Legal Update
Datenschutzrecht

Vorsicht bei der Auftragsdatenverarbeitung

Dr. Katharina Landes **Köln, 28.10.2015**

Ein Unternehmen, das die Verarbeitung von personenbezogenen Daten an einen externen Dienstleister auslagert, muss mit diesem einen umfassenden schriftlichen Vertrag über die Einhaltung der datenschutzrechtlichen Vorgaben abschließen („Auftragsdatenverarbeitungsvereinbarung“, kurz ADV). Fehlt die schriftliche Auftragserteilung ganz oder ist diese unzureichend formuliert, droht dem Auftraggeber eine Geldbuße.

I. Fall einer unzureichenden Auftragserteilung

In einem Fall einer unzureichenden ADV verhängte das Bayrische Landesamt für Datenschutzaufsicht (BayLDA) unlängst eine Geldbuße in fünfstelliger Höhe. Das Unternehmen, gegen das die Geldbuße verhängt wurde, hatte mehrere externe Dienstleister mit der Verarbeitung von personenbezogenen Daten beauftragt. In der schriftlichen Auftragserteilung hatte das Unternehmen jedoch keine konkreten technischen und organisatorischen Maßnahmen, die der Dienstleister zum Schutz der Daten einzuhalten hat, benannt. Der Vertrag enthielt lediglich pauschale Aussagen zur Auftragsdatenverarbeitung und die Wiederholung des Gesetzestextes. Das BayLDA entschied, dass dies keinesfalls ausreichend ist.

II. Die Auftragsdatenverabeitung

Was ist darunter zu verstehen?
Ein Unternehmen hat grundsätzlich die Möglichkeit, die Verarbeitung von personenbezogenen Daten (z.B. der Arbeitnehmer oder Kunden) auf externe Dienstleister zu übertragen, ohne dass der Betroffene der Weitergabe seiner Daten an den externen Dritten zustimmen muss. Die gesetzliche Grundlage für diese Auftragsdatenverarbeitung findet sich in § 11 Bundesdatenschutzgesetz (BDSG). Im Fall der Auftragsdatenverarbeitung macht das Unternehmen dem externen Auftragnehmer detaillierte Vorgaben dazu, wie die Datenverarbeitung erfolgen soll. Der Auftragnehmer fungiert quasi nur als verlängerter Arm des Unternehmens, die datenschutzrechtliche Verantwortung bleibt beim Unternehmen.

Abgrenzung zur Funktionsübertragung
Wenn der Auftragnehmer hingegen gewisse Freiheiten/Entscheidungsspielräume bei der Datenverarbeitung hat, liegt keine Auftragsdatenverarbeitung, sondern eine Funktionsübertragung vor. Hier bedarf es dann grundsätzlich des Einverständnisses des Betroffenen mit der Weitergabe seiner Daten an den Auftragnehmer (wenn kein gesetzlicher Erlaubnistatbestand vorliegt).

Beispiele für Auftragsdatenverarbeitungen
Eine Auftragsdatenverarbeitung liegt in der Regel bei folgenden Dienstleistungen vor:

- Erstellung der Gehaltsabrechnungen durch externen Dienstleister
- Auslagerung von Datenverarbeitungen im Rahmen von Cloud-Computing
- Beauftragung von Lettershops
- Datenerhebung durch ein Callcenter
- Auslagerung eines Teils des eigenen Telekommunikationsanlagenbetriebs (soweit nicht TKG)
- E-Mail-Verwaltung und sonstige Datendienste zu Webseiten durch externen Dienstleister
- Datenerfassung, Datenkonvertierung und Einscannen von Dokumenten durch externen Dienstleister
- Backup-Sicherheitsspeicherungen und andere Archivierungen durch externen Dienstleister
- Datenträgerentsorgung, Schreddern von Dokumenten durch externen Dienstleister

III. Verträge richtig gestalten

Es empfiehlt sich, die Verträge über die Auftragsdatenverabeitung möglichst ausführlich und konkretisiert auf den jeweiligen Fall zu gestalten. Die Mindestanforderungen ergeben sich aus §§ 9 und 11 BDSG.

Die organisatorischen und technischen Maßnahmen zum Schutz der Daten gemäß der Anlage zu § 9 BDSG sollten gemeinsam mit dem Dienstleister festgelegt werden. Die genaue Ausgestaltung und das zu gewährleistende Schutzniveau hängen insbesondere von der Sensibilität der Daten, aber auch von dem Datenschutzkonzept des jeweilgen Dienstleisters ab (Maßnahmen zur Zutrittskontrolle können z.B. sein Alarmanlage, Chipkarten-/Transponder-Schließsystem, Videoüberwachung/-aufzeichnung der Zugänge, Protokollierung der Besucher etc., Maßnahmen der Zugangskontrolle sind z.B. Zuordnung von Benutzerrechten, Erstellen von Benutzerprofilen, Kennwort-/ Passwortvergabe, Verschlüsselung von mobilen Datenträgern, Einsatz einer Hardware-Firewall etc.).

IV. Folgen unzureichender Verträge

Wie man der Bußgeld-Entscheidung des BayLDA entnehmen kann, nehmen die Datenschutzbehörden die Anforderungen an die ADV ernst. Auch die einzelnen Maßnahmen gemäß der Anlage zu § 9 BDSG sind im Vertrag konkret festzulegen. Bei Missachtung kann ein Bußgeld von immerhin bis zu € 50.000 verhängt werden.

Hinweis

Dieser Überblick dient ausschließlich der allgemeinen Information und kann konkreten Rechtsrat im einzelnen Fall nicht ersetzen. Sprechen Sie bei Fragen bitte Ihren gewohnten Ansprechpartner bei GÖRG bzw. die Autorin Dr. Katharina Landes unter +49 221-33660-284 oder klandes@goerg.de an. Informationen zur Autorin finden Sie auf unserer Homepage www.goerg.de.

Unsere Standorte

GÖRG Partnerschaft von Rechtsanwälten mbB

BERLIN
Klingelhöferstraße 5, 10785 Berlin
Tel. +49 30 884503-0, Fax +49 30 882715-0

HAMBURG
Dammtorstraße 12, 20354 Hamburg
Tel. +49 40 500360-0, Fax +49 40 500360-99

ESSEN
Alfredstraße 220, 45131 Essen
Tel. +49 201 38444-0, Fax +49 201 38444-20

KÖLN
Kennedyplatz 2, 50679 Köln
Tel. +49 221 33660-0, Fax +49 221 33660-80

FRANKFURT AM MAIN
Neue Mainzer Straße 69 – 75, 60311 Frankfurt am Main
Tel. +49 69 170000-17, Fax +49 69 170000-27

MÜNCHEN
Prinzregentenstraße 22, 80538 München
Tel. +49 89 3090667-0, Fax +49 89 3090667-90