MAYER·BROWN

Die neuen Regelungen zum Arbeitnehmerdatenschutz erschweren die unternehmensinterne Sicherstellung von Compliance.

Die neuen Regelungen zum Arbeitnehmerdatenschutz ab 1. September 2009

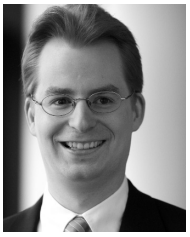
Vorständen und Geschäftsführern droht persönliche Haftung, wenn sie nicht die geeigneten Maßnahmen ergreifen, um Compliance, insbesondere zur Vermeidung von Korruption und anderen Wirtschaftsdelikten, sicherzustellen. Unternehmen riskieren zudem Bußgelder in Millionenhöhe. Wie die jüngsten sogenannten Datenschutzaffären zeigen, bewegen sich die Unternehmen aber bei der Auswahl und Umsetzung dieser Maßnahmen rechtlich auf dünnem Eis.

Diese Publikation soll einen ersten Überblick darüber geben, welche möglichen Auswirkungen der vom Gesetzgeber im neuen Bundesdatenschutzgesetz (BDSG) verstärkte Schutz der Beschäftigten auf die praktische Compliance-Arbeit haben kann.

Dr. Guido Zeppenfeld, LL.M.
Partner, Frankfurt
T: +49 69 79 41 1701
gzeppenfeld@mayerbrown.com

Tim Wybitul
Associate, Frankfurt
T: +49 69 79 41 2231
twybitul@mayerbrown.com

Dr. Andrea Patzak
Associate, Frankfurt
T: +49 69 79 41 1067
apatzak@mayerbrown.com



Kai Liebrich
Associate, Frankfurt
T: +49 69 79 41 1781
kliebrich@mayerbrown.com

Gesetzesverstöße in Unternehmen können existenzbedrohend sein: Schadenersatzforderungen in Millionenhöhe, Straf- und Bußgelder sowie Steuernachforderungen im In- und Ausland, massive Rufschäden – all das können Folgen gesetzeswidrigen Verhaltens von Mitarbeitern sein. Affären wie jene bei Volkswagen und Siemens haben das gezeigt. Daher gewinnt das Thema Compliance bei Unternehmen immer mehr an Bedeutung. Darunter versteht man organisatorische Maßnahmen, die sicherstellen, dass sämtliche rechtlichen Gebote und Verbote im Unternehmen eingehalten werden können.

Aber auch bei der Vermeidung und Verfolgung von Wirtschaftsdelikten gelten strenge Regeln. Bei Compliance-Kontrollen und internen Ermittlungen müssen Unternehmen vor allem den gesetzlichen Schutz personenbezogener Daten ihrer Mitarbeiter beachten. Befolgen sie diese Regeln nicht, kann das seinerseits zu Strafen, Bußgeldern, Schadenersatz und Rufschäden führen. Durch die Neufassung des Bundesdatenschutzgesetzes (BDSG) kommt es zu einer Verschärfung der datenschutzrechtlichen Grenzen praktischer Compliance-Arbeit.

Das Spannungsfeld zwischen Compliance und Arbeitnehmerdatenschutz

Am 3. Juli 2009 hat der Deutsche Bundestag eine Neufassung des BDSG beschlossen. Der Gesetzentwurf hat den Bundesrat am 10. Juli 2009 unverändert passiert. Die Gesetzesänderung wird ab dem 1. September 2009 zu einer Verschärfung des Arbeitnehmerdatenschutzes führen. Der Gesetzgeber reagiert damit auf die sogenannten „Spitzel"-Affären in deutschen Großunternehmen, wie etwa Lidl, Telekom, Deutsche Bahn und zuletzt Deutsche Bank, die in der Öffentlichkeit heftig kritisiert wurden. Ein Punkt wird in den hierzu geführten Diskussionen fast immer übersehen: Unternehmen führen interne Ermittlungen und andere Maßnahmen durch, um Wirtschaftskriminalität zu unterbinden und zu verfolgen. Hierzu sind Unternehmen wie Manager gesetzlich verpflichtet.

Bereits nach den bisherigen Regeln zum Schutz von Mitarbeiterdaten war es für Unternehmen schwer, effektive Ermittlungen in zulässiger Weise durchzuführen. Selbst Fachleute nannten das alte Datenschutzrecht unübersichtlich und kaum verständlich. Es enthielt zudem wenig brauchbare und klare Vorgaben dazu, was genau erlaubt und was verboten war. Verweise auf notwendige Interessenabwägungen waren wenig hilfreich, da sie keine Auslegungshilfen dafür gaben. Es bedurfte der Auslegung durch Spezialisten – aber selbst diese konnten sich auf die Auslegung einzelner Regelungen über den Mitarbeiterdatenschutz im BDSG nicht einigen.

Die bestehenden Unklarheiten haben die neuen Regelungen nicht beseitigt. Der Gesetzgeber hat es versäumt, Unternehmen und Arbeitnehmern vor dem Hintergrund der öffentlich diskutierten Datenschutzaffären klare, interessengerechte Richtlinien dafür an die Hand zu geben, was erlaubt und was verboten ist.

Das neue Arbeitnehmerdatenschutzrecht

Für den Datenschutz von Arbeitnehmern gilt künftig der neue § 32 BDSG, der die Grundregel zum Umgang mit Daten von Beschäftigten enthält. Nach § 32 Abs. 1 Satz 1 BDSG dürfen personenbezogene Daten grundsätzlich nur unter engen Voraussetzungen erhoben, verarbeitet oder genutzt werden.

Der Umgang mit den Daten muss entweder

- für die Entscheidung über die Einstellung oder die Beendigung des Beschäftigungsverhältnisses oder

- für die Durchführung des Beschäftigungsverhältnisses erforderlich sein.

Andernfalls sind die Erhebung, Verarbeitung oder Nutzung von Arbeitnehmerdaten unzulässig. Nach § 32 Abs. 3 BDSG bleiben die Beteiligungsrechte der Interessenvertretungen der Beschäftigten unberührt.

Erforderlichkeit des Umgangs mit Arbeitnehmerdaten

Nach dem Wortlaut des Gesetzes stellt sich für Unternehmen künftig die Frage, was „erforderlich“ ist. Den Begriff der Erforderlichkeit bestimmt der Gesetzgeber nicht näher. Allerdings soll der neue § 32 BDSG nach der Gesetzesbegründung die bislang von der Rechtsprechung erarbeiteten Grundsätze des Datenschutzes im Beschäftigungsverhältnis nicht ändern, sondern lediglich zusammenfassen. Es gelten also die zum bisherigen Arbeitnehmerdatenschutz entwickelten Grundsätze. Danach ist eine Datennutzung erforderlich, wenn die berechtigten Interessen des Unternehmens auf andere Weise nicht oder nicht angemessen gewahrt werden können. So ist die Erforderlichkeit beispielsweise für den Umgang mit Arbeitnehmerdaten bei der Personalverwaltung und der Gehaltsabrechnung grundsätzlich gegeben.

Arbeitnehmerdaten und interne Ermittlungen

Die Neufassung des Gesetzes enthält gravierende Neuerungen im Hinblick auf den Umgang mit Arbeitnehmerdaten zur Aufdeckung von Straftaten. Sofern keine ausdrückliche Zustimmung der Mitarbeiter vorliegt, dürfen zur Aufdeckung von Straftaten personenbezogene Daten von Beschäftigten künftig nur unter den engen Voraussetzungen des § 32 Abs. 1 Satz 2 BDSG erhoben, verarbeitet oder genutzt werden:

- Zunächst müssen tatsächliche Anhaltspunkte (Indizien) für eine begangene Straftat vorliegen; abstrakte Verdachtsmomente allein reichen nicht aus.

- Diese Indizien müssen nun mit einer hohen Wahrscheinlichkeit (Verdacht) darauf hinweisen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat.

- Die Straftat muss in einem engen Zusammenhang mit dem Arbeitsverhältnis stehen.

- Die Erhebung, Verarbeitung oder Nutzung von Mitarbeiterdaten muss zur Aufdeckung der Straftat erforderlich sein.

- Die Verwendung von Mitarbeiterdaten ist nur zulässig, wenn der Betroffene kein entgegenstehendes, überwiegendes schutzwürdiges Interesse hat. Insbesondere dürfen Art und Ausmaß des Umgangs mit den Daten im Hinblick auf den Anlass nicht unverhältnismäßig sein. Mit Anlass meint der Gesetzgeber zum einen die Art und Schwere der Straftat und zum anderen die Intensität des Verdachts.

- Der Arbeitgeber muss die vorliegenden Verdachtsmomente sowie die Abwägungskriterien dokumentieren, will er Ermittlungen durchführen, ohne gegen den Mitarbeiterdatenschutz zu verstoßen.

Diese Vorgaben gelten nach § 32 Abs. 2 BDSG für alle Mitarbeiterdaten, selbst wenn diese nicht automatisch verarbeitet werden.

Bei dieser Vielzahl von unbestimmten Voraussetzungen wird es für die Praxis schwer werden, belastbare Ermittlungskonzepte zu erstellen. Vor allem der systematische Abgleich von Arbeitnehmerdaten mit anderen Quellen ist damit wohl nur noch zulässig, wenn tatsächliche Anhaltspunkte für das Vorliegen von bereits begangenen Straftaten gegeben sind und sofern nur Arbeitnehmer aus dem engsten Verdachtskreis einbezogen werden. Die sogenannten „Massenscreenings“ wurden vor allem von IT-Fachleuten und Wirtschaftsprüfungsgesellschaften, die auf die Bekämpfung von Wirtschaftskriminalität spezialisiert sind, regelmäßig eingesetzt. Auch die protokollierte Befragung von Mitarbeitern im Rahmen von internen Ermittlungen und die spätere systematische Auswertung sind nur noch zulässig, wenn der befragte Mitarbeiter zustimmt oder die oben geschilderten Voraussetzungen vorliegen. Die Durchsicht von E-Mails oder Überprüfung von IT-Nutzerprotokollen dürfte hierbei allenfalls in Ausnahmefällen erlaubt sein, wenn eine ausdrückliche Zustimmung in Kenntnis der Ermittlungen nicht vorliegt. Das gilt selbst für Unternehmen, die die private Nutzung ihrer IT-Systeme ausdrücklich untersagen. Zum jetzigen Zeitpunkt sind die Folgen dieser Neuregelung kaum abzusehen.

Arbeitnehmerdaten und vorbeugende Compliance

Ein wesentlicher Zweck der praktischen Compliance-Arbeit ist Vorbeugung. Nach der Gesetzesbegründung gilt die Grundregel des § 32 Abs. 1 Satz 1 BDSG auch für Maßnahmen zur Verhinderung von Straftaten und sonstigen Rechtsverstößen, die im Zusammenhang mit dem Arbeitsverhältnis stehen. Kontrollen der Leistung, vor allem aber des Verhaltens der Mitarbeiter, sollen weiterhin zulässig bleiben. Aber auch sie müssen erforderlich sein.

Die neue gesetzliche Regelung wirkt sich auf eine Vielzahl von Maßnahmen in diesem Bereich aus, zum Beispiel:

- Verhaltensrichtlinien für Mitarbeiter (sogenannte Codes of Conduct);
- Benennung von Ombudsleuten, bei denen Arbeitnehmer und Dritte sich beim Vorliegen von Verdachtsmomenten melden und beraten lassen können;
- sogenannte Mitarbeiter-Screenings vor der Einstellung, um (zumindest in Kernbereichen des Unternehmens) zu vermeiden, dass nicht integre Mitarbeiter angestellt werden;
- für Compliance-Zwecke eingesetzte Schulungsprogramme (beispielsweise für Schulungen nach den Vorschriften des Allgemeinen Gleichbehandlungsgesetzes);
- die Einführung von sogenannten Whistleblowing-Programmen, mit denen Arbeitnehmer oder Dritte (oft anonym) Verdachtsmomente melden können, denen das Unternehmen dann nachgeht.

Folgen für die Praxis

Vor der Einleitung bzw. Durchführung interner Ermittlungen müssen noch intensiver als bislang datenschutzrechtliche Belange geprüft werden. Jeder Einzelfall ist hinsichtlich der vorwerfbaren Straftat, des Grades des Verdachts (Indizienlage) und der schutzwürdigen Interessen der betroffenen Mitarbeiter präzise abzuwägen. Diese Abwägung muss dokumentiert werden. Eine allgemeine Einordnung zulässiger und verbotener Untersuchungsschritte ist bei den stark einzelfallbezogenen Regelungen des BDSG nicht mehr möglich.

Ermittlungen sollten sich – zumindest auf einer ersten Stufe – auf die Analyse von Daten beschränken, die nicht als personenbezogene Daten gelten. Straf- und wirtschaftsrechtlich erfahrene Spezialisten sowie kriminalistische Ansätze können solche Ermittlungen soweit präzisieren, dass – auf einer zweiten Stufe – bei der Verwendung personenbezogener Daten ausreichend Verdachtsmomente vorliegen.

Die Praxis hat gezeigt, dass nach einer genauen rechtlichen Analyse in Zweifelsfällen eine Abstimmung mit der datenschutzrechtlichen Aufsichtsbehörde sinnvoll sein kann. Auch sollte stets eine Vertrauensperson der betrieblichen Mitbestimmungsorgane einbezogen werden.

Auf Compliance-Abteilungen, betriebliche Datenschützer und interne Revisionen kommt ein hoher zusätzlicher Aufwand zu. Kontrollmaßnahmen müssen nun präzise auf die Anforderungen des Datenschutzes abgestimmt werden. Insbesondere ist präventive Kontrolle von repressiver Ermittlung abzugrenzen.

Führen Unternehmen künftig Kontrollen ohne konkreten Verdacht auf Regelverstöße durch, müssen sie vorher die neue Rechtslage genau prüfen. Dabei ist vornehmlich die Frage zu klären, inwieweit bei solchen Kontrollen auf personenbezogene Daten von Mitarbeitern zugegriffen werden muss oder ob es stattdessen genügt, bloße Geschäftsdaten zu analysieren. Zumindest dann, wenn ein erster Verdacht gegenüber einem bestimmten Mitarbeiter vorliegt, wird das Stadium der Kontrolle verlassen und es beginnen Ermittlungen.

Kontrollen und Ermittlungen sollten ferner genau dokumentiert werden. Nur wenn eine Compliance-Kontrolle auf der Grundlage einer genauen Prüfung des Sachverhalts und einer präzisen Analyse der Rechtslage durchgeführt wird, sind Unternehmen auf der sicheren Seite.

Die Praxis wird genau zu beobachten haben, wie die jeweiligen Datenschutzaufsichtsbehörden die neuen Regelungen interpretieren und anwenden.

Ausblick

Die Neufassung des BDSG lässt viele Fragen offen. Der Gesetzgeber hatte sich das Ziel gesetzt, das Datenschutzrecht im Arbeitsverhältnis transparenter zu machen. Das ist nicht gelungen. Die Notwendigkeit, Wirtschaftsdelikte zu bekämpfen, wurde dabei nicht ausreichend berücksichtigt.

Bei internen Ermittlungen sind intelligente Untersuchungsansätze unter genauer Beachtung der datenschutzrechtlichen Grenzen praktischer Compliance-Arbeit unverzichtbar. Eine Fokussierung auf rechtlich relevante Geschäftsvorgänge und konkrete Abläufe sind den bislang in der Praxis oftmals üblichen „Massenuntersuchungen“ vorzuziehen.

About Mayer Brown

Mayer Brown is a leading global law firm with offices in major cities across the Americas, Asia and Europe. We have approximately 1,000 lawyers in the Americas, 300 in Asia and 500 in Europe. Our presence in the world's leading markets enables us to offer clients access to local market knowledge combined with global reach.

We are noted for our commitment to client service and our ability to assist clients with their most complex and demanding legal and business challenges worldwide. We serve many of the world's largest companies, including a significant proportion of the Fortune 100, FTSE 100, DAX and Hang Seng Index companies and more than half of the world's largest investment banks. We provide legal services in areas such as Supreme Court and appellate; litigation; corporate and securities; finance; real estate; tax; intellectual property; government and global trade; restructuring, bankruptcy and insolvency; and environmental.

OFFICE LOCATIONS

AMERICAS
- Charlotte
- Chicago
- Houston
- Los Angeles
- New York
- Palo Alto
- São Paulo
- Washington

ASIA
- Bangkok
- Beijing
- Guangzhou
- Hanoi
- Ho Chi Minh City
- Hong Kong
- Shanghai

EUROPE
- Berlin
- Brussels
- Cologne
- Frankfurt
- London
- Paris

ALLIANCE LAW FIRMS
- Mexico, Jáuregui, Navarrete y Nader
- Spain, Ramón & Cajal
- Italy and Eastern Europe, Tonucci & Partners

Please visit www.mayerbrown.com for comprehensive contact information for all Mayer Brown offices.