

Datenschutz bei IT-Verträgen

Monika Sekara, Rechtsanwältin in Hannover

No. 282 – September 2009

Bei der Beauftragung mit IT-Leistungen erhält der Anbieter regelmäßig die Möglichkeit des Zugriffs auf Bestände mit personenbezogenen Daten im Unternehmen des Auftraggebers. Die aufgedeckten Datenkandale gaben in der Öffentlichkeit den Anstoß zu aktuellen Diskussionen über den Umgang mit diesen Daten. Dennoch behandeln Wirtschaftsunternehmen den Datenschutz im Bereich B2B nach wie vor eher nachlässig. Oft fehlt die Sensibilität, IT-Verträge sorgfältig zu gestalten und im Unternehmen einen verantwortlichen Datenschützer einzusetzen.

Die am 01.09.2009 in Kraft getretene Änderung des Bundesdatenschutzgesetzes (BDSG) betrifft unter anderem die Auftragsdatenverarbeitung und die Stellung des betrieblichen Datenschutzbeauftragten. Der Gesetzgeber hat die Voraussetzungen und Grenzen einer Auftragsdatenverarbeitung nunmehr gesetzlich festgeschrieben. Er hat darüber hinaus einen Kündigungsschutz für den betrieblichen Datenschutzbeauftragten eingeführt.

IT-Leistungen als Auftragsdatenverarbeitung

Besondere Aufmerksamkeit sollte bei IT-Verträgen der Gestaltung von Vereinbarungen zum Datenschutz zukommen. Der Verstoß gegen die gesetzlichen Anforderungen an eine ordnungsgemäße Auftragsdatenverarbeitung soll nunmehr mit einem Bußgeld von bis zu 50.000,- EUR geahndet werden. Der Tatbestand ist verwirklicht, wenn ein Auftrag nicht

richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt wurde. Daneben erfüllt ein Auftraggeber den bußgeldbewehrten Tatbestand, wenn er sich vor Beginn der Datenverarbeitung nicht von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt. Die zuständigen Aufsichtsbehörden haben weitreichende Befugnisse erhalten, um Präventivmaßnahmen rechtzeitig einleiten bzw. Verstöße aufdecken zu können.

Pflichtinhalt für den Vertrag

Um mehr Rechtssicherheit zu schaffen, hat der Gesetzgeber in § 11 BDSG festgelegt, wie der Auftrag zur Datenverarbeitung inhaltlich ausgestaltet sein muss. Danach ist der Auftrag schriftlich zu erteilen. Er muss im Einzelnen folgende Inhalte festlegen:

- Gegenstand und Dauer des Auftrags,
- Umfang, Art und Zweck der Datenverarbeitung, die Art der Daten und den Kreis der Betroffenen,
- die technischen und organisatorischen Maßnahmen zur IT-Sicherheit (§ 9 BDSG),
- Datenberichtigung, -löschung und -sperrung,
- die gesetzlichen Pflichten des Auftragnehmers, einschließlich von ihm vorzunehmender Kontrollen,
- Einsatz von Subunternehmern,
- Kontrollrechte des Auftraggebers, Duldungs- und Mitwirkungspflichten des Auftragnehmers,
- mitzuteilende Verstöße des Auftragnehmers,

- Umfang der Weisungsbefugnisse des Auftraggebers,
- Rückgabe von Datenträgern und Löschung von Datenbeständen beim Auftragnehmer nach Beendigung des Auftrags.

Pflicht zur IT-Sicherheit

Die Vorschrift stellt zudem klar, dass der Auftraggeber sich erstmals vor Beginn der Auftragsdatenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen hat. Das Ergebnis dieser Prüfung muss der Auftraggeber dokumentieren. Der Auftraggeber muss die Kontrollen nicht persönlich durchführen. Vielmehr reicht das Testat eines Sachverständigen oder die Auskunft eines Auftragnehmers aus.

Die aktuelle Gesetzesänderung macht durch den ausdrücklichen Hinweis auf § 9 BDSG deutlich, dass die IT-Sicherheit notwendige Voraussetzungen für einen wirksamen Datenschutz ist. Die Anlage zu § 9 BDSG benennt als Prinzipien die Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags- und Verfügbarkeitskontrolle. Hierdurch sollen Integrität, Authentizität und Vertraulichkeit der Daten sichergestellt werden. Unternehmen müssen daher bestimmte IT-Sicherheitsstandards einhalten. Entsprechende Maßnahmen und Standards definiert das Bundesamt für Sicherheit in der Informationstechnik (BSI).

Der betriebliche Datenschutzbeauftragte

Insbesondere bei der Auftragsdatenverarbeitung wird deutlich, dass die Erfüllung der gesetzlichen Anforderungen die Einbindung der jeweiligen betrieblichen Datenschutzbeauftragten auf beiden Seiten erfordert.

Voraussetzungen der Bestellpflicht

Unter den folgenden gesetzlichen Voraussetzungen sind Unternehmen verpflichtet, einen betrieblichen Datenschutzbeauftragten zu bestellen (§ 4 f Abs. 1 BDSG):

Unabhängig von der Zahl der Beschäftigten ist dies immer bei automatisierten Verarbeitungen besonders sensibler personenbezogener Daten (z. B. Nationalität, Religion, Gewerkschaftszugehörigkeit, Gesundheit, Verhaltensbewertung), die einer Prüfung vor Beginn der Verarbeitung (Vorabkontrolle) unterliegen, der Fall oder bei Adresshandel und Scoring. Zudem, wenn in der Regel 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt werden oder schließlich, wenn in der Regel mindestens 20 Personen damit beschäftigt sind, personenbezogene Daten auf andere Weise (nicht automatisiert) zu erheben, zu verarbeiten oder zu nutzen.

Definition der personenbezogenen Daten

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer Person (§ 3 Abs. 1 BDSG, Art. 2 a RL 95/46/EG). Eine Person ist bestimmbar, wenn sie direkt oder indirekt identifiziert werden kann, insb. durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind. Bei der Entscheidung, ob ein Betroffener bestimmbar ist, sind alle Mittel zu berücksichtigen, die vernünftigerweise entweder von dem Verantwortlichen oder von einem Dritten eingesetzt werden könnten, um den Betroffenen zu bestimmen.

Der Begriff der personenbezogenen Daten umfasst folglich alle Informationen, die über eine Bezugsperson etwas aussagen oder mit ihr in Verbindung gebracht werden können. Hierzu gehören nicht nur klassische Daten wie z. B. der Name, Geburtsdatum, Familienstand etc., sondern auch Bildaufnahmen, Darstellungen des beruflichen Verhaltens, Meinungsäußerungen, Beurteilungen und Werturteile, die sich auf einen bestimmten oder bestimmbarer Betroffenen beziehen. Angaben zu vertraglichen oder sonstigen Beziehungen zu Dritten, Dateibezeichnungen und Prognose- und Planungsdaten können Verhältnisse des Betroffenen beschreiben und damit ebenfalls personenbezogen sein. Nach der gegenwärtig in der Rechtsprechung herrschenden Ansicht handelt es sich sowohl bei dynamischen als auch bei

statischen IP-Adressen um personenbezogene Daten, weil eine Zuordnung zu einer bestimmbar Person möglich ist.

Automatisierte Datenverarbeitung

Eine automatisierte Datenverarbeitung liegt vor, wenn Datenverarbeitungsanlagen zum Einsatz kommen (§ 3 Abs. 2 S. 1 BDSG) und eine programmgesteuerte Zugänglichkeit und Auswertung des Datenbestandes möglich ist. Ausreichend ist, dass die Daten manuell beschafft werden (z. B. bei Kunden im Ladengeschäft zum Zwecke der Markt- und Meinungsforschung) und im Anschluss mittels Datenverarbeitungsanlagen auf einem Datenträger gespeichert und genutzt werden können.

Pflicht zur Vorabkontrolle

Die Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten besteht unabhängig von der Zahl der Beschäftigten, die mit personenbezogenen Daten umgehen, wenn sich aus der Art der verarbeiteten Daten oder dem Verwendungszweck besondere Gefährdungen für das Persönlichkeitsrecht der Betroffenen ergeben können. In diesem Fall unterliegt das Verfahren der automatisierten Datenverarbeitung der Vorabkontrolle durch den Datenschutzbeauftragten. Gemeint sind einer bestimmten Zweckbestimmung dienende Verarbeitungspakete, nicht einzelne Verarbeitungsvorgänge. Solche Risiken bestehen insbesondere, wenn sensible Daten verarbeitet werden oder die Verarbeitung dazu bestimmt ist, Persönlichkeits- oder Leistungsprofile der Betroffenen zu erstellen und zu bewerten. Keinem besonderen Schutz unterliegen Grunddaten, die lediglich Rückschlüsse auf sensible Informationen zulassen würden, wenn keine Auswertungsabsicht besteht. Die Vorabkontrolle entfällt, wenn die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nach Gesetz oder Vertrag erforderlich ist oder mit Einwilligung des Betroffenen erfolgt.

Erreichter Mindestumfang der Datenverarbeitung

Grundsätzlich sieht das Gesetz erst ab einem bestimmten Mindestumfang der Datenverarbeitung eine

Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten vor. Die Pflicht besteht, wenn ein Unternehmen in der Regel mindestens **zehn** Personen ständig mit der automatisierten Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt (§ 4 f Abs. 1 S. 4 BDSG). Diese Regelung erfasst alle Personen, unabhängig von ihrem arbeitsrechtlichen Status, nämlich Angestellte, Arbeiter, freie Mitarbeiter, Heimarbeitskräfte, Leiharbeitnehmer, Auszubildende und Praktikanten. Mitglieder der Geschäftsleitung gehören nicht zum gesetzlich bestimmten Personenkreis.

Die eingesetzten Personen müssen „in der Regel“ und „ständig“ mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt sein (§ 4 Abs. 1 S. 4 BDSG). „In der Regel“ bezieht sich auf die Anzahl von mindestens zehn Beschäftigten, die auf Dauer personenbezogene Daten verarbeiten. Vorübergehende Änderungen (Überschreitungen oder Unterschreitungen) des Personalbestands sind unschädlich. Eine „ständige“ Beschäftigung liegt bereits vor, wenn die Mitarbeiter diese Aufgabe auf unbestimmte bzw. längere Zeit ausüben, d. h. immer wenn sie anfällt. Auf den Anteil bzw. Umfang dieser Arbeit kommt es nicht an. Die Verarbeitung personenbezogener Daten braucht nicht Hauptaufgabe zu sein. Hierbei genügt bereits eine einmalige Verarbeitung je Monat, sofern der Beschäftigte aufgrund seiner Tätigkeit verpflichtet ist, die Aufgabe im Zeitpunkt ihres Anfalls wahrzunehmen. Dabei muss die Datenverarbeitung auch nicht den Arbeitsplatz des Beschäftigten bestimmen. Ausgenommen sind jedoch Beschäftigte, die nur zufällig im Rahmen der Erledigung anderer Aufgaben mit der Verarbeitung personenbezogener Daten zu tun haben (z. B. Revision, Wartungstechniker).

Jedenfalls immer zu berücksichtigen sind Mitarbeiter, die unmittelbar an den Datenverarbeitungsanlagen tätig sind und die das Unternehmen eigens für die automatisierte Erhebung, Speicherung, Veränderung, Übermittlung, Sperrung und Löschung von personenbezogenen Daten angestellt hat (z. B. IT-Mitarbeiter, Personalsachbearbeiter). Des Weiteren sind von der Regelung auch Mitarbeiter betroffen, die nur mit Vorarbeiten oder Nacharbeiten betraut sind (z. B. Kassenmitarbeiter) oder die sich aufgrund von Zugriffsrechten die Daten per Terminal anzeigen lassen können.

Widerruf der Bestellung und Kündigungsschutz

Nach neuer Rechtslage ist die Kündigung des Arbeitsverhältnisses des Beauftragten für den Datenschutz immer nur aus wichtigem Grund im Sinne von § 626 BGB möglich (§ 4 f Abs. 3 S. 4 BDSG). D. h. das Beschäftigungsverhältnis des hauptberuflichen Datenschutzbeauftragten ist ordentlich nicht kündbar. Nach der Abberufung als Beauftragter für den Datenschutz gilt für ein Jahr nach Beendigung der Bestellung ein Kündigungsschutz (§ 4 f Abs. 3 S. 5, 6 BDSG). Damit bestehen die gleichen Kündigungsschutzregelungen wie für Betriebsratsmitglieder. Ist die Beauftragung mit dem Datenschutz nur Teilaufgabe, war nach bisheriger Rechtsprechung eine ordentliche Kündigung aus anderen als amtsbezogenen Gründen nicht ausgeschlossen. Mit dem beendetem Arbeitsverhältnis endete zugleich die Bestellung als Beauftragter für den Datenschutz, ohne dass es einer ausdrücklichen Abberufung bedurfte. Nach der Neuregelung dürfte der Kündigungsschutz auch in diesem Fall greifen.

Soll nur die Bestellung zum Datenschutzbeauftragten wirksam widerrufen werden, ist nach höchstrichterlicher Rechtsprechung die gleichzeitige Teilkündigung dieser arbeitsvertraglichen Abrede nötig. Die vertragliche Grundlage, mit der sich der Beauftragte zur Übernahme der Aufgaben eines Datenschutzbeauftragten verpflichtet, ist von der im BDSG geregelten einseitigen Bestellung zu trennen. Wird der Datenschutzbeauftragte als Arbeitnehmer beschäftigt, tritt diese Tätigkeit nach höchstrichterlicher Rechtsprechung regelmäßig zum Inhalt des Arbeitsvertrages hinzu. Die Abberufung wird daher nur wirksam, wenn auch der Inhalt des Arbeitsverhältnisses entsprechend geändert wird. Gegen den Willen des Arbeitnehmers kann der Wegfall der Tätigkeit als Datenschutzbeauftragter nur durch Teilkündigung erfolgen.

Die Bestellung eines Arbeitnehmers erfolgt in der Regel unter gleichzeitiger einvernehmlicher Änderung der arbeitsvertraglichen Rechte und Pflichten. Die Bestellung zum Datenschutzbeauftragten bedarf regelmäßig einer entsprechenden Erweiterung seiner arbeitsvertraglichen Aufgaben durch Vertragsänderung. Derartige Vereinbarungen zur Arbeitsleistung und zum Arbeitsentgelt sind keine Nebenabreden und damit formlos gültig.

caston.info

Daily News und Datenbank im Internet. Mehrere tausend Beiträge zu Recht & Wirtschaft International finden Sie kostenfrei im Internet bei www.caston.info. Dort können Sie nach Schlagwort und Sachgebieten recherchieren. Unsere Titelliste erhalten Sie auch per Mail.

HERAUSGEBER

HERFURTH & PARTNER Rechtsanwaltsgesellschaft mbH
Luisenstr. 5, D-30159 Hannover
Fon 0511-30756-0
Fax 0511-30756-10
Mail info@herfurth.de,
Web www.herfurth.de
Hannover · Göttingen · Brüssel · München
German & International Lawyers
Member of the ALLIURIS GROUP, Brussels

REDAKTION HANNOVER

Redaktion: Ulrich Herfurth, Rechtsanwalt, Hannover / Brüssel (verantw.); Philipp Neddermeyer, Rechtsanwalt (D);

unter Mitarbeit von Kenneth S. Kilimnik, LL.M., M.IUR., Attorney at Law (USA); Angelika Herfurth, Rechtsanwältin (D); Jens-Uwe Heuer, Rechtsanwalt (D); Dr. jur. Konstadinos Massuras, Rechtsanwalt (D) und Dikigoros (GR); Sibyll Hollunder-Reese, M.B.L., Rechtsanwältin (D); Thomas Gabriel, Rechtsanwalt (D); JUDr. Yvona Rampáková, Juristin (GR); Dr. Jona Aravind Dohrmann, Rechtsanwalt (D); Marc-André Delp, M.L.E., Rechtsanwalt (D); Tatiana Getman, Rechtsanwältin (D); Monika Sekara, Rechtsanwältin (D); Adeline Maler Berger, Advocate (SG) and Solicitor (UK); Peh-Wen Lin, Rechtsanwältin (D); Maimiti Cohen-Solal, Avocat (FR), Attorney at Law (USA); Alexia Calleja Cabeza, Abogada (ES); Prof. Dr. jur. Rüdiger Jach (D); Dr. jur. Christiane Trüe LL.M. (East Anglia), Rechtsanwältin (D).

KORRESPONDENTEN AUSLAND

u.a. Amsterdam, Athen, Bratislava, Brüssel, Budapest, Bukarest, Helsinki, Istanbul, Kiew, Kopenhagen, Lissabon, London, Luxemburg, Mailand, Madrid, Oslo, Paris, Prag, Sofia, Stockholm, Warschau, Wien, Zürich, New York, Sao Paulo, Moskau, Kairo, Tunis, Dubai, Peking, Hongkong, Tokio, New Delhi, Bangkok, Singapur, Sydney.

VERLAG

CASTON GmbH
Law & Business Information
Luisenstr. 5, D-30159 Hannover,
Fon 0511 - 30756-50
Fax 0511 - 30756-60
Mail info@caston.info
Web www.caston.info

Alle Angaben erfolgen nach bestem Wissen; die Haftung ist auf Vorsatz und grobe Fahrlässigkeit beschränkt. Wiedergabe, auch auszugsweise, nur mit Genehmigung der Herausgeber.