Auftragsdatenverarbeitung, IT-Outsourcing, Cloud & Co. – wichtige Grundregeln

21. Juni 2016

1. Einleitung

Bei der Frage, ob ein Unternehmen von Auftragsdatenverarbeitung betroffen ist, würde außerhalb einschlägiger Datenschutzkreise wohl fast jeder verneinend den Kopf schütteln. Doch Auftragsdatenverarbeitung betrifft beinahe jedes Unternehmen. Lassen Sie Ihre Werbemaßnahmen von einem externen Büro (Lettershop) erledigen? Holt ein Dienstleister Ihren Papierabfall zur Entsorgung ab? In beiden Fällen überlassen Sie personenbezogene Daten einem Dienstleister. Sie sind damit per Bundesdatenschutzgesetz zu genau vorgeschriebenen Vereinbarungen und Handlungsweisen verpflichtet. Folgen Sie dieser Verpflichtung nicht, kann dies ein Bußgeld der Datenschutzaufsicht nach sich ziehen. Im letzten Jahr wurde vom Bayerischen Landesamt für Datenschutzaufsicht ein 5-stelliges Bußgeld gegenüber einem Unternehmen verhängt, das seine Auftragsdatenverarbeitung mit Dienstleistern nicht datenschutzkonform regelte. Wie Sie dieses Risiko für Ihr Unternehmen vermeiden, lesen Sie in diesem Merkblatt.

2. Was ist eine ADV?

Unter Auftragsdatenverarbeitung („ADV“) i.S.d. Bundesdatenschutzgesetztes (BDSG) wird die Erhebung, Verarbeitung und/oder Nutzung von personenbezogenen Daten durch einen Dienstleister im Auftrag des Auftraggebers (verantwortlichen Stelle) verstanden (§ 11 Abs. 1 S. 1 BDSG). Trotz der Beauftragung des Dienstleisters bleibt der Auftraggeber im vollen Umfang für den Umgang mit den personenbezogenen Daten durch den Dienstleister verantwortlich („Datenhoheit“). Es handelt sich um eine gesetzliche Privilegierung, die die Datenverarbeitung durch externe Dienstleister erleichtern soll.

ADV zeichnet sich durch vier wesentliche Merkmale aus:

a) den Zugriff auf personenbezogene Daten durch einen Dritten (den Auftragnehmer);

b) die Weisungsgebundenheit des Auftragnehmers, d.h. der Auftragnehmer (Datenverarbeiter) handelt allein nach den Anweisungen des Auftraggebers und trifft im Hinblick auf die Art und Umfang der Datenerhebung, -verarbeitung und/oder -nutzung keine eigenen Entscheidungen;

c) der Auftragnehmer hat keine eigene vertragliche Beziehung zu den Personen, deren Daten er erhebt, verarbeitet oder nutzt; er arbeitet nur mit seinem Auftraggeber zusammen und

d) die ADV findet innerhalb der EU bzw. des EWR statt.

Besonders wichtig ist das Merkmal b) „Weisungsgebundenheit“. Es unterscheidet eine ADV von anderen Formen der Datenerhebung oder -nutzung durch externe Dienstleister. Ist der externe Dienstleister nämlich nicht umfassend weisungsgebunden, d.h. wenn ihm ein gewisses Maß an eigener Entscheidungsmacht zusteht, so liegt keine ADV vor, sondern in aller Regel eine sogenannte „Funktionsübertragung“ (z.B. bei der Übermittlung von Patientendaten an Fachärzte). In diesem Fall lässt sich die Datennutzung des externen Dritten nicht mit einem Verweis auf die ADV rechtfertigen, stattdessen muss eine andere Erlaubnis

nach dem BDSG oder sonstigen Datenschutzvorschriften gefunden werden, damit die Maßnahme rechtmäßig ist.

Eine Abgrenzung zwischen der „Funktionsübertragung“ und einer ADV ist in vielen Fällen schwierig, da sich die Tätigkeitsbilder ähneln. Als Faustformel gilt, je eigenständiger das Service-Unternehmen arbeitet, desto wahrscheinlicher ist eine Funktionsübertragung.

Als Auftragsdatenverarbeitung wird beispielsweise die Auslagerung personenbezogener Daten im Rahmen von Cloud-Computing oder anderes IT-Outsourcing (z.B. externes Rechenzentrum), die (rein technische) Datenverarbeitung für die Lohn- und Gehaltsabrechnung oder für die Finanzbuchhaltung, die Beauftragung eines Datenvernichters oder das Lettershop-Verfahren angesehen. Aber auch die IT-Wartung per Remote-Zugriff zählt dazu. Für die Frage der ADV ist die Anzahl oder Dauer der Inanspruchnahme eines Dienstleisters zur Datenverarbeitung unbeachtlich, d.h. bereits die einmalige Inanspruchnahme ist als Auftrag i.S.d. § 11 BDSG zu verstehen und bedarf eines entsprechenden ADV-Vertrages (z.B. der Auftrag an den Papierentsorger).

Wichtig ist schließlich, dass eine ADV gesetzlich nur dann möglich ist, wenn die Datenverarbeitung innerhalb der EU bzw. des EWR stattfindet. Bei internationalen Datenflüssen, bei denen Daten in Länder außerhalb dieses Gebiets übermittelt werden, sind Sonderregelungen zu beachten (§ 4b Abs. 2 BDSG). Aus diesem Grunde bieten viele Datenverarbeiter mittlerweile Verträge an, in denen eine Datenverarbeitung innerhalb der EU / des EWR zugesichert wird.

3. Vertragsinhalte

Um in den Genuss der ADV-Regelung zu kommen, muss der Auftraggeber zwei wichtige Voraussetzungen erfüllen:

a) er muss den Auftragnehmer sorgfältig auswählen und überwachen und

b) es muss mit dem Auftragnehmer ein sogenannter „Auftragsdatenverarbeitungsvertrag“ (ADV-Vertrag) abgeschlossen werden. § 11 BDSG beschreibt dazu sehr detailliert die einzelnen Rechte und Pflichten, die bei einem ADV-Vertrag zu regeln sind, vgl. dazu unten Ziffer 4 „Checkliste“. Die dort aufgeführten Punkte müssen jeweils individuell zwischen Auftraggeber und Dienstleister festgelegt werden, formelhafte Verweisungen auf den Gesetzestext, z. B. bei den technischen und organisatorischen Maßnahmen (TOM), sind nicht ausreichend.

Wichtig ist schließlich, dass der ADV-Vertrag stets der Schriftform bedarf. Mündliche Aufträge sind nicht ausreichend, auch Vertragsschlüsse per Email/Internet sollten vermieden werden. Auftraggeber sollten sich daher nicht scheuen, auch große ADV-Anbieter (vor allem Cloud-Anbieter) mit dem Wunsch nach einem schriftlichen Vertrag zu konfrontieren.

4. Checkliste

Mit dieser Checkliste prüfen und dokumentieren Sie, ob alle formalen Anforderungen aus dem §11 BDSG in der ADV-Vereinbarung enthalten sind:

Nach §11 BDSG zu regeln	Fundstelle in ADV-Vereinbarung	in Ordnung		Bemerkung
1. Gegenstand und Dauer des Auftrags		□ ja	□ nein	
2. a)Umfang, Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten **2. b) die Art der Daten und der Kreis der Betroffenen**		□ ja	□ nein	
3. die nach § 9 BDSG zu treffenden technischen und organisatorischen Maßnahmen (TOM)		□ ja	□ nein	
4. die Berichtigung, Löschung und Sperrung von Daten		□ ja	□ nein	
5. die nach § 11 Abs. 4 BDSG bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen		□ ja	□ nein	
6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen		□ ja	□ nein	
7. Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers (v.a. Besichtigungsrecht)		□ ja	□ nein	
8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen		□ ja	□ nein	
9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält		□ ja	□ nein	
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.		□ ja	□ nein	
Technische und organisatorische Maßnahmen (TOM) sind vorhanden und angemessen		□ ja	□ nein	

5. Tipps zur Prüfung einer ADV-Vereinbarung

Als Auftraggeber:

Sorgfältige Dienstleister, die sich ihrer Rolle als Auftragsdatenverarbeiter bewusst sind, legen Ihnen für ihre Dienstleistung passend vorbereitete ADV-Verträge vor. Hier sind Sie als Auftraggeber gefordert, zu prüfen, ob zum einen alle formalen Regelungspunkte in dem ADV-Vertrag enthalten sind (siehe obige Checkliste),

zum anderen, ob die zugesicherten Maßnahmen im Umfang Ihren Ansprüchen genügt. Stellen Sie sich auf jeden Fall folgende Fragen:

- Wird zugesichert, dass Ihre Daten nicht in Drittländern verarbeitet werden?
- Ist die Regelung für die Subunternehmer für Sie passend?
- Genügen die Maßnahmen der TOMs Ihren Ansprüchen für Ihre Daten?
- Hat der Auftragnehmer nicht nur die allgemeine Beschreibung der TOMs beifügt, sondern die in seinem Unternehmen für die angebotene Dienstleistung konkret umgesetzten Maßnahmen beschrieben?

Als Auftragnehmer:

Sind Sie der Dienstleister einer Auftragsdatenverarbeitung und Ihr Auftraggeber legt Ihnen einen ADV-Vertrag vor, dann prüfen Sie zum einen die Vollständigkeit der formalen Kriterien in Checkliste unter Ziffer 4. Stellen Sie sich außerdem mindestens noch folgende Fragen:

- Können Sie die Anforderungen aus dem ADV-Vertrag auch praktisch und organisatorisch umsetzen?
- Sind etwa Anforderungen enthalten, die Sie nicht erfüllen können?
- Können Sie die vorgegebenen Regelungen zu Subunternehmern sicherstellen?
- Können Sie die Vorgaben zur Datenlöschung auch technisch umsetzen?
- Haben Sie die interne Organisation für die an Sie gestellten Anforderungen, beispielsweise einem Auskunftsanspruch nachkommen zu können?

6. Ausblick

Mit Inkrafttreten der EU-Datenschutzgrundverordnung in 2018 müssen bestehende ADV-Verträge neu geprüft und bewertet werden. Denn die EU-Datenschutzgrundverordnung enthält zwar einerseits Erleichterungen für den Vertragsschluss, andererseits wird der Auftragnehmer einer ADV stärker in die Verantwortung für die personenbezogenen Daten genommen.

7. Autoren

LUTZ | ABEL Rechtsanwalts GmbH

Birgit Maneth, Rechtsanwältin
Fachanwältin für IT-Recht und für Gewerblichen Rechtsschutz
0821 999828-0, maneth@lutzabel.com

REUNTEC angewandte Informationssicherheit

Dipl.-Math. Petra Nietzer
Auditorin für Datenschutz, Auditorin für IT-Sicherheit, externe Datenschutzbeauftragte
0821 402 88 55, nietzer@reuntec.com

Dieses Merkblatt wurde im Rahmen der Kooperation IT-Sicherheit für Familienunternehmen der IHK Schwaben mit dem Branchennetzwerk aitiRaum e.V. erstellt.

Ihre Ansprechpartnerin:

Dr. Kristin Wirth
Stettenstraße 1 + 3 | 86150 Augsburg
Tel 0821 3162-406 | Fax 0821 3162-342
kristin.wirth@schwaben.ihk.de