Auftragsdatenverarbeitung

Eine Auftragsdatenverarbeitung liegt vor, wenn personenbezogene Daten eines Auftraggebers von einem Auftragnehmer erhoben, verarbeitet oder genutzt werden. Geschieht dies, muss ein entsprechender Vertrag nach § 11 Bundesdatenschutzgesetz abgeschlossen werden. Oft kommt es zu solchen Verträgen, wenn ein Unternehmen Aufgaben und Strukturen, wie zum Beispiel die Personalverwaltung, auf externe Dienstleister auslagert. (Outsourcing) Die Verantwortung für die ordnungsgemäße Datenverarbeitung bleibt hier jedoch bei dem Auftraggeber und dieser ist verpflichtet einen Vertrag zu erstellen und mit dem Arbeitnehmer schriftlich abzuschließen.

§ 11 Abs. 1 Satz 1 BDSG: 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.

Erstens müssen die Dauer des Auftrags und der Gegenstand, also die Art der Dienstleistung hinterlegt sein. (§ 11 Abs. 2 Nr. 1 BDSG) Zudem wird Umfang, Art und Zweck der vorgesehenen Datenverarbeitung gefordert. (§ 11 Abs. 2 Nr. 2 BDSG) Das beinhaltet eine Auskunft darüber, welche personenbezogenen Daten im Rahmen des Auftrages bearbeiten werden und wie groß der Kreis der Betroffenen ist. Zu den Daten zählen zum Beispiel Name, Vorname, Anschrift und Telefonnummer. Außerdem wird hier belegt, dass der Auftragnehmer die verwendeten Daten geheim hält, keine unbefugten Kopien anfertigt, nur die vorgesehenen Daten verwendet entsprechend seiner Leistungsbeschreibung handelt.

§ 11 Abs. 2 Satz 1 BDSG: Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen …

Der Auftraggeber muss sicherstellen, dass die im Vertrag hinterlegten technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit berücksichtigt werden und den Auftragnehmer dementsprechend sorgfältig auswählen.

§ 11 Abs. 2 Nr. 3 BDSG: die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen

Unter technischen Maßnahmen sind alle physischen Schutzversuche zu verstehen. Das ist zum Beispiel eine Umzäunung des Geländes, also generell alle baulichen Maßnahmen wie die Sicherung von Türen und Fenstern, sowie die Installation von Alarmanlagen. Technische Maßnahmen können jedoch auch in Soft- und Hardware umgesetzt werden. Geläufig ist hier das Einsetzen von Firewalls, sicheren Verschlüsselungsverfahren, Protokollen zur Datenübermittlung, eine unabhängige Stromversorgung, Passworterzwingung und Prüfung der Passwortqualität, der Einsatz von Routern zur Bildung von Netzwerksegmenten und vieles mehr.

Organisatorische Maßnahmen betreffen die Vorgehens- und die Verfahrensweisen der Mitarbeiter und sind in den Handlungsanweisungen enthalten. Beispielhaft für solche Maßnahmen sind die Erstellung von Passwortrichtlinien, Dokumentation von Datenvernichtungsmaßnahmen, Definitionen über die Arbeit mit personenbezogenen Daten, die Beauftragung zuverlässiger Transportunternehmen und Kontrolle von Fernwartungen.

Diese Maßnahmen sind in den vorgegebenen Anforderungen des BDSG enthalten:

|  |  |
| --- | --- |
| 1. Zutrittskontrolle 2. Zugangskontrolle 3. Zugriffskontrolle 4. Weitergabekontrolle | 1. Eingabekontrolle 2. Auftragskontrolle 3. Verfügbarkeitskontrolle 4. Trennungsgebot |

Falls der Auftragsdatenverarbeitungsvertrag nicht abgeschlossen wird oder inhaltlich nicht den gesetzlichen Vorgaben entspricht, handelt der Auftraggeber ordnungswidrig.

§ 43 Abs. 1 Nr. 2b BDSG: Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig entgegen § 11 Absatz 2 Satz 2 einen Auftrag nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt […].

Müssen Berichtigungen, Löschungen oder Sperrungen von personenbezogenen Daten vorgenommen werden, dürfen die Auftragnehmer nur nach vorheriger Zustimmung des Auftraggebers handeln. (§11 Abs. 2 Nr. 4 BDSG)

Der Auftragnehmer muss sich außerdem verpflichten seine Mitarbeiter mit den maßgebenden Bestimmungen des Datenschutzes vertraut zu machen und das Datengeheimnis laut § 5 BDSG zu wahren. Auch eine Überwachung der Vorschriften ist Pflicht. (§11 Abs 2. Nr. 5 BDSG)

Falls für gewisse Arbeiten, wie zum Beispiel eine Wartung oder Prüfung der automatisierten Verarbeitungen, muss für diese Unterauftragnehmer eine schriftliche Zustimmung des Auftraggebers vorhanden sein. Die vereinbarten Datenschutzregelungen müssen dann vom Auftragnehmer gegenüber dem Unterauftragnehmer vertraglich sichergestellt sein. (§11 Abs. 2 Nr. 6 BDSG)

Es folgen die Kontrollrechte des Auftraggebers. (§ 11 Abs. 2 Nr. 7 BDSG) Der Auftraggeber wird in diesem Abschnitt des Vertrages dazu berechtigt Kontrollen bezüglich der vertraglichen Vereinbarungen und der Einhaltung der Vorschriften des Datenschutzes durchzuführen.

Kommt es zu Verstößen gegen die Vorschriften zum Schutz personenbezogener Daten oder die im Auftrag getroffenen Festlegungen, ist dies laut §11 Abs. 2 Nr. 8 BDSG dem Auftragnehmer unverzüglich mitzuteilen. Hier wird auch erwähnt, wer im Falle eines Schadens Ersatz leisten muss.

Im vorletzten Punkt erklärt der Auftragnehmer sich damit einverstanden personenbezogene Daten nur der Weisungen des Auftraggebers entsprechend zu erheben, zu verarbeiten oder zu nutzen. (§11 Abs. 2 Nr. 9 BDSG)

Als letztes wir im Vertrag hinterlegt, was bei der Beendigung des Auftrags passiert. Dazu gehört die Löschung sämtlicher genutzter Daten, beziehungsweise die Rückgabe der Daten. Dabei können Sicherheitskopien ausgeschlossen werden, weil sie zur Erfüllung von Haftungs- und Gewährleistungsansprüchen dienen. Diese sind dann aber so zu sperren, dass der Auftragnehmer diese nicht mehr nutzen kann. (§11 Abs. 2 Nr. 10)

Fällt dem Auftragnehmer auf, dass eine Weisung des Arbeitgebers nicht dem Gesetz oder anderen Vorschriften des Datenschutzes entspricht, hat er den Auftraggeber unverzüglich darauf hinzuweisen. (§11 Abs. 3)

Kriterien zur Auftragsdatenverarbeitung

Es ist wichtig zu erkennen, wann eine Auftragsdatenverarbeitung vorliegt, denn oft ist es schwierig sie von der Funktionsübertragung abzugrenzen. Dazu gibt es in Aufsichtsbehörden oder auch in der Literatur Kriterienkataloge, die die wichtigsten Punkte beschreiben. Ein wichtiger Aspekt ist, dass der Auftragnehmer keine Entscheidungsbefugnis über die übermittelten Daten hat und ihm die Nutzung der persönlichen Daten verboten ist, solange es sich nicht um den vereinbarten Überlassungszweck handelt. Außerdem ist der Auftragnehmer verpflichtet dem Auftraggeber darüber zu informieren, was mit den Daten geschieht. Damit ist also der Auftraggeber für alle Daten nach außen hin verantwortlich. Ein weiteres Kriterium besagt, dass der Auftragnehmer in keiner vertraglichen Beziehung zum Betroffenen stehen darf.

Bei einer Funktionsübertragung hingegen, werden die Nutzungsrechte der persönlichen Daten dem Auftragnehmer überlassen. Dieser trägt damit die eigenverantwortliche Sichererstellung von Zuverlässigkeit und Richtigkeit der Daten. Damit ist der Dienstleister nun dafür zuständig die Rechte des Betroffenen zu berücksichtigen. Das sind zum Beispiel die Benachrichtigungspflicht und der Auskunftsanspruch.

Trotz dieser Kriterien, ist es oft nicht eindeutig, welcher Fall vorliegt. Es gibt einige Sonderfälle, wie zum Beispiel die Wartung und Prüfung von automatisierten Verarbeitungen, bei denen ein Auftragsdatenverarbeitungsvertrag notwendig ist, weil der Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. (§11 Abs. 5 BDSG)

Beispiele zur Auftragsdatenverarbeitung

1. Beauftragung eines Callcenters zur Kundenkommunikation
2. Ablage von personenbezogenen Daten auf extern gehosteten Servern. (Egal ob für Produktivsysteme oder Backups)(Gola/Schomerus verneinen hier ADV, da er Hoster ja nichts mit der eigentlichen DV zu tun hat. Anm. d. A: Der Hoster wird aber für die Wartung der Systeme verantwortlich sein, dabei kann eine Kenntnisnahme nicht ausgeschlossen werden, also doch ADV?)
3. Wartungsdienstleistungen, bei denen nicht ausgeschlossen werden kann, dass während der Wartung personenbezogene Daten zur Kenntnis gelangen
   * Wartung von IT-Systemen
   * Wartung von TK-Anlagen
4. Entsorgung von Akten oder Datenträgern durch externe Unternehmen

**Keine ADV** liegt per Definition beim Postversand oder Bankgeschäften vor.