IT-Outsourcing mit Hindernissen

Leitfaden zur Auftragsdatenverarbeitung

Eberhard Kiesche, Matthias Wilke

Betriebs- und Personalräte werden zunehmend mit dem Auslagern informationstechnischer Dienstleistungen an externe Rechenzentren oder Call Center konfrontiert. Eine große Herausforderung – zumal kein Outsourcing-Fall dem anderen gleicht. Dieser Leitfaden und eine ausführliche Online-Checkliste helfen Belegschaftsvertretern, die Daten der Beschäftigten dabei effektiv zu schützen.

Darum geht es:

- Das Auslagern informationstechnischer Dienstleistungen ist in Unternehmen und Behörden en vogue.
- Arbeitgeber tun sich bei der korrekten Umsetzung der Verarbeitung außer Haus immer noch schwer.
- Umfassende Mitbestimmungsrechte helfen beim Schutz der Beschäftigtendaten.

Die weisungsgebundene Auftragsdatenverarbeitung innerhalb Deutschlands kommt sehr häufig vor. Sie basiert auf § 11 des Bundesdatenschutzgesetzes (BDSG). Die Vorschrift wurde vor einigen Jahren geändert. Doch viele Arbeitgeber stehen bei der Umsetzung immer noch vor großen Schwierigkeiten.[1]

Auftragsdatenverarbeitung oder Funktionsübertragung?

Wenn Interessenvertretungen verschiedene Formen von Outsourcing in Form einer Betriebs- oder Dienstvereinbarung und damit den Umgang mit der Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten überwachen und mitbestimmen wollen, müssen sie vor allem die rechtliche Einordnung des Outsourcings korrekt vornehmen.

Denn wird die Vereinbarung von der zuständigen Aufsichtsbehörde für den Datenschutz überprüft, stellt das Beachten der gesetzlichen Datenschutzregelungen eine Hürde dar, an der das betriebliche Regelwerk als rechtliche Erlaubnisvorschrift scheitern kann. In der Praxis von Rahmen-IKT-Vereinbarungen fällt den Betriebsparteien

1 Bayrisches Landesamt für den Datenschutz 2009-2010, 4. Tätigkeitsbericht, 35 ff; siehe auch 6. Tätigkeitsbericht 2013-2014, 38 ff., www.thm.de/zaftda/tb-bundeslaender/cat_view/25-tb-bundeslaender/7-bayern/43-aufsichtsbehoerde

oftmals die Abgrenzung der Auftragsdatenverarbeitung von der Funktionsübertragung schwer.[2]

Bei der Auftragsdatenverarbeitung[3], die die Erhebung, Verarbeitung und Nutzung personenbezogener Daten umfasst, wird lediglich der zur Aufgabenerledigung erforderliche Umgang mit den Daten ausgelagert. Der beauftragten Serviceeinrichtung wird der Umgang mit den Daten nach Weisung und unter materieller Verantwortung des Auftraggebers als Hilfstätigkeit oder DV-Dienstleistung übertragen.

Die Verantwortung des Auftraggebers bezieht sich vor allem auf die Zulässigkeit der Datenerhebung und Datenverwendung und auf die Einhaltung von § 11 BDSG. Der Auftraggeber verantwortet die technischen und organisatorischen Maßnahmen zur Datensicherheit beim Auftragnehmer. Der Auftraggeber ist zudem für die Information über Datenpannen des Auftragnehmers nach § 42 a BDSG in der Informationspflicht. Als Erkennungsmerkmale werden beispielsweise in der Konzernbetriebsvereinbarung Beschäftigtendatenschutz (KBV BDS) der Deutschen Bahn AG definiert:

- Fehlende Entscheidungsbefugnis des Auftragnehmers,
- Weisungsgebundenheit des Auftragnehmers bezüglich dessen, was mit den Daten geschieht,
- Umgang nur mit personenbezogenen Daten, die der Auftraggeber zur Verfügung stellt; es sei denn, der Auftrag ist auch auf die Erhebung von Daten gerichtet,
- Ausschluss der Verarbeitung oder Nutzung der Daten zu eigenen Zwecken des Auftragnehmers,
- keine (vertragliche) Beziehung des Auftragnehmers zum Betroffenen,
- Auftragnehmer tritt (gegenüber dem Betroffenen) nicht in eigenem Namen auf.

Bei der Funktionsübertragung wird die der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zugrunde liegende Funktion oder Aufgabe ganz oder teilweise abgegeben. Die in Anspruch genommene Serviceeinrichtung erbringt weitgehend eigenständige Leistungen mit Hilfe der überlassenen Daten. Sie handelt hierbei in eigener Verantwortung. Erkennungsmerkmale für Funktionsübertragung sind nach der KBV BDS[4]:

- Weisungsfreiheit des Dienstleisters bezüglich dessen, was mit den Daten geschieht,
- Überlassung von Nutzungsrechten an den Daten,
- eigenverantwortliche Sicherstellung von Zulässigkeit und Richtigkeit der Daten durch den Dienstleister, einschließlich des Sicherstellens der Rechte von Betroffenen (Benachrichtigungspflicht, Auskunftsanspruch),
- Handeln des Dienstleisters (gegenüber dem Betroffenen) im eigenen Namen,
- Entscheidungsbefugnis des Dienstleisters in der Sache.

Beispiele hierfür sind das Outsourcing der Personalverwaltung oder der Mitarbeiterrekrutierung. Das Merkmal für die Funktionsübertragung ist die Weisungsungebundenheit des Auftragnehmers. Die korrekte Abgrenzung ist deshalb wichtig, weil sich aus der Auftragsdatenverarbeitung oder der Funktionsübertragung unterschiedliche rechtliche Anforderungen ergeben.

Bei der Auftragsdatenverarbeitung bleibt der Auftraggeber die allein verantwortliche Stelle für die Einhaltung des BDSG und anderer Vorschriften über den Datenschutz (§ 11 Abs. 1 Satz 1 BDSG).

Der Auftragnehmer ist nicht Dritter, sondern Empfänger. Er wird im Sinne einer gesetzlichen Fiktion der verantwortlichen Stelle zugerechnet und ist der verlängerte Arm des Auftraggebers. Die verantwortliche Stelle umfasst nach § 3 Abs. 7 BDSG somit die Personen oder Stellen, die sie in ihrem Auftrag tätig werden lässt. Dies gilt für Auftragnehmer im Inland, in der Europäischen Union und im Europäischen Wirtschaftsraum. Der Weitergabe der Daten an den Auftragnehmer liegt eine Datennutzung gemäß § 3 Abs. 5 BDSG zugrunde.

Bei der Funktionsübertragung werden Daten an einen Dritten übermittelt. Der Vorgang der Übermittlung (§ 3 Abs. 4 Nr. 3 BDSG) an einen Dritten bedeutet, dass hierfür eine gesonderte Zulässigkeitsvoraussetzung nach § 4 Abs. 1 BDSG notwendig ist. Für die Auftragsdatenverarbeitung gilt § 11 BDSG, für die Funktionsübertragung nicht. Die Auftragsdatenverarbeitung ist somit gegenüber der Funktionsübertragung datenschutzrechtlich privilegiert, da die Datennutzung einfacher zu rechtfertigen ist als die Datenübermittlung.

Rechtsgrundlage für Auftragsdatenverarbeitung

Die Anforderungen an eine Auftragsdatenverarbeitung sind in § 11 BDSG geregelt.[5] Im Sozialrecht gilt der inhaltsgleiche § 80 Sozialgesetzbuch (SGB) IX. § 11 BDSG wurde 2009 novelliert.

In der Praxis ist es wiederholt vorgekommen, dass für die externe Datenverarbeitung kein Vertrag nach § 11 BDSG geschlossen wurde. Deshalb wurden die inhaltlichen Anforderungen an den Vertrag zur Auftragsdatenverarbeitung in § 11 BDSG[6] präzisiert und eine sorgfältige Auswahl beziehungsweise Prüfung des Auftragnehmers und Kontrollen zu Beginn und während des Zeitraums der Auftragsdatenverarbeitung verlangt.

Für die vorzunehmenden Kontrollen durch den Auftraggeber wurde jedoch auf eine starre Frist verzichtet. Ebenso gibt es keine Pflicht zur Überprüfung vor Ort oder in Person des Auftraggebers.[7] Besondere Anforderungen ergeben sich bei der Datenschutz-Prüfung von Rechenzentren.[8]

2 Fallbeispiele bei GDD (Hrsg.), Datenschutz beim Outsourcing – Praxisleitfaden mit Muster, 3. Auflage 2014, 20 ff.

3 Die folgende Darstellung orientiert sich an der KBV BDS in der DB AG (Glossar), www.evg-online.org/Arbeitswelt/Mitbestimmung/Betriebsverfassung/.Aktuelles/13_04_10_KBV_BDS/; Bericht »Konzerninterner Datentransfer« der Arbeitsgruppe der Aufsichtsbehörden, www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/Personalwesen/Inhalt/5_Beschaeftigtendatenschutz_Konzern/arbeitspapier_ad_hoc_idv.pdf

4 KBV BDS in der DB AG, Glossar, aaO.

5 Siehe grundlegend Kremer, Auftragsdatenverarbeitung nach § 11 BDSG – Praxishinweise zur Vertragsgestaltung, Vortrag beim GDD Infotag 2014

6 Frei verfügbare Muster in: GDD (Hrsg.), www.gdd.de/downloads/materialien/muster/gdd-ratgeber-201edatenschutz-beim-outsourcing201c-3-auflage-mustertexte

7 Siehe BT-Drs. 16/13657, 18

8 Dazu ausführlich der aktuelle GDD-Ratgeber, Datenschutz-Prüfung von Rechenzentren, 2015

Pflichten des Auftraggebers: Sorgfältige Auswahl

Somit ergeben sich aus § 11 BDSG folgende Aufgaben für den Auftraggeber. Nach § 11 Abs. 2 Satz 1 BDSG hat er den Auftragnehmer sorgfältig auszuwählen, unter besonderer Berücksichtigung der von ihm getroffenen technischen und organisatorischen Maßnahmen im Sinne von § 9 und Anlage zu § 9 BDSG.

Belegschaftsvertretungen können kontrollieren, wie die Auswahl und Überprüfung des Auftragnehmers vorgenommen worden ist. Kriterien oder Instrumente sind zum Beispiel Eigenerklärungen, Selbstauskünfte, Sicherheitskonzepte, Normen, Checklisten, Zertifikate oder Standards[9], Ausschreibungen, Referenzen/Nachweise oder Vorort-Prüfungen. Der Prüfschwerpunkt für die Auswahl ist der Stand der Umsetzung von technisch-organisatorischen Maßnahmen beim Auftragnehmer, wobei insbesondere die Angemessenheit der bei ihm getroffenen Maßnahmen zu bewerten ist. Der Auftraggeber bleibt für die Datensicherheit nach § 9 und Anlage zu § 9 BDSG verantwortlich.

Nach § 11 Abs. 2 Satz 4 BDSG hat sich der Auftraggeber vor Beginn der Datenverarbeitung und anschließend regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Zur »Überzeugungsarbeit« und zu den laufenden Kontrollen gehören die Berücksichtigung der rechtlichen Standards des Datenschutzes und der technischen Standards der Datensicherheit.

Bei der Risikoabschätzung sind die branchenspezifischen Besonderheiten zu berücksichtigen, etwa bei der Aktenarchivierung oder Datenträgervernichtung. Immer sind die Standardprozesse, beispielsweise für die Datenträgervernichtung, zu definieren und die Risiken je nach Schutzbedarf der personenbezogenen Daten zu minimieren. In der Regel ist zuvor der Schutzbedarf der outgesourcten Prozesse und Daten im Sinne einer Risikofolgenabschätzung zu bewerten.

Im folgenden Schritt ist die Ist-Situation beim Auftragnehmer zu bewerten. Es ist also zu prüfen, ob sie dem Stand der Technik und den eigenen Anforderungen als Auftraggeber entspricht. Die Audits oder Ergebnisse der Prüfungen sind zu dokumentieren. Zertifikate, Testate und Nachweise des Auftragnehmers sind vom Auftraggeber stets auf Eignung, Plausibilität und Vollständigkeit zu prüfen.

»Belegschaftsvertretungen können kontrollieren, wie die Auswahl und Überprüfung des Auftragnehmers vorgenommen worden ist.«

Pflichten des Auftragnehmers: Strikte Weisungsgebundenheit

Auftragnehmer dürfen die Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten. Er hat den Auftraggeber darauf hinzuweisen, wenn dessen Weisungen gegen geltendes Datenschutzrecht verstoßen. Aus dem Vertrag mit dem Auftragnehmer, den der Auftraggeber schriftlich abzuschließen hat, ergeben sich eine Reihe vertraglicher Pflichten, so beispielsweise die Duldungs- und Mitwirkungspflichten bei den vom Auftraggeber durchzuführenden Kontrollen. Aus § 11 Abs. 4 BDSG ergibt sich, welche Datenschutzpflichten der Auftragnehmer zu beachten hat. Hier ist insbesondere das Treffen der technisch-organisatorischen Maßnahmen nach § 9 BDSG von großer Bedeutung.

Interessenvertretungen sollten auch darauf hinweisen, dass bei der Auswahl des Auftragnehmers eine Selbstauskunft schwerlich ausreicht. Geeignetere Mittel sind zum Beispiel ein Audit beim Auftragnehmer durch den Auftraggeber oder unabhängige Stellen. Hierfür werden Check- oder Fragelisten eingesetzt, die branchenspezifisch ausgerichtet sein sollten. Betriebsräte können nach § 80 Abs. 2 BetrVG die Dokumentation der Auswahl und der durchgeführten Kontrollen verlangen. Das gilt für die Anforderung des Vertrags nach § 11 BDSG durch die Arbeitnehmervertretung, da der Betriebsrat ebenso wie der Personalrat befugt ist, die Einhaltung des BDSG als ein zugunsten der Arbeitnehmer geltendes Gesetz gemäß § 80 Abs. 1 Nr. 1 BetrVG (Personalräte nach § 68 Abs.1 Nr. 2 BPersVG) zu überwachen.

Nicht ohne schriftlichen Vertrag

Beim Entwickeln eines Vertrags zur externen Datenverarbeitung können Unternehmen Mustertexte nutzen. Diese sind je nach Dienstleistung aber noch anzupassen. Für die Prüfung oder Wartung automatisierter Verfahren oder Datenverarbeitungsanlagen gibt es spezielle Muster, die berücksichtigen, dass der 10-Punkte-Katalog für den Vertrag zum Verarbeiten der Daten gemäß § 11 Abs. 5 BDSG die Absätze 1 bis 4 BDSG nur »entsprechend anzuwenden« ist. Für den Vertrag zur Datenträgervernichtung kann auf die technisch-organisatorischen Maßnahmen gemäß DIN 66399 verwiesen werden.[10]

Der Vertrag für den Auftrag, dessen Bestandteile mindestens den Anforderungen gemäß § 11 Abs. 2 Satz 2 BDSG genügen müssen und für den die Schriftform erforderlich ist, sollte mindestens beinhalten:

- Gegenstand und Dauer des Auftrags,
- Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung personenbezogener Daten der Beschäftigten,
- Art der Daten und der Kreis der Betroffenen,
- technische und organisatorische Maßnahmen (als Anlage zum Vertrag oder als Datensicherheitskonzept des Auftragnehmers),
- Berichtigung, Löschung und Sperrung von Daten,
- Pflichten des Auftragnehmers nach § 11 Abs. 4 BDSG,
- Unterauftragsverhältnisse,
- Duldungs- und Mitwirkungspflichten,

9 Siehe etwa den Standard »Anforderungen an Auftragnehmer nach § 11 BDSG«, Datenschutzstandard DS-BvD-GDD-01, www.gdd.de/downloads/materialien/ds-bvd-gdd-01-v0.1/adv-standard/

10 GDD-Ratgeber, Datenschutzgerechte Datenträgervernichtung, 3. Auflage 2014

- mitzuteilende Verstöße des Auftragnehmers,
- Laufzeit des Auftrags, Kosten der Durchführung der Auftragsdatenverarbeitung, Mitwirkungen, Beistellungen des Auftraggebers.

Wenn ein Auftrag entgegen § 11 Abs.2 Satz 2 BDSG nicht richtig, nicht vollständig oder in der vorgeschriebenen Weise erteilt wird, oder der Auftraggeber entgegen § 11 Abs. 2 Satz 4 BDSG die »Überzeugungsbildung« nicht vornimmt, ist dies nach § 43 Abs. 1 Nr. 2b BDSG bußgeldbewehrt. Betriebsräte sind deshalb in ihrer Überwachungsfunktion gemäß § 80 Abs. 1 Nr. 1 BetrVG besonders gefordert.

Sie sollten unbedingt überprüfen, ob vertraglich die strikte Weisungsgebundenheit des Auftragnehmers festgelegt ist. Sie sollten sich des Weiteren für Unterauftragnehmer interessieren, das heißt stets klären, ob Subunternehmer[11] nur mit Zustimmung des Auftraggebers vom Auftragnehmer eingeschaltet werden dürfen und die Kontrollen durch den Auftraggeber sich auf alle Unterauftragsverhältnisse beziehen. Besonders schwierig wird es, wenn Unterauftragnehmer eingeschaltet werden, die in Drittstaaten wie den USA tätig werden.[12] Unterbeauftragungen können ausgeschlossen werden, zum Beispiel durch eine Nichtregelung im Vertrag.[13]

Der Auftraggeber hat Duldungs- und Mitwirkungspflichten für den Auftragnehmer bei Kontrollen zu vereinbaren. Er kann dann Personen mit der Kontrolle beauftragen, zu denen der betriebliche Datenschutzbeauftragte, Betriebsräte und gegebenenfalls Mitarbeiter der Revision gehören sollten. Belegschaftsvertreter sollte stets prüfen, inwieweit besondere Arten von Daten gemäß § 3 Abs. 9 BDSG vom Auftragnehmer erhoben, verarbeitet und genutzt werden. Hier interessieren im Beschäftigtendatenschutz vor allem die Gesundheitsdaten der Mitarbeiter.

Die Betriebsparteien können und sollten den Vertrag nach § 11 BDSG bei der Funktionsübertragung zugrunde legen. Die Gesellschaft für Datenschutz und Datensicherheit stellt zu Recht fest:

»Eine gesetzliche Pflicht zum Abschluss einer schriftlichen Vereinbarung besteht im Rahmen der Funktionsübertragung nicht. Allerdings ist es aufgrund haftungsrechtlicher Überlegungen und zum Schutz von Betroffenen im Einzelfall sinnvoll, die in § 11 BDSG aufgeführten Kriterien auch bei der Funktionsübertragung als Maßstab für die Auswahl des Outsourcing-Nehmers und die Vertragsgestaltung anzuwenden.«[14]

Handlungsmöglichkeiten der Interessenvertretung

Betriebsräte haben nach § 80 Abs. 1 Nr. 1 BetrVG die Pflicht zu überwachen, ob § 11 zur Auftragsdatenverarbeitung und die anderen Schutzvorschriften des BDSG eingehalten werden. Denn das BDSG ist ein zugunsten der Beschäftigten geltendes Gesetz.

Zur Überwachungsaufgabe der Interessenvertretung gehört das Recht auf rechtzeitige und umfassende Information durch den Arbeitgeber. Zu den erforderlichen Unterlagen gehören der Vertrag nach § 11 BDSG, das Konzept des Arbeitgebers zur Kontrolle der Auftragsdatenverarbeitung, das Verfahrensverzeichnis nach § 4 g Abs. 2 BDSG des Auftraggebers und das Datensicherheitskonzept des Auftragnehmers.

Das Informationsrecht des Betriebsrats bei der Auftragsdatenverarbeitung ist 1987 vom Bundesarbeitsgericht (BAG) bestätigt worden.[15] Betriebliche Interessenvertretungen sollten die Verfahrensverzeichnisse überprüfen, inwieweit Auftragsdatenverarbeitung oder Funktionsübertragung dort erkennbar werden.

Die Auftragskontrolle gehört zu den acht Geboten des Datenschutzes nach § 9 BDSG und der Anlage Nr. 6. Da der Gesetzgeber hier für den Arbeitgeber Handlungsspielraum belässt, Beschäftigtendaten in der Regel verarbeitet werden und die gesetzlichen Vorgaben keinesfalls abschließend sind, können Interessenvertretungen ihre Mitbestimmungsrechte gemäß § 87 Abs.1 Nr. 6 BetrVG und § 75 Abs. 3 Nr. 17 BPersVG nutzen und insbesondere die Anforderungen an technisch-organisatorische Maßnahmen vom Auftraggeber mitbestimmen. Betriebs- und Personalräte sollten möglichst Datenschutzaudits beim eigenen Arbeitgeber als Auftraggeber und beim Dienstleister vereinbaren.[16]

Fazit

Es lohnt auch für Belegschaftsvertretungen, sich mit dem schwierigen Thema des Outsourcings von informationstechnischen Dienstleistungen auseinanderzusetzen. Betriebs- und Personalräte haben bekanntermaßen im Beschäftigtendatenschutz eine Rechtsüberwachungs- und zusätzlich auch eine Rechtssetzungsfunktion.

Insbesondere dann, wenn Betriebs- und Personalräte ihre Mitbestimmung bei Vereinbarungen als vorrangige Rechtsvorschrift für die Erlaubnis von Datenverarbeitung und Datenverwendung nutzen wollen, ist es bedeutsam, die richtige Begrifflichkeit und die richtigen gesetzlichen Grundlagen des Datenschutzrechts zu beherrschen. Bislang wird in der Praxis Auftragsdatenverarbeitung und Funktionsübertragung noch zu wenig überwacht und mitbestimmt. Hier bietet dieser Leitfaden für Interessenvertretungen praxisorientierte Hilfestellung.

Autor

Dr. Eberhard Kiesche, Arbeitnehmerorientierte Beratung (AoB), Bremen
» eberhard.kiesche@t-online.de
» www.aob-bremen.de

Matthias Wilke, Datenschutz- und Technologieberatung (dtb), Kassel
» info@dtb-kassel.de
» www.dtb-kassel.de

cua-web.de
SERVICE
Arbeitshilfe » Checkliste ✔

11 Siehe Bongers/Krupna, Der Subauftragnehmer im Rahmen der Auftragsdatenverarbeitung – Weisungs- und Kontrollrechte in einer Auftragskette, in: RDV 2014, 19 ff.

12 Siehe Eckhardt, Auftragsdatenverarbeitung. Gestaltungsmöglichkeiten und Fallstricke, in: DuD 2013, 585 ff., insbesondere Kapitel 4

13 Siehe Kremer, aaO.

14 GDD (Hrsg.), Datenschutz beim Outsourcing, aaO., 151

15 BAG vom 17.3.1987, Az.: 1 ABR 59/85, in: JurionRS 1987, 10107

16 Probst, Datenschutzaudits, in: Stoppkotte/Wilke, Big Data im Betrieb, in: AiB Extra, 3/2015, 38 ff.