usdruck gebracht, dass die
grundsätzlich nicht vor der
11. 2006 - B 6 KA 7/06 R
ine wirtschaftliche Verord-

ihrung kann die Gefahr der
bar ist ein regelmäßiges

ht jederzeit eine genaue
skosten, welche mit dem
enzusteuern.
für seine Genesung durch
chen, Sport), so dass die
. Selbstverständlich sollte
für Wechsel- und Neben-
Patient stark ansteigt.
r Zulassungsgründe noch
h zu machen. Die damit
für die Verordnung inno-

kostenintensiven Patien-
digkeiten eine selbstver-
gen festgesetzt, weil der
onnte.

essverfahrens wegen
Vielmehr gilt es, die
it dem Ziel der Re-
n fundierte Argumenta-
r Notwendigkeit der
gelingt erfahrungsge-
ntation (statistisch,
: hat hierbei die
heiten.

rtner der überörtlichen Sozietät
ts tätig ist. Am Standort
ztliche Leistungserbringer
gütungsrechts, des Berufsrechts

Herausforderung für Unternehmen durch das neue Datenschutzgesetz

Datenschutz-Compliance

DR. JOSÉ A. CAMPOS NAVE · FELIX VON BAUMBACH*

Die Thematik „Datenschutz in der Personalarbeit" hat an Bedeutung gewonnen. In zahlreichen Presseberichten der jüngeren Vergangenheit wurde über Skandale im Zusammenhang mit dem Umgang von Mitarbeiterdaten berichtet. Hierbei ging es nicht nur um die Überwachung der persönlichen Sphäre der Mitarbeiter, sondern auch um den gezielten Abgleich von betrieblichen Bankkonten mit Bankverbindungen der Mitarbeiter oder um die Auswertung der Telefonverbindungsdaten der Arbeitnehmer. Ungeachtet dessen, dass sicherlich in einigen Fällen das angemessene Maß für eine sachgerechte Datenerhebung und -kontrolle des Mitarbeiters durch den Arbeitgeber überschritten wurde, bildeten diese Fälle jedoch die Ausnahme. In der weit überwiegenden Anzahl der bekannt gewordenen Fälle ging es den Unternehmen um die Korruptionsbekämpfung und darum, sicherzustellen, dass einzelne Mitarbeiter keine Straftaten aus dem Unternehmen heraus begehen, für die dieses dann einzustehen hat. Es kollidieren hierbei die berechtigten Arbeitgeberinteressen an der Einführung einer effizienten Korruptionskontrolle unter Nutzung einer Datenschutz-Compliance und das allgemeine Persönlichkeitsrecht der Arbeitnehmer. Durch das Inkrafttreten der jüngsten Novelle des Bundesdatenschutzgesetzes (BDSG) am 1. 9. 2009 haben sich gewichtige Änderungen hinsichtlich des Umgangs mit Personaldaten ergeben. Die Gesetzesnovelle hat zur deutlichen Verschärfung des Datenschutzes geführt. Bedauerlicherweise hat der Gesetzgeber jedoch durch die Einführung von unbestimmten Rechtsbegriffen zu weiteren Unsicherheiten bei dem Umgang mit Personaldaten beigetragen. Es ist zudem mit einem gesteigerten Aktionismus der Datenschutzbehörden gegenüber den privaten Unternehmen zu rechnen. Ein Abwarten wäre, insbesondere angesichts der nunmehr deutlich angehobenen Geldbußen, verfehlt.

Arbeitshilfe: Die elektronische Fassung des Beitrags enthält als PDF-Anhang eine Checkliste zum Datenschutz bei der Korruptionsbekämpfung.

Inhaltsübersicht

I. Compliance als Bestandteil der modernen Unternehmensführung
II. Einschränkung bei der Korruptionsbekämpfung durch den Mitarbeiterdatenschutz
III. Bewertung und Ausblick

* Dr. José A. Campos Nave, EMBA (Accounting & Controlling) ist Rechtsanwalt, Fachanwalt für Steuerrecht, Fachanwalt für Handels- und Gesellschaftsrecht sowie Partner und Niederlassungsleiter im Eschborner Büro der internationalen Sozietät Rödl & Partner; Felix von Baumbach ist Rechtsanwalt und Senior Associate bei Rödl & Partner am selben Standort.

I. Compliance als Bestandteil der modernen Unternehmensführung

Compliance beinhaltet ein neues Verständnis ordnungsgemäßer Unternehmensführung

Compliance ist als ein neueres Verständnis bei der Unternehmensführung zu betrachten, demzufolge das Unternehmen in jedem Bereich Gesetze, Regeln und eigene Selbstverpflichtungen einhält, um Schäden für das Unternehmen und für Dritte zu verhindern. Hierbei ist es sachgerecht, die unternehmerische Compliance in eine Corporate Compliance Organisation im Unternehmen einzubinden.

Die Einführung von Compliance im Unternehmen erfasst auch den Bereich des Personalwesens. Letztlich werden Straftaten immer durch natürliche Personen und nicht abstrakt durch das Unternehmen als juristische Person begangen. Eine Korruptionsprävention sollte daher auf der Mitarbeiterebene eines Unternehmens beginnen.

Beispiel 1 *Die Geschäftsführung muss ein effizientes Kontrollsystem zur Unterbindung von Scheinrechnungen einrichten. Diese Verpflichtung für die Buchhaltung gilt bei Konzernobergesellschaften auch im Hinblick auf abhängige Gesellschaften (OLG Jena, Urteil v. 12. 8. 2009 - 7 U 244/07).*

Compliance ergänzt das bestehende Risikomanagement

Die **Corporate Compliance Organisation** ergänzt darüber hinaus das bereits im Unternehmen bestehende Risikomanagementsystem oder auch ein Total Quality Management-System. Daher beruht die von der aktuellen Gesetzgebung geforderte professionelle Corporate Compliance Organisation auf dem Gedanken eines funktionierenden Risikomanagements im Unternehmen. Hierbei werden nicht nur bestandsgefährdende Risiken einbezogen, die eine Haftung der Gesellschaft sowie ihrer Lenkungs- und Aufsichtsorgane auslösen können. Ihre Identifizierung und Kommunikation gegenüber den verantwortlichen Unternehmensleitern schärft bei diesen das Bewusstsein für die rechtlichen Rahmenbedingungen ihrer Entscheidungen und Strategien, ohne ihnen den unverzichtbaren unternehmerischen Handlungsspielraum zu nehmen.

Compliance hilft, Unternehmenswerte zu erhalten

Bei professioneller Gestaltung, Durchführung und Fortentwicklung kann die Corporate Compliance Organisation als offensives Mittel zur Positionierung des Unternehmens bei Banken, Kunden und Lieferanten eingesetzt werden und zum guten Ruf des Unternehmens beitragen, der sich auf Marken und Produkte und damit langfristig auch auf das Unternehmensergebnis und den Unternehmenswert überträgt. Die Zielsetzung der Unternehmenslenker und deren Aufsichtsorgane sollte es daher sein, eine unternehmensbezogene leistungsfähige Corporate Compliance Organisation zu entwickeln und im Unternehmen zu implementieren.

Da der richtige Umgang mit Mitarbeiterdaten von höchster Brisanz ist und bei Unternehmen mit großer Öffentlichkeitspräsenz im Fall einer falschen Handhabung zu deutlichen Schäden des Unternehmensrufs führt, ist die **Datenschutz-Compliance** ein wichtiger Bestandteil des umfassenden Compliance-Systems im Unternehmen.

II. Einschränkung bei der Korruptionsbekämpfung durch den Mitarbeiterdatenschutz

Datenschutz ist Bestandteil der Compliance

Um die Verwendungsmöglichkeit der Mitarbeiterdaten beim Einsatz gegen Korruption bzw. bei der Umsetzung von Compliance im Unternehmen zu bestimmen, bedarf es zunächst der Klärung, welche Daten der Mitarbeiter überhaupt geschützt sind und welche Konsequenzen sich hieraus für das Unternehmen in der Datenanalyse und -verwendung ergeben.

1. Geschützte Personaldaten

Schutzumfang für Daten

Geschützt sind diejenigen Daten, anhand deren ein Bezug zu einer natürlichen Person hergestellt werden kann. Hierzu gehören Namen und Adressdaten sowie auch darüber

hinausgehende Informationen, z. B. das Alter, der Gesundheitszustand oder Informationen über das Verhalten einer Person. Erfasst sind sowohl elektronisch gespeicherte Daten als auch Daten in Papierform. Somit gehören auch Listen, Tabellen, Zielvereinbarungen, Umsatzergebnisse und persönliche Beurteilungen zu den geschützten Daten.

Daten mit herstellbarem Personenbezug

Unter den Datenschutz fallen auch Daten, deren Personenbezug nicht offensichtlich ist, die aber genügend Informationen enthalten, anhand deren mit nicht unverhältnismäßig hohem Aufwand ein Bezug zu einer bestimmten Person hergestellt werden kann. Hierzu gehören etwa Daten, die unter einem Aktenzeichen oder einem Kürzel abgelegt sind oder die über einen Nummerncode verschlüsselt werden.

Anonymisierte Daten

Nicht geschützt sind anonymisierte Daten sowie Daten ohne Personenbezug, etwa reine Statistiken, wie z. B. durchschnittliche betriebliche Fehlzeiten etc. Soweit allerdings derartige Informationen einen Bezug zu den einzelnen dahinterstehenden Personen zulassen, z. B. aufgrund einer geringen Gruppengröße, fallen sie wiederum unter den Datenschutz. Je kleiner die Gruppe, umso eher lässt sich im Zweifel ein konkreter Bezug zu einer natürlichen Person herstellen. Von einer **Anonymisierung** kann erst dann ausgegangen werden, wenn ein Personenbezug nur unter unverhältnismäßig hohem Aufwand hergestellt werden könnte. Hieraus lässt sich bereits entnehmen, dass im Zweifel nicht von einer Anonymisierung ausgegangen werden kann. Ausgenommen vom Schutz sind auch solche Daten, die ohnehin jedermann öffentlich zugänglich sind. Dies ist bei Mitarbeiter- und Bewerberdaten jedoch i. d. R. nicht der Fall.

2. Besonderer Beschäftigtendatenschutz nach § 32 BDSG

Während vor Inkrafttreten der Datenschutzrechtsnovelle zum 1. 9. 2009 kein spezieller Datenschutz für Beschäftigte existierte, sondern der Schutz von solchen Daten unter den allgemeinen Datenschutz fiel, hat der Gesetzgeber mit § 32 BDSG eine eigene Regelung zur Zulässigkeit der Erhebung und Verarbeitung von Beschäftigtendaten geschaffen.

a) Kriterium der Erforderlichkeit

„Erforderlichkeit" als zentraler Begriff für die Datenverwendung

Daten von Beschäftigten dürfen nur erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Einstellung oder die Beendigung des Beschäftigtenverhältnisses oder für dessen Durchführung erforderlich ist. Entscheidendes und zugleich unbestimmtes Merkmal ist das der „Erforderlichkeit". Der Gesetzgeber hat die Ausgestaltung dieses Merkmals bewusst der Rechtsprechung überlassen. Erforderlich dürfte eine Datenerhebung sowie -verarbeitung aber dann sein, wenn die berechtigten Interessen des Arbeitgebers auf andere Weise nicht gewahrt werden können.

Berechtigte Interessen des Arbeitgebers

Beispiel 2 *Dies ist gegeben, wenn zur Abwicklung eines bestehenden Arbeitsverhältnisses Namen und Adressdaten sowie Kontodaten der Lohnbuchhaltung zur Verfügung gestellt werden. Soweit diese von einem Dienstleister, z. B. einem Auftragsdatenverarbeiter, vorgenommen wird, ist der Arbeitgeber auch für den datenschutzrechtlich unbedenklichen Umgang des externen Dienstleisters mit den Daten verantwortlich.*

Datensparsamkeit – Beispiel: Austausch im Konzern

Generell ist bei der Weitergabe von personenbezogenen Daten auch innerhalb des Unternehmens oder Konzerns Zurückhaltung geboten. Das Merkmal der „Erforderlichkeit" dürfte hier insbesondere dann verletzt sein, wenn Daten aus reinen Praktikabilitätsgründen anderen Stellen oder Personen zugänglich gemacht werden, die diese nicht zwingend benötigen.

Beispiel 3 *Die Erfassung personenbezogener Daten von Bewerbern im Rekrutierungsprozess dürfte nur solange unter das Merkmal der Erforderlichkeit fallen, wie der Rekrutierungsprozess läuft. Mit der Absage an einen Bewerber und der Abwicklung der sich*

daraus ergebenden Arbeitgeberpflichten, wie z. B. Überweisung der Fahrtkosten, sind Bewerber-Daten zu löschen. Ohne gesonderte Einwilligung dürfen die Daten von Bewerbern nicht gespeichert werden. Eine sog. Vorratsdatenverarbeitung ist nicht erlaubt.

Hinweis Sensible Felder tun sich vor allem auf bei der Verwendung von Personalfragebögen oder bei der Speicherung personenbezogener Daten auf einem Server, auf den Dritte unbeschränkten Zugriff haben. Analog dazu ist der Zugriff auf Akten, Listen und Vereinbarungen vor dem Zugriff und der Kenntnisnahme unberechtigter Dritter effizient zu beschränken. Die Beobachtung oder Überprüfung des laufenden E-Mail-Verkehrs ist in jedem Fall rechtlich höchst bedenklich, sofern nicht die **private Nutzung der Kommunikationsmittel ausdrücklich und wirksam verboten ist** und die Einhaltung dieses Verbots regelmäßig und effizient überwacht wird. In jedem Fall sind sowohl die Anforderungen beim Umgang mit Personaldaten im Unternehmen nach der Novellierung des Bundesdatenschutzgesetzes erheblich gestiegen als auch die Gefahr, bei der täglichen Personalarbeit rechtlichen Anforderungen nicht zu genügen.

b) Schutzbereich der Norm

Gleicher Schutz für Beschäftigten- und Bewerberdaten

Dass nicht nur die Daten von Mitarbeitern, mit denen aktuell ein Arbeitsverhältnis besteht, geschützt sind, stellt jetzt § 3 Abs. 11 BDSG klar. Hiernach fallen neben den angestellten Mitarbeitern auch eine Vielzahl weiterer Personen unter den besonderen Datenschutz i. S. des § 32 BDSG. „Beschäftigte" sind also nicht nur angestellte Mitarbeiter, sondern der Personenkreis ist wesentlich weiter und bezieht insbesondere auch Bewerber und ehemalige Mitarbeiter mit ein.

c) Aufdeckung von Straftaten

Einschränkungen bei der Korruptionsbekämpfung

Die Erhebung von personenbezogenen Daten zur Aufdeckung von Straftaten ist nur noch zulässig bei einem konkreten Tatverdacht in Bezug auf eine konkrete Person. Die Wertung nähert sich durchaus dem strafprozessualen Erfordernis des **„hinreichenden Tatverdachts"** an, der Voraussetzung für die Einleitung eines Verfahrens durch die Staatsanwaltschaft ist. Insofern sind dem Unternehmen zur Aufdeckung eventueller Pflichtverstöße die Hände gebunden, soweit sich der Tatverdacht nicht hinreichend konkretisieren lässt. Das führt dazu, dass der Sachverhalt bereits vor der Datenerhebung umfangreich ermittelt worden sein muss. Ein Massenscreening zur Aufdeckung einer Straftat ist nicht zulässig. Das Interesse der Betroffenen am Schutz ihres Persönlichkeitsrechts wird gegenüber dem Interesse des Unternehmens an der Ermittlung von Straftaten und Vertragsbrüchen tendenziell höher eingestuft.

Dies hat wiederum Auswirkungen auf eine effiziente Korruptionsbekämpfung. Im Rahmen der Korruptionsbekämpfung geplante Maßnahmen sind daher vor deren Umsetzung im Lichte des § 32 BDSG zu überprüfen. Insbesondere bei Tochter- oder Beteiligungsgesellschaften von an der US-amerikanischen Börse notierten Unternehmen kann ein Widerspruch insoweit entstehen, als die amerikanische Börsenaufsicht regelmäßig Angaben zu Mitarbeitern des Unternehmens und deren Beteiligungen fordert und für den Fall einer Weigerung hohe Geldbußen verhängt.

d) Umsetzung im Unternehmen

Kritische Prüfung der bisherigen Praxis geboten – neue interne Richtlinien notwendig?

Es bedarf daher einer umfassenden Revision der Personalpraxis und der Prozessabläufe im Hinblick auf den Datenschutz im Unternehmen. Zur Umsetzung der gesteigerten datenschutzrechtlichen Anforderungen sollten entsprechende datenschutzrechtliche Richtlinien zur Datenverwendung im Unternehmen implementiert werden. Zudem bietet sich der Abschluss von **Betriebsvereinbarungen** zum Datenschutz an.

III. Bewertung und Ausblick

Die Einführung eines besonderen Mitarbeiterdatenschutzes durch § 32 BDSG hat zur Rechtsklarheit und zum sicheren Umgang für die Unternehmen mit den Daten nicht wesentlich beigetragen. Durch den Begriff der „Erforderlichkeit" bei der Verwendung der Mitarbeiterdaten können die rechtlichen Grenzen nicht eindeutig bestimmt werden. Die Konkretisierung bleibt der Rechtsprechung überlassen, dies jedoch mit der verbleibenden Unsicherheit für die Unternehmen und deren Berater.

Haftung des Compliance Officers

Diese Unsicherheit beeinflusst – ungeachtet der Existenz eines Datenschutzbeauftragten – insbesondere auch einen Compliance Officer im Unternehmen, der aufgrund seiner Garantenstellung für Verstöße gegen den Datenschutz haftet (zur Strafbarkeit des Compliance Officers aufgrund einer Garantenstellung BGH, Urteil v. 17. 7. 2009 - 5 StR 394/08 [⇒MAAAD-26472]; Kommentierung dazu Campos Nave, BB 2009 S. 2059).

Das Bundesverfassungsgericht hat in seinem aktuellen Urteil zur Vorratsdatenspeicherung nochmals die Bedeutung des Datenschutzes im Verhältnis zum Schutz der Bevölkerung vor Terror deutlich herausgestellt (BVerfG, Urteil v. 2. 3. 2010 - 1 BvR 256/08, 263/08 und 586/08). Wenngleich sich das Gericht nicht direkt zum Umgang mit Daten in der Privatwirtschaft äußerte, dürfte sich die darin enthaltene Wertung bei Abwägung der Mitarbeiterinteressen mit dem Interesse des Unternehmens an einer effizienten Korruptionsbekämpfung doch durchaus wiederfinden. Die Verarbeitung und Nutzung von Mitarbeiterdaten kann nicht von vornherein oder pauschal mit dem Argument der gesetzlich ebenfalls geforderten effektiven Korruptionsbekämpfung gerechtfertigt werden. Der Compliance Officer steht im Spannungsfeld zwischen Korruptionsprävention und Mitarbeiterdatenschutz. Dieser Konflikt wiederum dürfte Auswirkungen auf die Bereitschaft geeigneter, zuverlässiger Personen haben, diese Aufgabe überhaupt wahrzunehmen. Sie übernehmen eine Aufgabe und mit ihr eine Garantenstellung für eine Gefahrenquelle, die für sie kaum beherrschbar ist. In jedem Fall bewegen sich Compliance Officers auf unsicherem Boden.

FAZIT

Mitarbeiterdatenschutz hat seine Berechtigung im Unternehmen. Allerdings muss den Unternehmen auch die Möglichkeit belassen werden, Compliance und in diesem Zusammenhang die Korruptionsbekämpfung im Unternehmen umsetzen zu können. Durch Korruption wird nicht nur das Unternehmen geschädigt. Die hieraus resultierenden Schäden sind auch für die Volkswirtschaft beachtlich. Der Gesetzgeber hätte im Rahmen des § 32 BDSG zur Rechtsklarheit für alle Beteiligten beitragen können. Dies ist ausgeblieben. Es bleibt abzuwarten, ob die im Koalitionsvertrag genannte Ankündigung, den Mitarbeiterdatenschutz durch ein eigenes Kapitel im BDSG näher auszugestalten, in dieser Legislaturperiode tatsächlich umgesetzt wird.

AUTOREN

Dr. José A. Campos Nave, EMBA (Accounting & Controlling), ist Rechtsanwalt, Fachanwalt für Steuerrecht, Fachanwalt für Handels- und Gesellschaftsrecht sowie Partner und Niederlassungsleiter im Eschborner Büro der internationalen Sozietät Rödl & Partner.

Felix von Baumbach ist Senior Associate bei Rödl & Partner am Standort Eschborn und leitet dort den Bereich Arbeitsrecht. Seine Tätigkeitsschwerpunkte sind neben dem Arbeitsrecht das Handels- und Gesellschaftsrecht sowie das Datenschutzrecht.