Auftragsbearbeiter bezeichnet, wenn sie im Auftrag des Verantwortlichen Personendaten bearbeitet. Der Auftragsbearbeiter handelt ausschliesslich gemäss Weisung des Verantwortlichen und verfügt daher nicht über eigenständige Befugnisse zur Festlegung von Zweck und wesentlicher Mittel der Datenbearbeitung. Der Auftragsbearbeiter ist also der «verlängerte Arm des Verantwortlichen».

Gemeinsame Verantwortlichkeit

Im Gegensatz zur DSGVO normiert das DSG die Situation nicht ausdrücklich, in der mehrere Personen gemeinsam über die Mittel und Zwecke einer Datenbearbeitung entscheiden. Gemeinsame Verantwortlichkeit besteht immer dann, wenn keiner der beteiligten Akteure auf Weisung des anderen handelt und in einer Gesamtbetrachtung eine gemeinsame Zweckverfolgung stattfindet, selbst wenn die einzelnen Verantwortlichen eigene Zwecke innerhalb dieser Datenbearbeitung verfolgen.

Innerhalb eines Konzerns besteht oft eine solche gemeinsame Verantwortlichkeit, beispielsweise dann, wenn eine Dienstleistungsgesellschaft HR-Dienstleistungen für die Gruppengesellschaft erbringt. Diese Dienstleistungsgesellschaft hat einen erheblichen Einfluss auf die Umstände der Datenbearbeitung von Mitarbeiterdaten der anderen Gruppengesellschaften und bestimmt in Zusammenarbeit mit den übrigen Konzernunternehmen auch viele Bearbeitungszwecke wie beispielsweise die Art und Weise der Leistungsbeurteilungen. Ferner kann auch eine Nutzung einer gemeinsamen Infrastruktur zu einer gemeinsamen Verantwortlichkeit führen, auch wenn die Nutzer jeweils eigene Zwecke mit den darin bearbeiteten Personendaten anstreben. So nahm auch der EuGH in der Vergangenheit eine gemeinsame Verantwortlichkeit an, wenn einer der Verantwortlichen nur schon eine geringe Einwirkungsmöglichkeit auf die Datenbearbeitung des anderen hat. So muss dieser nicht einmal einen faktischen Zugriff auf die Personendaten haben (siehe Urteil vom 5.6.2018, Facebook, C-210/16).

Im Gegensatz zur DSGVO hält das DSG keine Pflicht zum Abschluss einer Vereinbarung zwischen den gemeinsamen Verantwortlichen fest. Nichtsdestotrotz empfiehlt es sich, die Verantwortlichkeiten im Innenverhältnis der involvierten gemeinsamen Verantwortlichen klar zu regeln. Dies kann z. B. in einem Anhang zu schon bestehenden Intercompany-Verträgen geregelt werden.

Nachfolgende Punkte können unter anderem inhaltliche Punkte einer solchen Vereinbarung darstellen:

- Festlegung der Zwecke und Dauer der Datenbearbeitung
- Beschreibung der Art der Personendaten und Kategorie der betroffenen Personen
- Beschreibung der Datenströme und Beziehungen zwischen den Verantwortlichen
- Festlegung, welche Pflichten weiterhin von allen Verantwortlichen wahrgenommen werden müssen
- Festlegung der Anlaufstelle für Datensubjekte
- Aufteilung der externen Kommunikation mit betroffenen Personen (insbesonder hinsichtlich der Erfüllung der Informationspflicht)
- Vereinbarungen über die Durchführung von Datenschutz-Folgenabschätzungen
- und über die Erfüllung von Meldepflichten bei Datenschutzverletzungen
- Vereinbarungen über die technischen Massnahmen für die Datensicherheit und
- über die Massnahmen zu Privacy by Design and by Default
- Vereinbarungen über die Führung der Verzeichnisse der Bearbeitungstätigkeiten
- Vorgehen bei Datenübermittlungen in einen Staat ohne angemessenen Schutz
- gegenseitige Informationspflichten bei relevanten organisatorischen Änderungen der gemeinsam Verantwortlichen

- Vereinbarungen über die Haftung im Innenverhältnis

Ferner gilt es zu beachten, dass gemäss Art. 12 DSG die Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten besteht, wenn das Unternehmen mehr als 250 Mitarbeitende beschäftigt und deren Datenbearbeitung ein hohes Risiko von Verletzungen der Persönlichkeit der betroffenen Personen mit sich bringt. Abs. 1 hält fest, dass sowohl der Verantwortliche als auch der Auftragsbearbeiter (siehe Kapitel «Auftragsbearbeiter») je ein Verzeichnis ihrer Bearbeitungen zu führen haben. Einer der gesetzlich vorgeschriebenen Mindestinhalte eines solchen Verzeichnisses ist die Angabe der Identität des Verantwortlichen. Im Konzernverhältnis gilt es darauf zu achten, dass die jeweils tatsächlich verantwortliche Gruppengesellschaft aufgeführt wird.

Bekanntgabe von Personendaten ins Ausland

Art. 16 DSG regelt die Übermittlung von Personendaten ins Ausland. Personendaten dürfen ins Ausland bekannt gegeben werden, wenn das entsprechende Land über ein gemäss der Schweiz vergleichbares datenschutzrechtliches Niveau verfügt (vgl. Art. 16 Abs. 1 und Art. 8 Abs. 1 und Anhang 1 DSV). Wenn dies nicht der Fall ist, so sieht Art. 16 Abs. 2 Bst. e DSG für internationale Konzerne die Möglichkeit vor, Daten an eine ihrer Konzerngesellschaften im Ausland weiterzugeben, indem sie interne Datenvorschriften festlegen (sog. Binding Corporate Rules; Kurzform: BCR). Diese Bestimmung wurde im Vergleich zum alten Recht verschärft. Unternehmen müssen die BCR nun vorab dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) oder einer anderen zuständigen Behörde in einem Land mit angemessenem Datenschutz zur Genehmigung vorlegen. Ohne diese entsprechende Genehmigung dürfen sie gestützt auf Art. 16 Abs. 1 Bst. e DSG keine Daten an ihre Konzerngesellschaften übertragen. Damit übernimmt das DSG die Vorgaben der DSGVO. Der EDÖB hat 90 Tage Zeit, um das Ergebnis seiner Prüfung mitzuteilen (Art. 11 Abs. 3 DSV). Im Gegensatz dazu erfordern Datenschutzklauseln in einem Vertrag gemäss Art. 16 Abs. 2 Bst. b DSG, spezifische Garantien eines Bundesorgans nach Abs. 2 Bst. c sowie Standarddatenschutzklauseln nach Abs. 2 Bst. d, sofern sie bereits vom EDÖB anerkannt wurden, keiner Genehmigung durch den EDÖB. Es genügt, dem EDÖB eine Mitteilung zu machen. Die internen Richtlinien müssen für das Unternehmen verbindlich sein, wobei der Mindestinhalt gemäss Art. 11 DSV für die BCR festgelegt ist.

Es ist jedoch nicht erforderlich, dass die BCR in allen Teilen des Konzerns Anwendung findet. Es genügt, wenn sie nur für diejenigen Teile des Konzerns gelten, die sich in einem Land ohne angemessenen Datenschutz befinden. Ein Vorteil der BCR besteht darin, dass sie für eine Vielzahl von Datenbearbeitungen innerhalb eines Konzerns verwendet werden können. Trotzdem haben solche Klauseln in der Schweiz bisher eine untergeordnete Rolle gespielt, da konzernweite Transferverträge auf der Grundlage der (EU-) Standarddatenschutzklauseln (sog. SCC) einfacher und mit geringerem Aufwand umzusetzen waren.

Schlussfolgerung

In grossen Unternehmensgruppen werden oft Dienstleistungsgesellschaften eingesetzt, die beispielsweise IT-, HR- oder Finanzdienstleistungen für die operativen Gruppengesellschaften erbringen. Solche Dienstleistungsgesellschaften werden in vielen Fällen als Auftragsbearbeiter betrachtet, insbesondere im Bereich der IT-Dienstleistungen. Es besteht jedoch auch die Möglichkeit, dass sie als gemeinsame Verantwortliche oder eigenständige Verantwortliche agieren. Aus diesem Grund ist eine detaillierte Analyse der jeweiligen Datenbearbeitung und der entsprechenden Datenflüsse von entscheidender Bedeutung.

Im Bereich des DSG existiert kein spezielles Konzernprivileg, daher muss auch innerhalb von Konzernen jede Übermittlung von Daten zwischen den Konzerngesellschaften separat auf ihre Zulässigkeit geprüft und datenschutzrechtlich korrekt eingeordnet werden. In vielen Konzernen wird häufig einer der Konzerngesellschaften als zentrale Dienstleistungsgesellschaft durch Organisationsregelungen oder interne Weisungen die Datenbearbeitung von Kunden- oder Mitarbeiterdaten ganz oder teilweise delegiert. Sofern eine solche Dienstleistungsgesellschaft in die Entscheidungsprozesse hinsichtlich der Mittel und Zwecke der Datenbearbeitung einbezogen wird oder ihr die Verfolgung eigener Interessen gestattet ist, wird wohl regelmässig von einer gemeinsamen datenschutzrechtlichen Verantwortlichkeit auszugehen sein. Der interne Datenschutzbeauftragte (DSB), sofern vorhanden, sollte stets in den Bewertungsprozess einbezogen werden, um die Situation angemessen zu beurteilen.

WICHTIGER HINWEIS

- Es gibt kein Konzernprivileg im DSG. Jeder Datenaustausch zwischen Gruppengesellschaften muss gesondert qualifiziert werden.
- Vielfach besteht eine gemeinsame Verantwortlichkeit.
- Auch wenn gesetzlich nicht ausdrücklich vorgeschrieben, sollten solche gemeinsame Verantwortlichkeiten vertraglich geregelt werden.
- Bei vielen und häufigen Datentransfers zwischen Konzerngesellschaften in Ländern ohne angemessenen Datenschutz können Binding Corporate Rules sinnvoll sein.

AUTOR

Lukas Lezzi ist selbstständiger Rechtsanwalt in Zürich (LezziLegal). Seine Tätigkeitsschwerpunkte liegen im Bereich Datenschutz- und Finanzmarktrecht.