CASTON

SINCE 1988 · INTERNATIONAL LAW & BUSINESS INFORMATION · WWW.CASTON.INFO

COMPACT

Unternehmensführung und Arbeitnehmerdatenschutz

Monika Sekara, Rechtsanwältin in Hannover

No. 283 – Oktober 2009

Der Gesetzgeber hat die rechtlichen Anforderungen für einen effektiven Datenschutz erheblich verschärft. Die Änderungen sind am 01.09.2009 in Kraft getreten.

Damit reagiert der Gesetzgeber auf die in den vergangenen Jahren bekannt gewordenen Missbrauchsfälle insbesondere in namhaften großen deutschen Unternehmen. Scheingeschäfte und staatsanwaltschaftliche Ermittlungen zur Aufdeckung der Wirtschaftskriminalität haben dem Ruf dieser Unternehmen erheblich geschadet. Der heimliche Abgleich von Mitarbeiterdaten zur Korruptionsbekämpfung führte in der Öffentlichkeit zu Forderungen nach klaren Regeln für interne Ermittlungen.

Das Gesetz sieht nunmehr ausdrücklich den Schutz der Daten von Beschäftigten vor. Insbesondere unternehmensinterne Ermittlungen zur Vermeidung und Verfolgung von Wirtschaftsdelikten sind nur noch in engen Grenzen erlaubt. Das Gesetz legt auch bestimmte notwendige Inhalte für die Gestaltung der Datenverarbeitung fest, soweit diese als Auftrag vergeben wird.

Zur Umsetzung der aktuellen rechtlichen Anforderungen sollten Unternehmen sorgfältig den Einsatz sowohl administrativer als auch technischer Maßnahmen planen. Der vorliegende Beitrag befasst sich mit den wesentlichen Änderungen des Bundesdatenschutzgesetzes und gibt einen Überblick über die Voraussetzungen, die Unternehmen zur wirksamen Prävention vor Missbrauch personenbezogener Daten beachten müssen.

Compliance als Pflicht des Managements

Zum gegenwärtigen Zeitpunkt ist Compliance für Unternehmen ein zentrales Thema. „Compliance“ bedeutet gesetzeskonformes Verhalten und umfasst das Ergreifen organisatorischer Maßnahmen zur Sicherstellung der Einhaltung relevanter rechtlicher Gebote und Verbote.

Rechtliche Mindestanforderungen

Die rechtlichen Mindestanforderungen an ein Risikomanagementsystem hat das Landgericht München I in einer vielbeachteten Entscheidung konkretisiert (LG München I, Urt. v. 05.04.2007). Danach muss der Vorstand einer Aktiengesellschaft geeignete Maßnahmen treffen, damit er Entwicklungen frühzeitig erkennen kann, die den Fortbestand der Gesellschaft gefährden.

Für notwendig erachtet das Gericht insbesondere die Einrichtung eines Überwachungssystems. Im Unternehmen seien unmissverständliche Zuständigkeiten zu begründen, ein engmaschiges Berichtswesen und eine entsprechende Dokumentation festzulegen. Vom verantwortlichen Sachbearbeiter über die jeweilige Hierarchieebene bis hin zur Unternehmensleitung müssen sämtliche relevanten Stellen von vor-

handenen Risiken Kenntnis erlangen, um die entsprechenden Maßnahmen zur Beherrschung dieser Risiken einleiten zu können. Die damit einhergehende Dokumentation des Risikomanagementsystems gehöre zu den zentralen Aufgaben des Vorstands. Unterbleibt diese Dokumentation, liege ein wesentlicher Gesetzesverstoß vor.

Sorgfaltspflichten

Aber auch unterhalb einer Existenzbedrohung sind Inhaber von Unternehmen und Betrieben verpflichtet, Aufsichtsmaßnahmen zu ergreifen, um betriebsbezogene Straf- und Ordnungswidrigkeiten zu verhindern. Die Verletzung dieser Aufsichtspflicht ist mit einer erheblichen Geldbuße bedroht. Weitergehende Compliance-Anforderungen ergeben sich auch aus anderen Vorschriften.

Bei Sorgfaltspflichtverletzungen können die Mitglieder des Vorstands einer Aktiengesellschaft gegenüber der Gesellschaft persönlich auf Schadensersatz haften. Entsprechende Verpflichtungen zur Einrichtung eines Risikomanagements gelten auch für die Geschäftsführer einer GmbH.

Die ordnungsgemäße Organisation des Unternehmens gehört zu den vordringlichsten Aufgaben eines Geschäftsführers. Gegenüber der GmbH steht ein Geschäftsführer bei Verletzung der ihm obliegenden Pflichten für die Sorgfalt eines ordentlichen Geschäftsmannes ein (§ 43 Abs. 2, Abs. 1 GmbHG). Nach herrschender Ansicht liegt in einem nach außen gerichteten rechtswidrigen Verhalten der Gesellschaft zugleich eine Pflichtverletzung des Geschäftsführers im Innenverhältnis. Der Geschäftsführer hat daher dafür zu sorgen, dass die Gesellschaft die für sie geltenden gesetzlichen und vertraglichen Ge- oder Verbote befolgt. Dieser strenge Haftungsmaßstab kann insbesondere vor dem Hintergrund der neuen Regeln zum Arbeitnehmerdatenschutz weitreichende Konsequenzen haben.

Compliance-Strategien und interne Kontrollen

Die Geschäftsleitung sollte ihre Compliance-Strategie an den jeweils individuell zu ermittelnden Compliance-Risiken ausrichten. Es ist wichtig, an Mitarbeiter eindeutige Verhaltenserwartungen und Handlungsanweisungen zu richten. International gehört die Einführung verbindlicher unternehmensinterner Compliance-Richtlinien (Codes of Conduct) mittlerweile zum Standard für jedes Unternehmen. Gegenüber Arbeitnehmern werden diese Richtlinien über das Direktionsrecht des Arbeitgebers oder eine Betriebsvereinbarung oder durch individuelle Abrede Bestandteil des Arbeitsvertrages und damit verbindlich. Arbeitnehmerdaten dürfen – auch bei Compliance-Kontrollen – in der Regel auf der Grundlage einer Betriebsvereinbarung erhoben, verarbeitet und genutzt werden. Nach ständiger Rechtsprechung des Bundesarbeitsgerichts gehört die von den Betriebsparteien im Rahmen ihrer Regelungskompetenz geschlossene Betriebsvereinbarung zu den Normen, die das Persönlichkeitsrecht einschränken kann (u.a. Beschluss v. 28.08.2008 – 1 ABR 16/07).

Zudem besteht nach den gesetzlichen Vorgaben die Pflicht, die Einhaltung der Vorgaben zu überwachen. Dabei kann die Geschäftsleitung auf einen vorhandenen bzw. mittels Datenverarbeitungsverfahren leicht generierbaren umfassenden Datenbestand zugreifen. Wie sich in der Praxis immer wieder zeigt, ist die Gefahr des Missbrauchs gerade bei internen Kontrollen und Ermittlungen besonders hoch. Rechtlich unzulässig wird die interne Überprüfung nämlich, wenn die Datenbestände losgelöst von konkreten Verdachtsmomenten vollständig ausgewertet und Profile unverdächtiger Mitarbeiter oder Dritter erfasst werden. Zum Schutze der rechtstreuen Arbeitnehmer hat der Gesetzgeber mit dem neuen Arbeitnehmerdatenschutz unternehmenseigenen Kontrollsystemen bestimmten Schranken auferlegt.

Das neue Arbeitnehmerdatenschutzrecht

Die Datenschutzskandale bei einer Reihe von deutschen Großunternehmen haben den Gesetzgeber veranlasst, mit § 32 Bundesdatenschutzgesetz (BDSG) eine neue Vorschrift zum Arbeitnehmerdatenschutz einzuführen. Die Vorschrift regelt, zu welchen Zwecken und unter welchen Voraussetzungen personenbezogene Daten vor, im und nach dem Beschäftigungsverhältnis erhoben, verarbeitet und genutzt werden dürfen.

Erforderlichkeit

Im Wesentlichen fasst die Vorschrift die in ständiger Rechtsprechung erarbeiteten Grundsätze zusammen. Danach sind Erheben, Verarbeiten und Nutzen personenbezogener Daten eines Beschäftigten nur zulässig, wenn dies erforderlich ist für:

- die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder
- später für dessen Durchführung oder
- Beendigung.

Erforderlich ist eine Datennutzung, wenn einem Unternehmen zur Wahrung eigener berechtigter Interessen in der konkreten Situation kein anderes, gleich wirksames und das Persönlichkeitsrecht eines Arbeitnehmers weniger einschränkendes Mittel zur Verfügung steht. Anzuwenden ist diese Grundregel auf alle relevanten Bereiche, z. B. Personalverwaltung, Gehalts- und Lohnabrechnung, Ausübung des Weisungsrechts, Leistungs- und Verhaltenskontrollen, Abmahnungen und Kündigungen. An der Grundregel bemisst sich auch die Zulässigkeit von betriebsinternen Maßnahmen zur Verhinderung von Straftaten und sonstigen Rechtsverstößen.

Aufdeckung von Straftaten und Rechtsverstößen

Die neue Vorschrift zum Arbeitnehmerdatenschutz regelt des Weiteren die Voraussetzungen, unter denen ein Arbeitgeber zur Aufdeckung von Straftaten Beschäftigtendaten erheben, verarbeiten und nutzen darf, nämlich nur unter der folgenden Bedingung:

Der Verdacht auf eine Straftat des betroffenen Beschäftigten muss durch tatsächliche Anhaltspunkte dokumentiert werden können und die Datenverarbeitung zur Aufdeckung erforderlich sein und schließlich muss eine Interessenabwägung unter Berücksichtigung des Verhältnisses von eingesetztem Mittel zum Anlass ergeben, dass die Maßnahme verhältnismäßig ist.

Folglich reichen abstrakte Verdachtsmomente für betriebsinterne Ermittlungen nicht aus.

Die Ermittlungen dürfen sich zudem auch nicht umfassend auf die gesamte Belegschaft und sonstige Dritte erstrecken oder gar auf den systematischen Abgleich eines beliebigen Bestands von Arbeitnehmerdaten mit anderen Quellen abzielen.
Verdachtsunabhängige Massenscreenings dürften damit eindeutig unzulässig sein. Betriebsinterne Compliance-Kontrollen müssen jedenfalls Mitarbeiter und Dritte auslassen, die als Täter eines möglichen Verstoßes nicht oder sehr wahrscheinlich nicht in Frage kommen. Vielmehr sind Indizien zu dokumentieren, die den Verdacht begründen, dass ein Betroffener im Beschäftigungsverhältnis eine Straftat begangen hat. Etwaige Maßnahmen gegen diesen Betroffenen sind dann nur zulässig, wenn ihnen keine überwiegenden schutzwürdigen Interessen des Betroffenen entgegenstehen. Dies muss der Arbeitgeber im Rahmen einer sorgfältigen Verhältnismäßigkeitsprüfung abwägen, bevor er entsprechende Maßnahmen ergreift.

Ausblick

Die Politik hält die eingeführten Änderungen für nicht ausreichend. Im Zuge dieser Diskussion hat das Bundesministerium für Arbeit und Soziales Anfang September 2009 einen Diskussionsentwurf für ein Gesetz zum Datenschutz im Beschäftigungsverhältnis (Beschäftigungsdatenschutzgesetz) vorgelegt. Der Gesetzentwurf sieht umfassende Regelungen zum Umgang mit Arbeitnehmerdaten vor. Er enthält zudem Vorgaben zum Einsatz von z. B. Videoüberwachung, Ortungssystemen und biometrischen Verfahren und statuiert weitreichende Benachrichtigungspflichten im Falle von Verstößen. Es bleibt abzuwarten, ob sich die Gesetzesinitiative in der nächsten Legislaturperiode durchsetzt.

Arbeitgebern ist zu empfehlen, permanente und umfassende betriebsinterne Compliance-Kontrollen zu unterlassen. Bereits der ständige bei Mitarbeitern erzeugte Überwachungsdruck macht die Nutzung der betroffenen Datenbestände unzulässig. Zudem sollte der Betriebsfrieden nicht unnötig gestört werden. Die Unternehmensleitungen müssen in Zukunft den Einsatz von IT und Wirtschaftsprüfungsgesellschaften zur Bekämpfung von Wirtschaftsdelikten sorgfältig planen. Daneben sollten sie besonderes Augenmerk auf die datenschutzkonforme Ausgestaltung der Auslagerung von Datenverarbeitungsprozessen legen.

Informationspflicht bei Datenpannen

Erhebliche Auswirkungen für die Unternehmenspraxis hat die Informationspflicht, die der Gesetzgeber neu ins Bundesdatenschutzgesetz aufgenommen hat. Bei eklatanten Datenverstößen sind Unternehmen verpflichtet, Betroffene und die zuständige Datenschutzaufsichtsbehörde zu informieren (§ 42 a BDSG).

Die Benachrichtigungspflicht besteht, wenn ein Unternehmen tatsächliche Anhaltspunkte dafür erhält, dass gespeicherte besonders sensible personenbezogene Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten zur Kenntnis gelangt sind und dadurch schutzwürdige Interessen der Betroffenen schwerwiegend beeinträchtigt werden könnten.

Als besonders sensible Daten gelten etwa Gesundheitsdaten, Bank- oder Kreditkartenkonten und solche personenbezogenen Daten, die im Zusammenhang mit einer Straftat oder Ordnungswidrigkeit stehen. Der betriebliche Datenschutzbeauftragte ist mit einzubeziehen. Die Benachrichtigung muss unverzüglich, d. h. ohne schuldhaftes Zögern erfolgen.

Die Vorschrift legt zudem fest, welchen Inhalt die Benachrichtigungen haben müssen. Gibt es in einem Fall eine Vielzahl von Betroffenen, ist die Öffentlichkeit durch mindestens halbseitige Anzeigen in mindestens zwei bundesweit erscheinenden Tageszeitungen zu informieren.

Unternehmen die dieser Informationspflicht nicht nachkommen, müssen mit Geldbußen in einer Höhe von bis zu 300.000 EUR rechnen.

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
Fon0511-30756-O
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); Sibyll Hollunder-Reese, M.B.L., Rechtsanwältin (D); Thomas Gabriel, Rechtsanwalt (D); JUDr. Yvona Rampáková, Juristin (CR); 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.