

Ergänzend zum Bericht in der Print-Ausgabe über geänderte datenschutzrechtliche Anforderungen bei Outsourcing und IT-Wartung

Beispiele zur Auftragsdatenverarbeitung

Durch Outsourcing können Unternehmen besser planen oder sie bedienen sich dadurch eines besseren Know-hows bei ihren Auftragnehmern. Das ist auch legitim, wenn die datenschutzrechtlichen Anforderungen beachtet und berufsspezifische Grenzen, wie etwa durch die unzulässige Offenbarung, von Sozial- oder Gesundheitsdaten nicht überschritten werden.

Klassische Bereiche der Auftragsdatenverarbeitung sind beispielsweise die Entgeltabrechnung durch externe Unternehmen oder Rechenzentren, die Datenträgervernichtung mit dem Löschen der Daten als letzten Schritt der Datenverarbeitung, Dienstleistungen durch Call-Center oder der Versand von Broschüren und Infomaterial durch Lettershops. Weiterhin beachtet werden muss jedoch das allgemeine Persönlichkeitsrecht der Betroffenen sowie die Schutzwürdigkeit bestimmter Datenkategorien und deren eingeschränkte zulässige Verarbeitung, wie zum Beispiel bei Angaben über die rassische und ethnische Herkunft, die Religionszugehörigkeit, die Gesundheit und das Sexualleben oder bei der Bewertung von Leistungen oder des Verhaltens.

Ein weiterer Bereich der Auftragsdatenverarbeitung stellt gemäß § 11 Abs. 5 BDSG die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen dar, wenn „dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann“, so der Wortlaut des Gesetzestextes. Das heißt, dass die Wartung einschließlich der Fernwartung durch externe IT-Unternehmen praktisch regelmäßig unter die gesetzlichen Anforderungen der Datenverarbeitung im Auftrag fällt, auch wenn durch die IT-Dienstleister im Rahmen ihrer Wartungstätigkeiten eigentlich keine personenbezogenen Daten ihrer Auftraggeber verarbeitet oder genutzt werden. Unternehmen, die für ihre Auftraggeber die Installation und Pflege oder den Support von Netzwerken, Hardware und Software übernehmen, Fernwartung durchführen, Datenbanken administrieren oder Softwaresysteme mi-

grieren, fallen unter die datenschutzrechtlichen Anforderungen, auch wenn die Dienstleistung nur einmalig erbracht wird.

Rechtliche Stellung des Auftraggebers

Die europäischen Datenschutzgesetze privilegieren auf Grundlage des Artikels 17 der EU-Datenschutzrichtlinie 95/46/EG unter bestimmten Voraussetzungen die Verarbeitung personenbezogener Daten durch Auftragnehmer. Entsprechend gilt dies auch für die deutschen Datenschutzvorschriften. Hinsichtlich der ausgelagerten Datenverarbeitung treten Auftraggeber und Auftragnehmer nach Außen als (datenschutz)rechtliche Einheit auf, wobei der Auftraggeber auch für die Verarbeitung seiner Daten beim Auftragnehmer weiterhin verantwortlich ist! Auch innerhalb von Konzernstrukturen gelten für die einzelnen Unternehmen innerhalb eines Konzernverbands die Vorgaben zur Auftragsdatenverarbeitung.

Auftragsdatenverarbeitung im Ausland

Bei der Auswahl eines Auftragnehmers wird keine Unterscheidung mehr getroffen, ob dieser die Daten in Deutschland oder in einem Staat innerhalb der Europäischen Union (EU) oder des Europäischen Wirtschaftsraumes (EWR) verarbeitet. Für Unternehmen in sog. Drittländern außerhalb der EU bzw. des EWR gelten jedoch andere Voraussetzungen. Die Zulässigkeit der Verarbeitung personenbezogener

Daten in Drittländern ist daher durch den betrieblichen Datenschutzbeauftragten gesondert zu prüfen.

Was ist eine Auftragsdatenverarbeitung?

Wesentliche Merkmale einer Datenverarbeitung im Auftrag nach § 11 BDSG sind insbesondere die Weisungsgebundenheit der Datenverarbeitung, das Einräumen von Kontrollrechten des Auftraggebers zur Überprüfung der ordnungsgemäßen Verarbeitung seiner Daten beim Auftragnehmer, eine fehlende (vertragliche) Beziehung zwischen Auftragnehmer und der betroffenen Personen, deren Daten verarbeitet werden sowie eine klar abgegrenzte Aufgabe, die der Auftragnehmer durch sein (technisches) Know-how für den Auftraggeber übernimmt, die der Auftraggeber jedoch auch ggf. selbst durchführen könnte. Erhält der Auftragnehmer weitreichende Befugnisse, mit den Daten in eigener Regie umgehen zu können (sog. Funktionsübertragung), ist die Abgrenzung zu einer weisungsgebundenen Datenverarbeitung nicht mehr klar zu ziehen. Eine solche Verarbeitung stellt dann keine privilegierte Auftragsdatenverarbeitung im Sinne der Datenschutzanforderungen (des BDSG) dar, sondern wäre dann eine Datenübermittlung, deren Zulässigkeit gesondert datenschutzrechtlich zu prüfen ist.

Datenschutzmaßnahmen

Die im Rahmen der Auftragsvergabe beim Auftragnehmer zu treffenden technischen und organisatorischen Maßnahmen müssen gewährleisten, dass die Datenschutzanforderungen insbesondere hinsichtlich der IT-Sicherheit in einem angemessenen Verhältnis zum Schutzzweck erfüllt sind und entsprechend umgesetzt werden. Im Vordergrund stehen hierbei die Verpflichtung der Beschäftigten auf das Datengeheimnis, der kontrollierte Zutritt zu den Serverräumen, die Sicherstellung der Zugangs- und Zugriffsberechtigung auf Netzwerk- und Programmebene, die Protokollierung bzw. Nachvollziehbarkeit der Eingabe, Veränderung oder Löschung personenbezogener Daten sowie ihr Schutz bei der elektronischen Übertragung, während des Transports oder der Speicherung auf (externen) Datenträgern. Darüber hinaus sind die Daten entsprechend ihrer Zweckbestimmung getrennt von anderen Datenbeständen zu verarbeiten und ein Backupkonzept ist zu implementieren, das die gespeicherten Daten zuverlässig gegen Verlust oder Zerstörung schützt. Mit der Änderung der datenschutzrechtlichen Anforderungen des BDSG im September

2009 wird hierzu explizit vom Gesetzgeber die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsmaßnahmen empfohlen.

Anforderungen an die Vertragsgestaltung

Die Vertragsgestaltung richtet sich natürlich in erster Linie nach der Zweckbestimmung der verarbeiteten Daten bzw. wahrgenommenen Aufgabe des Auftragnehmers. Beispielsweise stehen bei der Entgeltabrechnung in einem Rechenzentrum oder der IT-Wartung insbesondere die technischen und organisatorischen Maßnahmen zur IT-Sicherheit im Vordergrund, bei der Datenträgervernichtung sind Anforderungen an den Transport und die Vernichtung der Datenträger (umschlossene Fahrzeuge, Schlüsselmanagement der Containerschließung, Sicherheitsstufe bei der Vernichtung nach DIN 32757-1) zu stellen, beim Lettershop ist der Zugriff auf die Versandliste und die Weitergabe an Dritte z.B. zu Werbezwecken entsprechend zu reglementieren. Für die Übermittlung personenbezogener Daten an Datenverarbeiter in Drittländern außerhalb der EU-Mitgliedstaaten bzw. des EWR besteht die Möglichkeit zum Abschluss von Datenschutzvereinbarungen durch sog. EU-Standardvertragsklauseln. Für die geplante Datenübermittlung in ein Drittland ist jedoch eine gesonderte datenschutzrechtliche Zulässigkeitsprüfung durch den betrieblichen Datenschutzbeauftragten durchzuführen.

Musterverträge zur Auftragsdatenverarbeitung bieten eine gute Orientierung hinsichtlich der umfangreichen abzubildenden Erfordernisse. Sie sind z.B. über die Webseiten des Dezernats Datenschutz beim Regierungspräsidium in Darmstadt oder des Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) unter herunter zu laden. Eine ausführliche Praxishilfe zur Auftragsdatenverarbeitung samt Mustervertrag kann zudem bei der Gesellschaft für Datenschutz und Datensicherung e.V. bestellt werden.

i Kontakt

Alkemade IT-Security e.K.
 Dipl.-Ing. (FH) Jan Alkemade
 Tel.: 06002 / 939593
 E-Mail: jan.alkemade@alkemade-it.de