Vereinbarung zur Auftragsdatenverarbeitung gem. § 11 Abs. 5 BDSG

Werden personenbezogene Daten im Auftrag verarbeitet, muss vom beauftragenden Unternehmen nach § 11 BDSG ein Vertrag zur Auftragsdatenverarbeitung abgeschlossen werden. In der Regel unterhalten Unternehmen eine Vielzahl von Auftragsdatenverarbeitungsverhältnissen, insbesondere in den Bereichen IT und Personalverwaltung.

Wozu brauche ich einen Vertrag zur Auftragsdatenverarbeitung?

Ein Vertrag, der die sog. Auftragsdatenverarbeitung regelt, ist natürlich nur dann erforderlich, wenn es sich der Natur der Datenverarbeitung nach um eine Auftragsdatenverarbeitung handelt. Unter Auftragsdatenverarbeitung versteht man die weisungsgebundene Datenverarbeitung durch Externe, bei der die Verantwortung für die ordnungsgemäße Datenverarbeitung beim Auftraggeber verbleibt. In der Regel unterhalten Unternehmen eine Vielzahl von Auftragsdatenverarbeitungsverhältnissen, insbesondere in den Bereichen IT und Personalverwaltung. So liegt häufig bereits eine Auftragsdatenverarbeitung vor, wenn Unternehmen z.B. für ihre Datenverarbeitung Kapazitäten externer Rechenzentren nutzen oder die Lohn- und Gehaltsabrechnung durch andere Unternehmen durchführen lassen. Liegt eine Auftragsdatenverarbeitung vor, ist zwischen den Parteien vor Beginn der Auftragsdatenverarbeitung ein entsprechender Vertrag zu schließen.

Was, wenn ich keinen Vertrag abgeschlossen habe?

Die Anforderungen an die Auftragsdatenverarbeitung sind durch den Gesetzgeber im Rahmen einer Novellierung des Bundesdatenschutzgesetzes 2009 massiv verschärft worden. Wird ein Auftrag zur Auftragsdatenverarbeitung u.a. nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt, stellt dies eine Ordnungswidrigkeit dar, die mit einem Bußgeld von bis zu 50.000,- Euro geahndet werden kann (§ 43 Abs. 1 Nr. 2b, Abs. 3 BDSG)

Wie sehen Verträge zur Auftragsdatenverarbeitung aus?

Hat man also nun festgestellt, dass tatsächlich ein Auftragsdatenverarbeitungsverhältnis vorliegt, so kann man den Inhalt dieses Vertrages nicht etwa selbst bestimmen. Ausnahmsweise hat sich der Gesetzgeber hier mal in die Privatautonomie der Vertragsparteien eingemischt und einen Mindest-Vertragsinhalt in § 11 BDSG vorgegeben. Demgemäß muss ein Vertrag zur Auftragsdatenverarbeitung Festlegungen zu folgenden 10 Punkten enthalten:

1. der Gegenstand und die Dauer des Auftrags,
2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
3. die nach § 9 BDSG zu treffenden technischen und organisatorischen Maßnahmen,
4. die Berichtigung, Löschung und Sperrung von Daten,
5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,

9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Hier finden Sie eine Auswahl von Musterverträgen zur Auftragsdatenverarbeitung, die im Internet zu finden sind:

- Landesbeauftragten für Datenschutz Niedersachsen
- BfDI Datenschutz Wiki
- Hessischer Datenschutzbeauftragter

Die Musterverträge sind auf die Gegebenheiten des jeweiligen Auftragsdatenverarbeitsverhältnisses anzupassen und sollten nicht ohne vorherige Prüfung übernommen werden.

Was ist bei technischen und organisatorischen Maßnahmen zu beachten?

Besonders schwierig ist es, die zu treffenden technischen und organisatorischen Maßnahmen (Nr. 3) zu bestimmen. Hier reicht leider kein allgemeiner Satz, dass diese eingehalten werden. Vielmehr ist auf jeden der in Anlage zu § 9 Satz 1 BDSG genannten Punkte einzugehen. Zu beachten ist allerdings auch hier, dass nicht immer sämtliche getroffenen Maßnahmen gegenüber dem Auftraggeber offenbart werden können. Denn immerhin muss auch die eigene Daten- und Informationssicherheit noch gewährleistet bleiben.

Welche besonderen Problemfelder gibt es?

Leider wäre es zu einfach, wenn die oben genannten 10 Punkte immer gelten würden, doch tatsächlich können sie nicht immer strikt und vollumfänglich umgesetzt werden. Denn in vielen Fällen weicht die Praxis von den zugrundeliegenden Vorstellungen des Gesetzgebers ab. Ein Beispiel hierfür ist etwa der externe IT-Dienstleister, der nur In-House arbeitet und für den daher nur wenige der gesetzlich vorgeschriebenen Punkte tatsächlich zutreffend sind.

Ein weiteres Problem in der Praxis ist außerdem, wenn der Auftragnehmer im datenschutzrechtlichen Sinne zufällig der Mutterkonzern des Auftraggebers ist. Hier ist es in der Praxis oft sehr schwierig, den Mutterkonzern auf die Einhaltung bestimmter datenschutzrechtlicher Maßnahmen zu verpflichten oder diesem gar zu erklären, dass er abhängig von den Weisungen des Tochterunternehmens ist. Ärger ist hier meist vorprogrammiert.

Gibt es Gestaltungsspielräume?

Trotz Vorgaben des Vertragsinhaltes durch den Gesetzgeber bleibt die genaue Ausgestaltung der Verträge einzelfallabhängig. Insbesondere verbleiben gewisse Gestaltungsspielräume, die zugunsten des jeweiligen Auftraggebers oder Auftragnehmers ausgeschöpft werden können.