



Datenschutz
Einfach
Digital
Gestalten

Auftragsdatenverarbeitung ADV

Die Schattenkosten



Impressum:

Herausgeber:
Datenschutz | Einfach | Digital | Gestalten
eine Initiative der
Marc Weber Management GmbH

Autor:
Marc Weber

Bezugsquelle:
Marc Weber Management GmbH
Lackerbauerstraße 23
81241 München
www.datenschutz-einfach-digital-gestalten.de
datenschutz@marcweber.de
Telefon 089 66 62 86 0
Fax 089 66 62 86 25

Stand:
März 2018

Bildnachweis:
Titelseite: Grundgrafiken: ROverhate - pixaby; Komposition und Gestaltung: Marc Weber Management GmbH

Wichtiger Hinweis zur Nutzung:

Der vorliegende Ratgeber und dessen Inhalt wurden mit größtmöglicher Sorgfalt eruiert und verfasst. Dieses Werk spiegelt die Auffassung des Autors zum Zeitpunkt der Veröffentlichung wider, erhebt jedoch keinen Anspruch auf Vollständigkeit und Richtigkeit. Der Herausgeber sowie der Autor schließen daher die Haftung für etwaige Schäden aus, die sich unmittelbar oder indirekt aus der Nutzung des Werkes und der darin verfassten Informationen ergeben können. Ausgenommen ist hierbei die Haftung für Vorsatz und grobe Fahrlässigkeit.

Der Ratgeber versteht sich als allgemeine Informationsquelle für einen ersten Überblick und eine erste Einschätzung des zugrundeliegenden Themas in Form einer unverbindlichen Anregung. Die Nutzerin / Der Nutzer ist hierbei nicht von einer sorgfältigen eigenverantwortlichen Prüfung entbunden. Vor einer Übernahme des unveränderten Inhalts (auch in Teilauszügen) ist von der Nutzerin / vom Nutzer daher genau abzuwägen, ob und in welchen Abschnitten eine Anpassung an die konkret zu regelnde Situation und Rechtsentwicklung erforderlich ist. Der Herausgeber ist nicht für die Nachnutzung der zugrundeliegenden Inhalte verantwortlich.

Liebe Leserinnen und Leser,

Die Auftragsdatenverarbeitung ist immer wieder Anlass für Unklarheiten und Diskussionen auf Seiten der verantwortlichen Stellen. Bei Aufsichtsbehörden gehören diese Vereinbarungen zu dem Standardprüfkatalog und sind regelmäßig Grundlage für Sanktionen und Bußgelder. Für Unternehmen und Vereine, die die Voraussetzungen zum Abschluss einer derartigen Vereinbarung erfüllen, jedoch noch keine Vereinbarung getroffen haben, sollten zügig die vorhandenen Lücken im Vertragsmanagement beseitigen.

Mit diesem Ratgeber beschäftigen wir uns allerdings nicht mit der eigentlichen Vereinbarung zur Auftragsdatenverarbeitung, sondern beleuchten die Schatten rund um diese Vereinbarungen. In zahlreichen Orientierungsblättern und Leitfäden werden kompakt die Bereiche und Prozesse aufgelistet, für die eine Auftragsdatenverarbeitung benötigt wird und welche Tätigkeiten externer Dienstleister regulär nicht unter diesem Gesichtspunkt zu betrachten sind. Weiterhin halten diverse Behörden und Organisationen Mustervereinbarungen zu unterschiedlichen Anwendungsfeldern bereit. Was der überwiegenden Mehrheit fehlt ist der Blick auf die notwendigen Grundlagen und die sich darin verbergenden Aufwendungen. Mit der reinen Vertragsunterzeichnung ist es genau betrachtet nicht erledigt.

Viel Spaß bei der Lektüre

Ihr Marc Weber

Kurzer Einblick in die aktuelle Lage

In dem Bundesdatenschutzgesetz (BDSG) ist die Grundlage für Auftragsdatenverarbeitungen in § 11 - Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag - festgehalten. Dort heißt es unter anderem:

„(1) Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Die in den §§ 6, 7 und 8 genannten Rechte sind ihm gegenüber geltend zu machen.

[...]

(5) Die Absätze 1 bis 4 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.“

Der Absatz 5 ist von besonderer Bedeutung. Dieser trifft auf IT-Wartungsverträge, externe IT-Dienstleister und Hostinganwendungen für Onlinedienste zu. Themen, die nahezu für jedes Unternehmen oder jeden Verein von Bedeutung sein können und eine Auftragsdatenverarbeitung aktuell werden lassen.

Regelmäßig sind unter anderem folgende Tätigkeiten und serviceangebote externer Dienstleister im Fokus (Bezug zu personenbezogenen Daten vorausgesetzt):

- Datenerhebung eines Callcenters*
- Cloud-Computing*
- E-Mail-Postfach-Verwaltung*
- Webhosting*
- IT-(Fern)Wartung*
- Daten- und Dateimanagement*
- Akten- und Datenvernichtung*

Tätigkeiten, die allgemein keine Auftragsdatenverarbeitung im Sinne der Datenschutzbestimmungen darstellen sind:

- Auslagerung von Aufgaben und/oder Funktionen (bspw. Mitarbeiterrekrutierung, Vertragskundenbetreuung)*
- Bezug von Fachleistungen externer Dienstleister (bspw. Finanzberatung, Steuerberatung, Wirtschaftsprüfung)*
- Tätigkeiten externer Dienstleister zu deren Durch- und Ausführung personenbezogene Daten ein unausweichliches Beiwerk darstellen (bspw. Post- oder Bankdienstleistungen)*

Allen drei Schwerpunkten liegt der Umstand zugrunde, dass die erbrachten Tätigkeiten der externen Dienstleister auf deren fachliche Expertise und Spezialisierung eigenständig erbracht werden. Der Auftraggeber, als verantwortliche Stelle, greift nicht in den Arbeitsprozess ein, sodass der Auftragnehmer weisungsfrei die Tätigkeit erbringt. Ein entscheidendes Indiz zur Beurteilung einer vorliegenden Auftragsdatenverarbeitung.

Die beiden Übersichten über Tätigkeiten, die einer Auftragsdatenverarbeitung zuzurechnen sind und diejenigen, die regulär nicht als eine Auftragsdatenverarbeitung gesehen werden sind relativ umfangreich und könnten noch weiter ausgeführt werden. Gerade beim Outsourcen im IT- und Digitalbereich kommen täglich neue Angebote und Dienstleister hinzu. Grund genug für jedes Unternehmen und jeden Verein, sich einmal mit dieser Thematik zu befassen und die eigenen Prozesse zu prüfen. Heutzutage kommt es nur noch in den seltensten Fällen dazu, dass Unternehmen oder Vereine alle Tätigkeiten rund um personenbezogene Daten im eigenen Hause abbilden können.

Im nachfolgenden Themenblock versuchen wir einmal das Thema der Auftragsdatenverarbeitung etwas ganzheitlicher zu betrachten und die möglichen Folgeaufwendungen näher zu skizzieren.

Die Schattenkosten berücksichtigen und planen

Vielfach ist in Vorträgen und Seminaren zur Digitalisierung und deren gelungenen Umsetzung die Rede von der Cloud und die Auslagerung von IT und IT-Dienstleistungen. Oftmals kommt dieser Ratschlag schon einem Heilsbekenntnis gleich, wonach es ohne eine Auslagerung und externer Dienstleister für die Unternehmen gar keine Zukunft mehr in der digitalen Epoche geben wird. Zugegeben ist das schon etwas stark aufgetragen. Berater leben vielfach von der Zahl der geleisteten Veränderungen und nicht von den tatsächlichen Verbesserungen, die erst eintreten – oder eben auch nicht, wenn der Berater längst wieder das Unternehmen verlassen hat. Neben den tatsächlichen Vorteilen der Cloud und der Inanspruchnahme externer Dienstleister, werden die Aufwendungen und Risiken gerne vernachlässigt oder gar nicht erwähnt. Dabei ist die juristische Lage eindeutig:

„Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.“ (§ 11 Abs. 2 BDSG)

Bevor die Vereinfachung des Arbeitsalltages durch das Outsourcen im eigenen Unternehmen ankommt, sind erst einmal zahlreiche anspruchsvolle Tätigkeiten zu bewältigen. Ein kleiner Auszug aus einer möglichen Vorbereitungsphase:

- Marktsondierung
- Anbieter anhand Preis und Leistung vergleichen
- Technische Spezifikationen klären
- Auftragsdatenverarbeitung vertraglich formulieren
- Vor-Ort-Prüfung (Organisation und Sicherheit)

Ist ein Anbieter ausgewählt, gilt es den Vertrag zu schließen und die Vereinbarung zu einer Auftragsdatenverarbeitung final zu fassen und ebenfalls zu unterschreiben. Mit diesem Schritt kehrt vorerst Ruhe ein, doch kann das Thema nicht

zu den Akten gelegt werden. Regelmäßige Folgekontrollen während des laufenden Prozesses sind abzuhalten. Ein relativ umfassender Arbeitsablauf, der sehr zeit- und auch kostenintensiv ist.

Für eine qualifizierte Markt- und Anbieter sondierung ist meist die Unterstützung externer IT-Kenner notwendig, um ein umfassendes Marktbild zu erhalten und um das Preis-Leistungs-Verhältnis richtig einschätzen zu können. Für die vertragliche Seite sollten im Bedarfsfall Rechtsanwälte und/oder Datenschutzexperten mit einbezogen werden. Werden vorgelegte Vertragsmuster des Dienstleisters nicht akzeptiert, ist es übliche Praxis, dass der künftige Auftraggeber auch die Kosten des Rechtsbeistandes des Auftragnehmers zu begleichen hat. Je nach Standort der Datenverarbeitung können hohe Aufwendungen für die Anreise zu Buche schlagen. Die eigenen Reisekosten und Spesen sind zu übernehmen und meist auch Tagespauschalen beim Dienstleister für die Betreuung durch die dortigen Mitarbeiter.

Die nächste Falle lauert in der fachlichen Einschätzung der Lage. Meist werden externe Experten beauftragt, weil im eigenen Hause das notwendige Fachpersonal fehlt. Hat ein Unternehmen keine eigene Fachkompetenz, sind Kontrollmaßnahmen gefährdet. Für eine umfassende Einschätzung werden wieder externe Experten oder Berater benötigt. Dabei ist ein derartiger Aufwand durch die gesetzlich geforderte Regelmäßigkeit von Kontrollen konstant im Haushaltsplan zu berücksichtigen.

Je nach Art und Umfang der ausgelagerten Tätigkeit, kann ein Kontrolltag die eigentlichen Jahresgebühren der Dienstleistung um ein vielfaches übersteigen.

Tipp:

Bevor sich Unternehmen oder Vereine auf eine Auslagerung der Prozesse stürzen, sollte in Anbetracht der Kosten-Nutzen-Rechnung auch berücksichtigt werden, ob eine vergleichbare Leistung nicht auch im eigenen Hause umsetzbar ist.