BRUNO SCHIERBAUM

Datenschutz bei Auftragsdatenverarbeitung, Wartung und Fernwartung

Die Auftragsdatenverarbeitung war datenschutzrechtlich schon immer ein besonderes Problem. Erst recht gilt das für die immer mehr um sich greifende Fernwartung von Softwaresystemen und PC-Netzwerken. Betriebs- und Personalräte haben ein Recht darauf, dass die Situation so gestaltet wird, dass sie ihre Beteiligungsrechte ungehindert wahrnehmen können.

Wird Wartung oder auch Fernwartung von Hard- und Software durch externe Unternehmen vorgenommen, haben die Unternehmen die besonderen Vorgaben des Bundesdatenschutzgesetzes (BDSG) einzuhalten. Denn mit der Novellierung des BDSG im Jahr 2001 ist Wartung durch Externe eindeutig ebenso zu behandeln wie die ›Datenverarbeitung im Auftrag‹ (§ 11 BDSG).

Immer mehr Unternehmen sind dazu übergangen, bestimmte Teile ihrer Datenverarbeitung oder auch die gesamte Datenverarbeitung durch andere Unternehmen durchführen zu lassen. So hat es in kleineren Unternehmen eine lange Tradition, dass zum Beispiel die Lohn- und Gehaltsabrechung nicht im eigenen Haus erstellt wird, während in Konzernen häufig ein externes oder ein bestimmtes zum Konzern gehörendes Unternehmen als Rechenzentrum für die Datenverarbeitung aller Konzernunternehmen zuständig ist.

Auch Mitarbeiter- und Kundenbefragungen werden häufig durch Fremdunternehmen durchgeführt – im Fall von Kundenbefragung zunehmend telefonisch durch Call-Center. Als weitere Facette kommt seit einiger Zeit nun hinzu, dass Unternehmen ihre Hard- und Software zum Beispiel durch die Hersteller oder andere externe Unternehmen warten lassen. Dies geschieht direkt vor Ort oder (häufiger werdend) durch Fernwartung.

Rechtliche Vorgaben des BDSG

Bei Datenverarbeitung im Auftrag, bei Wartung oder auch Fernwartung durch externe Unternehmen sind die Besonderheiten des BDSG einzuhalten – dann jedenfalls, wenn dabei personenbezogene Daten erhoben, verarbeitet oder genutzt werden oder wenn auf diese zugegriffen werden kann. Auch die Landesdatenschutzgesetze enthalten entsprechende Regelungen.

Wartung ist die Summe der Maßnahmen, die zur Sicherstellung der Verfügbarkeit und Zuverlässigkeit von Hard- und Software ergriffen werden (müssen). Dazu gehören auch die Installation, Pflege, Überprüfung und Korrektur der Software sowie die Überprüfung und Reparatur oder Austausch von Hardware. Fernwartung liegt immer dann vor, wenn

diese Wartung mithilfe von Datenübertragung von einem Ort außerhalb der Stelle vorgenommen wird, an der die Verarbeitung der personenbezogenen Daten erfolgt.

Verantwortlich für die Einhaltung des BDSG und anderer Rechtsvorschriften über den Datenschutz (§ 11 Abs. 1 BDSG) ist bei Auftragsdatenverarbeitung, Wartung und Fernwartung immer der Auftraggeber, da er rechtlich die ›verantwortliche Stelle‹ ⊏→ bleibt. Er bleibt ›Herr der Daten‹ und hat somit auch dafür zu sorgen, dass die bestehenden Rechte des Betriebsrats nach dem BetrVG, sowie die Rechte der Beschäftigten nach dem BDSG eingehalten werden.

Das heißt, dass der Auftragnehmer auch mit Blick auf das BDSG sorgfältig auszuwählen ist. Vor allem muss der Auftraggeber die vom Auftragnehmer umzusetzenden technischen und organisatorischen Maßnahmen des Datenschutzes vor der Auftragserteilung prüfen. Der Auftraggeber muss also verlangen und sich vergewissern, dass die technischen und organisatorischen Maßnahmen, die er selber treffen müsste, wenn er die Wartung durch interne Personen durchführen ließe, auch beim Auftrageber eingehalten werden.

Außerdem muss durch vertragliche Regelung sichergestellt werden, dass der Auftragnehmer mit den ihm zugänglichen personenbezogenen Daten nur entsprechend den Weisungen des Auftraggebers umgeht. Umgekehrt muss der Auftragnehmer bei Weisungen, deren Ausführung gegen das Datenschutzrecht verstoßen würde, den Auftraggeber hierauf unverzüglich hinweisen.

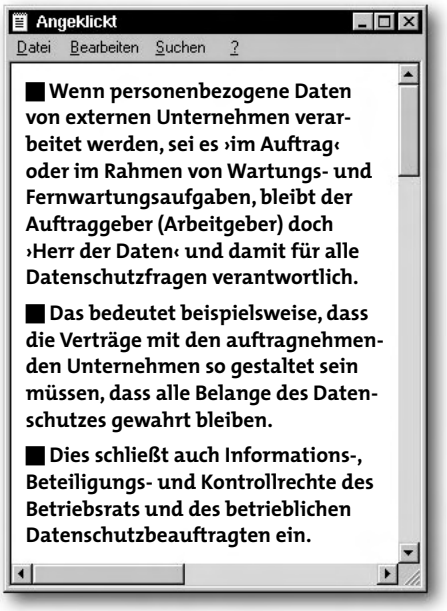
Pflichten des Auftraggebers

Die Pflichten des Auftraggebers sind in § 11 BDSG festgelegt. So ist der Auftraggeber verantwortlich für ...

- die Rechtmäßigkeit der Datenerhebung, -verarbeitung und -nutzung,
- die Gewährleistung der Rechte der Betroffenen,
- die sorgfältige Auswahl des Auftragnehmers,
- die Überprüfung der Datenschutz- und Datensicherungsmaßnahmen.

Der Auftraggeber ist sowohl für die Einhaltung des BDSG als auch der anderen Bestimmungen über den Datenschutz verantwortlich. So hat er die Zulässigkeitsprüfung der Datenverarbeitung vorzunehmen und unter Umständen auch eine Vorabkontrolle durchzuführen. Zudem ist der Auftraggeber Adressat in Bezug auf die Rechte der Beschäftigten auf Auskunft, Berichtigung, Löschung und Sperrung sowie auf Schadenersatz.

Wie bei allen anderen unter den Geltungsbereich des BDSG fallenden Datenverarbeitungen hat die verantwortliche Stelle (hier also der Auftraggeber) sich deshalb auch bei der Auftragsdatenverarbeitung, Wartung und Fernwartung zu vergewissern, ob die beabsichtigte Verarbeitung personenbezogener Daten überhaupt zulässig ist. Das ist prinzipiell immer nur dann der Fall, wenn diese Datenverarbeitung durch das BDSG selber oder durch eine andere Rechtsvorschrift (das kann auch eine Betriebsvereinbarung sein) erlaubt ist oder wenn die jeweils Betroffenen ausdrücklich eingewilligt haben. Dies schließt das Recht der Betroffenen ein, etwa bei unrichtigen Daten deren Berichtigung zu verlangen oder bei unzulässig erhobenen Daten ihre Löschung. In Zweifelsfällen kommt auch eine Sperrung infrage, bei der die beanstandeten Daten mit einem entsprechenden Vermerk versehen und nur



info

Gliederungsvorschlag:

Vertragliche Regelung zur Datenverarbeitung im Auftrag

- ***Gegenstand des Vertrags***
  - **Verarbeitung personenbezogener Daten im Auftrag**
  - **Vertragsparteien (Auftraggeber, Auftragnehmer)**
  - **genaue und abschließende Festlegung der Aufgaben**
- ***Verantwortlichkeit***
  - **Auftragsdatenverarbeitung richtet sich nach § 11 BDSG**
  - **Auftraggeber ist verantwortlich für die Einhaltung des Datenschutzes**
  - **Auftraggeber ist für die Zulässigkeitsprüfung zuständig**
  - **Auftraggeber ist für die Gewährleistung der Rechte der Betroffenen zuständig (Recht auf Auskunft, Berichtigung, Löschung und Sperrung)**
  - **Auftragnehmer verarbeitet die Daten nur nach Weisung des Auftraggebers**
- ***Pflichten des Auftragnehmers***
  - **Hinweispflicht des Auftragnehmers bei Verstößen gegen das Datenschutzrecht**
  - **Anfertigung der Übersichten nach § 4e BDSG**
- ***Datengeheimnis/Vertraulichkeit***
  - **Auftragnehmer wahrt das Datengeheimnis nach § 5 BDSG**
  - **Mitarbeiter sind auf das Datengeheimnis zu verpflichten**
  - **Verpflichtung besteht auch nach Beendigung des Vertragsverhältnisses fort**
- ***Datenschutz und Datensicherheit***
  - **Auftragnehmer gewährleistet ein Sicherheitskonzept mit den erforderlichen und geeigneten Datenschutz- und Datensicherungsmaßnahmen**
  - **Auftragnehmer bringt dem Auftraggeber das Sicherheitskonzept zur Kenntnis**
  - **Auftragnehmer sichert die Bestellung eines fachkundigen und zuverlässigen Datenschutzbeauftragten zu**
- ***Haftung***
  - **Auftragnehmer haftet für die ordnungsgemäße Ausführung des Auftrags**
- ***Vertragsstrafe***
  - **bei Verletzung des Datenschutzrechts durch Auftragnehmer und damit verbundener öffentlicher Berichterstattung**
  - **Festlegung der Vertragsstrafe**
- ***Unterauftragsverhältnisse***
  - **Festlegung von Unterauftragsverhältnissen (z.B. Vernichtung von Datenträgern)**
- ***Vergütung***
- ***Dauer und Kündigungsmöglichkeiten des Vertrags, Gerichtstand***

noch eingeschränkt verwendet werden.

Die bei der Novellierung des BDSG 2001 neu aufgenommene ›Vorabkontrolle‹ (§ 4 d Abs. 5 und 6 BDSG – siehe auch: ›Vorabkontrolle – neu im novellierten BDSG‹ in CF 11/01 ab Seite 25) ist als Ergänzung der obligatorischen Zulässigkeitsprüfung gedacht. Dabei handelt es sich um eine Prüfung, die vom betrieblichen Datenschutzbeauftragten vor der Inbetriebnahme besonderer Datenverarbeitungen durchzuführen ist. Dies ist immer dann der Fall, wenn es um besonders sensible personenbezogene Daten (›Besondere Arten personenbezogener Daten ...‹ in CF 11/04 ab Seite 4) geht und wenn Daten dazu bestimmt sind, die Persönlichkeit eines Betroffenen einschließlich seiner Leistung und seines Verhaltens zu bewerten.

Grundsätzlich ist der Auftraggeber bei der Auswahl des Auftragnehmers frei. Er hat jedoch den Auftragnehmer sorgfältig auszuwählen und zwar unter besonderer Berücksichtigung der von ihm getroffenen technischen und organisatorischen Datenschutz- und Datensicherungsmaßnahmen nach § 9 BDSG. Über das Vorliegen eines entsprechenden Datenschutzkonzepts hat sich der Auftraggeber vor der Vergabe des Auftrags zu überzeugen.

Zentraler Maßstab für die Auswahl des Auftragnehmers ist also »die Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen« (siehe den info-Kasten ›Die acht Gebote des Datenschutzes‹ auf Seite 8).

Pflichten des Auftragnehmers

In § 11 Abs. 4 BDSG ist genau festgelegt, welche Vorgaben der Auftragnehmer einzuhalten hat. Er darf die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten und nutzen. Dieses muss sich aus dem abzuschließenden Vertrag genau ergeben. Die Verantwortung liegt also – wie schon gesagt – eindeutig beim Auftraggeber. Ist der Auftragnehmer aber der Ansicht, dass eine Weisung des Auftraggebers gegen das BDSG oder eine andere Rechtsvorschrift verstößt, dann hat er den Auftraggeber unverzüglich darauf hinzuweisen.

Dies kann beispielsweise dann der Fall sein, wenn der Auftragnehmer als DV-Dienstleistungsanbieter über die besseren Datenschutzkenntnisse verfügt. Allerdings besteht keine Verpflichtung des Auftragnehmers, jeden einzelnen Auftrag sorgfältig auf die Datenschutzvorschriften hin zu überprüfen, denn die generelle Prüfung des Datenschutzes muss der jeweilige Auftraggeber bereits vor der Auftragsvergabe vorgenommen haben.

Der Auftragnehmer hat auch die folgenden generellen Vorschriften des BDSG zu beachten:

- die Beschäftigen müssen das Datengeheimnis nach § 5 BDSG beachten,
- es sind die Datenschutz- und Datensicherungsmaßnahmen nach § 9 BDSG umzusetzen (›8 Gebote des Datenschutzes‹),
- bei unbefugter Datenverarbeitung greift die Strafvorschrift des § 44 BDSG,
- Ordnungswidrigkeiten des Auftragnehmers unterliegen den Bußgeldvor-

schriften des § 43 BDSG (Ordnungswidrigkeitstatbestände wären z.B. Nichtbestellen eines Datenschutzbeauftragten, Zuwiderhandeln gegen eine Anordnung der Aufsichtsbehörde).

Inhalt und Form des Auftrags

Der Auftraggeber ist bei Datenverarbeitung im Auftrag und auch bei Wartung/Fernwartung verpflichtet, die von ihm festzulegenden datenschutzrechtlichen Anforderungen schriftlich niederzulegen. Der Vertrag muss dabei mindestens folgende Punkte enthalten:

- Art und Umfang der Erhebung, Verarbeitung und Nutzung personenbezogener Daten,
- Datenschutz- und Datensicherungsmaßnahmen beim Auftragnehmer,
- Regelung von Unterauftragsverhältnissen.

Es ist also festzulegen, welche personenbezogenen Daten zu verarbeiten sind, welche Aufgaben wahrgenommen werden sollen und welche Phasen der Datenverarbeitung durchgeführt werden. Hierzu gehört auch, ob personenbezogene Daten an Dritte (z.B. Unterauftragnehmer) übermittelt werden. Dabei ist es sinnvoll, die getroffenen Datenschutz- und Datensicherungsmaßnahmen als Anlage zum Bestandteil des Vertrags zu machen (siehe dazu die info-Kästen auf dieser Seite).

Aufgaben des Betriebsrats

Die Wahrnehmung der Beteiligungsrechte des Betriebsrats wird bei Auftragsdatenverarbeitung oder Wartung/Fernwartung durch Fremdfirmen nicht gerade einfacher. Entscheidend ist jedoch, dass die Beteiligungsrechte des Betriebsrats dennoch weder eingeschränkt noch ausgeschlossen werden. Dieses hat das Bundesarbeitsgericht bereits 1987 nachdrücklich festgestellt (vergl. BAG vom 17. 3. 1987 – in: ›Arbeitsrecht im Betrieb‹ 12/87 ab Seite 287).

info

Gliederungsvorschlag:

Vertragliche Regelung zur Wartung/Fernwartung

- ***Gegenstand des Vertrags***
  - **Festlegung des Umfangs der (Fern-)Wartungsarbeiten**
- ***Allgemeine Pflichten des Auftragnehmers***
  - **Auftragnehmer führt (Fern-)Wartungsarbeiten nur auf Weisung des Auftraggebers durch**
  - **Autorisierte Personen werden dem Auftraggeber mitgeteilt**
  - **Verpflichtung der Mitarbeiter auf das Datengeheimnis**
- ***Unterauftragsverhältnisse***
  - **Einschaltung von Subunternehmern bedarf der schriftlichen Vereinbarung mit dem Auftraggeber**
- ***Zweckbindung***
  - **Fernwartung nur im Rahmen der vertraglichen Vereinbarung**
  - **Keine Weitergabe oder Übermittlung personenbezogener Daten**
- ***Kontrollrecht des Auftraggebers***
  - **Kontrolle durch den betrieblichen Datenschutzbauftragten**
  - **Kontrolle durch den Betriebsrat**
- ***Technische und organisatorische Maßnahmen***
  - **Aufbau der Fernwartungsverbindung darf nur durch Auftraggeber erfolgen**
  - **Fernwartungspersonal arbeitet mit Benutzererkennung (Passwort)**
  - **Fernwartungsaktivitäten werden protokolliert**
  - **Downloads (Herunterladen von Dateien) oder Filetranfers (Übertragung von Dateien) zur Fehleranalyse und -behebung müssen schriftlich vereinbart sein**
- ***7. Dauer und Kündigungsmöglichkeiten des Vertrags, Gerichtsstand***

Der Auftraggeber hat deshalb in einem Vertrag mit dem Auftragnehmer festzulegen, dass die Rechte des Betriebsrats und auch abgeschlossene Betriebsvereinbarungen in vollem Umfang umgesetzt werden müssen. Bei der Datenverarbeitung im Auftrag oder bei Wartung/Fernwartung durch Externe kommen dabei in Bezug auf den Datenschutz vor allem folgende rechtliche Vorgaben des BetrVG zum Tragen:

(1) Nach § 75 Abs. 2 BetrVG haben Arbeitgeber und Betriebsrat die *freie Entfaltung der Persönlichkeit* und damit die *Persönlichkeitsrechte* der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern. Hierbei handelt es sich um eine Generalklausel von einiger Bedeutung für die Umsetzung der betriebsverfassungsrechtlichen Überwachungs- und Mitbestimmungsrechte durch den Betriebsrat.

(2) Auch hat der Betriebsrat nach § 80 Abs. 1 Nr. 1 BetrVG darüber zu wachen, dass die *zugunsten der Arbeitnehmer geltenden Gesetze und Betriebsvereinbarungen eingehalten* werden. Ein Gesetz in diesem Sinne ist das BDSG. Um zu überprüfen ob und wie weit das sichergestellt ist, kann der Betriebsrat den abgeschlossen Vertrag zur Datenverarbeitung im Auftrag und zur Wartung/Fernwartung einsehen.

(3) Im Rahmen seines Überwachungsrechts steht dem Betriebsrat ein *Zutrittsrecht* zu allen Räumen und Betriebsstellen zu, in denen personenbezogene Daten der Beschäftigten verarbeitet werden. Dieses muss natürlich auch für das Unternehmen gelten, das als Auftragnehmer die Datenverarbeitung im Auftrag durchführt. Die Einzelheiten der Kontrollen (die auch der betriebliche Datenschutzbeauftragte beim Auftragnehmer ausüben können muss!) sind im Vertrag zur Auftragsdatenverarbeitung zu regeln. Eine Regelung im Rahmen einer Betriebsvereinbarung könnte folgendermaßen aussehen:

info

Anlage zu § 9 Bundesdatenschutzgesetz (BDSG):

Die acht Gebote des Datenschutzes

Zutrittskontrolle	**Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.**
Zugangskontrolle	**Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.**
Zugriffskontrolle	**Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.**
Weitergabekontrolle	**Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.**
Eingabekontrolle	**Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.**
Auftragskontrolle	**Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.**
Verfügbarkeitskontrolle	**Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.**
Getrennte Verarbeitung	**Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.**

»Der Betriebsrat hat jederzeit das Recht, die Einhaltung der Betriebsvereinbarung zu überprüfen. Bei Datenverarbeitung im Auftrag/Wartung/Fernwartung hat die Geschäftsleitung dafür Sorge zu tragen, dass das Überwachungsrecht des Betriebsrats nach § 80 Abs. 1 Nr. 1 BetrVG auch vor Ort beim Auftragnehmer stattfinden kann.«

(4) Die wichtigste Voraussetzung dafür, dass der Betriebsrat seine Rechte nach dem Betriebsverfassungsgesetz wahrnehmen kann, ist das Informationsrecht nach § 80 Abs. 2 und nach § 90 Abs. 1 BetrVG. In dem bereits erwähnten Urteil des Bundesarbeitsgerichts ist festgelegt, dass der Betriebsrat insbesondere über folgende Punkte zu informieren ist:

- Übersicht über alle verwendeten Dateien mit personenbezogenen Daten der Beschäftigten, gleichgültig ob die Speicherung im eigenen Unternehmen oder bei einem anderen Untenehmen erfolgt,
- personenbezogene Daten, die an andere Unternehmen übermittelt werden,
- Maßnahmen, die getroffen werden, damit die an andere Unternehmen (Auftragnehmer) weitergebenen Daten nur zu den vereinbarten Zwecken übermittelt werden,
- die eingesetzten Programme mit Namen und Kurzbeschreibung,
- das Pflichtenheft und die Systembeschreibung.

Und selbstverständlich wird der Betriebsrat über den Vertrag zur Auftrag sdatenverarbeitung/Wartung/Fernwartung informiert werden müssen.

Nicht zuletzt gilt auch bei der Auftragsdatenverarbeitung/Wartung/Fernwartung das zentrale Mitbestimmungsrecht des Betriebsrats nach § 87 Abs. 1 Nr. 6 BetrVG. Denn bei der eingesetzten Informations- und Kommunikationstechnik (IKT) handelt es sich ohne Frage um technische Einrichtungen, die bestimmt (oder zumindest geeignet) sind, Leistung oder Verhalten der Beschäftigten zu überwachen.

Im Rahmen einer Betriebsvereinbarung zur Auftragsdatenverarbeitung sollten die eingesetzten technischen Systeme, der genaue Umfang der Verarbeitung personenbezogener Daten, Auswertungen mit personenbezogenen Daten, zugriffsberechtigte Personen und Löschungsfristen geregelt werden.

Ob auch Wartung und Fernwartung im Rahmen von Betriebsvereinbarung geregelt werden sollten, hängt insbesondere vom Umfang des dabei stattfindenden Zugriffs auf personenbezogene Daten und von der Häufigkeit der Zugriffe ab. Auf jeden Fall aber müssen Wartung und Fernwartung durch externe Unternehmen vertraglich zwischen Auftraggeber und Auftragnehmer geregelt werden.

Bruno Schierbaum ist als Berater für Betriebs- und Personalräte bei BTQ Niedersachsen tätig; Kontakt: BTQ Niedersachsen, Donnerschweer Straße 84, 26123 Oldenburg, fon 0441-82068, **schierbaum@btq.de**, **www.btq.de**

Verantwortliche Stelle (im Sinne des Datenschutzes) = jede natürliche oder juristische Person oder Stelle (egal, ob Behörde, Wirtschaftsunternehmen, Kanzlei, Verein o.ä.), die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt, oder die dies durch andere im Auftrag vornehmen lässt (§ 3 Absatz 7 BDSG)