

Outsourcing: Auftragsdatenbearbeitung

Im heutigen Wirtschaftsumfeld setzen Unternehmen zunehmend auf Outsourcing, um die Effizienz zu steigern, Kosten zu senken und Zugang zu spezialisiertem Know-how zu erhalten. Insbesondere profitieren kleine und mittlere Unternehmen (KMU) von der Auslagerung bestimmter Prozesse, da sie sich auf ihre Kernkompetenzen konzentrieren können. Allerdings ist nicht jede Form des Outsourcings aus datenschutzrechtlicher Sicht relevant. Entscheidend ist, ob Personendaten durch den externen Dienstleister bearbeitet werden.

■ Von Lukas Lezzi

Das Wichtigste in Kürze

- Outsourcing stellen in vielen Fällen Auftragsbearbeitungen dar, welche entsprechende datenschutzrechtliche Implikationen haben.
- Die Dienstleister sind im Vorfeld zu prüfen, ob sie in der Lage sind den Datenschutz und die Datensicherheit einzuhalten.
- Es ist ein Auftragsbearbeitungsvertrag mit dem Dienstleister abzuschliessen. Dieser Vertrag ist sorgfältig zu prüfen, ob er für die in Frage stehenden Datenbearbeitung die nötigen Datenschutz- und Datensicherheitsstandards bietet.

Definition Auftragsbearbeitung

Eine Auftragsbearbeitung liegt vor, wenn ein Dritter die Personendaten nach Weisung und im Interesse des für die Datenbearbeitung Verantwortlichen bearbeitet. Der Auftragsbearbeiter ist der «verlängerte Arm» des Verantwortlichen. Dabei bearbeitet der Auftragsbearbeiter die Personendaten nicht für die eigenen Zwecke, sondern für diejenigen, welche der Verantwortliche ihm vorgibt. Der Verantwortliche ist an dieser Stelle der Auftraggeber. Beispiele hierfür sind die Nutzung von Cloud-Diensten oder die Auslagerung der Lohnbuchhaltung.

Pflichten des Auftragsbearbeiters

Der Auftragsbearbeiter ist strikt daran gebunden, Personendaten ausschliesslich im Rahmen des Auftrags zu bearbeiten. Eine Bearbeitung zu eigenen

Zwecken ist nicht erlaubt. Der Auftragsbearbeiter ist bei der Festlegung der technischen und organisatorischen Massnahmen (TOMs) weitgehend frei bzw. kann er dem Verantwortlichen die eingesetzten Mittel vorschlagen. In der Praxis hat ein Verantwortlicher häufig nur einen sehr eingeschränkten Spielraum, dem Auftragsbearbeiter die TOMs vorzugeben. Insbesondere bei Cloud-Dienstleistungen gibt es in der Regel keinen grossen Verhandlungsspielraum.

Der Auftragsbearbeiter darf für die Datenbearbeitung grundsätzlich nur nach Genehmigung des Verantwortlichen weitere Dritte beiziehen. In der Praxis wird dies häufig so gelöst, dass der Auftraggeber bei Unterzeichnung des Vertrags die vom Auftragsbearbeiter eingesetzten Unter-Auftragsbearbeiter genehmigt. Häufig wird dann für spätere Wechsel vorgesehen, dass ein Wechsel angezeigt werden muss und dem Auftraggeber im Fall der Ablehnung ein ausserordentliches Kündigungsrecht zugestanden wird.

Auftragsbearbeitungsvertrag

Wichtig zu verstehen ist, dass der Verantwortliche für die Datenbearbeitung auch bei einem Outsourcing verantwortlich gegenüber den betroffenen Personen bleibt. Ein zentrales Element der Auftragsbearbeitung ist deshalb der Abschluss eines Auftragsbearbeitungsvertrags zwischen dem Auftraggeber und dem Auftragsbearbeiter. Dieser Vertrag regelt die Bearbeitung der Personendaten und stellt sicher,

dass die datenschutzrechtlichen Vorschriften eingehalten werden.

Dementsprechend ist es wichtig, auf den Inhalt von Auftragsbearbeitungsverträgen Wert zu legen. Auch wenn viele der Auftragsbearbeitungsverträge im Outsourcing-Bereich, insbesondere bei grossen Cloud-Anbietern, schwierig bis gar nicht zu verhandeln sind, ist eine sorgfältige Prüfung vorzunehmen und ggf. von einem Provider ganz abzusehen, falls der Vertragsinhalt nicht genügend erscheint. Vor allem bei kleinen Unternehmen, welche einem Berufsgeheimnis unterstehen, ist darauf zu achten, dass die regulatorischen Vorgaben und die Geheimhaltung vom Auftragsbearbeiter eingehalten werden. Das DSG und die Datenschutzverordnung (DSV) setzen keinen detaillierten Mindestinhalt für den Auftragsbearbeitungsvertrag voraus.

Folgende Punkte sollten jedoch vertraglich geregelt werden:

- die ausdrückliche Verpflichtung, dass der Auftragsbearbeiter die Personendaten ausschliesslich gemäss den Weisungen des Verantwortlichen bearbeiten darf
- Ein wirksames Auditrecht sollte vereinbart werden. Dies kann durch eigene Audit-Berichte oder Berichte eines unabhängigen Dritten erfüllt werden.
- Der Auftragsbearbeiter muss sich verpflichten, die Geheimhaltung der Personendaten des Auftraggebers sicherzustellen. Insbesondere müssen seine Mitarbeitenden zur Geheim-

haltung verpflichtet werden. Dies ist bei besonders schützenswerten Personendaten oder Daten, welche einem Berufs- oder Amtsgeheimnis unterliegen, zentral.

- Die TOMs sollten als Anhang im Vertrag aufgenommen werden.
- Die eingesetzten Unter-Auftragsbearbeiter sollten im Vertrag namentlich, mit Ort und Art der Bearbeitung erwähnt sein.
- Der Auftragsbearbeiter muss sich verpflichten, allfällige Datenschutzverletzungen, welche bei ihm vorgefallen sind, unverzüglich dem Verantwortlichen zu melden. Hier sollten kurze Fristen von maximal 48 Stunden vereinbart werden.
- Weiter sollten auch Unterstützungspflichten des Auftragsbearbeiters im Hinblick auf die Erfüllung der Betroffenenrechte (z. B. Auskunft oder Löschung) und die Durchführung von Datenschutz-Folgenabschätzungen vereinbart werden.
- Schliesslich muss vereinbart werden, dass der Auftragsbearbeiter bei Beendigung des Auftragsbearbeitungsvertrags die Personendaten des Verantwortlichen löscht oder diesem zurückgibt.

Datenbekanntgabe ins Ausland

Befindet sich ein Auftragsbearbeiter im Ausland, so ist ferner zu prüfen, ob die Voraussetzungen des DSG zur Auslandsbekanntgabe erfüllt sind. Bei einer Bekanntgabe in den EU-/EWR-Raum sind keine weiteren Massnahmen zu treffen. Wenn sich das Zielland ausserhalb der Schweiz oder des EU-/EWR-Raums befindet, ist abzuklären, ob ein angemessenes Datenschutzniveau vorliegt. Der Anhang 1 der Datenschutzverordnung enthält eine Liste mit Ländern, welche einen angemessenen Datenschutz haben.

Bei einer Bekanntgabe in Länder ohne ausreichendes Datenschutzniveau sind zusätzliche Massnahmen wie Standardvertragsklauseln der EU (angepasst nach den Vorgaben des EDÖB) erforderlich, um die Daten der

betroffenen Personen zu schützen. Mit diesen Standardvertragsklauseln kann ein angemessenes Datenschutzniveau hergestellt werden, und eine Auslandsbekanntgabe kann stattfinden. Ferner ist immer daran zu denken, dass gegebenenfalls andere Massnahmen, wie beispielsweise eine Verschlüsselung der Personendaten, nötig ist (sog. technische Massnahmen).

Viele Outsourcing-Dienstleister haben ihren Sitz in den USA. Die USA verfügen über einen angemessenen Datenschutz, aber nur wenn das fragliche Unternehmen nach dem Data Privacy Framework zertifiziert ist.

Auswahl der Dienstleister

Der Verantwortliche ist verpflichtet, einen Auftragsbearbeiter sorgfältig auszuwählen; dieser ist also einer vorgängigen Prüfung zu unterziehen. Die Ausgestaltung und Prüftiefe hängen wesentlich von der Sensitivität der infrage stehenden Personendaten, von den regulatorischen Vorgaben (wie z. B. im Finanzmarktrecht), vom Risikoappetit und nicht zuletzt auch von der Verhandlungsmacht ab.

Für kleine und mittlere Unternehmen ohne regulatorische Vorgaben hat sich eine kurze Red-Flag-Prüfung in der Praxis als sinnvoll erwiesen. Folgende Punkte sind hier zu prüfen:

- War der Dienstleister in den letzten fünf Jahren in ein Vollstreckungsverfahren einer Aufsichtsbehörde verwickelt?
- Hatte der Dienstleister in den letzten fünf Jahren eine wesentliche Verletzung der Datensicherheit erlitten?
- Ist gegen den Dienstleister in den letzten fünf Jahren eine Sanktion oder Geldstrafe wegen Verletzung des Datenschutzes verhängt worden?
- Ist der Dienstleister in den letzten drei Jahren durch Datenschutzvorfälle in den Medien negativ aufgefallen?
- Verfügt der Dienstleister über eine interne Organisation für die Einhaltung des Datenschutzes und der Datensicherheit?

Fazit

Outsourcing bietet Unternehmen zahlreiche Vorteile, birgt jedoch auch Risiken, insbesondere im Hinblick auf den Datenschutz. Zuerst ist der Dienstleister sorgfältig zu prüfen, ob er für die fragliche Datenbearbeitung überhaupt technisch und organisatorisch in der Lage ist. Neben der technischen und organisatorischen Datensicherheit sind vertragliche Vereinbarungen und eine transparente Kommunikation mit den Dienstleistern essenziell. Insbesondere ist auch darauf zu achten, dass die betroffenen Personendaten und Bearbeitungstätigkeiten richtig vertraglich abgebildet werden. Beim Auslandstransfer von Personendaten ist stets darauf zu achten, ob der Zielstaat ein angemessenes Datenschutzniveau besitzt. Fehlt es an einem angemessenen Datenschutzniveau, so können Standardvertragsklauseln eingesetzt werden. In komplexen Fällen oder bei sensiblen Daten kann die Hinzuziehung externer Experten sinnvoll sein.

- Es ist unternehmensintern zu identifizieren, welche Dienstleister als Auftragsbearbeiter gelten.
- Auftragsbearbeiter müssen die Datensicherheit einhalten und eine DSGVO-konforme Bearbeitung gewährleisten können. Generell kann dies anhand einer kurzen Red-Flag-Prüfung festgestellt werden.
- Es muss ein Vertrag mit dem Auftragsbearbeiter abgeschlossen werden.
- Dieser ist sorgfältig zu prüfen. Insb. bei regulierten Unternehmen mit Berufsgeheimnis sind Anpassungen auch bei Standardverträgen mit grossen Anbietern in der Regel nötig.
- Bei einem ausländischen Dienstleister ist zu prüfen, ob der Sitzstaat ein angemessenes Datenschutzniveau hat.

AUTOR



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