Auftragsverarbeitung

Von Datenverarbeitung im Auftrag spricht man, wenn die datenverarbeitende Stelle (verantwortliche Stelle) sich einer Stelle bedient (Dienstleister), die für die Einrichtung im Auftrag und weisungsabhängig personenbezogene Daten erhebt, verarbeitet oder nutzt. Dabei haftet der Auftraggeber (die Einrichtung) dem Dateneigentümer (Betroffener) gegenüber.

In dem seit dem 24.Mai 2018 geltenden Gesetz über den Kirchlichen Datenschutz ist die Auftragsverarbeitung in § 29 KDG geregelt. Der Begriff „Auftragsdatenverarbeitung“, welcher sich in der KDO fand, wurde durch den Terminus „Auftragsverarbeitung“ ersetzt.

Beispiele für Auftragsverarbeitung sind: Rechenzentren, externe Agenturen (Headhunter, Assessment-Center), externe Dienstleister mit „Remote-Zugriff“ (Server, Wartungsverträge, Softwarepflege), externe Dienstleister für Peripherie-Geräte (Fax, Drucker, Multifunktionsgeräte, Scanner, Kopierer), Entsorger (IT, TK, Aktenentsorgung), externe Berater mit Zugriff auf Software und personenbezogene Daten, Internet-Service-Provider (Fremdsoftware als Dienstleistung).

Nach § 29 Abs. 1 KDG ist der Auftragnehmer (Dienstleister), der personenbezogene Daten im Auftrag des Auftraggebers (Einrichtung) verarbeitet, sorgfältig auszuwählen. Dabei sind die vom Dienstleister getroffenen technischen und organisatorischen Maßnahmen zu Datenschutz und Datensicherheit gemäß § 26 KDG zu prüfen. Die Überprüfung kann durch einen Termin vor Ort, über eine schriftliche Validierung der Umsetzung (z.B. per Fragebogen) oder durch Vorlage von passenden Zertifizierungen erfolgen. Die Prüfung erfolgt durch den betrieblichen Datenschutzbeauftragten.

Der Vertrag zur Datenverarbeitung im Auftrag ist schriftlich zu erteilen (Auftragsverarbeitungsvertrag) und muss den Anforderungen des § 29 KDG genügen. Folgende Punkte müssen im Vertag aufgeführt werden:

- **Gegenstand und Dauer des Vertrages**
  Der Auftrag der Verarbeitung muss verständlich bezeichnet werden. Auch wenn nicht einzelne Verarbeitungsschritte benannt werden müssen, so muss aber deutlich gemacht werden, welchen Umfang die Arbeiten haben, die vom Auftragnehmer erledigt werden.

- **Regelung von Umfang, Art und Zweck**
  Im Auftragsdatenerarbeitungsvertrag sind konkrete Weisungen im Hinblick auf die Verarbeitung zu treffen, dies kann auch einzelne Verarbeitungsschritte betreffen. Im Vertrag sollten die Möglichkeiten aber auch die Grenzen der Datenverarbeitung durch den Auftragnehmer deutlich werden.
  Der Zweck der Verarbeitung der Daten ist im Vertag zu benennen. Die Art der Daten ist genau zu beschreiben (hier helfen die Angaben aus den Verfahrensverzeichnissen). Der Kreis der Betroffenen ist so konkret wie möglich zu erfassen.

- **Festlegung der zu treffenden technischen und organisatorischen Maßnahmen**
  Der Vertrag muss konkrete Regelungen beinhalten, welche technischen und organisatorischen Maßnahmen vom Auftragnehmer bei der Durchführung des Auftrages eingehalten werden müssen. Diese Maßnahmen sind konkret zu bezeichnen.

- **Regelungen zu Berichtigung, Löschung und Sperrung von Daten im Auftrag**
  Der Vertrag sollte Regelungen enthalten, aus denen sich Berichtigung, Löschung und Sperren von Daten durch den Auftraggeber ergeben. Diese Maßnahmen dürfen nur auf Weisung des Auftraggebers erfolgen.

- **Regelungen zu den Pflichten des Auftragnehmers**
  Im Vertrag sind die gesonderten Anforderungen an den Auftragnehmer auszuführen, z. B. Verpflichtung auf das Datengeheimnis, Bestellung eines betrieblichen Datenschutzbeauftragten etc.

- **Regelungen zu Untervertragsverhältnisses**
  Es ist zu regeln, ob und wie eine Beauftragung von Unterauftragnehmern durch den Auftragnehmer bei der Verarbeitung von Daten erfolgen kann. Diese können Support- und Entwicklungsangebote großer Softwarefirmen sein (24h-Dienstleistung; Tochterfirmen im Ausland).

- **Regelungen zu Kontrollrechten des Auftraggebers und entsprechenden Duldungspflichten des Auftragnehmers**
  Um eine wirksame Kontrolle des Auftragnehmers vornehmen zu können, müssen Kontrollrechte vertraglich vereinbart werden. Damit gehen entsprechende Duldungspflichten des Auftragnehmers einher (Zugang zu den Geschäftsräumen).

- **Regelungen zu Informationspflichten des Auftragnehmers bei Verstößen gegen Datenschutzvorschriften oder Pflichten gegenüber dem Auftraggeber**
  Bei Unregelmäßigkeiten bzw. Verstößen gegen Rechtsvorschriften oder vertragliche Pflichten ist der Auftraggeber zu informieren.

- **Regelung des Weisungsrechts**
  Aus dem Vertrag muss sich ergeben, dass die dort getroffenen Regelungen abschließenden Charakter haben. Ergänzende Weisungsrechte des Auftraggebers sind genau zu regeln (Wer kann Weisungen aussprechen? In welcher Form werden diese kommuniziert?).

- **Regelungen zur Rückgabe bzw. Löschung der Daten nach Auftragsbeendigung**
  Es muss gewährleistet sein, dass nach Beendigung des Auftrags keine personenbezogenen Daten mehr beim Auftragnehmer verbleiben.