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 und 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. Der Umfang des zu betreibenden Aufwands der Maßnahmen muss dem angestrebten Schutzweck entsprechen. (§11 Abs. 2 Nr. 3 BDSG)

Unter technischen Maßnahmen sind alle physischen Schutzversuche zu verstehen. Das ist zum Beispiel eine Umzäunung des Geländes, also generell alle baulichen Maßnahmen, jedoch auch Maßnahmen in Form von Soft- und Hardware.

Organisatorische Maßnahmen betreffen die Vorgehens- und die Verfahrensweisen der Mitarbeiter und sind in den Handlungsanweisungen enthalten. Beispielhaft für solche Maßnahmen sind Richtlinien, Dokumentation und Kontrollen.

Diese Maßnahmen sind in den vorgegebenen Anforderungen des BDSG enthalten und behandeln folgende Schutzziele:

* Vertraulichkeit:
  + Zutrittskontrolle: Die Zutrittskontrolle soll die räumliche Annäherung an die Datenverarbeitungsanlagen verhindern. Unbefugten kann hierbei zum Beispiel durch bauliche/technische Maßnahmen wie Alarmanlagen oder abgesicherte Türen und Fenster der Zutritt verwehrt werden. Passende organisatorische Maßnahmen sind Kontrollgänge, die Protokollierung der Zutritte und Abgänge, Pförtner oder auch das Begleiten von Besuchern.
  + Zugangskontrolle: Verhindert unberechtigte Nutzung der IT-Systeme durch technische Barrieren, wie eine technische Prüfung der Passwortqualität, Firewalls oder automatische Sperrmechanismen. Organisatorische Maßnahmen dazu sind Passwortrichtlinien, Arbeitsanweisungen zur Bildschirmsperre und Ausrichtung der Monitore, sodass sie nicht direkt für Dritte einsehbar sind.
  + Zugriffskontrolle: Wenn IT-Systemen auf persönliche Daten zugegriffen wird, darf dies nur durch berechtigte Nutzer geschehen. Das Einsehen, Lesen, Kopieren, Verändern oder Entfernen sensibler Daten, darf unbefugten Personen nicht möglich sein. Das kann auf technischer Ebene durch aktuelle Verschlüsselungsverfahren, durch Kopierkontrollen und durch passende Zugriffsrechte der Nutzer in der Software gewährleistet werden. Organisatorische Maßnahmen könnten Fernwartungskontrollen, Dokumentationen von Datenvernichtungsmaßnahmen oder auch die Verriegelung von Laufwerken sein.
  + Trennungsgebot: Daten die nichts miteinander zu tun haben und zu unterschiedlichen Zwecken erhoben werden, sind vollständig von einander zu trennen. Hierfür sind Router hilfreich um Netzwerksegmente zu bilden. Ebenso können logische Datenbanken für die technische Trennung eingesetzt werden. Daraus folgen dann ausführliche Dokumentationen als organisatorische Maßnahmen.
  + Auftragskontrolle: Bei der Auftragskontrolle muss sichergestellt werden, dass der Dienstleister die personenbezogenen Daten strikt nach den Weisungen des Auftraggebers behandelt werden. Ein Beispiel hierfür ist der Auftragsdatenverarbeitungsvertrag an sich.
* Integrität
* Weitergabekontrolle: Werden Daten übermittelt oder transportiert, ist unbefugtes Einsehen oder Verarbeiten ebenfalls zu verhindern. Technische Maßnahmen sind hier wie bei der Zugriffskontrolle Verschlüsselungsverfahren die dem Stand der Technik entsprechen. Auch die Protokollierung des Datenverkehrs und ein sicheres, permanentes Löschen der Daten ist wichtig. Um die organisatorischen Maßnahmen zu erfüllen, sollten Firmen zuverlässige Transportunternehmen beauftragen und den Transportweg dokumentieren.
* Eingabekontrolle: Eine Überprüfung der Mitarbeiter darüber, wann personenbezogene Daten behandelt hat, findet unter der Eingabekontrolle statt. Protokolle von Eingaben, Änderungen und Löschungen dieser Daten und entsprechende Auswertungssysteme können das technisch umsetzen. Außerdem sollten aus organisatorischer Sicht Regeln für die Bearbeitung der persönlichen Daten geschaffen werden. Und Protokolle fristgerecht gelöscht werden.
* Verfügbarkeit
  + Verfügbarkeitskontrolle: Damit Verfügbarkeit gewährleistet werden kann, sollten Datenverluste und Datenzerstörung vermieden werden. Vorkehrungen zur Wiederherstellung sind dabei Pflicht. Technische Maßnahmen können Archivierungssysteme, eine unabhängige Stromversorgung oder Virenschutzprogramme sein. Klimaanlagen in Serverräumen können Systemausfälle verhindern und als organisatorischen Maßnahmen kann man die sichere Aufbewahrung der Datensicherungen sehen.

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 externe Unternehmen für Arbeiten, wie zum Beispiel Wartungen oder Prüfungen der automatisierten Verarbeitungen beauftragt werden, 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 wird 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)