MME

Datenbearbeitung durch Dritte – Fallstrick Datenschutz

Dr. Martin Eckert

In IT-Verträgen mit Dritten (Outsourcing, Cloud Computing, etc.) sind griffige Datenschutzklauseln eine Selbstverständlichkeit. Oft geht jedoch vergessen, dass auch bei weniger technischen Dienstleistungsverträgen der Auftragnehmer Personendaten bearbeitet. Diese sog. Auftragsdatenverarbeitung unterliegt gesetzlichen Regeln (Datenschutzgesetz; DSG). Wie stellen Sie sicher, dass Sie sich als Auftraggeber gesetzeskonform verhalten?

Wann liegt eine Auftragsdatenbearbeitung vor?

Sobald Sie die Bearbeitung von Personendaten an Dritte auslagern oder Dritte involvieren, liegt eine sog. Auftragsdatenbearbeitung vor. Als Personendaten gelten nicht nur Namen, Adressen, Alter, etc., sondern auch IP-Adressen, biometrische Daten, Device Identifiers, UDID, UUID, Windows ID, Google Advertising ID, IMEI Code, etc. und sonstige Angaben, die sich auf eine bestimmte Person oder ein bestimmtes Unternehmen beziehen. Im technischen Bereich (IT-Verträge) ist die Auftragsdatenbearbeitung offensichtlich. Als Auftragsdatenbearbeitung gelten beispielsweise Outsourcing, Cloud Computing, Hosting, Archivierung, Backup-Dienstleistungen, Speicherung von Personendaten auf fremden Servern, etc. Weniger offensichtlich ist, dass auch andere Arten von Dienstleistungsverträgen eine Auftragsdatenbearbeitung nach sich ziehen, weil Ihr Dienstleister zur Erbringung seiner Dienstleistungen mit Personendaten arbeitet, die von Ihnen zur Verfügung gestellt werden. Nachfolgende Dienstleistungsverträge enthalten in der Regel eine Datenbearbeitung durch Dritte:

X	**Auftrag (insbesondere Outsourcing):** Auslagerung der Lohnbuchhaltung, des Personalwesens sowie der Kundenbewirtschaftung und -befragung oder des Case Managements.
X	**Marketing:** Tracking der Kunden auf den Websites; Auswertung Kunden- und Besucherdaten; Profiling; Google Analytics; Data Mining; kundenspezifisches Advertising.
X	**Factoring:** Mittels eines Factoring-Vertrages werden das Risiko der Zahlungsunfähigkeit sowie die administrativen Debitorenumtriebe gegen eine Factoring-Gebühr an ein Factoring-Unternehmen übertragen.
X	**Begutachtungs- und Beratungsvertrag:** Auswertung von Personendaten bei Gutachtertätigkeiten mit wirtschaftlichen, rechtlichen, sozialen, medizinischen oder vergleichbaren Fragestellungen.
X	**Softwareentwicklungs- und Softwarepflegevertrag:** Testing und Support von Datensammlungen mit Personendaten.
X	**Kollektiver Taggeldversicherungsvertrag:** Datenbearbeitung durch die Versicherung.

Was sind Ihre Pflichten?

Sie sind gesetzlich verpflichtet sicherzustellen, dass die Datenbearbeitung durch den Dritten in Übereinstimmung mit den gesetzlichen Bestimmungen erfolgt (Art. 10a DSG). Auftragsdatenbearbeitung ist zwar grundsätzlich ohne Einwilligung der betroffenen Personen zulässig, aber nur dann, wenn die datenschutzrechtlichen Grundsätze eingehalten werden und gewährleistet ist, dass die Persönlichkeitsrechte der betroffenen Personen auch im Rahmen der Übertragung der Datenbearbeitung gewahrt sind. Der Auftraggeber hat die den Umständen angemessenen Sorgfaltspflichten anzuwenden; insbesondere ist er verpflichtet, den Auftragnehmer sorgfältig auszuwählen, klar zu instruieren und zu überwachen. Die Übertragung der Datenbearbeitung an einen Dritten darf die Rechtsstellung der betroffenen Personen nicht verschlechtern.

Was sind Ihre Risiken (Haftung)?

Im Alltag wird das Vorliegen von Auftragsdatenbearbeitungen oft übersehen und die entsprechenden Verträge werden in der Folge nicht datenschutzrechtskonform ausgearbeitet. Dies kann aufgrund der Verantwortlichkeitsaufteilung von Art. 10a DSG für Sie als Auftraggeber unangenehme Folgen haben. Der Auftraggeber haftet für den Schaden, der durch Übertragung der Datenbearbeitung an Dritte verursacht wird, namentlich wenn die Datensicherheit nicht sichergestellt wird. Die betroffenen Personen können Rechtsansprüche nach Art. 15 DSG i.V.m. Art. 28 ZGB geltend machen (beispielsweise Sperrung der Datenbearbeitung, keine Bekanntgabe an Dritte, Berichtigung oder Vernichtung von Personendaten, Forderung auf Rückübertragung der Datenbearbeitung, Schadenersatz, Genugtuungsansprüche aus Persönlichkeitsverletzung). Die Praxis zeigt, dass Datenschutzprobleme immer auch mit Reputationsrisiken verbunden sind.

Was haben Sie konkret vorzukehren (Compliance-Massnahmen)?

Ihre Datenschutz-Compliance-Pflichten können Sie erfüllen, in dem Sie Ihre Datenbearbeitungspflichten dem Vertragspartner vertraglich über-

binden. Sie müssen sich zudem vergewissern, dass die Datensicherheit (angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten; Art. 7 DSG) durch Ihre Auftragnehmer eingehalten wird.

Achten Sie darauf, dass in allen Dienstleistungsverträgen Klauseln enthalten sind, die eine datenschutzkonforme Bearbeitung von Personendaten sicherstellen:

Generelle Klauseln:

- Generelle Datenschutzklausel (Rechtmässige Bearbeitung; Richtigkeit der Daten, Datensicherheit)
- Zulässigkeit / Unzulässigkeit der Weitergabe an Unterauftragnehmer/Subakkordanten
- Verbot der grenzüberschreitenden Bekanntgabe (Daten dürfen CH/EU nicht verlassen; Regelung betr. Ort der Bearbeitung/Zugriff und Serverstandorte)
- Sicherstellung des Auskunftsrechts für betroffene Personen (Art. 8 DSG)
- Auditklausel: Vereinbarung eines Kontrollrechts für den Auftraggeber oder neutrale Dritte und Einsicht in Auditberichte
- Zertifizierungsklausel: Verpflichtung des Anbieters zum Nachweis und der Aufrechterhaltung von Zertifizierungen (z.B. DIN ISO/IEC 2700x:2014; ISAE 3000)
- Informationspflicht des Auftragnehmers bei wichtigen Vorkommnissen (z.B. Datenlecks)

Individuelle Klauseln (Beschreibung der Datenbearbeitung):

- Sie müssen mit ausreichender Präzision die Art und Weise der Datenbearbeitung und Bekanntgabe definieren. Sie haben sicherzustellen, dass die Daten durch den Dritten nur so bearbeitet werden, wie Sie es selbst tun dürften. Die Antwort auf die Frage, was Sie dürfen, ist nicht banal (Verhältnismässigkeitsprinzip, Zweckbindungsgrundsatz, Rechtfertigungsgründe) und muss im Einzelfall analysiert werden (vgl. Art. 4 DSG).
- Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde oder aus den Umständen ersichtlich ist. Die Beschaffung von Personendaten und der Zweck ihrer Bearbeitung müssen für die betroffenen Personen erkennbar sein.
- Zu prüfen ist im Einzelnen insbesondere, ob eine Einwilligung der betroffenen Personen erforderlich ist und wie diese rechtsgültig erlangt werden kann.

Gerne beraten und unterstützen wir Sie bei der Ausarbeitung von Verträgen und entsprechenden Compliance-Massnahmen.

MME kompakt

MME bietet integrierte Lösungen in den Bereichen Legal, Tax und Compliance. In den Bereichen IT Law und Datenschutz Compliance hat sich MME bereits früh spezialisiert (1999). Wir unterstützen in allen IT, Datenschutz, Outsourcing und Compliance Fragen. Als einzige Schweizer Anwaltskanzlei ist MME Mitglied von World IT Lawyers (www.worlditlawyers.com). Dieses internationale Spezialisten-Netzwerk ermöglicht uns eine effiziente, grenzüberschreitende Rechtsberatung.

Zürich
Kreuzstrasse 42
Postfach 1412
8032 Zürich
T +41 44 254 99 66
F +41 44 254 99 60
office@mme.ch

Zug
Gubelstrasse 11
Postfach 613
6301 Zug
T +41 41 726 99 66
F +41 41 726 99 60
office@mme.ch

Dr. Martin Eckert
Partner/Rechtsanwalt
martin.eckert@mme.ch

Dr. Andreas Glarner, LL.M.
Partner/Rechtsanwalt
andreas.glarner@mme.ch

lic.iur. Gabriela Spühler
Rechtsanwältin/Notarin
gabriela.spuehler@mme.ch