GPS, Internet & Video

Datenschutz am Arbeitsplatz

Symposium 2008

LDI NRW

Landesbeauftragte
für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen

Herausgeberin:

Landesbeauftragte für
Datenschutz und Informationsfreiheit
Nordrhein-Westfalen
Bettina Sokol

Kavalleriestraße 2 - 4
40213 Düsseldorf

Tel.: 0211/38424-0
Fax: 0211/3842410
E-mail: poststelle@ldi.nrw.de

Diese Broschüre kann unter www.ldi.nrw.de abgerufen werden.

Druck: jva druck+medien, Geldern
www.jva-druckmedien.de

ISSN: 1864-5291
Düsseldorf 2009

Gedruckt auf chlorfrei gebleichtem Recyclingpapier

Bettina Sokol (Hrsg.)

GPS, Internet & Video
Datenschutz am Arbeitsplatz

Düsseldorf 2009

Vorwort

Am 29. Oktober 2008 haben das Institut für Informations-, Telekommunikations- und Medienrecht der Westfälischen Wilhelms-Universität Münster und ich als Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen unser 12. gemeinsames Symposium durchgeführt. Zum Thema "GPS, Internet & Video – Datenschutz am Arbeitsplatz" haben wir gefragt, welche Beschäftigtendaten ein Unternehmen erheben darf, an wen die Daten weitergegeben werden dürfen und ob ein Beschäftigtendatenschutzgesetz erforderlich ist. Die auf dem Symposium gehaltenen Vorträge sind in dem vorliegenden Band dokumentiert. Den Vortragenden ebenso wie allen anderen Personen, die am erfolgreichen Tagungsverlauf und am Erstellen dieser Dokumentation mitgewirkt haben, danke ich ganz herzlich.

Düsseldorf 2009 *Bettina Sokol*

Inhaltsverzeichnis

Eröffnung

Bettina Sokol

Einen wunderschönen guten Tag, meine sehr geehrten Damen und Herren! Ich freue mich, Sie heute zu unserem Symposium "GPS, Internet & Video – Datenschutz am Arbeitsplatz" begrüßen zu dürfen. In diesem Jahr war das Interesse am Thema unseres Symposiums so groß wie noch nie. Darüber bin ich natürlich froh, weil wir ein wichtiges Anliegen aufgreifen. Leider aber muss ich Sie auch um Verständnis bitten, dass der Raum heute ein wenig eng bestuhlt ist. Wir haben versucht, möglichst vielen Interessierten die Teilnahme zu ermöglichen. Dennoch mussten wir einige Absagen erteilen. Für diejenigen, die heute nicht selbst die Gelegenheit haben, bei uns zu sein, hoffe ich, dass wir die Vorträge dieses Tages möglichst bald veröffentlichen können.

Meine Damen und Herren, gerade in diesem Jahr haben die Medien immer wieder Fälle aufgedeckt und aufgegriffen, in denen die Datenschutzrechte von Arbeitnehmerinnen und Arbeitnehmern teilweise eklatant verletzt wurden. Es ist zu befürchten, dass dies nur die Spitze des Eisbergs ist. Die Fälle haben einer breiten Öffentlichkeit vor Augen geführt, welche unzulässigen Methoden von Unternehmen mitunter zur Überwachung ihres Personals eingesetzt werden.

Aber es gibt nichts Negatives, das nicht doch auch für etwas gut wäre: Viele sind durch die Ereignisse darauf aufmerksam geworden, dass die Persönlichkeitsrechte im Arbeitsverhältnis möglicherweise mit den bestehenden Regelungen und Kontrollmechanismen nicht ausreichend geschützt sind. Diese Aufmerksamkeit möchten wir für unsere heutige Diskussion nutzen.

Sie haben vielleicht der Presse entnommen, dass wir vom Datenschutz Nordrhein-Westfalen im August und September gegen ein Unternehmen und eine Unternehmensgruppe Bußgelder in nicht unbeträchtlicher Höhe wegen unzulässiger Videoüberwachung und Bespitzelung von Beschäftigten verhängt haben. An diesen Fällen war besonders erschreckend, wie lax dort mit den Persönlichkeitsrechten der eigenen Mitarbeiterinnen und Mitarbeiter umgegangen wurde, wie gering das Datenschutzbewusstsein ausgeprägt war und wie mangelhaft die Kenntnis der Rechtslage war. Von vertrauensvoller Zusammenarbeit, wie sie ein gut geführtes Unternehmen kennzeichnet, fand sich keine Spur. Wenn die Beschäftigten sogar mit Kameras in Umkleideräumen und Kantinen beobachtet werden, ist das kein Kavaliersdelikt. Hier wurde nicht bloß eine falsche Gewichtung zwischen im Einzelfall möglicherweise berechtigten Kontrollinteressen eines Unternehmens und den Interessen der Beschäftigten an der Wahrung ihrer Privatsphäre vorgenommen, sondern die Interessen der Beschäftigten wurden komplett missachtet. Datenschutz am Arbeitsplatz ist also ein ganz aktuelles und ganz wichtiges Thema.

Im Arbeitsverhältnis ist der Datenschutz als Schutz der informationellen Selbstbestimmung deswegen oft so schwer zu gewährleisten, weil die Beschäftigten in einem speziellen Rechtsverhältnis zu Arbeitgeberinnen und Arbeitgebern stehen: Regelmäßig besteht ein Machtgefälle zulasten der Beschäftigten. Die meisten Beschäftigten sind auf das Einkommen angewiesen und möchten ihren Arbeitsplatz nicht verlieren. Sie können unter Druck gesetzt werden oder fühlen sich aus Angst um den Arbeitsplatz unter Druck gesetzt und wehren sich deswegen nicht gegen Verletzungen ihrer Datenschutzrechte. Sie verdienen deshalb besonderen Schutz.

Außerdem wird die Kontrolltechnik mit dem technischen Fortschritt immer leistungsfähiger und damit gefährlicher für die Persönlichkeitsrechte. Es stehen immer mehr, bessere und billigere Mittel zur Verfügung, um Kontrolle auszuüben: E-Mails lesen, Computer- und Internetnutzung kontrollieren, beim Telefonieren zuhören, Persönlichkeitsprofile aus leistungsfähigen Personalinformationssystemen erstellen, GPS-Sender oder Videokameras installieren, biometrische Daten verwenden, Gentests nutzen… Die Aufzählung ließe sich noch lange fortführen.

Unter diesen Voraussetzungen kommt es auf den richtigen Ausgleich von Rechten und Interessen an. Es bedarf klarer Konturen für die zulässige Verarbeitung von Informationen über Beschäftigte

und es bedarf effektiver Kontrollen, ob diese Konturen eingehalten sind. Beim Datenschutz am Arbeitsplatz helfen die wenigen bestehenden gesetzlichen Regelungen oft nicht recht weiter. Häufig sind wir allein auf die arbeitsgerichtliche Rechtsprechung angewiesen, die allerdings in vielen Fällen sehr zu begrüßende Problemlösungen gefunden hat. Tarifvertragliche Regelungen oder Betriebsvereinbarungen sollen Regelungslücken schließen. Nicht immer ist das Ergebnis einer rechtlichen Bewertung vorhersehbar. Oft wissen weder Beschäftigte noch Arbeitgeberinnen und Arbeitgeber sicher und genau, was "ihre Rechte" sind. Es fehlt die Rechtsklarheit und es fehlt die Transparenz.

Rechtsklarheit und Transparenz sind entscheidende Anforderungen an den rechtlichen Rahmen für den Datenschutz am Arbeitsplatz. Schon lange fordern deshalb sowohl die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie viele weitere Datenschützerinnen und Datenschützer als auch die Gewerkschaften ein eigenständiges Beschäftigtendatenschutzgesetz, das die Rechte der Beschäftigten klar formuliert.

Heute wollen wir uns dem Datenschutz am Arbeitsplatz aus ganz unterschiedlichen Positionen und Perspektiven nähern. Zunächst einmal freue ich mich, dass der Minister für Arbeit, Gesundheit und Soziales des Landes Nordrhein-Westfalen Karl-Josef Laumann unsere Diskussion unterstützt. Leider kann er heute nicht persönlich hier sein, wünscht unserer Veranstaltung aber einen erfolgreichen Verlauf. Sein Grußwort finden Sie in der Tagungsmappe.

Zu Beginn werden wir uns in einer Bestandsaufnahme anschauen, wie das geltende Recht und die Rechtsprechung den Beschäftigtendatenschutz heute bestimmen. Danach werden wir unterschiedliche Antworten auf die Frage hören, ob wir eine gesetzliche Regelung des Beschäftigtendatenschutzes brauchen und wie ein solches Gesetz denn möglicherweise aussehen könnte, welche Sachverhalte welcher Regelung bedürften und wie der schwere Weg zu einem guten Gesetz zu bewältigen wäre.

Im dritten Teil unseres Programms werden wir uns dem Datenschutz in der Praxis konkreter zuwenden. Wir werden erfahren, welche Fragen sich den betrieblichen Datenschutzbeauftragten vor Ort stellen. Und wir werden sehen, aus welcher Sicht Detektivinnen und Detektive das Thema betrachten.

Zum Abschluss des Tages diskutieren wir – hoffentlich unter Ihrer regen Beteiligung – gemeinsam mit allen Vortragenden, wie ein Gesetz zum Schutz der Persönlichkeitsrechte am Arbeitsplatz denn aussehen muss, damit es seinen Namen verdient.

Meine Damen und Herren, sicher werden auch wir heute nicht den Königsweg zum guten Datenschutz am Arbeitsplatz so deutlich auf die Landkarte zeichnen können, dass er schon morgen ohne Hindernisse zu begehen ist. Trotzdem ist das Thema wichtig genug für jeden weiteren Versuch. Ich hoffe, dass unsere Diskussionen heute ein kleiner Beitrag dazu sein werden. In diesem Sinne wünsche ich uns allen einen interessanten, erkenntnisreichen und optimistischen Tag.

Grußwort

Karl-Josef Laumann

Über die Einladung zum Symposium "GPS, Internet & Video – Datenschutz am Arbeitsplatz" und die damit verbundene Bitte, ein Grußwort zu sprechen, habe ich mich sehr gefreut. Bedauerlicherweise ist es mir aufgrund anderer längerfristiger Terminverpflichtungen nicht möglich, dieser Einladung Folge zu leisten. Gestatten Sie mir dennoch, Ihnen auf diesem Wege einige grundsätzliche Überlegungen zum Thema "Datenschutz am Arbeitsplatz" zu übermitteln:

Mit der ständig zunehmenden Digitalisierung unserer Lebensumwelt wachsen die Bedrohungen für die Privatsphäre der Bürgerinnen und Bürger durch die Wirtschaft, aber auch durch den Staat, stetig an. Deshalb ist die Schärfung des Datenschutzbewusstseins, aber auch eine funktionierende Datenschutzkontrolle wichtiger denn je.

Weil unser Alltag immer mehr von informationstechnischen Systemen regelrecht beherrscht wird und diese zunehmend zum Einsatz kommen, ist eine verstärkte Kontrolle zur Vermeidung von Missständen unbedingt erforderlich.

Ich begrüße daher die Durchführung dieser Informationsveranstaltung zum Thema "Datenschutz am Arbeitsplatz" durch die unabhängige Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen in Zusammenarbeit mit dem Institut für Informations-, Telekommunikations- und Medienrecht der Universität Münster sehr.

Eine Bestandaufnahme der derzeitigen Lage sowie die Entwicklung von Positionen und Perspektiven halte ich für wichtig.

Die in jüngster Zeit bekannt gewordenen Datenschutzverstöße namhafter deutscher Handelsunternehmen in grundgesetzlich geschützte Persönlichkeitsrechte ihrer Mitarbeiterinnen und Mitarbeiter sind von der Landesregierung mit Besorgnis zur Kenntnis genommen worden. Die Empörung der Öffentlichkeit über unzulässige Überwachungsmethoden, die selbst vor den intimsten Lebensbereichen der Beschäftigten nicht Halt machten, ist daher für mich verständlich.

Diese Vorgänge haben die zuständigen Datenschutzaufsichtsbehörden konsequent aufgeklärt und mit dem Erlass von Bußgeldbescheiden geahndet.

Dies zeigt: Arbeitnehmer sind nicht schutzlos, wenn es um die Verletzung ihrer Persönlichkeitsrechte durch Überwachung und Ausspähung am Arbeitsplatz geht. Sie werden vielmehr durch zahlreiche datenschutzrechtliche Bestimmungen zum Arbeitsverhältnis sowohl im Bundesdatenschutzgesetz als auch in Spezialgesetzen geschützt.

Die Notwendigkeit, dem technischen Fortschritt immer neue, entsprechend angepasste Datenschutzregelungen entgegenzusetzen, ist grundsätzlich anerkannt.

Ich halte es für wichtig, dass die bestehenden Vorschriften zum Arbeitnehmerdatenschutz konsequent eingehalten und überwacht werden, so dass eine echte Datenschutzkultur entstehen kann.

Das entschlossene Handeln der Datenschutzaufsichtsbehörden zum Beispiel im Fall Lidl trägt hoffentlich dazu bei, dass Arbeitnehmerinnen und Arbeitnehmer künftig besser vor Datenmissbrauch und Verletzung ihres Grundrechtes auf informationelle Selbstbestimmung geschützt werden.

Ich wünsche Ihrer Veranstaltung einen erfolgreichen Verlauf.

Beschäftigtendatenschutz heute

Geltendes Recht und Aussagen der Rechtsprechung

Peter Wedde

Arbeitnehmerdatenschutz hat im Jahr 2008 in der Öffentlichkeit und in der rechtspolitischen Diskussion eine intensive Beachtung gefunden. Der Grund hierfür war allerdings nicht die Einsicht in die Notwendigkeit, auf diesem lange vernachlässigten Feld etwas tun zu müssen. Ausgelöst wurde die Debatte vielmehr durch eine Reihe von Skandalen, die ihren Beginn im Frühjahr bei Lidl nahmen und die inzwischen auch vor so bekannten Firmen wie IKEA oder der Deutschen Telekom nicht halt gemacht haben. Fast schon verwunderlich ist aber, dass die Diskussion im Herbst dieses Jahres immer noch anhält und nicht schon längst von anderen Themen verdrängt worden ist. Das Interesse am Arbeitnehmerdatenschutz besteht ebenso fort wie die weit verbreitete Einsicht, dass gesetzliche Regelungen erforderlich sind. Vielleicht liegt dies daran, dass die zahlreichen Varianten der unzulässigen Verwendung personenbezogener Daten vielen Bürgern verdeutlicht haben, wie groß die Gefahren für Persönlichkeitsrechte inzwischen geworden sind.

Allerdings ist es bedauerlich, dass erst große Skandale notwendig waren, um das Thema in das Bewusstsein der Öffentlichkeit zu bringen. Die vielen kleinen Datenschutzskandale, die es schon in den Jahren vorher gegeben hat, wurden hingegen weder von der Öffentlichkeit noch von der Politik nachhaltig zur Kenntnis genommen. Dies mag darin begründet sein, dass die Namen der Firmen, in denen sich kleinere Verstöße zugetragen haben, im Regelfall nicht übermäßig bekannt sind. Auch die Zahl der betroffenen Beschäftigten hält sich dort in Grenzen. Dennoch sind diese "kleinen" Fälle optimal geeignet, ein kontrastreiches Bild von der aktuellen datenschutzrechtlichen Situation in der Arbeitswelt zu zeichnen.

Datenschutz in der Arbeitswelt – die Praxis

Ich möchte zunächst ein paar dieser wenig beachteten Beispiele vorstellen und beginne mit einem Fall, der schon fast ein Klassiker ist: In einem Betrieb erkrankte ein Mitarbeiter überraschend und schwer. Der Vorgesetzte stellte erschreckt fest, dass sich wichtige Daten ausschließlich auf der Festplatte des Arbeitsplatz-PCs des Beschäftigten befanden. Diese war zwar durch ein Standardpasswort gesichert. Dem mit der Beschaffung der Daten beauftragten DV-Mitarbeiter gelang es aber, dieses zu "knacken". Der Vorgesetzte identifizierte die benötigten Daten und überspielte sie auf einen anderen Rechner. Danach warf er noch einen Blick auf andere auf dem Arbeitsplatz-PC des erkrankten Mitarbeiters befindliche Daten: In einem als "privat" gekennzeichneten Ordner entdeckte er eine kleine Sammlung von Musik- und Videodateien. Da die private Nutzung dienstlicher Geräte im Betrieb ausdrücklich verboten war, nahm der Vorgesetzte dies zum Anlass für eine Abmahnung. Diese fand der Beschäftigte nach der Rückkehr in den Betrieb auf seinem Schreibtisch vor.

In einer anderen Variante dieses Falls wurde die Ehefrau eines im Krankenhaus liegenden Beschäftigten vom direkten Vorgesetzten angerufen und gebeten, das Passwort bei Ihrem Mann zu erfragen. Als dieser sich weigerte, es herauszugeben, drohte der Vorgesetzte der Frau mit der sofortigen Kündigung. Daraufhin teilte der Beschäftigte über seine Frau das Passwort mit. Bevor der Vorgesetzte allerdings auf den Account zugreifen konnte, wurde der von der Ehefrau informierte Betriebsrat tätig. Dieser informierte die Geschäftsleitung und forderte sie auf, Zugriffe auf den Account des erkrankten Mitarbeiters zu unterbinden. Besagte doch eine konzernweite Anweisung zur IT-Sicherheit, dass die Beschaffung und Weitergabe individueller Passworte unzulässig und mit Abmahnung oder in schweren Fällen auch mit Kündigung zu ahnden seien. Ein Zugriff auf die Daten fand nicht statt.

In beiden Fällen haben sich die Arbeitgeber keine tief greifenden Gedanken ob der Tatsache gemacht, dass es aus Gründen der Datensicherheit eigentlich ein Unding ist, wenn betriebliche Daten ausschließlich auf dem persönlichen Rechner eines Beschäftigten vorhanden sind und nicht zugleich auch auf einem zentralen Server. Die zwingenden Vorgaben zum technischen und organisatorischen Datenschutz, die in § 9 Bundesdatenschutzgesetz (BDSG) ihren Niederschlag gefunden haben, wurden in beiden Fällen nicht ausreichend berücksichtigt. Wären die in der Anlage zu § 9 Satz 1

BDSG festgeschriebenen Maßnahmen hinreichend umgesetzt worden, wäre eine Kopie der Daten auf einen anderen Rechner schon mit Blick auf die dort unter der Nr. 7 festgeschriebene Verfügbarkeitskontrolle erforderlich gewesen.

Neben den Daten in den persönlichen Dateien von Beschäftigten haben Arbeitgeber immer wieder ein großes Interesse daran zu wissen, welche Seiten von ihren Arbeitnehmern im Internet aufgerufen werden. Ist die private Nutzung verboten, sehen sie es teilweise als ihr gutes Recht an zu kontrollieren, was ihre Arbeitnehmer während der Arbeitszeit tun. Die hierfür notwendige Software steht zumeist in Form von Firewalls oder ähnlichen Programmen aus dem Bereich der Systemsicherung zur Verfügung. Ist dies nicht der Fall, lässt sie sich mit wenig Aufwand und für billiges Geld installieren.

In einem Fall hatte das festgestellte Internetverhalten eines Beschäftigten zur Folge, dass sein Chef ihn bei einer eigentlich anstehenden Beförderung überging. Als der Betroffene nach den Gründen fragte, verwies dieser den Arbeitnehmer darauf, dass er sich in einschlägigen Online-Jobbörsen intensiv nach anderen offenen Stellen umgesehen habe und dass damit der Abwanderungswille nicht zu übersehen sei.

In einem anderen Fall bemerkte ein Beschäftigter in seiner Abteilung einen massiven Stimmungsumschwung, nachdem er sich wegen eines arbeitsrechtlichen Problems sowohl auf der Internetseite einer Gewerkschaft als auch in einem speziellen Diskussionsforum informiert hatte. Hier stellte sich im Nachhinein ebenfalls heraus, dass der Arbeitgeber den Administrator gebeten hatte, die auf dem zentralen Internetserver vorhandenen Zugriffsprotokolle entsprechend auszuwerten.

In beiden Fällen wurden die Beschäftigten von den geplanten Kontrollen ebenso wenig vorab informiert wie die Betriebsräte. Als der Betriebsrat aus dem zweiten Beispiel sich darüber beschwerte, dass er seine Mitbestimmungsrechte nicht ausüben konnte, hielt ihm der Arbeitgeber entgegen, dass entsprechende Rechte nicht bestehen, weil es sich nur um technische Maßnahmen der Systemsicherung gehandelt habe.

Probleme gibt es in der betrieblichen Praxis auch immer wieder bezüglich des Umgangs mit E-Mails. So verlangte ein Vorgesetzter beispielsweise von seinen direkten Mitarbeitern, dass diese wäh-

rend ihres Urlaubs alle E-Mails an einen Kollegen ihrer Wahl oder an ihn selbst umleiten sollten. Da die Privatnutzung der E-Mail-Accounts in diesem Betrieb ausdrücklich erlaubt war, weigerte sich ein Beschäftigter bei Urlaubsantritt, den Abwesenheitsassistenten zu aktivieren. Daraufhin wies der Vorgesetzte einen Administrator an, die elektronische Umleitung auf seine E-Mail-Adresse einzurichten – natürlich ohne Information an den Betroffenen. Dieser sah sich nach der Rückkehr aus seinem Urlaub mit dem Hinweis des Vorgesetzten konfrontiert, dass die vielen privaten E-Mails ihn genervt hätten und dass er sie deshalb kurzerhand gelöscht habe.

Dieses Beispiel macht deutlich, wie gering manche Arbeitgeber den Wert von Persönlichkeitsrechten einschätzen. Dass es längst bewährte Konzepte für den datenschutz- und persönlichkeitsrechtskonformen Umgang mit E-Mails während des Urlaubs gibt, wird immer wieder ignoriert. Manche Arbeitnehmer denken in dieser Situation darüber nach, ob sie ihren Arbeitgebern die Nutzung ihres Namens als Teil einer "sprechenden" E-Mail-Anschrift nicht untersagen sollten. Nur so lässt sich sicherstellen, dass wirklich keine privaten E-Mails mehr ungewollt an den dienstlichen Account geschickt und dem Arbeitgeber bekannt werden können.

Ignoranz der gesetzlichen Situation ist auch ein gutes Stichwort für das nächste Beispiel. Es geht um die Kündigung eines Betriebsratsmitglieds. Diese wurde damit begründet, dass der Beschäftigte betriebliche E-Mail- und Internet-Systeme in ausschweifender Weise genutzt und hiermit das Maß der zugelassenen gelegentlichen Privatnutzung weit überschritten habe. Zum Beweis für den Umfang der Privatnutzung legte der Arbeitgeber im Kammertermin des vom Beschäftigten angestrengten Kündigungsschutztermins dem Arbeitsgericht drei dicke Aktenordner vor. Einer enthielt in chronologischer Reihenfolge alle privaten E-Mails der letzten drei Monate, ein weiterer alle dienstlichen und ein dritter alle persönlichen oder vertraulichen E-Mails mit dienstlichem Charakter. Der zuständige Systemadministrator hatte diese Unterlagen auf Anweisung eines Geschäftsführers ausgedruckt. Die anschließende Sichtung und Sortierung hatte dessen Assistentin vorgenommen. Die vorgelegten Aktenordner wurden allerdings aus dem Verfahren zurück gezogen, nachdem der Arbeitsrichter laut darüber nachgedacht hatte, dass das Ausdrucken und Sichten der privaten und persönlichen E-Mails möglicherweise Straftatbestände aus dem Bereich des Telekommunikationsrechts erfüllen könnte. Der Arbeitgeber nahm daraufhin die Kündigung zurück. Das betroffene Be-

triebsratsratsmitglied wurde bei der folgenden Neuwahl mit großer Mehrheit in seinem Amt bestätigt.

Der Umgang mit dienstlichen und privaten E-Mails im Betrieb verbindet sich mit einem anderen Problemfeld, das in der betrieblichen Praxis immer wieder für Schwierigkeiten sorgt: Dem Verbot der Privatnutzung dienstlicher E-Mail- und Internetsysteme. Dass dies ein arbeitsrechtliches Thema geworden ist, hängt herausragend mit dem Telekommunikationsrecht zusammen: Erlaubt ein Arbeitgeber die private Nutzung betrieblicher Systeme oder verbietet er diese nicht ausdrücklich, wird er gemäß § 3 Nr. 6 Telekommunikationsgesetz (TKG) beziehungsweise gemäß § 2 Abs. 1 Telemediengesetz als Diensteanbieter qualifiziert. Eine Konsequenz dieser Einordnung ist, dass es Arbeitgebern mit Blick auf das Fernmeldegeheimnis gemäß § 88 Abs. 3 TKG verwehrt ist, vom Inhalt der E-Mail-Kommunikation oder von den Zielseiten der Internetnutzung Kenntnis zu nehmen.

In der Praxis führt diese normative Situation dazu, dass auch Arbeitgeber, die eigentlich kein Problem damit haben, dass ihre Beschäftigten gelegentlich eine private E-Mail schreiben oder einen außerdienstlichen Blick in das Internet werfen, inzwischen die Privatnutzung vollständig verbieten. Dies ist für sich zwar noch nicht problematisch, weil Arbeitgeber natürlich das Recht haben, bestimmte Verhaltensweisen während der Arbeit zu verlangen beziehungsweise Verbote auszusprechen. Das Verbot der Privatnutzung führt jedoch in Einzelfällen dazu, dass Arbeitgeber davon ausgehen, dass sie im Ergebnis weitergehende Befugnisse bekommen. In einem großen Unternehmen vertrat der Arbeitgeber beispielsweise die Meinung, dass er nach dem Verbot der privaten Nutzung unbeschränkte Kontrollrechte bezüglich der E-Mail-Inhalte habe. Der Betriebsrat hielt ihm entgegen, dass es auch im dienstlichen Bereich persönliche E-Mails gibt, die sich dem Zugriff verschließen. Als Beispiele führte er die E-Mails an, die er selbst an Beschäftigte schreibt oder die er von diesen empfängt. Darüber hinaus sah der Betriebsrat eine entsprechende Vertraulichkeit für die E-Mail-Kommunikation mit dem Betriebsarzt, der Gleichstellungsbeauftragten, dem Suchtbeauftragten, der Personalabteilung und so weiter. Der Arbeitgeber bestritt das Bestehen eines besonderen Schutzes und wollte unterschiedslos alle E-Mails kontrollieren und darüber hinaus auch langfristig archivieren. Dem Betriebsrat schlug er vor, dass dieser ja für die vertrauliche Kommunikation mit Belegschaftsmitgliedern auf Angebote privater E-Mail-Anbieter zurückgreifen könne, die dann unkontrolliert bleiben sollen.

Das Thema beschäftigt derzeit eine Einigungsstelle. Diese wird sich auf Bestreben des Betriebsrats auch mit der Frage beschäftigen müssen, wie die Situation zu bewerten ist, wenn Arbeitnehmer gegen ihren Willen private E-Mails erhalten. Diese Gefahr besteht, weil in dem Unternehmen grundsätzlich "sprechende E-Mail-Adressen" verwendet werden, die Vor- und Nachnamen enthalten.

Kommen wir zu einem anderen Feld, das in der betrieblichen Praxis immer öfter für Probleme sorgt und das sich mit dem Stichwort "Compliance als Grund für E-Mail-Kontrollen" treffend beschreiben lässt. Der Begriff "Compliance" steht in der betrieblichen Diskussion insbesondere für Prozesse, durch die die Einhaltung von Gesetzen und Richtlinien gewährleistet werden soll.

Vor einigen Monaten hatte ein von der US-amerikanischen Konzernmutter vorgegebenes Compliance-Verfahren bei der deutschen Unternehmenstochter nach dem Auftauchen von Bestechungsvorwürfen zur Folge, dass die E-Mails der hiesigen Mitarbeiter in einer Vielzahl von Fällen durch Mitarbeiter eines weltweit tätigen Anwaltsbüros ausgewertet wurden. Technisch war dies möglich, weil die Anwälte über Administratorenrechte für das betriebliche E-Mail-System in der Bundesrepublik Deutschland verfügten. Der Betriebsrat erfuhr von diesem Vorgehen nur zufällig und drohte dem Arbeitgeber mit der sofortigen Einleitung arbeitsrechtlicher Maßnahmen. Darauf wurden die weiteren Untersuchungen eingestellt.

Überhaupt scheint es so, dass gerade US-amerikanische Unternehmen mit dem deutschen und dem europäischen Datenschutzrecht immer wieder große Schwierigkeiten haben. Diese Feststellung überrascht vor dem Hintergrund der Erkenntnis, dass dort doch in der Regel hochkarätig besetzte Rechtsabteilungen bestehen. Diesen scheint es aber nicht zu gelingen, konzernweit dafür zu sorgen, dass unternehmens- oder grenzüberschreitende Datenübermittlungen nur dann erfolgen dürfen, wenn die einschlägigen datenschutzrechtlichen Minimalvoraussetzungen erfüllt sind. Konsequenz dieser Situation ist, dass die Datenübermittlung innerhalb von Konzernen und insbesondere die Übertragung von Arbeitnehmerdaten in die USA in einer nicht geringen Zahl von Fällen datenschutzrechtliche Minimalanforderungen nicht erfüllt. Beispielsweise erfolgt eine Datenübermittlung in die USA immer wieder ohne Abschluss sogenannter "EU-Standardverträge" oder außerhalb der Anwendbarkeit der alternativ möglichen "Safe Harbor Principles".

Und sind die datenschutzrechtlichen Mindestvoraussetzungen erfüllt, halten Konzerne den Abschluss weiterer Vereinbarungen, die etwa den Regelungsgehalt von § 11 BDSG entsprechend abbilden oder die eine Abwägung der berechtigten Interessen des Arbeitgebers mit den schützwürdigen Interessen der Beschäftigten vornehmen, für vollkommen entbehrlich. In der Konsequenz ist damit die Übermittlung von Daten in datenschutzrechtliche Drittstaaten ohne Datenschutzmindeststandard vertraglich oft weniger reguliert als bei Übermittlung innerhalb der Europäischen Union. Ein Zustand, der aus datenschutzrechtlicher Sicht weder legitim noch tolerabel ist.

Ich beende die Reihe von Beispielen an dieser Stelle. Die referierten Fälle verdeutlichen die brennenden Probleme, die es bezüglich der Umsetzung einschlägiger datenschutzrechtlicher Vorgaben in der Arbeitswelt gibt. Die Aufzählung soll nun nicht bedeuten, dass sich Unternehmen generell nicht datenschutzkonform verhalten. Den vielen Arbeitgebern, die die Datenschutzrechte ihrer Beschäftigten angemessen wahren und schützen, steht aber eine nicht kleine Zahl gegenüber, die dies vorsätzlich oder fahrlässig gerade nicht tut. Und die Zahl der Datenschutzverstöße könnte zunehmen, wenn sich herumspricht, welche neuen umfassenden Kontrollmöglichkeiten sich für Arbeitgeber aus neuen IT-Anwendungen ableiten lassen. Auch dies möchte ich an ein paar Beispielen illustrieren.

Neue Technologien und Arbeitnehmerdatenschutz

Der Einsatz neuer IT-basierender Anwendungen erfolgt in der Arbeitswelt in einem immer atemberaubenderen Tempo. Neue Endgeräte, neue Software und die hiermit verbundenen Systeme machen Beschäftigten das Leben in vielen Zusammenhängen leichter. Gleichzeitig schafft jede neue Technik neue technische Kontrollmöglichkeiten. Diese werden in einer zunehmenden Zahl von Fällen von Arbeitgebern genutzt.

Vielfach wird beim Einsatz neuer IT-Anwendungen indes übersehen, dass auch im arbeitsrechtlichen Bereich Grundrechte zu beachten sind wie insbesondere das durch Artikel 2 Absatz 1 Grundgesetz garantierte allgemeine Persönlichkeitsrecht. Hieraus leitet sich beispielsweise das Recht von Beschäftigten ab, während der Arbeitszeit gelegentlich über private Dinge reden zu dürfen, wenn dies die Arbeitsleistung nicht nennenswert beeinträchtigt. Gefällt einem Arbeitgeber dieses nicht, kann er ausufernde Privatgesprä-

che zwar verbieten, mit Blick auf das Persönlichkeitsrecht der Beschäftigten steht es ihm aber nicht zugleich frei, die Einhaltung seines Verbotes durch die heimliche oder offene Installation von Mikrophonen oder anderen Abhörmitteln zu kontrollieren. Derartige permanente Überwachungsmöglichkeiten würden ebenso wie der heimliche oder ausufernde Einsatz von Videokameras in Büroräumen unangemessen weit in Persönlichkeitsrechte eingreifen.

Problematisch ist in diesem Zusammenhang, dass technische Innovationen im IT-Bereich mit einem teilweise hohen Kontrollpotenzial ausgestattet sind. Wie hoch dieses ist, lässt sich ermessen, wenn man einen Blick auf neue Techniken wie beispielsweise Voice over IP (VoIP) wirft. Auf den ersten Blick stellt VoIP eine neue Variante des altbekannten Telefons dar. Von diesem unterscheidet es sich scheinbar nur dadurch, dass die Kommunikation nicht mehr über ein separates Telefonnetz erfolgt, sondern über das Internet. Zum altbekannten Telefonnetz gibt es jedoch bei VoIP einen grundlegenden Unterschied: Mit dieser Technik wird es beispielsweise in Betrieben möglich, relativ einfach eigene Vermittlungsrechner aufzubauen. Darüber hinaus ist es aus technischer Sicht relativ unproblematisch, Telefongespräche, die ja ohnehin digitalisiert werden, mitzuschneiden und im Nachhinein abzuhören. Auch wenn ein solches Vorgehen möglicherweise den Tatbestand der Verletzung der Vertraulichkeit des Wortes gemäß § 201 Abs. 1 Nr. 1 Strafgesetzbuch (StGB) erfüllt und damit strafbar ist, lässt sich nicht sicher ausschließen, dass einzelne Arbeitgeber die Möglichkeiten der Technik missbräuchlich ausnutzen.

Dass solche missbräuchlichen Nutzungen von verfügbarer Technik in der Praxis immer wieder erfolgen, lässt sich sehr gut am Beispiel der Videoüberwachung erkennen. Es kann insoweit vermutet werden, dass die Vorfälle im Frühjahr des Jahres bei Lidl keine Ausnahmen sind. Hierfür sprechen Beispiele aus der Vergangenheit. Bereits vor drei Jahren haben etwa Fernsehjournalisten anlässlich einer Sicherheitsmesse in Essen mit einem speziellen Scanner nach Signalen von WLAN-Kameras gesucht. Sie sahen nicht nur pikante Bilder aus privaten Schlafzimmern, die von aktiven Kameras stammten, die eigentlich zur Überwachung des Kinderbetts aufgestellt waren. Im arbeitsrechtlichen Bereich wurden sie in einer Bäckerei fündig, wo die Kamera heimlich in der Deckenbeleuchtung über der Kasse installiert war. Die von dem Fernsehteam mit Liveaufnahmen konfrontierte Mitarbeiterin war von der Tatsache, dass sie heimlich gefilmt wird, naturgemäß überrascht und entsetzt. Die Inhaberin der Bäckerei vertrat hingegen offensiv die Auf-

fassung, dass sie ja schließlich wissen wolle, was ihre Mitarbeiterin macht.

Da die notwendigen technischen Einrichtungen für derartige individuelle Videokontrollen schon für Preise ab 120,- € bequem über das Internet bestellt werden können, kann man nur darüber spekulieren, dass die Zahl derartiger Kontrollmaßnahmen schon heute hoch ist.

Sehr gut für Kontrollen von Beschäftigten eignet sich die RFID-Technik. Dieser Begriff steht für "Radio Frequency Identification". Praktisch handelt es sich bei der RFID-Technologie um miniaturisierte Sende- und Empfangseinrichtungen nebst kleinem Speicher, die beispielsweise in Preisschildern integriert sind. RFID-Chips finden sich aber auch in Betriebsausweisen.

Die Technik wird zudem schon seit einigen Jahren von Tierärzten genutzt, um Haustieren ein Identifikationsmerkmal unter die Haut einzupflanzen. Katzen und Hunde können sich ja nicht wehren. Hier und da sind aber auch Menschen bereit, dies mit sich machen zu lassen. So wird beispielsweise aus Spanien berichtet, dass RFID-Chips unter der Haut von Gästen in Clubs und Diskotheken zu Abrechnungszwecken eingesetzt werden. In Mexico City sollen inzwischen mehr als 5.000 Bürger durch RFID-Chips unter der Haut dafür sorgen, dass sie nach einer Entführung besser geortet werden können. Es stellt sich allerdings die Frage, ob Entführer nicht selbst mit entsprechenden Empfangsgeräten das Vorhandensein dieser kleinen Senderanlage identifizieren können. Bleibt zu hoffen, dass die Entfernung für Entführungsopfer halbwegs schmerzfrei verläuft.

Kommen wir zurück zu den üblichen Anwendungen der RFID-Technologie im Arbeitsleben. Dass diese sich in Werksausweisen verbreiten, wurde ja bereits angesprochen. Durch die Anbringung entsprechender Sende- und Empfangsanlagen ist es in Betriebsgebäuden möglich, ohne großen Aufwand festzustellen, wo sich Mitarbeiter gerade befinden. In bestimmten Produktionsbereichen mag eine solche Ortbarkeit aus Sicherheitsgründen sinnvoll sein. In "normalen" Bürogebäuden stellt sie eine unzulässige Verhaltens- und Leistungskontrolle dar. Insbesondere für Betriebs- und Personalräte tut sich hier ein neues Regelungsfeld auf.

Problematisch wird die RFID-Technologie, wenn die entsprechenden Empfangseinrichtungen nicht nur den Sender im Firmenaus-

weis empfangen können, sondern auch die Signale von anderen Gegenständen mit RFID-Chips, die sich etwa in einer Handtasche oder einer Jacke befinden. Technisch wäre es beispielsweise möglich, dass festgestellt werden kann, ob Arbeitnehmer Zigaretten, kleine Flaschen mit alkoholischen Getränken oder Medikamente bei sich haben. Da die nächste Generation der RFID-Chips sich in Kleidungsstücken wiederfinden könnte, könnte ein Arbeitgeber anhand der Marken erkennen, was seinen Beschäftigten ihr gutes Aussehen wert ist.

Intensive Überwachungsmöglichkeiten bieten auch moderne Mobiltelefone und Bordcomputer in Autos. Insbesondere in fest eingebauten GPS-Navigationsgeräten werden hier in vielen Fällen mehr Informationen dauerhaft gespeichert, als Arbeitnehmern lieb sein kann. Hinzu kommen Betriebsdaten, die in den Bordcomputern von Autos gespeichert werden. Würden diese Informationen kombiniert, ließe sich beispielsweise im Nachhinein feststellen, wo sich Vertriebsmitarbeiter wann befunden haben. Diese Möglichkeiten sind vielen Beschäftigten, die entsprechende technische Einrichtungen schon in ihren Dienstwagen haben, nicht bekannt.

Die Entwicklung steht hier erst am Anfang. Derzeit arbeiten beispielsweise Anbieter von Navigationssystemen daran, entsprechende Möglichkeiten der Ortung unter dem Begriff des Flottenmanagements im Vertriebs- und Servicebereich aktiv zu vermarkten. Für betroffene Außendienstmitarbeiter wird Konsequenz dieser Entwicklung sein, dass ihr Arbeitgeber beispielsweise jederzeit im Nachhinein feststellen kann, wie lange sie gebraucht haben, um von einem Kunden zum nächsten zu kommen, und ob sie hierbei die optimale Route gewählt haben. Mit den kleinen Freiheiten im Außendienst wird es damit wohl schnell vorbei sein.

Eine weitere IT-Einrichtung, die Arbeitgebern völlig neue Kontrollmöglichkeiten einräumt, haben wir alle inzwischen in der Tasche. Die Rede ist von den Mobiltelefonen, die inzwischen flächendeckend verbreitet sind. Diese Geräte können inzwischen viel mehr als nur Telefongespräche ermöglichen. Derzeit nimmt insbesondere ihr Einsatz als Navigationsgerät intensiv zu. Die Technik, die dies ermöglicht, lässt sich auch einsetzen, um den Standort des Handys für Dritte kenntlich zu machen. Diese Möglichkeit wird beispielsweise als Mittel zum Auffinden von Freunden von Mobiltelefonanbietern aktiv beworben.

Neue Perspektiven könnte in diesem Bereich die neue herstellerunabhängige Handysoftware Android bieten, für die derzeit die ersten Geräte auf den Markt kommen. Dass diese Software vom Suchmaschinenanbieter Google aktiv mit entwickelt wurde, verdeutlicht den datenschutzrechtlichen Standard, der zu erwarten ist. Android macht es einfach möglich, Anwendungen frei zu programmieren. Wie weit dies gehen kann, wurde für die Beta-Version im Rahmen einer Diplomarbeit an der Fachhochschule Frankfurt geprüft. Der Diplomand kam dabei zu dem Ergebnis, dass die Software sich theoretisch optimal für die Kontrolle von Mitarbeitern umprogrammieren lässt. Insbesondere die Ortungsfunktion scheint hierfür wirkungsvoller zu sein als die der bisher am Markt befindlichen Geräte.

Eine individuelle Anpassung der Android-Software scheint gerade für Arbeitgeber nicht uninteressant zu sein. Hierfür spricht, dass der zitierte Diplomand schnell einen ersten Arbeitsvertrag bekam. Ihm wurde in einem Vertriebsunternehmen die Aufgabe zugewiesen, die Möglichkeiten für eine Programmierung zu prüfen, die ein Optimum an Kontrolle ermöglichen soll. Seien Sie also vorsichtig, wenn Ihr Arbeitgeber Ihnen ein neues, modernes Handy zur Verfügung stellt. Und auch über ein geschenktes Handy von Ihrem Ehe- oder Lebenspartner sollten Sie sich nur richtig freuen, wenn Sie sicher sein können, dass die Kontrollfunktion nicht vorab aktiviert wurde.

Arbeitnehmerdatenschutz nach geltendem Recht

Die zahlreichen datenschutzrechtlichen Skandale, die es in diesem Jahr in verschiedenen Betrieben und Unternehmen gegeben hat, haben das Eine deutlich gemacht: In der Bundesrepublik Deutschland fehlt nach wie vor eine einheitliche Datenschutzregelung, die den besonderen Gegebenheiten im Rahmen von Arbeitsverhältnissen gerecht wird. Das Fehlen eines Gesetzes zum Arbeitnehmer- oder Beschäftigtendatenschutz wird insbesondere von Gewerkschaften und Wissenschaftlern seit längerer Zeit bemängelt. Ernstzunehmende gesetzgeberische Aktivitäten sind jedoch nach wie vor nicht zu verzeichnen.

Damit bleibt zur juristischen Aufarbeitung von datenschutzrechtlichen Problemen im Arbeitsleben nur der Rückgriff auf allgemeine Rechtsregeln, wie sie insbesondere das BDSG zur Verfügung stellt. Für den Umgang mit personenbezogenen Daten im Arbeitsverhält-

nis ist § 4 Abs. 1 BDSG die zentrale Norm. Nach dieser Vorschrift ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies ausdrücklich erlaubt oder anordnet. Darüber hinaus ist die Verwendung von Daten im Arbeitsverhältnis zulässig, wenn Arbeitnehmer dieser im Rahmen einer Einwilligung zugestimmt haben. Bedeutsam ist allerdings, dass die nach § 4a Abs. 1 BDSG erforderliche Einwilligung freiwillig sein muss.

Aus diesen eindeutigen gesetzlichen Vorgaben leitet sich für die Zulässigkeit der Verwendung von Daten im Rahmen eines Arbeitsverhältnisses ein eng begrenzter Bereich ab. Soweit es sich um personenbezogene Daten handelt, die eindeutig zur Vertragsabwicklung benötigt werden, wie etwa Name, Anschrift oder Ausbildungsverlauf, darf der Arbeitgeber diese als Bestandteil der Vertragsbeziehung nach § 28 Abs. 1 Nr. 1 BDSG verarbeiten. Die Anwendung dieser datenschutzrechtlichen Vorgaben ist im Arbeitsverhältnis im Regelfall unproblematisch. Schwierigkeiten treten allerdings dann ein, wenn Arbeitgeber als Grundlage der Verarbeitung nicht den unmittelbaren Vertragszweck anführen, sondern auf die Notwendigkeit der Wahrung ihrer berechtigten Interessen hinweisen. Dies ist heute oft im Zusammenhang mit Compliance-Verfahren der Fall. Grundsätzlich ist die Erhebung, Speicherung oder Übermittlung personenbezogener Daten zur Wahrung berechtigter Interessen in diesem Rahmen zwar nach § 28 Abs. 1 Nr. 2 BDSG möglich. Allerdings darf diese aber nach dem klaren Wortlaut im zweiten Halbsatz von Absatz 1 Nr. 2 nur erfolgen, wenn kein Grund zu der Annahme besteht, dass schutzwürdige Interessen der Betroffenen am Ausschluss der Verarbeitung oder Nutzung überwiegen.

Gerade dieser zweite Halbsatz der Vorschrift wird von Arbeitgebern immer wieder übersehen. Er steht beispielsweise der Übermittlung von personenbezogenen Daten aus einem deutschen Konzernunternehmen an die amerikanische Konzernmutter im Regelfall selbst dann entgegen, wenn US-amerikanisches Recht entsprechende Übermittlungen fordert. Maßgeblich für die Bewertung der Zulässigkeit ist in derartigen Fällen allein das nationale Datenschutzrecht der Bundesrepublik Deutschland. Bei der vorzunehmenden Rechtsgüterabwägung ist davon auszugehen, dass schutzwürdige Interessen der Betroffenen immer überwiegen, wenn Daten an Stellen oder Länder übermittelt werden, in denen der Standard des nationalen beziehungsweise des europäischen Datenschutzrechts nicht garantiert werden kann.

Diese Bindung an nationale Rechtsstandards ist sinnvoll und üblich. Wer hieran Zweifel hat, möge sich nur einmal vorstellen, dass morgen beispielsweise russische Firmen Gaslieferungen an die Bundesrepublik Deutschland davon abhängig machen würden, dass dem KGB oder einer anderen staatlichen Stelle in Russland vorab die Mitarbeiterakten der Arbeitnehmer deutscher Energiekonzerne in elektronischer Form zur Prüfung übergeben werden. Ein solches Vorgehen würde in der Bundesrepublik Deutschland sicher einen parteiübergreifenden Sturm der Entrüstung auslösen. Nichts anderes muss aber gelten, wenn entsprechende Informationen von US-amerikanischen Konzernmüttern unter Berufung auf dortige Rechtsgrundsätze oder auf die Regeln des Sarbanes-Oxley Act (SOX) eingefordert werden. Dies hat das Bundesarbeitsgericht in einer Entscheidung vom 22.07.2008 im Ergebnis ebenso gesehen. Folgerichtig hat es dem Betriebsrat ein Mitbestimmungsrecht bezüglich Ethik-Richtlinien zugesprochen, die die deutsche Konzerntochter eines US-amerikanischen Unternehmens auf Weisung der Konzernzentrale einführen wollte.

Beruft sich ein Arbeitgeber, der Daten zu Kontrollzwecken auswerten will, auf § 28 Absatz 1 Satz 1 Nr. 1 und 2 BDSG, muss er das dort festgelegte Zweckbindungsgebot zur Kenntnis nehmen. In Absatz 1 Satz 2 der Vorschrift wird hierzu ausgeführt, dass die Zwecke, für die Daten verarbeitet und genutzt werden sollen, bereits bei der Erhebung konkret festzulegen sind. Zweckänderungen sind nur unter sehr engen normativen Voraussetzungen möglich. Die eindeutigen Vorgaben des BDSG stehen freien Auswertungen von personenbezogenen Daten mit dem Ziel der Verhaltens- und Leistungskontrolle ebenso entgegen wie die Einführung von Konzepten des Datamining oder Screening. Damit ist es im Regelfall beispielsweise unzulässig, dass Anwesenheitsdaten, die zu Abrechnungszwecken erfasst worden sind, im Nachhinein daraufhin ausgewertet werden, wie viele Krankheitstage pro Mitarbeiter vorliegen. Auch die Verwendung dieser Daten für Krankenrückkehrgespräche ist im Regelfall datenschutzrechtlich unzulässig.

In der arbeitsrechtlichen Praxis als problematisch stellt sich immer wieder der Umgang mit Einwilligungen der Betroffenen zu Datenverarbeitungen heraus, die durch einschlägige gesetzliche Vorgaben nicht legitimiert sind. Nach § 4a Abs. 1 Satz 1 BDSG sind Einwilligungen von Beschäftigten nur wirksam, wenn sie auf deren freier Entscheidung beruhen. Bezogen auf ein Arbeitsverhältnis bestehen am Vorliegen einer Freiwilligkeit grundlegende Zweifel. Ursache hierfür ist die im Arbeitsverhältnis immer bestehende Dispa-

rität zwischen Arbeitnehmern und Arbeitgebern. Insbesondere bei Vertragsabschluss wird ein Arbeitnehmer sich im Regelfall gar nicht weigern können, "freiwillig" in bestimmte Kontrollmaßnahmen einzuwilligen. Erteilt er eine Einwilligung unter Hinweis auf die Vorgaben in § 4a Abs. 1 BDSG nicht, führt dies in der Praxis nach kurzer Zeit zur Aufhebung des Beschäftigungsverhältnisses. Insoweit bestehen im Arbeitsverhältnis immer grundlegende Zweifel am Vorliegen der Freiwilligkeit. Diese Rechtsauffassung hat sich in einschlägiger Rechtsprechung indes noch nicht niedergeschlagen.

Begrenzt sind die Vorgaben, die das BDSG bezüglich der Videoüberwachung von Beschäftigten enthält. In § 6b BDSG finden sich nur Vorgaben, die sich auf öffentlich zugängliche Räume beziehen. Damit stehen gesetzliche Regelungen beispielsweise für Arbeitsplätze in Kaufhäusern zur Verfügung. Nicht gesetzlich geregelt ist hingegen der Einsatz von Kameras in nicht-öffentlichen Räumen wie beispielsweise in Produktionshallen oder in Bürogebäuden. Die damit bestehende Gesetzeslücke hat der Gesetzgeber bei Verabschiedung der derzeit geltenden Fassung des BDSG im Jahre 2001 durchaus gesehen. In den Gesetzesmaterialien wird darauf verwiesen, dass eine entsprechende Regelung für nicht-öffentliche Räume im Rahmen eines besonderen Gesetzes zum Arbeitnehmerdatenschutz erfolgen soll. Die Rechtsprechung hat die bestehende Regelungslücke inzwischen teilweise gefüllt. Insbesondere der erste Senat des Bundesarbeitsgerichts hat in Entscheidungen aus den Jahren 2004 und 2008 ausgeführt, dass die Videoüberwachung von Arbeitnehmern ausnahmsweise nur dann zulässig sein kann, wenn im Rahmen einer Verhältnismäßigkeitsprüfung die Interessen des Arbeitgebers überwiegen. Dies kann beispielsweise im Wertbriefbereich eines Postverteilzentrums der Fall sein. Ausgeschlossen sind nach der Rechtsprechung Totalkontrollen, die Arbeitnehmern keinen kontrollfreien Raum lassen.

Weitere normative Vorgaben mit Auswirkungen auf den arbeitsrechtlichen Bereich lassen sich aus § 9 BDSG ableiten. Diese Vorschrift listet technische und organisatorische Maßnahmen auf, die die Ausführung des Gesetzes gewährleisten sollen. Aus dem Katalog der Schutzmaßnahmen lässt sich beispielsweise folgern, dass der Zugriff auf fremde Daten auch im Arbeitsverhältnis im Regelfall nicht zulässig ist. Entsprechendes gilt für die Weitergabe oder gemeinsame Nutzung von individuellen Passwörtern. Diese Regelung steht damit den in den Beispielsfällen angesprochenen "Zwangsabfragen" durch Vorgesetzte entgegen.

Aus der Vorgabe in Nr. 8 der Anlage zu § 9 Satz 1 BDSG lässt sich darüber hinaus ableiten, dass gemäß dem ursprünglichen Verarbeitungszweck eine Trennung der Daten erfolgen muss. Diese Vorgabe steht beispielsweise dem Verlangen einer Konzernspitze entgegen, personenbezogene Daten unternehmensübergreifend auswerten zu wollen. Datenverarbeitung darf vor diesem Hintergrund im Regelfall nur unternehmensbezogen, nicht aber konzernweit erfolgen.

Die Liste der datenschutzrechtlichen Problemfelder, die sich im Bereich eines Arbeitsverhältnisses ergeben, setzt sich im Bereich der Auftragsdatenverarbeitung fort. Sollen Daten unternehmensübergreifend erhoben, verarbeitet oder genutzt werden, muss ein Auftrag nach § 11 BDSG vorliegen. Dieser ist auch zwischen Konzernunternehmen zwingend erforderlich, da das BDSG insoweit keine Privilegierung für die konzernweite Datenverarbeitung enthält. In der Praxis wird diese zwingende gesetzliche Vorgabe gerade in multinationalen Konzernen oft nicht ausreichend berücksichtigt. Dies bestätigen Betriebsräte aus diesem Bereich, die der Einführung entsprechender Verarbeitungen beziehungsweise entsprechender Systeme wegen des Fehlens einer ausreichenden datenschutzrechtlichen Fundierung unter Hinweis auf ihr Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG) erfolgreich widersprochen haben.

Im Ausland und insbesondere außerhalb Europas trifft diese an sich eindeutige normative Situation im günstigsten Fall auf Unverständnis. Oft ist ausländischen Konzernspitzen oder dortigen Schwesterunternehmen nicht bewusst, dass die unternehmensübergreifende Übermittlung von personenbezogenen Daten ohne entsprechende vertragliche Fundierung einen Verstoß gegen das deutsche und das europäische Datenschutzrecht darstellt.

Fasst man die angesprochenen Regelungsspielräume und Normen des BDSG zusammen, wird deutlich, dass Arbeitnehmerdatenschutz nach diesem allgemeinen Gesetz nicht umfassend und eindeutig festgelegt wird. Das Gesetz trifft insbesondere dort auf seine Grenzen, wo es von gleichrangigen Vertragspartnern ausgeht, die es im Arbeitsverhältnis im Regelfall nicht gibt. Darüber hinaus stellt es sich problematisch dar, dass Betroffene aus dem BDSG zwar umfangreiche Auskunfts- und Löschungsrechte ableiten können. Im Arbeitsverhältnis müssen diese Ansprüche aber im Streitfall vor dem Arbeitsgericht durchgesetzt werden. Viele Arbeitnehmer verzichten hierauf aus Angst vor Karrierenachteilen oder Ar-

beitsplatzverlust. Ingesamt besteht damit auf der normativen Ebene eine unbefriedigende Situation.

Wo die gesetzlichen Möglichkeiten enden, beginnt die Rechtsprechung

In der Rechtsprechung des Bundesverfassungsgerichts und des Bundesarbeitsgerichts gibt es zu Themen wie "Zulässigkeit heimlicher Kontrolle", "Einsatz von Videokameras im Betrieb" und "Zulässigkeit von allgemeinen Verhaltens- und Leistungskontrollen mittels technischer Einrichtungen" zahlreiche einschlägige Entscheidungen.

Auch für den arbeitsrechtlichen Bereich von grundlegender Bedeutung ist die Entscheidung des Bundesverfassungsgerichts vom 15.12.1983 zur Rechtmäßigkeit der damals geplanten Volkszählung. In dieser Entscheidung hat das höchste deutsche Gericht ein neues "Grundrecht auf informationelle Selbstbestimmung" begründet, das das aktuelle BDSG entscheidend geprägt hat. Das Recht auf informationelle Selbstbestimmung sichert dem Einzelnen die Verfügungsgewalt über seine persönlichen Daten. In dieses Grundrecht darf nur nach Durchführung einer Verhältnismäßigkeitsprüfung eingegriffen werden, wenn höherrangige staatliche Interessen dies zwingend erfordern.

Bezieht man diese allgemeinen Verfassungsgrundsätze auf das Arbeitsrecht, wo das Recht auf informationelle Selbstbestimmung per Drittwirkung ebenfalls zur Anwendung kommt, wird deutlich, dass dem Umgang mit personenbezogenen Daten der Beschäftigten allgemeine Grenzen gesetzt sind. Arbeitgeber sind aus verfassungsrechtlichen Erwägungen gehindert, beliebige Bearbeitungsvorgänge mit personenbezogenen Daten durchzuführen.

Entsprechendes gilt für das durch das allgemeine Persönlichkeitsrecht ebenfalls geschützte "Recht am eigenen Bild". Auf dieses können Arbeitnehmer sich beispielsweise berufen, wenn ein Arbeitgeber die Fotos aller Mitarbeiter auf seiner Firmenwebsite präsentieren möchte. Einer besonderen Begründung bedarf die Wahrung des Rechts am eigenen Bild nicht. Höherrangige Interessen des Arbeitgebers, die eine Veröffentlichung zulässig machen könnten, können ausnahmsweise gegeben sein, wenn etwa Beschäftigte in einem Unternehmen herausragende Funktionen wahrnehmen, die einen klaren Bezug zur Öffentlichkeit haben.

Berücksichtigung finden muss im Arbeitsverhältnis schließlich auch das neue Grundrecht auf "Vertraulichkeit und Integrität informationstechnischer Systeme", das am 27.02.2008 bezogen auf ein neues Gesetz zur Onlineüberwachung in Nordrhein-Westfalen vom Bundesverfassungsgericht begründet wurde. Das Gericht hat hierzu ausgeführt, dass aus technischer Sicht in komplexen IT-Systemen neue und weitgehende Überwachungsmöglichkeiten bestehen. Es hat die Zulässigkeit der heimlichen Erfassung von in IT-Systemen vorhandenen Daten davon abhängig gemacht, dass eine massive Gefährdung für das Gemeinwesen oder für das Leben von Menschen besteht. Auch für diese Fälle hält das Bundesverfassungsgericht elektronische Ausforschung jedoch nur für zulässig, wenn vorher eine richterliche Anordnung erfolgt ist.

Überträgt man diese Vorgaben des Bundesverfassungsgerichts zum Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme auf der Basis der Drittwirkung von Grundrechten auf das arbeitsrechtliche Gebiet, lässt sich hieraus zunächst ein grundsätzliches Verbot heimlicher Überwachungsmaßnahmen im Betrieb ableiten, wenn hierzu die Informationen aus vernetzten IT-Systemen verwendet werden sollen. Auch die offene Ausforschung und Verwendung der in IT-Systemen vorhandenen Daten zur Verhaltens- und Leistungskontrolle kann unter Beachtung der Vorgaben des Bundesverfassungsgerichts unzulässig sein, wenn Beschäftigte im Arbeitsverhältnis darauf angewiesen sind, bestimmte IT-Anwendungen intensiv für ihre Arbeit zu nutzen. Das Grundrecht soll für diese Fälle garantieren, dass die zwingend anfallenden Daten nicht dazu verwendet werden dürfen, umfassende Persönlichkeitsprofile zu erstellen.

Die Rechtsprechung des Bundesarbeitsgerichts hat sich der vom Bundesverfassungsgericht verfolgten Linie, die heimliche und verdeckte Überwachungsmaßnahmen für unzulässig hält, in einer Reihe von Entscheidungen angeschlossen. Besonders deutlich wird dies bei der Bewertung von Fällen, in denen Arbeitgeber (oder auch Arbeitnehmer) Telefongespräche heimlich aufgezeichnet haben. Hierzu hat das Bundesarbeitsgericht regelmäßig ein Beweisverwertungsverbot angenommen. Die Nutzung der heimlich gewonnenen Informationen für Kündigungen oder Forderungen ist somit nicht möglich. Entsprechendes gilt für den Bereich heimlicher oder umfassender Videoüberwachung. Das Bundesverfassungsgericht hat in einer der schon angesprochenen Entscheidungen aus dem Jahre 2004 diesbezüglich ausdrücklich festgestellt, dass heimliche oder dauerhafte Kontrollen tief in das Persönlichkeitsrecht

von Beschäftigten eingreifen. Heimliche Kontrollen hält auch der 1. Senat des Bundesarbeitsgerichts in Entscheidungen vom 29.06.2004 und vom 14.12.2004 für unzulässig. Der 2. Senat dieses Gerichts hat sie in einer Entscheidung vom 27.03.2003 ausdrücklich für den Fall zugelassen, dass nur so ein Diebstahlsverdacht des Arbeitgebers bestätigt werden kann. Allerdings bestehen für diese Fälle Mitbestimmungsrechte des Betriebsrats nach § 87 Abs. 1 Nr. 6 BetrVG.

Offene Kontrollen sind nach der angesprochenen Rechtsprechung des 1. Senats des Bundesarbeitsgerichts ausnahmsweise zulässig, wenn dem Arbeitgeber keine anderen Kontrollmöglichkeiten zur Verfügung stehen. Insoweit hat der 1. Senat die Zulässigkeit einer komplexen Videoanlage in einem Postverteilzentrum unter Hinweis darauf verneint, dass dem Arbeitgeber hier gegebenenfalls andere Kontrollmöglichkeiten, wie etwa die Einstellung zusätzlichen Personals, zur Verfügung stehen würden. Durch die restriktive Zulassung soll vermieden werden, dass Arbeitnehmer während ihrer Tätigkeit einem umfassenden Überwachungsdruck ausgesetzt werden. Allerdings hat der 1. Senat des Bundesarbeitsgerichts diese restriktive Position in einer aktuelleren Entscheidung vom 26.08.2008 relativiert und dem Arbeitgeber zugestanden, dass er vorhandene Videokameras beim Vorliegen eines Diebstahlsverdachts bezogen auf konkret abgegrenzte Bereiche einschalten darf. Die Zulässigkeit einer Generalüberwachung hat der 1. Senat des Bundesarbeitsgerichts allerdings auch für diese Fälle verneint.

Fasst man die aktuelle Rechtsprechung des Bundesverfassungsgerichts und des Bundesarbeitsgerichts zusammen, leitet sich hieraus ein überschaubarer Rahmen für zulässige beziehungsweise unzulässige Überwachungsmaßnahmen ab. Sind Kontrollen mittels IT-Einrichtungen oder mit entsprechenden Endgeräten unumgänglich, weil es aus objektiver Sicht keine zumutbaren Überwachungsalternativen für den Arbeitgeber gibt, muss sichergestellt werden, dass Eingriffe in Persönlichkeitsrechte der Beschäftigten so gering wie möglich bleiben. Erfolgt beispielsweise in Bankfilialen aus Sicherheitsgründen eine permanente Kameraüberwachung, ist durch entsprechende organisatorische Vorkehrungen sicherzustellen, dass eine Auswertung nur durchgeführt wird, wenn es zu Straftaten gekommen ist. Die Praxis zeigt, dass vor dem Hintergrund solcher Regelungen Mitarbeiter in Bankfilialen ihrer Arbeit unbeschwert nachgehen, weil kein permanenter Überwachungsdruck besteht.

Entsprechendes gilt für die aus Sicht von Arbeitgebern notwendige Kontrolle von dienstlichen E-Mails mit geschäftlichem Inhalt, wenn hierbei sogleich sichergestellt wird, dass persönliche E-Mails, die ein Beschäftigter etwa an einen Betriebsrat schreibt, hiervon nicht erfasst werden. Das betriebliche Interesse bezüglich dienstlicher E-Mails ließe sich im Ergebnis einer Interessenabwägung dadurch befriedigen, dass diese in betriebs- oder abteilungsöffentlichen Ordnern gespeichert werden, während persönliche E-Mails in einem Bereich verbleiben, der nur den Beschäftigten selbst zugänglich ist. Hält ein Arbeitgeber weitergehende Maßnahmen zum Schutz von missbräuchlicher Nutzung für unumgänglich, können E-Mail- oder Internetsysteme softwaretechnisch so ausgestaltet werden, dass zunächst nur der Verstoß selber anzeigt wird und die notwendigen Daten gesichert werden. Der Zugriff auf die entsprechenden Daten und deren Auswertung muss dann erst möglich sein, wenn vorher Einvernehmen hierüber zwischen Betriebsrat und Arbeitgeber hergestellt wurde. Derartige Konzepte funktionieren inzwischen in einer Reihe von Unternehmen problemlos.

Fazit

Fasst man die geschilderten Beispiele für den Missbrauch von personenbezogenen Daten, die technischen Möglichkeiten, die gesetzlichen Grundlagen und die Positionen der Rechtsprechung zusammen, wird deutlich, dass sich ein Teil der aktuell erkennbaren Probleme juristisch unbedenklich lösen lässt. Es verbleibt aber ein nicht kleiner Graubereich, in dem es zu Gefährdungen der Rechte von Betroffenen kommt, weil personenbezogene Daten von Beschäftigten in datenschutzrechtlich unzulässiger Weise verarbeitet werden. Problematisch ist die "Außenwirkung" dieser Verstöße: Der eine oder andere Arbeitgeber fragt sich nämlich schon, warum ausgerechnet er sich rechtskonform verhalten soll, während andere Unternehmen dies nicht tun und sich durch die Einsparung von "Datenschutzkosten" einen unlauteren Wettbewerbsvorteil verschaffen. Dies alles stellt die Einhaltung des Datenschutzes im Arbeitsleben auf eine harte Probe.

Hinzu kommt, dass auch der Staat derzeit seiner Vorbildfunktion bezüglich der Wahrung von Persönlichkeitsrechten mittels restriktiver Datenschutzregeln nur noch begrenzt gerecht wird. Dies macht die lange Reihe von Kontrollmaßnahmen deutlich, die seit dem 11.09.2001 unter der Überschrift der Terrorismusbekämpfung eingeführt wurden und die inzwischen zu einem kaum noch über-

schaubaren Anschwellen staatlicher Kontrollmöglichkeiten geführt haben. Das fatale an diesen gesetzlichen Vorgaben ist zudem, dass sie teilweise auch Arbeitgeber zwingen, bestimmte zusätzliche Kontrollen durchzuführen, ohne dass zugleich staatlicherseits adäquate Datenschutzmaßnahmen verordnet wurden. Insbesondere die zuständigen Datenschutzaufsichtsbehörden wurden nämlich nicht angemessen ausgestattet.

Auch die gesetzlichen Grundlagen, die Bürgern Rechte gegen eine ausufernde Überwachung durch den Staat einräumen, können mit den ausufernden staatlichen Überwachungsbefugnissen längst nicht mehr mithalten. So ist es heutzutage für Finanzbeamte leichter denn je, auf die Kontodaten von Steuerschuldnern zuzugreifen, wenn es auch nur einen vagen Missbrauchsverdacht gibt. Den Bürgern wurde aber nicht gleichzeitig die Möglichkeit eingeräumt, effektiv überprüfen zu können, ob ein solches Handeln noch im Bereich pflichtgemäßen Ermessens der Steuerverwaltung steht.

In der Praxis zeigt sich immer wieder, dass gerade staatliche Stellen einschlägige Datenschutznormen eher weit interpretieren. So wird beispielsweise berichtet, dass das Einwohnermeldeamt einer großen deutschen Stadt auf eine elektronische Anfrage aus einem wissenschaftlichen Forschungsprojekt ohne nähere Prüfung umfassende Dateien mit Namen und aktuellen Anschriften verschickt hat. Glücklicherweise handelte es sich in diesem Fall tatsächlich um ein seriöses Forschungsprojekt und nicht um einen getarnten Datenhändler.

Kommen wir zurück zu den bekannt gewordenen Fällen von Datenmissbrauch. Hier hat sich in den letzten Monaten gezeigt, dass die datenschutzrechtlichen Sanktionsmöglichkeiten im Fall von Gesetzesverstößen ein relativ stumpfes Schwert sind. So fällt doch die Gesamtsumme der Bußgelder, zu der Lidl verurteilt wurde und die dem Vernehmen nach im einstelligen Millionenbereich lag, vergleichsweise bescheiden aus gegenüber den Kosten, die das Unternehmen allein für die folgende bundesweite Anzeigenkampagne zur Hebung des Images gezahlt hat. Dass hier einmal große Namen im Zusammenhang mit Datenschutzverstößen gebracht wurden, mag für die Debatte um den Arbeitnehmer- und Beschäftigtendatenschutz und eine gesetzliche Regelung sinnvoll sein. Dies ändert aber nichts daran, dass nach wie vor Arbeitnehmer hilflos vor Eingriffen in ihre Persönlichkeitsrechte stehen, wie etwa die Mitarbeiterin, die am Montag nebenbei von ihrem Vorgesetzten erfuhr, dass dieser über ein Administratorenkennwort für ihren

Rechner verfügte. Dies hatte er sich besorgt, um am Wochenende auf Dateien der Mitarbeiterin zugreifen zu können, wenn diese nicht im Büro ist.

Ob strengere gesetzliche Regeln und höhere Strafen alle Fälle des missbräuchlichen Umgangs mit Arbeitnehmerdaten verhindern können, kann man bezweifeln. Ein klares Bekenntnis des Staates dazu, dass es für den Umgang mit Arbeitnehmerdaten durch Arbeitgeber besondere Sorgfaltspflichten gibt, könnte jedoch ein klares Signal setzen. Wenn der auf die Umgehung von gesetzlichen Schutzvorschriften zielende Umgang mit personenbezogenen Daten nicht mehr als Kavaliersdelikt, sondern als Straftat gebrandmarkt würde, wäre dies für die meisten Arbeitgeber ein klares Signal, in Zukunft anders mit personenbezogenen Daten umgehen zu müssen. Allein ein solcher Gesinnungswechsel könnte zu einer Verbesserung der Situation der Beschäftigten führen. Gefordert bleibt im Ergebnis also der Gesetzgeber, der zu einer Klärung der Situation durch Verabschiedung eines Gesetzes zum Arbeitnehmer- und Beschäftigtendatenschutz beitragen könnte. Für die laufende Legislaturperiode ist dieses allerdings kaum noch zu erwarten. Damit bleibt wieder einmal die Hoffnung auf eine nächste Bundesregierung, die dieses Thema nicht nur in großen Lettern in ihren Koalitionsvertrag aufnimmt sondern auch schnell ein entsprechendes Gesetz verabschiedet.

Beschäftigtendatenschutzgesetz

Praktische Hilfe oder unnötige Zwangsjacke für Unternehmen?

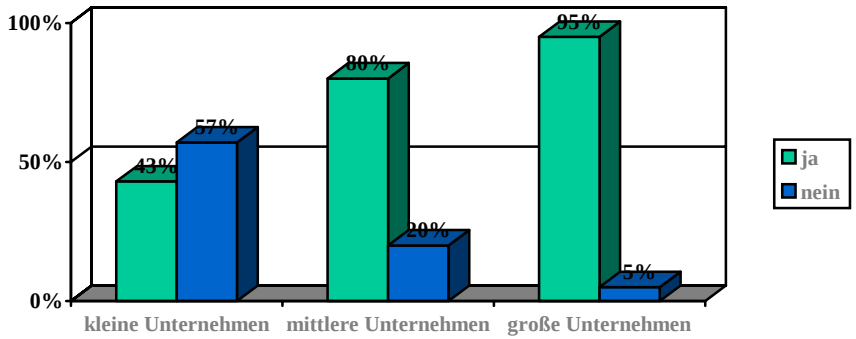
Thomas Prinz

Das Thema Datenschutz ist ein alltäglich präsentes Thema in den Unternehmen. Um von vornherein den Eindruck zu vermeiden, dass hier bei den Unternehmen ein genereller Nachholbedarf besteht, möchte ich Ihnen gern ein paar Zahlen vorstellen, die wir schon mit einer Umfrage im Jahre 2002 bei 400 Unternehmen mit Mitarbeiterzahlen von 6 bis 400.000 erhoben haben. Bei diesen Zahlen sind mit

- kleinen Unternehmen Unternehmen mit bis zu 50 Arbeitnehmern,
- mittleren und größeren Unternehmen Unternehmen mit über 50 und unter 1.000 Arbeitnehmern und mit
- großen Unternehmen Unternehmen mit über 1.000 Arbeitnehmern gemeint.

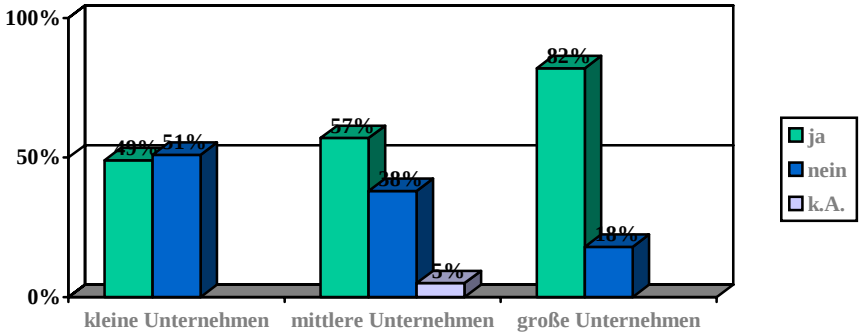
Von diesen befragten Unternehmen hatten 43 Prozent der kleinen, 80 Prozent der mittleren und 95 Prozent der großen Unternehmen einen internen oder externen Datenschutzbeauftragten.

Verfügt Ihr Unternehmen über einen Datenschutzbeauftragten?



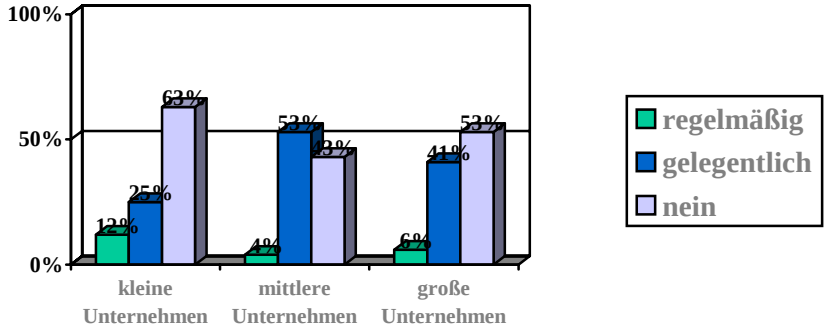
In 49 Prozent der kleinen, 57 Prozent der mittleren und 82 Prozent der großen Unternehmen werden auch Mitarbeiter, die nicht Datenschutzbeauftragte sind, speziell zum Thema Datenschutz geschult.

Werden Mitarbeiter, die nicht Datenschutzbeauftragte sind, im Datenschutz geschult?



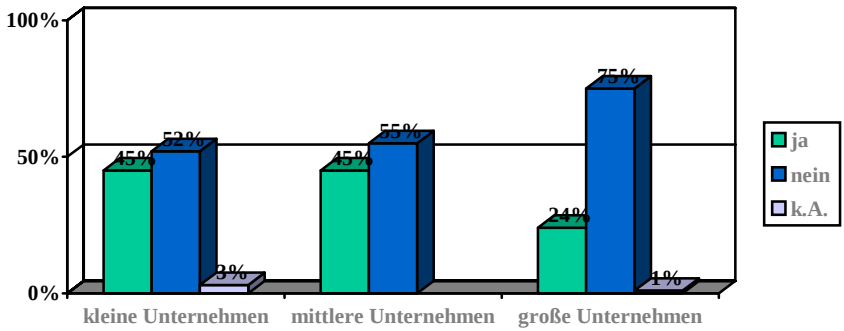
Allein 53 Prozent der mittleren Unternehmen nehmen von Zeit zu Zeit zu rechtlichen Fragen im Datenschutz externe Hilfe in Anspruch.

Nehmen Sie bei Ihrer Information über rechtliche Fragen im Datenschutz externe Hilfe in Anspruch?



45 Prozent der kleinen, 45 Prozent der mittleren und 24 Prozent der großen Unternehmen gestatteten zum damaligen Zeitpunkt ihren Arbeitnehmern die private E-Mail- und Internetnutzung.

Ist die private E-Mail- und Internet-Nutzung in Ihrem Unternehmen gestattet?



Diese Zahlen stammen – wie gesagt – aus dem Jahr 2002 und die Frequenz der Anfragen aus unseren Mitgliedsverbänden und Unternehmen zeigt, dass diese Zahlen seitdem tendenziell noch deutlich angestiegen sind.

Der Datenschutz ist in den Unternehmen ein Kernthema im Bereich der Unternehmenscompliance und der Compliance im Bereich des Arbeitsrechts. Das Thema Datenschutz im Arbeitsverhältnis im weitesten Sinne hat eine Vielzahl von Facetten für das Unternehmen: Dazu gehören

- Fragen der dienstlichen und privaten Nutzung von Internet und E-Mail,
- Fragen der Führung elektronischer Personalakten,
- Fragen der Datensicherheit und mögliche Sanktionen bei Missbrauch und Datenklau,
- Fragen der Mitbestimmung des Betriebsrats und der Nutzung von Internet und E-Mail durch den Betriebsrat,
- Fragen der Zulässigkeit von Gewerkschaftswerbung im Intranet und per E-Mail,
- Fragen der Erforderlichkeit und Zulässigkeit der Überwachung von Internet- und E-Mail-Nutzung und der Videoüberwachung (wobei dieses Thema in allererster Linie nur die Unternehmen beschäftigt, die in teilweise öffentlich zugänglichen Räumen für Sicherheit und zum Beispiel für Schutz vor Diebstahl zu sorgen haben),
- Fragen des Telekommunikationsgeheimnisses und zur Providereigenschaft des Arbeitgebers, wenn er einen Internetzugang zur Verfügung stellt.

Das Arbeitsverhältnis ist dabei allen allgemeinen Regelungen zum Datenschutz unterworfen, zu beachten sind insbesondere die Vorschriften des Bundesdatenschutzgesetzes, des Telekommunikationsgesetzes, des Telemediengesetzes, die Vorschriften des Betriebsverfassungsgesetzes und des Post- und Fernmeldegeheimnisses aus Art. 10 GG. Hinzu kommt eine inzwischen umfangreiche Rechtsprechung.

Ich möchte aber auch einen Blick auf die Tatsache werfen, dass das Thema Datenschutz und sichere Anwendung moderner Informations- und Kommunikationsmittel im Unternehmen weit über das Thema Datenschutz im Rahmen des Arbeitsverhältnisses hinausgeht. Mit dem Thema Datenschutz und IT-Sicherheit sind zum Beispiel umfangreiche Fragen der Haftung der Unternehmensführung beziehungsweise des Unternehmensmanagements verbunden.

Die weit verzweigten rechtlichen Regelungen zum Datenschutz fordern eine umfangreiche IT-Sicherheit im Unternehmen. Sie fordern

außerdem ein sorgfältiges Risikomanagement. Ich will mit diesem kleinen Exkurs zeigen, dass das Unternehmen nicht nur im Bereich des Schutzes der Daten von Arbeitnehmern sondern auch darüber hinaus umfangreiche Verpflichtungen hat. Auch diese ergeben sich in erster Linie aus dem Bundesdatenschutzgesetz (BDSG) und dem Telekommunikationsgesetz (TKG). Darüber hinaus existiert eine Vielzahl allgemeiner zivilrechtlicher Verpflichtungen zum Beispiel aus Verträgen mit Kunden, aus Versicherungsverträgen und aus deliktischer Haftung gegenüber Dritten.

Weiterhin wurden durch das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) spezielle Risikomanagementpflichten insbesondere in das Aktiengesetz eingeführt. Hinzu kommen unterschiedlichste strafrechtliche Vorschriften. Bei Verstößen drohen dem Unternehmen und seinen Organen nicht nur Schadensersatzpflichten, Rechtsverluste und die persönliche Haftung, sondern vor allem auch ein Reputationsverlust sowie eine strafrechtliche Verantwortlichkeit.

Zunächst zu den datenschutzrechtlichen Pflichten im Hinblick auf die IT-Sicherheit: Das Unternehmen hat die Pflicht zur Sicherung personenbezogener Daten gemäß § 9 BDSG und § 87 TKG. Es muss angemessene technische und organisatorische Schutzmaßnahmen wie zum Beispiel Zugangs- und Zugriffskontrollen und Weitergabekontrollen sicherstellen. Insgesamt ist hierzu ein abgeschlossenes Datenschutz-Konzept erforderlich.

Bei schuldhaften Verstößen kann sich eine Schadensersatzpflicht zum Beispiel aus § 7 BDSG oder aus den §§ 3 und 4 Nr. 11 des Gesetzes gegen unlauteren Wettbewerb wegen eines Vorsprungs durch Rechtsbruch ergeben. Es können Unterlassungsansprüche Dritter entstehen und die Bußgeld- und Strafvorschriften der §§ 43 und 44 BDSG greifen.

Das Unternehmen haftet für die rechtswidrige Nutzung moderner Informations- und Telekommunikationseinrichtungen durch seine Mitarbeiter. Hier will ich nur einige prägnante Beispiele nennen:

Es kann sich um Urheberrechtsverletzungen handeln, zum Beispiel durch den Download geschützter Software und Daten. Hieraus können Schadensersatzansprüche und Unterlassungsansprüche auch gegen das Unternehmen folgen. Das Unternehmen muss ein besonderes Augenmerk darauf haben, dass seine Mitarbeiter nicht in strafrechtlich relevanter Weise tätig werden, zum Beispiel durch

das Ausspähen von Daten nach § 202a des Strafgesetzbuchs (StGB), durch Datenveränderungen nach § 303a StGB oder durch Computersabotage nach § 303b StGB. Die Haftung kann bei mangelnder Kontrolle beziehungsweise Verhinderung solcher Straftatbestände auf das Unternehmen beziehungsweise sein Management durchschlagen, zum Beispiel auf Grund von Spezialvorschriften wie zum Beispiel § 99 des Urhebergesetzes oder auf Grund der allgemeinen Grundsätze über Täterschaft und Teilnahme beziehungsweise Beihilfe im Strafrecht.

Darüber hinaus kann das Unternehmen sich weiteren zivilrechtlichen Ansprüchen ausgesetzt sehen. Eine Haftung gegenüber Dritten kann auch ohne Vertrag greifen, zum Beispiel aus § 823 des Bürgerlichen Gesetzbuchs bei Eigentumsschäden durch Datenverlust oder wegen der Störung des Gewerbebetriebs Dritter, zum Beispiel durch die Schädigung der Informations- und Kommunikationsinfrastruktur Dritter oder durch den Versand von Viren oder Spams durch unternehmenseigene Rechner. Bei einem Verschulden kommen auf das Unternehmen Schadensersatzansprüche zum Beispiel für Datenverlust und einen damit verbundenen Mehraufwand in Frage. Auch ohne Verschulden können Unterlassungsansprüche gegeben sein.

Spezielle Versicherungen können zwar die IT-Risiken des Unternehmens abdecken, aber auch die Versicherer knüpfen selbstverständlich den Schutz an die Beachtung der Obliegenheiten des Unternehmens und seiner Leitung. Bei einer Missachtung dieser Obliegenheiten droht eine Reduzierung oder ein Ausschluss des Versicherungsschutzes. Typische in Versicherungspolicen erwähnte Obliegenheiten sind

- die regelmäßige und sachgerechte Datensicherung,
- der Schutz des internen Netzes durch Firewalls,
- der Schutz interner Schnittstellen, Server und Arbeitsplätze durch Virenscanner,
- die regelmäßige Aktualisierung der Schutzsysteme, bei aktuellen Gefahren möglicherweise auch sehr kurzfristig und
- die Erstellung eines Notfallplans.

Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich, das in erster Linie für Aktiengesellschaften gilt, dessen Grundsätze aber auch für die GmbH sowie die GmbH & Co. KG anwendbar sind, regelt die persönliche Haftung von Unternehmensorganen bei Verstößen auch im Bereich der IT-Sicherheit. Diese

Haftung betrifft den Vorstand, den Aufsichtsrat und die Geschäftsführer. § 91 Abs. 2 des Aktiengesetzes lautet:

„Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden."

§ 93 Abs. 2 AktG regelt:

„Vorstandsmitglieder, die ihre Pflichten verletzen, sind der Gesellschaft zum Ersatz des daraus entstehenden Schadens als Gesamtschuldner verpflichtet. Ist es streitig, ob sie die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters angewandt haben, so trifft sie die Beweislast."

Diese Vorschriften erfordern ein effizientes Risikomanagement, dessen Inhalte zwar vom Gesetz nicht definiert werden, die aber zumindest ein System der Früherkennung, der Risikobewältigung und der Kontrollen enthalten sollten.

Zur Risikoprävention im Bereich der IT-Infrastruktur zählen zum Beispiel die Datensicherung, der Sabotageschutz und der Schutz vor Angriffen von außen. Außerdem muss ein effizienter Schutz vor missbräuchlicher Nutzung durch die Mitarbeiter des Unternehmens sichergestellt werden.

Die Haftung des technisch zuständigen Leiters, also zum Beispiel des EDV-Leiters oder des so genannten Administrators ergibt sich dabei nicht aus dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich. Seine persönliche Haftung ergibt sich aus dem Arbeitsvertrag oder aus strafrechtlichen Vorschriften. Der Pflichtenumfang dieses Administrators muss im Arbeitsvertrag klar niedergelegt sein um seine gesteigerte vertragliche Pflicht zur Wahrung von Sicherheitsinteressen zu definieren. Hierzu gehören die Grundsätze ordnungsgemäßer Datenverarbeitung, die Durchführung von Schutzmaßnahmen und die Aufklärungspflicht gegenüber der Geschäftsleitung.

Als Maßstab gelten die durchschnittlichen Kenntnisse eines Arbeitnehmers in vergleichbarer Position mit höheren Sorgfaltspflichten als Mitarbeiter tieferer Hierarchieebenen. Eine Pflichtverletzung des Arbeitsvertrages durch den EDV-Leiter führt zu einer Schadensersatzpflicht. Nach den Grundregeln der Rechtsprechung zur Arbeitnehmerhaftung trifft ihn allerdings bei nur leichter Fahrlässigkeit

keine Haftungspflicht. Bei mittlerer Fahrlässigkeit wird der Schaden geteilt und nur bei grober Fahrlässigkeit und Vorsatz haftet der EDV-Leiter in der Regel voll (anders nach der Rechtsprechung des Bundesarbeitsgerichts eventuell bei einem groben Missverhältnis zwischen Verdienst und Schaden). Die arbeitsrechtlichen Sanktionen sind die Abmahnung oder die Kündigung.

Die genannten Beschränkungen der Haftung des Arbeitnehmers, der für die Herstellung und Bewahrung der IT-Sicherheit zuständig ist, zeigt bereits das daraus folgende Dilemma der Unternehmensleitung. Im Zweifel muss die Unternehmensleitung für Mängel bei der IT-Sicherheit und die daraus resultierenden Folgen haften und hat daher ein besonderes Kontroll- und Überwachungsinteresse. Dem gesetzlichen Zwang zur Risikovermeidung zum Beispiel aus dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich und aufgrund der Außenhaftung des Unternehmens muss durch eine effektive Kontrolle Rechnung getragen werden. Dem stehen die rechtlichen Hürden des Persönlichkeitsrechts, der arbeitsrechtlichen Vorschriften und insbesondere des Datenschutzrechts und des Fernmeldegeheimnisses entgegen.

Das Unternehmen muss also innerhalb des Risikomanagements regelmäßig abwägen zwischen der Erforderlichkeit beziehungsweise Geeignetheit des Einsatzes von Mitteln zur Risikoabwehr und der Zulässigkeit ihres Einsatzes.

Typische technische Maßnahmen zur Risikoabwendung sind zum Beispiel Schutzmaßnahmen gegen Viren, Firewalls und komplexe Content-Filter. Hiermit verbunden ist immer zumindest die Möglichkeit der individuellen oder automatisierten Kenntnisverschaffung der Telekommunikationsvorgänge durch das Unternehmen. Die strafrechtlichen Folgen für den Arbeitgeber bei einer rechtswidrigen Überwachung ergeben sich zum Beispiel aus § 43 BDSG für den Fall einer unbefugten Datenverarbeitung, die mit einer Freiheitsstrafe von bis zu zwei Jahren sanktioniert wird. Eine Verantwortlichkeit kann sich auch aus § 206 StGB bei Verletzung des Fernmeldegeheimnisses ergeben – sanktioniert mit einer Freiheitsstrafe von bis zu fünf Jahren. Ein Verstoß gegen die Benachrichtigungspflicht aus § 44 Abs. 1 Nr. 3 i. V. m. § 33 BDSG ist mit einem Bußgeld von bis zu 25.000 Euro sanktioniert. Hinzu kommen Unterlassungsansprüche, Löschungsansprüche, Schadensersatz und möglicherweise Schmerzensgeld.

Betrachtet man diesen Komplex der Haftung und der Pflicht zur Risikovermeidung, so scheint – um den Titel meiner Ausführungen zu bemühen – die Zwangsjacke des Datenschutzes bereits eng angelegt. Betrachtet man alle Aspekte und Verästelungen rechtlicher Regelungen und der Rechtsprechung zur Nutzung moderner Kommunikationsmedien und -technik am Arbeitsplatz, so fühlt man sich an die Kompliziertheit des Steuerrechts erinnert.

Umso befremdlicher ist es daher, dass viele der Forderungen nach einem Arbeitnehmerdatenschutzgesetz implizieren, dass es im Bereich des Arbeitsverhältnisses größere Rechtslücken oder gar einen rechtsfreien Raum im Bereich des Datenschutzes und der Nutzung moderner Telekommunikationsmedien gibt. Das ist nicht der Fall. Und das belegen auch die immer wieder zitierten Missbrauchsfälle, in denen immer Rechtsverstöße gegen geltendes Recht vorlagen. Die Begründung für die Forderung nach einem Arbeitnehmerdatenschutzgesetz, es gebe zu wenig oder gar keine Regelungen, fällt daher komplett weg. Man kann sie schon fast als Schlag ins Gesicht der absoluten Mehrheit der Unternehmen verstehen, die höchst verantwortungsvoll mit dem Thema Datenschutz und Nutzung moderner Informations- und Kommunikationstechnologie umgehen.

Als Begründung könnte daher allenfalls noch herhalten eine Vereinfachungsabsicht beziehungsweise die Absicht, das Recht des Datenschutzes im Rahmen des Arbeitsverhältnisses handhabbarer und transparenter zu machen. Hier stößt man aber schnell auf dogmatische Grenzen, die bisher mit gutem Grund gezogen wurden. Ist es wirklich sinnvoll, für verschiedene Ausschnitte des Zivilrechts – für verschiedene Vertragsbeziehungen – jeweils spezielle beziehungsweise besondere Datenschutzvorschriften zu erlassen? Wäre es sinnvoll, ein separates Verbraucherdatenschutzgesetz zu erlassen, ein Mieterdatenschutzgesetz oder ein Arbeitgeberdatenschutzgesetz? Oder sind die Schutzbedürfnisse nicht grundsätzlich völlig gleich gelagert, so dass die gesetzlichen Regelungen für alle Adressaten passen müssen? Sollten nicht vielmehr die in den unterschiedlichsten Gesetzen untergebrachten Vorschriften zum Datenschutz in einem transparenten Regelwerk zusammengefasst werden?

Die Forderungen nach einem Arbeitnehmerdatenschutzgesetz sind außerdem sehr einseitig, weil dann, wenn man von einem besonderen Schutzbedürfnis über die geltende Gesetzeslage hinaus im Arbeitsverhältnis ausgehen würde, selbstverständlich auch die Da-

ten des Unternehmens, des Arbeitgebers eines solchen besonderen Schutzes bedürften. Ich will über die im Rahmen des Risikomanagements erwähnten Stichworte hinaus hierzu nur das Stichwort des Betriebsgeheimnisses ergänzen.

Es liegt auf der Hand, dass den Vorteilen der modernen Informations- und Kommunikationstechnologie auf Seiten des Unternehmens enorme Nachteile und Gefahren gegenüberstehen, die alltägliche Herausforderungen für die Unternehmen sind: Das reicht von der erwähnten Datenspionage über die Möglichkeit des Aufrufens strafrechtlich relevanter Internetseiten durch die Arbeitnehmer und der damit verbundenen Rufschädigung des Unternehmens bis hin zu Gefahren für betriebliche Abläufe durch Würmer, Trojaner, Viren und Spammails.

Würde man daher ernsthaft über Regelungen zum Datenschutz im Arbeitsverhältnis nachdenken, so hätte sicher auch das eine oder andere Unternehmen Wünsche an den Gesetzgeber, zum Beispiel zu den folgenden Stichworten:

- Transparente Regelungen des Datenaustauschs in den Geltungsbereichen verschiedener Rechtsordnungen,
- klare Regelungen der Vertraulichkeit von Daten des Unternehmens als Arbeitnehmerpflicht,
- klare Sanktionsregelungen beim Missbrauch von Internet und E-Mail,
- klare Regelungen zur Kontrolle von Internet- und E-Mail-Nutzung, möglicherweise kombiniert mit einem Verbot der privaten Nutzung mit Erlaubnisvorbehalt,

um nur einige wenige Punkte zu nennen.

Vorausgesetzt, dass solche Wünsche existieren, heißt das aber noch nicht zwangsläufig, dass entsprechende Regelungen auch zwingend erforderlich sind, um einen verantwortungsvollen Umgang mit moderner Informations- und Kommunikationstechnologie am Arbeitsplatz sowohl durch Arbeitnehmer als auch durch Arbeitgeber zu gewährleisten.

Hier muss man im Grunde einen ganz grundsätzlichen juristischen Streit entscheiden zwischen den Befürwortern allgemeingültiger Regelungen, die alle möglichen Sachverhalte regeln und dementsprechend auslegungsfähig sind, und den Befürwortern einer Viel-

zahl von Detailregelungen, die möglichst jeden einzelnen Sachverhalt regulieren.

Wie schon angedeutet: Die möglichen Missbrauchsfälle scheinen mir als Rechtfertigung für neue Regulierungen nicht geeignet. Es handelt sich bereits um Missbräuche beziehungsweise Verstöße gegen geltendes Recht, und wenn sie zum Anlass für neue Regulierungen genommen werden, leidet hierunter nur die Vielzahl der Rechtsanwender beziehungsweise Unternehmen, die sich rechtstreu verhält und verantwortungsvoll mit Datenschutzfragen umgeht.

Ganz unabhängig davon ist klar, dass das Thema Datenschutz eine Vielzahl rechtlicher und praktischer Herausforderungen für die Unternehmen und Betriebspartner bereithält, die die Unternehmen zwingen zu handeln und – möglicherweise mit dem Betriebsrat – und in Abstimmung mit dem Datenschutzbeauftragten betriebsindividuelle Lösungen zu treffen und Vereinbarungen zu schließen. Dass eine Nichtbefassung mit dem Thema seitens des Unternehmens fatal wäre, haben schon meine Ausführungen zum Risikomanagement gezeigt. Ich möchte aber auch noch das Beispiel einer fehlenden Regelung zur Internet- und E-Mail-Nutzung erwähnen.

Sobald der Arbeitnehmer private E-Mails schreiben darf, ist sein gesamter E-Mail-Account – sofern keine eindeutige Trennung von privater und dienstlicher E-Mail-Adresse vorgenommen wird – vor dem Kontrollzugriff des Arbeitgebers geschützt. Der Arbeitgeber hat also keine Möglichkeit der Kontrolle der dienstlichen E-Mails mehr. Praktische Folge: Wird der Arbeitnehmer plötzlich krank und sind bei ihm wichtige E-Mail-Eingänge, zum Beispiel von Kunden zu erwarten, kann der Arbeitgeber nicht einen Kollegen des Arbeitnehmers anweisen, dessen E-Mail-Eingang zu prüfen.

Es gibt zahlreiche weitere Themen im Zusammenhang mit der Nutzung von modernen Kommunikationsmedien, die eines verantwortungsvollen Umgangs bedürfen und immer wieder neue Herausforderungen für die Betriebspartner liefern. Dazu gehören zum Beispiel

- die Führung elektronischer Personalakten,
- die Aufbewahrung von Daten im Zusammenhang mit Bewerbungsverfahren und Einstellungen, zum Beispiel aufgrund der Vorschriften des allgemeinen Gleichbehandlungsgesetzes (AGG),

- die Nutzung des Internets durch den Betriebsrat und damit zusammenhängende Fragen einer eigenen Intranetseite oder Homepage,
- die Frage der Zulässigkeit von Gewerkschaftswerbung per E-Mail,

um nur einige wenige Beispiele zu nennen.

Die meisten Unternehmen haben daher Betriebsvereinbarungen geschlossen und Leitlinien zur Nutzung von Internet und E-Mail entwickelt, die an den konkreten Bedürfnissen und den konkreten Arten der Nutzung moderner Informations- und Kommunikationstechnologie im Unternehmen ausgerichtet sind. Diese Bedürfnisse sind je nach Branche und Unternehmen naturgemäß sehr unterschiedlich, so dass nur betriebs- beziehungsweise unternehmensindividuelle Lösungen sinnvoll sind.

Dieser Gestaltungsspielraum, der von der absoluten Mehrheit der Unternehmen und Betriebspartner verantwortungsvoll ausgefüllt wird, muss in jedem Fall erhalten bleiben. Ein separates Arbeitnehmerdatenschutzgesetz, das noch zu den geltenden Regelungen des Datenschutzes hinzutreten würde, lehnen wir deshalb ab. Es würde die Zwangsjacke des Datenschutzes nur noch enger schnüren und die weit verstreuten Regelungen zum Datenschutz noch unüberschaubarer machen.

Immer auf die Kleinen?

Beschäftigtendatenschutz gesetzlich verankern!

Mirjam Alex

Der Umgang mit Internet, E-Mail und Mobiltelefonen, Online-Banking und Internethandel ist in den letzten Jahren für die meisten zur Selbstverständlichkeit geworden. Bequem und schnell wird kommuniziert und gehandelt. Dabei fallen persönliche Daten an, die oft nur unzureichend gegen unrechtmäßige Nutzung und Weitergabe an Dritte gesichert sind.

Im Arbeitsverhältnis werden Chipkarten eingesetzt, die den Zugang der Beschäftigten aufzeichnen, bei der Verwendung von RFID-Funkchips können Tätigkeitsprofile erstellt werden und Handys ermöglichen über GPS jederzeit die Feststellung, wo sich Beschäftigte befinden. Leistungskontrollen sind über die Benutzerprofile am Computer auch ohne besondere Software möglich. Und nicht zuletzt werden unter dem Stichwort Terrorbekämpfung von staatlichen Stellen über den Arbeitgeber im Rahmen der Sicherheitsüberprüfung Daten zum Beispiel über religiöse Präferenzen oder ethnische Herkunft ermittelt und weitergegeben – sogar an ausländische Stellen und für Daten, die eigentlich dem Persönlichkeitsschutz unterliegen. Zusätzlich entstehen mit Vorhaben wie der elektronischen Gesundheitskarte und dem Verfahren des Elektronischen Einkommensnachweises (ELENA) riesige Datensätze, deren Verwendung zwar gesetzlich geregelt ist, die aber durchaus neue Begehrlichkeiten wecken können.

Durch all dies entstehen erhebliche Gefahren. So wurde von Seiten der Landesbeauftragten für den Datenschutz erhebliche verfassungsrechtliche Bedenken gegen das ELENA-Verfahren geäußert. Denn unter staatlicher Verantwortung und Verfügungsmacht würde

eine riesige Datensammlung entstehen. Die betroffenen Arbeitnehmer hätten keine Einflussmöglichkeiten. Diese riesige Datensammlung verstößt gegen das verfassungsrechtliche Verbot einer Datenspeicherung auf Vorrat. Sie wäre ein unverhältnismäßiger Eingriff in das Grundrecht auf informationelle Selbstbestimmung.

Im Übrigen hat sich gezeigt, dass die persönlichen Daten insbesondere von Beschäftigten aber auch im allgemeinen Geschäftsverkehr außerordentlich missbrauchsanfällig sind. Die Vorfälle bei Lidl und anderen Discountern, die die Überwachung von Mitarbeitern bis hin zur Videobeobachtung in Umkleideräumen angeordnet haben, die Telefonbespitzelung bei der Telekom und die Weitergabe von Angaben zur Gewerkschaftsmitgliedschaft im Rahmen des Abkommens zur Datenübermittlung zwischen Deutschland und den USA haben gezeigt, dass die Hemmschwelle, das Persönlichkeitsrecht von Beschäftigten und Bürgern zu verletzen, soweit überhaupt noch vorhanden, zumindest außerordentlich niedrig ist.

Der DGB und seine Mitgliedsgewerkschaften fordern seit Jahren wirksame gesetzliche Regelungen in einem eigenständigen Arbeitnehmerdatenschutzgesetz, die sicherstellen, dass dem Persönlichkeitsrecht der Beschäftigten im Arbeitsverhältnis endlich Rechnung getragen wird. Datenschutz bedeutet dabei Schutz personenbezogener und -beziehbarer Daten von Beschäftigten vor Missbrauch. Zweck des Datenschutzes muss es sein, den Einzelnen davor zu schützen, dass durch Missbrauch seiner Daten eine Beeinträchtigung seines grundrechtlich geschützten Persönlichkeitsrechts erfolgt. Obwohl der Koalitionsvertrag der ersten rot-grünen Regierung ein solches gesetzgeberisches Vorhaben vorsah, ist dieses Vorhaben weder auf nationaler Ebene noch auf europäischer Ebene bislang auch nur ansatzweise verwirklicht worden. Gerade auf Grund der aktuellen Vorfälle ist es deshalb notwendig, die bisherigen Forderungen zu bekräftigten und die Politik aufzufordern, ihrer Verpflichtung, die Grundrechte zu schützen, durch wirksame Gesetze nachzukommen und deren Einhaltung durch wirksame Sanktionen zu gewährleisten.

Die Regelung dieses wichtigen Bereiches darf nicht der Rechtsprechung allein überlassen werden, die nur in der Lage ist, in Einzelfällen zu entscheiden. Zudem kann die Rechtsprechung keine unmittelbare Bindungswirkung im Allgemeinen entfalten. Das informationelle Selbstbestimmungsrecht und das allgemeine Persönlichkeitsrecht müssen im Arbeitsverhältnis geschützt werden.

Insgesamt ist die Forderung nach einem Arbeitnehmerdatenschutzgesetz nach wie vor dringlich. Zurzeit stellt sich die Rechtslage unübersichtlich und unklar dar. Ziel einer eigenständigen gesetzlichen Regelung muss daher auch sein, für Arbeitgeber und Arbeitnehmer klare und möglichst verständliche Regelungen zu schaffen. Die Vorschriften müssen klar strukturiert und möglichst präzise formuliert sein. Der Schutz der Beschäftigten vor unzulässiger Datenerhebung, -verarbeitung und -nutzung könnte besser in der Praxis durchgesetzt werden, und die Arbeitgeber bekämen den Rahmen aufgezeigt, in dem sie sich legal bewegen können. Dabei muss ebenfalls klargestellt werden, dass das Datenschutzgesetz einen Minimalstandard regelt, der auch durch Betriebsvereinbarungen nicht unterschritten werden darf.

1. Dazu ist es notwendig, dass die gezielte Beobachtung und Überwachung von Beschäftigten am Arbeitsplatz aber auch im privaten Umfeld ausdrücklich verboten wird. Es muss klargestellt werden, dass eine direkte Überwachung weder durch Beauftragte oder Externe noch durch Mitarbeiter oder eine indirekte Überwachung durch Video- oder Tonaufnahmen gerechtfertigt ist. Ebenso wenig kann die Kontrolle der Beschäftigten durch Auswertung oder mit Hilfe computergesteuerter oder biometrischer Systeme erlaubt sein. Nur für den Fall, dass der begründete Verdacht einer strafbaren Handlung oder einer schwerwiegenden Schädigung des Arbeitgebers besteht, kann gesetzlich vorgesehen werden, dass eine Überwachung im Einzelfall zulässig sein kann. Die Anordnung einer solchen Überwachung bedarf jedoch immer der Zustimmung der betrieblichen Interessenvertretung.

2. Bei elektronischer Datenverarbeitung ist eine besondere Schutzbedürftigkeit in Bezug auf das allgemeine Persönlichkeitsrecht gegeben, da im Hinblick auf die Vielzahl und die Qualität der verwendeten Daten, die Kombinations- und Auswertungsmöglichkeit, den Kontextverlust und die zeitlich unbegrenzte Verfügbarkeit besondere Risiken bestehen. Um der strukturellen Unterlegenheit von Beschäftigten Rechnung zu tragen, kann deshalb das grundsätzliche Verbot des Zugriffs auf personenbezogene oder -beziehbare Nutzerdaten bei der Verwendung moderner Kommunikationsmittel durch den Arbeitgeber auch nicht durch eine generelle Einwilligung des Arbeitnehmers ausgeschlossen werden. Nur dann, wenn das Gesetz selbst bestimmte Fälle vorsieht, in denen der Arbeitgeber aus dringenden betrieblichen Gründen Daten erfassen darf, kann

eine solche Datenerfassung mit schriftlicher Einwilligung (das heißt vorheriger Zustimmung und nicht nachträglicher Genehmigung) des Beschäftigten für den konkreten Fall erfolgen. Grundsätzlich muss gesetzlich geregelt werden, dass der Arbeitgeber verpflichtet ist, sicherzustellen, dass die technischen Anlagen so organisiert sind, dass ein Rückschluss auf die Person oder das Verhalten des Verwenders von modernen Kommunikationsmitteln ausgeschlossen ist. Dazu gehört auch, dass der Arbeitgeber unvermeidbare Daten bei der Nutzung solcher Kommunikationsmittel unverzüglich löschen muss und die Weitergabe von Daten, auch an andere Konzernunternehmen, ausgeschlossen ist.

3. Außerdem müssen das Fragerecht des Arbeitgebers bei Einstellungen und die Anordnung von ärztlichen Untersuchungen gesetzlich auf die Fälle beschränkt werden, die die Rechtsprechung bislang vorsieht. Das bedeutet, dass nur die Fragen bei der Einstellung zulässig sind, die für die konkrete Tätigkeit von entscheidender Bedeutung sind. Ebenso darf nur dann eine ärztliche Untersuchung angeordnet werden, wenn dies ausdrücklich gesetzlich geregelt ist (zum Beispiel im Jugendarbeitsschutzgesetz). Verboten werden muss außerdem, dass der Arbeitgeber die Ergebnisse ärztlicher Untersuchungen entgegennimmt oder verwendet, insbesondere im Zusammenhang mit Pflichtverletzungen aus dem Arbeitsvertrag. Dies muss im besonderen Maße für Genomanalysen gelten. Für Drogen- und Alkoholtests muss gelten, dass ihre Durchführung weder angeordnet, noch die Ergebnisse entgegengenommen werden dürfen, es sei denn, es liegt ein begründeter Verdacht des Drogen- und Alkoholmissbrauchs vor und der Beschäftigte hat in den Test eingewilligt. Außerdem muss vor Anordnung aller Untersuchungen die Zustimmung des Betriebsrates vorliegen.

4. Flankiert werden sollten diese Maßnahmen zum verbesserten Schutz des Persönlichkeitsrechts der Beschäftigten dadurch, dass der betriebliche Datenschutzbeauftragte und die Mitbestimmungsrechte der Betriebsräte beim Datenschutz gestärkt werden. Für den betrieblichen Datenschutzbeauftragten kommt in Betracht, dass er, wie Betriebsräte, auch vor Kündigungen geschützt wird. Um sicher zu stellen, dass der Datenschutzbeauftragte die Interessen der Beschäftigten tatsächlich wahrnimmt, ist dem Betriebsrat ein Zustimmungsverweigerungsrecht bei der Benennung aller Datenschutzbeauftragten zu gewähren.

5. Die Einhaltung der gesetzlichen Bestimmungen kann nur dann gewährleistet werden, wenn die alleinige Last der Durchsetzung ihrer Rechte durch Klage von den betroffenen Beschäftigten genommen wird. Die Erfahrung zeigt, dass Arbeitnehmer im bestehenden Beschäftigungsverhältnis in der Regel nicht gegen den Arbeitgeber klagen können. Zu groß ist die Gefahr von Repressalien bis hin zur Kündigung. Deshalb reicht es nicht aus, dass gesetzlich ein sogenanntes Maßregelungsverbot vorgesehen wird, das heißt, dass dem Arbeitgeber verboten wird, Beschäftigte wegen der Wahrnehmung ihrer Ansprüche aus einem Arbeitnehmerdatenschutzgesetz zu benachteiligen. Vielmehr muss ein Verbandsklagerecht vorgesehen werden.

6. Um den gesetzlichen Regelungen auch tatsächlich Wirkung zu verleihen, sind angemessene und abschreckende Sanktionen vorzusehen. Zum einem muss für denjenigen, dessen Persönlichkeitsrecht verletzt worden ist, ausdrücklich ein konkreter Anspruch auf Schmerzensgeld in Form einer Entschädigung, entsprechend der Entschädigungsregelung in § 15 Allgemeines Gleichbehandlungsgesetz bei Verstoß gegen das Diskriminierungsverbot, zugebilligt werden. Dieser Entschädigungsanspruch kann entweder direkt für bestimmte Verstöße die Höhe der Entschädigung regeln, oder die gesetzliche Regelung muss den abschreckenden Charakter einer solchen Entschädigungszahlung ausdrücklich hervorheben. Darüber hinaus muss die Verletzung des allgemeinen Persönlichkeitsrechts strafbewehrt werden. Die bloße Ordnungswidrigkeit reicht angesichts der rechtsverneinenden Praxis der Arbeitgeberseite nicht aus.

7. Bei Verfahren wie der elektronischen Gesundheitskarte und ELENA muss zwingend sichergestellt werden, dass die persönlichen Daten der Betroffenen vor unbefugtem Zugriff geschützt und nur in Kenntnis und mit Zustimmung der Betroffenen verwendet werden können. Solange daran Zweifel bestehen, muss die Verwendung ausgeschlossen sein.

8. Auch das Bundesdatenschutzgesetz muss den heutigen technischen Gegebenheiten des Internets angepasst werden. Im Falle einer Datenverarbeitung im Auftrag müsste § 11 Bundesdatenschutzgesetz dahingehend präzisiert werden, dass für die in Auftrag gegebene Datenverarbeitung und die zu treffenden technisch-organisatorischen Maßnahmen ein Vertrag abzuschließen ist und welchen Mindestanforderungen er entsprechen

sollte. Die Nutzung sollte lückenlos dokumentiert werden. Außerdem wird der Sanktionsrahmen weder im Bereich des Ordnungswidrigkeitenrechts noch im Strafrecht vollständig ausgeschöpft. Deshalb sollten Verstöße gegen das Bundesdatenschutzgesetz statt Antrags- Offizialdelikte sein.

Datenschutz vor Ort

Gelingt der Interessenausgleich?

Marco Biewald

I. Die Rahmenbedingungen im Beschäftigtendatenschutz

Die Frage, ob der Interessenausgleich im Beschäftigtendatenschutz gelingt, hängt im großen Maße von den Rahmenbedingungen ab. Stimmen die Rahmenbedingungen, gelingt der Ausgleich zwischen Persönlichkeitsrechten einerseits und Wahrung der Arbeitgeberinteressen andererseits. Passen also die Rahmenbedingungen?

Im Grunde sind die Rahmenbedingungen einfach. Es kommt beim praktischen Beschäftigtendatenschutz darauf an, zwei Fragen zu beantworten: Zum einen ist zu klären, ob die Verwendung der Daten von Beschäftigten erlaubt ist, die jeweilige Verarbeitung das Persönlichkeitsrecht des Beschäftigten nicht verletzt. Zum anderen ist zu fragen, ob die Daten, die verwendet werden, ausreichend geschützt sind.

1. Rahmenbedingung 1: Die Erlaubnis klären

Die Frage, ob die Beschäftigtendaten verwendet werden dürfen, beantwortet der Grundsatz in § 4 Bundesdatenschutzgesetz (BDSG) beziehungsweise in den jeweiligen landesrechtlichen Vorschriften: Ein Gesetz oder eine Einwilligung müssen die Verarbeitung legitimieren. Dieser theoretische Ansatz läuft in der Praxis auf vier Fallgruppen hinaus:

- In wenigen Fällen, wie zum Beispiel bei Datenübermittlung an Sozialbehörden oder Finanzämter, gibt es spezielle Gesetze, die

den Verwendungsschritt erlauben. Dieser Fall ist einfach zu klären und stellt in der Praxis nicht das Problem dar.

- Häufig greift im Beschäftigtenverhältnis die Erlaubnis, die in § 28 Abs. 1 Nr. 1 BDSG beschrieben ist: Die Beschäftigtendaten werden zur Erfüllung des Vertrages mit dem Beschäftigten verwendet. Dies ist zum Beispiel der Fall bei den vielen Datenerhebungen und -verarbeitungen zur Entgeltabrechnung. Tarifverträge geben vor, welche Faktoren, zum Beispiel Kinderzahl, Ausbildung, Arbeitsjahre, erfasst werden müssen.

- In einigen Fällen findet die Einwilligung des Beschäftigten Anwendung; dies ist zugleich die Universalerlaubnis, sie findet Anwendung, wenn sonst gar nichts mehr geht. Das Spektrum für Einwilligungen ist groß: Von der Erlaubnis, Bilder zu veröffentlichen, bis hin zur Kontrolle von PC-Nutzungen finden sich Einwilligungen im Leben am Arbeitsplatz.

- Praktisch am häufigsten findet jedoch die allgemeine, unspezifische Erlaubnisnorm Anwendung, wie sie in § 28 Abs. 1 Nr. 2 BDSG beschrieben ist: Beschäftigtendaten können verarbeitet werden, wenn ein berechtigtes Interesse an der Verarbeitung gegenüber dem Interesse der Betroffenen an der Nichtverarbeitung überwiegt.

Diese allgemeine Formel muss Antwort geben auf Fragen wie zum Beispiel: Darf der Arbeitgeber die Protokolle über die Internetnutzung auswerten? Darf er das Lager mittels Video überwachen? Darf der Arbeitgeber seinen Lastkraftwagenfahrer per Handy orten? Die korrekte Antwort lautet: Ja er darf, wenn dies für die Durchsetzung eines legitimen Interesses erforderlich ist und dies gegenüber dem Interesse des Arbeitnehmers überwiegt.

Hier zeigt sich schon das Kernproblem in der Praxis: Die Antwort auf die Frage, ob der Interessenausgleich gelingt, ist die Frage selber! Mit anderen Worten: Der Interessenausgleich gelingt, wenn die Interessen ausgeglichen sind.

Die gesetzlichen Vorgaben der Datenschutzgesetze helfen in der Praxis bei der Frage "Darf man das?" nicht viel. Braucht es überhaupt eine gesetzliche Normierung dieser Erlaubnisnorm "Interessenausgleich"? Im Grunde besagt diese Erlaubnisnorm nur: Sei nicht willkürlich! Für Christen ergibt sich diese Verhaltensweise bereits aus der Bibel, für Moslems aus dem Koran, sie ist Teil der Phi-

losophie der Grundrechte, und sie findet ihren Ansatz durch das Bürgerliche Gesetzbuch (Prinzip von Treu und Glauben) und damit auch direkt auf einen Arbeitsvertrag Anwendung.

Gelingt der Interessenausgleich – das BDSG jedenfalls gibt darauf keine Antworten. Für die Fälle, die praktisch nach einer Antwort suchen, ist das Datenschutzgesetz nicht viel wert. Das, was wir unter Datenschutzrecht verstehen, hilft so nicht, Klarheit und einen Interessenausgleich in der Praxis herzustellen. Dazu ist mehr notwendig.

2. Rahmenbedingung 2: Schutzmaßnahmen treffen

Wie steht es um die zweite Rahmenbedingung? Nach § 9 BDSG müssen Unternehmen Maßnahmen treffen, um den Missbrauch der Beschäftigtendaten zu verhindern. Allerdings zeigt sich auch hier ein Dilemma: Was genau muss man tun? Wann sind Arbeitnehmerdaten ausreichend geschützt?

Das Gesetz verlangt "die erforderlichen Maßnahmen", um "die Ausführung des Gesetzes zu gewährleisten". Gleichzeitig spricht es davon, dass nur die Maßnahmen erforderlich sind, deren Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzweck stehen, § 9 BDSG. Gleich mehrere unklare, auslegungsfähige Begriffe enthält die Vorgabe: Erforderliche Maßnahmen, angemessenes Verhältnis, angestrebter Schutzzweck. Was heißt das praktisch?

Beispiel: Ein Unternehmen möchte die Daten der Zeiterfassung dem Mitarbeiter sichtbar machen und den Zugriff Fremder darauf verhindern. Ist ein 5-stelliges oder ein 8-stelliges Passwort oder gar ein 10-stelliges Passwort mit mindestens 3 Buchstaben und wöchentlicher Änderung oder aber die Zugangskarte mit Fingerabdruck richtig?

Einige Unternehmen fragen bei solchen Maßnahmen konkret: Was kostet es mich, die (vom Datenschutzbeauftragten) vorgeschlagene Maßnahme, zum Beispiel die umfassende Protokollierung (= Eingabe- und Weitergabekontrolle) oder die sichere Zugangskarte (= Zugangskontrolle) einzuführen? Und was kostet es mich, sie nicht einzuführen? Andere Unternehmen verfolgen eine andere Philosophie: Sie möchten gern ihren Mitarbeitern ausreichend Schutz bieten und fragen, welche Maßnahme die sinnvollste ist.

Was kann man antworten? Ausreichend ist alles, was du dir leisten kannst?

Auf der anderen Seite ist zu fragen, ob ein Mitarbeiter seinem Arbeitgeber vorwerfen kann, nicht genügend getan zu haben. Beispiel: Die Kollegen können über ihre Zugangsberechtigung die Kommen- und Gehenzeiten der ganzen Abteilung einsehen. Kann man dem Unternehmen etwas vorwerfen und, wenn ja, was? Anderer Fall: Ist es vorwerfbar, wenn eine große Personengruppe Zugriff auf die elektronischen Personalakten hat, statt einer kleinen?

Hier zeigt sich übrigens noch ein anderes enormes praktisches Problem. Die Pflicht, Schutzmaßnahmen umzusetzen, wird nicht sanktioniert. Welchen Wert hat eine Pflicht deren Nichtbefolgung ohne Konsequenzen bleibt? So kann ein Interessenausgleich nicht gelingen.

Oft trifft man in der Praxis auf Unternehmen, die vorgeben: Wir möchten nur das Gesetz erfüllen, aber nicht mehr machen. Was soll man in einem solchen Fall bei diesem Gesetz antworten? Was heißt denn "nur" das Gesetz erfüllen, wenn das Gesetz unbestimmt, offen und weit auslegungsfähig ist?

Der Gedanke, zu aktiven Schutzmaßnahmen zu verpflichten, ist sicher sinnvoll. Ein Arbeitgeber muss die Daten seiner Arbeitnehmer schützen. Viele wollen dies auch. Aber Orientierungshilfe bieten die Datenschutzgesetze dabei wenig.

3. Die Rahmenbedingungen aus praktischer Sicht

Es bleibt festzuhalten: Der Interessenausgleich gelingt nicht deshalb, weil die Gesetze gut und ideal sind, sondern im Gegenteil. Datenschutz ist eine schwer greifbare Materie. Die Gesetze lassen extrem weiten Spielraum. Das klingt gut, denn so kann ein Unternehmen individuell reagieren. Das ist aber häufig nur in der Theorie gut. In der Praxis zeigt sich Orientierungslosigkeit und Hilflosigkeit. Alles hängt davon ab, wie die entscheidenden Personen die Argumente für und gegen eine Verarbeitung gegeneinander abwägen und wie die entscheidenden Personen ausreichenden Schutzbedarf interpretieren. Personen mit hohem Sachverstand sehen die Dinge anders als ungeübte Personen. Der gesetzliche Spielraum zur Herstellung des Interessenausgleichs nutzt nichts, wenn das

Know How fehlt, ihn zu nutzen. Der Interessenausgleich gelingt nur mit den richtigen Personen.

II. Die praktischen Grenzen an 9 Beispielen

An welchen Stellen stoßen in der Praxis die Möglichkeiten des Interessenausgleichs auf ihre Grenzen? Im Folgenden werden anhand einiger praktischer Szenarien die Schwierigkeiten dargestellt.

1. Die sinnentleerte Einwilligung

Gern werden in der Unternehmenspraxis Einwilligungen eingesetzt – um eine Verarbeitung zu legitimieren. Beschäftigte willigen ein, dass bestimmte Daten erhoben oder dass bestimmte Verarbeitungen durchgeführt werden. Hierzu folgende Praxisbeispiele:

Unternehmen der Lebensmittelindustrie: "Mit meiner Unterschrift erkläre ich mich einverstanden, dass meine Daten während der Betriebszugehörigkeit gespeichert und zur Erfüllung des mit mir abgeschlossenen Arbeitsvertrages verwendet werden. Ich bin damit einverstanden, dass Sozialversicherungsbehörden und anderen Behörden die Daten übermittelt werden, die zur Abwicklung des Arbeitsvertrages übermittelt werden müssen."

Aus einem Industriebetrieb: "Mit dem Befahren des Parkplatzes erklären Sie sich bereit, dass Sie per Video überwacht und Daten von Ihnen aufgezeichnet werden."

Spiegeln die Einwilligungen tatsächlich den Willen des jeweiligen Beschäftigten wieder? Vom Sinn her sollte die Einwilligung ermöglichen, dass ein Beschäftigter individuell nach seinem Maßstab von informationeller Selbstbestimmung Verarbeitungen erlaubt oder eben nicht. In der Praxis funktioniert die Einwilligung jedoch nicht. Hier bestehen mehrere Probleme:

1. Der Arbeitgeber möchte primär möglichst einheitliche und einfache Prozesse, der individuelle Wille des einzelnen Arbeitnehmers soll nicht entscheiden. Die Einwilligung "Ich bin damit einverstanden, dass zur Durchführung meiner Gehaltsabrechnung die erforderlichen Daten über mich an das Rechenzentrum XY übermittelt werden" darf praktisch nicht mit Nein beantwortet werden. Der Gehaltsabrechnungsprozess wäre nicht mehr ausführbar.

2. Der Arbeitnehmer ist nicht frei, einzuwilligen. Auf ihn kann enormer Druck ausgeübt werden, denn er ist abhängig von der Beschäftigung. Theoretisch könnte er einem datenschutzunfreundlichen Arbeitgeber kündigen – aber das ist nur Theorie. Wenn der Arbeitgeber eine Unterschrift "wünscht", wird sie allzu oft geliefert. In der Praxis ist der Arbeitnehmer nicht frei, wie vom Gesetz für die Einwilligung gefordert.

In der Unternehmenspraxis verkommt die Einwilligung oft zu einer leeren Hülse: Unternehmen glauben, so handeln zu müssen. Alle Arbeitnehmer müssen unterschreiben, die aber gar nicht wollen. Für alle Beteiligten ist es nur bürokratischer Aufwand. (Hier ist übrigens eine der Ursachen, warum Datenschutz gern als bürokratisches Mittel angesehen wird).

Mit Einwilligungen gelingt der Interessenausgleich kaum. Arbeitnehmer sind nicht frei, Arbeitgeber benötigen sie in den meisten Fällen nicht. Sie werden meist aufgrund mangelnden Sachverstandes eingesetzt. Für Arbeitnehmer wird eine Freiheit vorgegaukelt, die tatsächlich nicht besteht. Arbeitgeber bürden sich selbst eine Hürde auf, die tatsächlich nicht notwendig ist.

2. Das Internetnutzungsproblem

Wohl kaum ein Thema ist so schwierig in der Praxis zu realisieren wie die "richtige" Regelung der Internet- und E-Mailnutzung. Gestattet der Arbeitgeber die private Nutzung, wird er zum Provider, zum Anbieter von Telekommunikationsdienstleistungen. Überprüfungen, ob ein Arbeitnehmer übermäßig surft, oder eine Kontrolle des E-Mailverkehrs sind so nicht möglich. Verbietet der Arbeitgeber die private Nutzung, hat er zwar bestimmte Überprüfungsmöglichkeiten, ist jetzt jedoch zu streng gegenüber seinen Beschäftigten und spricht Verbote aus, die keiner möchte.

Kein anderer Praxisfall verdeutlicht so sehr, wie schwer es ist, den Interessenausgleich herzustellen. Unternehmen betreiben zahlreiche Konstruktionen, um diesen Ausgleich rechtlich hinzubekommen. Teilweise werden Einwilligungen eingesetzt. Beispiel: "Ich bin damit einverstanden, dass meine privaten E-Mails durch das Unternehmen XY gespeichert und archiviert werden. Außerdem bin ich einverstanden, dass mein privates Surfverhalten während meiner Arbeitszeit aufgezeichnet wird und darauf hin geprüft wird, ob es geringfügig oder übermäßig erfolgt".

Andere Unternehmen legen fest, dass zu einer bestimmten Uhrzeit privat gesurft werden kann, in der Regel die Mittagszeit (12 – 13 Uhr beispielsweise). Andere Unternehmen wollen es mengenmäßig begrenzen: Erlaubt sind nur kurze private Seitenaufrufe. Wer länger als 10 Minuten eine Seite aufruft, fällt in den Aufzeichnungsgenerator.

Wie man die Situation auch dreht und wendet, entweder erfasst der Arbeitgeber privates Verhalten oder aber er hat nicht mehr unter Kontrolle, was passiert. Wie schwer das praktisch abzugrenzen ist, zeigt ein delikater Fall: Die Mitarbeiter einer Abteilung besitzen alle Firmen-Notebooks. Es ist allgemein festgelegt, dass diese nicht privat genutzt werden dürfen. An einem Samstagabend, 22:30 Uhr wurde für etwa 50 Minuten über die Einwahl eines solchen PC´s der Aufruf pornografischer Seiten festgestellt. Ein bestimmter Mitarbeiter wurde identifiziert; der Mitarbeiter befand sich auf einer 10-tägigen Geschäftsreise. Er bestätigte auf Nachfragen diesen Sachverhalt. Eine formal korrekte Missbrauchskontrolle der Arbeitsmittel oder eine Beeinträchtigung des Persönlichkeitsrechts? Eine Gefährdung der Netzwerksicherheit oder eine überschießende Detailüberwachung?

3. Die unqualifizierten Datenschutzbeauftragten

Datenschutz wird unzureichend umgesetzt, wenn unqualifizierte Datenschutzbeauftragte mitwirken. Unternehmen werden durch unqualifizierte Beauftragte mit bürokratischen Hürden als einen scheinbaren Datenschutz belastet.

Unternehmen müssen (ab einer bestimmten Anzahl von mit Datenverarbeitung beschäftigten Personen) einen Datenschutzbeauftragten bestellen. Wer diese Pflicht nicht erfüllt, erfüllt den Tatbestand einer Ordnungswidrigkeit. Soweit ist die Regel klar und verständlich. Eine Bestellungsurkunde ist schnell geschrieben und damit die formelle Pflicht erfüllt. Ab diesem Punkt jedoch beginnen die praktischen Probleme. Was muss der Datenschutzbeauftragte können? Wie muss er sein? Was muss man ihm zur Verfügung stellen? Die Gesetze geben darauf außer der bekannten allgemeinen Formulierung "Fachkunde und Zuverlässigkeit" keine Antwort. Ist der Datenschutzbeauftragte, der seine Arbeit pünktlich beginnt, schon zuverlässig? Die mangelnde Konkretisierung der Anforderungen führt in der Praxis zu einer gefährlichen Konstellation. Arbeitgeber glauben, mit der bloßen Bestellung die Datenschutzvor-

schriften zu erfüllen. Arbeitnehmer fühlen sich durch die Existenz des Beauftragten in einer Sicherheit, die es nicht gibt ("Wie mit dem Datenschutzbeauftragten vereinbart…"). Aufsichtsbehörden lassen sich mit der Bestellungsurkunde und dem Teilnahmenachweis eines Seminars ruhig stellen. Aber Datenschutzbeauftragte ohne Kenntnis von Recht und Technik befürworten Verarbeitungsvorgänge, die kritisch sind (Originalton: "Wenn der Auftragnehmer diesen Vertrag unterschreibt, können wir alle Daten auslagern."). Beauftragte mit Halbwissen belasten und bestehen auf unwirksamen, falschen Dingen, nicht zuletzt auch, um eine gewisse Aktivität zu zeigen (zum Beispiel das Bestehen auf Einwilligungserklärungen in Situationen, wo dies entbehrlich wäre).

Der Berufsverband der Datenschutzbeauftragten (BvD) hat auf dieses Problem bereits reagiert. Berufsgrundsätze für die Tätigkeit des Datenschutzbeauftragten sollen Orientierung geben und einen Standard an Qualität schaffen. Heute ist es möglich, dass der arbeitslose Gärtner in einem Tag zum Datenschutzbeauftragten umsatteln kann. Der Berufsverband fordert, dass Beauftragte in der Lage sein müssen, bestimmte Prüfungs- und Beratungsaufgaben zu lösen. Die Berufsgrundsätze des BvD sollten zum deutschen Standard für den Beruf des Datenschutzbeauftragten werden. Solange unser gesellschaftlicher Anspruch an die Überwachungsinstanz "Datenschutzbeauftragter" so niedrig ist, dass ein Zweitageskurs "Ausbildung" als ausreichend empfunden wird, so lange wird es Konzerne geben, deren Überwachungskameras in Sozialräumen durch Journalisten aufgedeckt werden müssen.

4. Die Überwachung mittels RFID-Karten

RFID-Karten gefährden die Freiheit der Arbeitnehmer erheblich und schaffen gegenwärtig mehr Missbrauchsmöglichkeiten als Nutzen. Für einen Interessenausgleich sind erhebliche Aktivitäten notwendig.

Mitarbeiterkarten werden vielfältig eingesetzt. Die kontaktlose Übertragung von Informationen der Mitarbeiterkarte schafft zunehmend neue Anwendungsmöglichkeiten. Vielfach bekannt ist der Einsatz am Zeiterfassungsterminal oder als "Türöffner", also als Zutrittskontrollmaßnahme. Diese häufigen Anwendungen sind mit gängigen Mitteln beherrschbar, solange Chip und das Lesegerät nur wenige Millimeter voneinander entfernt sein dürfen. Aktuelle RFID-Chip-Technik ermöglicht jedoch, dass Lesegerät und Chip bis

zu mehreren Metern voneinander entfernt stehen können. Der Chip kann daher ausgelesen werden, ohne dass der Arbeitnehmer dies durch äußere Umstände wie Leseterminals oder Durchgänge erkennen kann und ohne dass er eine aktive Handlung, wie das zum Lesegerät Führen, vornehmen muss. Hier besteht ein erhebliches Risiko, dass von den Personen, die einen solch auslesbaren Chip bei sich führen, Bewegungsprofile und Verhaltensprofile erstellt werden.

Ein Praxisbeispiel zeigt die realen Risiken: Ein Industrieunternehmen möchte für mehr Sicherheit im Unternehmen sorgen. Damit im Brandfall alle Personen evakuiert werden können, soll jeder Mitarbeiter eine RFID-Mitarbeiterkarte erhalten. Auf einem Bildschirm kann im Brandfall festgestellt werden, wo sich noch Personen im Gebäude befinden. Zugleich kann das Unternehmen damit den Zutritt zu den einzelnen Unternehmensbereichen regeln. Wie soll man mit dieser Situation umgehen? Ist der Datenschützer gegen mehr Sicherheit? Rechtfertigt eine wahrscheinlich bessere Evakuierungsquote im Brandfall die Erstellung der Bewegungsprofile?

Leider ist dies erst der Anfang. Die Werksleitung selbst erkannte in dem genannten Fall in dem Chip eigene Nutzungsmöglichkeiten: Die Werksleitung sah, dass man mit diesen Karten aufzeichnen kann, wie sich Mitarbeiter bewegen, mit diesem Wissen plante die Werksleitung, Maschinen und Material optimal zu platzieren.

Mit dem RFID-Chip können neue, durchaus positive und nachvollziehbare Unternehmensziele verfolgt werden. Es kann unterstellt werden, dass niemand Böses möchte. Aber wo ist die Anwendungsgrenze? Datenschutz führt hier nicht mehr zum Ergebnis. Die neue Technik ermöglicht neue, bisher unbekannte Möglichkeiten und neue, bisher unbekannte Informationserfassungen. Herkömmliche Betrachtungen helfen hier nicht, das Gleichgewicht herzustellen. Wir brauchen eine neue, ethische Diskussion: Wie viel unbekannter Mensch darf ein Arbeitnehmer sein, wie viel berechenbares Produktionsmittel soll er sein?

5. Die schwer beherrschbare Videoüberwachung

Die Praxis der Videoüberwachungen ist schwierig – ein Instrument scheinbarer Sicherheit. In den letzten Jahren ist ein regelrechter Boom an Videokameras in Unternehmen zu verzeichnen. Gebäude-

eingänge, Einfahrten, Höfe werden fast schon standardmäßig beobachtet. Selbstverständlich sind grundlegende Maßnahmen vielerorts festgelegt: Die Aufzeichnungsdauer, Beschränkungen in den Zugriffsberechtigungen. Zwei Aspekte führen jedoch dazu, dass das Persönlichkeitsrecht nicht ausreichend berücksichtigt wird.

1. Eine genaue Beschäftigung mit den Zielen, aber auch Schutzmaßnahmen erfolgen häufig erst hinterher. Ein Grund: Der Datenschutzbeauftragte wird erst nach Anschaffung hinzugezogen. Gerade bei der Videoüberwachung zeigt sich ein allgemeines praktisches Problem: Die oft beschworene Vorabkontrolle funktioniert in der Praxis nicht. Kaum ein Praktiker versteht den Gesetzestext: Wann muss ich eine Vorabkontrolle durchführen, wann nicht? Weiß ich endlich, wann, ist nicht klar, was alles eine solche Vorabkontrolle enthält. Schließlich ist diese Pflicht der Vorabkontrolle wenig wert: Was passiert, wenn sie nicht durchgeführt wird? Die bitter notwendige Vorabkontrolle ist ein totes Instrument. Videoüberwachung braucht in der Praxis eine detaillierte Klärung von Sinn und Zweck im Vorfeld. Jede Menge Kameras in Unternehmen würde nicht hängen, wenn eine Pflicht zur Detailprüfung vorab bestehen würde. Hierzu zwei Beispiele:

Ein produzierendes Industrieunternehmen stellt fest, dass die Menge von Metallplattenresten, die bei der Produktion entstehen und weiterverkauft werden, immer geringer wird. Da diese im Hof lagern, steht für den Werksschutz fest, dass hier gestohlen wird. Für einen vierstelligen Eurobetrag werden hochwertige Videokameras aufgebaut. Der Schwund ändert sich nicht. Jetzt wird neu nachgeforscht. Schließlich stellt man fest, dass nach dem Wechsel des Fabrikleiters eine lasche Praxis in die Fabrik eingezogen ist: Immer mehr Meister haben den Arbeitern ihrer Gruppe erlaubt, die Reste direkt von der Werkbank weg mit nach Hause zu nehmen.

In einem anderen Fall überwachte ein Unternehmen den Kellereingang, da dort gelegentlich die Tür beschädigt wird und Graffiti-Schmierereien auftreten. Erst nachdem die Kameras erfolglos hingen, fand eine nüchterne Analyse statt: Der immer wieder angeführte Vandalismus trat nur nachts auf, Täter tauchten überraschend von der Seite nur kurz im Bild auf und waren durch Kapuzen und Mützen nicht erkennbar. Außer einer Aufzeichnung ein- und ausgehender Mitarbeiter wurde also nichts aufgezeichnet. Die Erfolglosigkeit beider Überwachungssituationen hätte man in einer Vorabprüfung bereits ermitteln können.

2. Ein völlig anderes Problem ist die verfeinerte Aufnahmetechnik. Während vor einigen Jahren Kameras noch mit dem Argument installiert werden konnten, dass man die einzelne Person nicht genau erkennt sondern nur ein Ereignis, sind heute gestochen scharfe Detailaufzeichnungen möglich. Beispiel: Ein für die Sicherheit des Unternehmensgeländes zuständiger Wachdienstmitarbeiter führt bei der Datenschutzprüfung stolz den Zoom der Kamera vor: "Die Kamera kann von 500 m weit entfernten Mitarbeitern die Uhrzeit vom Handgelenk ablesen. Kameras blicken heute in den Pkw des parkenden Mitarbeiters auf dem Firmenparkplatz."

Das Pendel verschiebt sich: Videoüberwachung kann heute genauer, detaillierter und situationsbezogener Mitarbeiter überwachen. Sowohl Verwendungsweck, als auch die Maßnahmen Zugriff auf die Daten und Löschung müssen neue, höhere Anforderungen erfüllen.

6. Die unendlichen Protokollinformationen

IT-Systeme hinterlassen mehr Informationen, als benötigt werden, und gefährden so das Persönlichkeitsrecht in einem ungeahnten Ausmaß: PC und IT-Geräte "erzählen" sehr viel über das Verhalten eines Mitarbeiters. Die Nutzung eines PC´s, Zeitpunkt und Versenden von E-Mails, das Aufrufen von Dokumenten, das Anmelden an Datenbanken, das Eingeben, Ändern von Datensätzen, Zeitpunkte von Abwesenheit und Anwesenheit, Inhalte und Zeitpunkt aufgerufener Webseiten sind Standardprotokollierungen. Hinzu kommen diverse unternehmensspezifische Protokollierungen und neuere Geräte: Kommunikationsdaten des Firmenhandys, Rechnungen zur Lkw-Maut, Zeitpunkt, Ort der Firmenkreditkartennutzung. Es ist möglich, sehr detailliert aus hinterlassenen Daten das Verhalten eines Mitarbeiters zu rekonstruieren.

Beispiel: Ein Unternehmen setzt Lotus Notes ein. Sämtliches Wissen ist in Notes-Datenbanken gespeichert. Jeder Aufruf einer Notes-Datenbank wird protokolliert. So kann lückenlos der Tagesablauf eines Mitarbeiters sichtbar gemacht werden: Wann ruft er in der Regel seine E-Mails ab, hat er im Adressbuch recherchiert, war er in der Projektdatenbank und, wenn ja, wann und wie lange, welche Wissensdatenbanken hat er wann aufgemacht. Hinzu kommt die Digitalisierung des Telefonverkehrs. Ankommende Anrufe, gewählte Nummern, Zeitpunkt und Gesprächsdauer sind in einer Datenbank gespeichert – und sollen dem Mitarbeiter zum Kontaktmanagement zur Verfügung stehen.

Anderes Beispiel: Ein Unternehmen hat viele reisende Beschäftigte. Sie nutzen Firmenkreditkarten. Mit dem Kreditkartenunternehmen vereinbarte das Unternehmen, Auswertungen über häufig genutzte Hotels und Umsätze mit bestimmten Dienstleistern zu ermitteln. Die Auswertungen wurden später auch angefordert, um Nutzungszeiten, zum Beispiel Zeitpunkt der Hotelzahlungen, mit Reisekostenabrechnungen zu vergleichen.

Das Problem ist vielschichtig. Die Protokollierung lässt sich nicht überall ausschalten. Die Protokollierung ist aber auch notwendig: Der Mitarbeiter beklagt, eine Datenbank nicht aufrufen zu können. Dafür ist der Blick in die Zugriffshistorie der Datenbank notwendig. Genau genommen fängt erst an dieser Stelle das Problem an: Der Zugriff auf die Protokollierungen kann kaum nachvollzogen werden. Zwar lässt sich der Kreis zugriffsberechtigter Personen bei bestimmten Protokollierungen einschränken. Missbrauch von Protokollierungsdaten ist aber praktisch nur schwer nachweisbar. Was mit diesen vielen Nachweisen über das Verhalten eines Mitarbeiters gemacht wird, kann praktisch nicht kontrolliert werden. Mitarbeiter sind mehr oder weniger ausgeliefert. Hier stößt Datenschutz an eine reale Grenze: Der Einsatz von Informationstechnologie macht menschliches Verhalten sehr transparent. Je mehr IT im Einsatz, umso nachvollziehbarer der Arbeitstag. Je IT-lastiger die Arbeitsprozesse, umso detaillierter kann individuelles Verhalten sichtbar gemacht werden. Hier müssen wir ehrlicherweise von einem Verlust an Privatheit sprechen.

7. Der unbeherrschbare Administrator

Datenschutz steht und fällt in der Praxis mit einzelnen Personen: Handeln diese nicht korrekt, sind die Mitarbeiter hoch gefährdet. Der einzelne Mitarbeiter lässt sich über diverse Zugriffsrechtesteuerungen noch relativ gut reglementieren und beherrschen. Aus der Datenschutzsicht praktisch kaum beherrschbar ist der Administrator. Administratoren sind in der Lage, den ein- und ausgehenden E-Mailverkehr zu überwachen, die aufgerufenen Internetseiten nachzuvollziehen, die gespeicherten Dokumente von und über Mitarbeiter einzusehen, Daten in Personalinformationssystemen einzusehen. Aber wie lässt sich das korrekte Verhalten eines Administrators überwachen? Hier muss der ehrliche Datenschutzbeauftragte sagen: Wir können es nicht.

Verschiedene Unternehmen reagieren in der Praxis so, dass die Personalabteilung einen eigenen Server betreibt oder ihr Personalinformationssystem selbst administriert und nicht ein Mitarbeiter, der IT-Zugriffsrechte besitzt. Das allerdings verlagert nur das Problem: Ein administrierender Mitarbeiter der Personalabteilung eines großen Unternehmens berichtete in einem vertraulichen Gespräch, dass er mehrmals im Jahr Besuche von Versicherungsvertretern und angeblichen Versicherungsvertretern erhält. Ihm wurden verschiedene Gegenleistungen für bestimmte Listen von Mitarbeiterdaten geboten. Die wertvollste waren 5 Euro pro Datensatz. Druckt der Administrator diese Liste, sieht er Daten ein, gibt er sie weiter - wie kann ich das praktisch nachprüfen? Es ist in der Praxis nahezu ausgeschlossen, solche Dinge immer aufzudecken. Je komplexer die Software, die die Personaldaten verwaltet, umso schwieriger die Handhabung und die Überprüfung.

Das wiederum führt schließlich zu einem weiteren Problem. Die Praxis zeigt immer wieder, dass Personalinformationssoftware nicht gehandhabt werden kann, weil sie zu komplex ist. Folgendes Beispiel soll dies verdeutlichen: Bei der Überprüfung der Zugriffsrechte in einem Unternehmen wurden 38 User im Personalinformationssystem festgestellt. 22, also 58%, besaßen administrative Rechte. Damit jedoch nicht genug: 20 dieser 22 Administratoren, waren gar keine Angehörigen des Unternehmens, sondern Berater.

Administratoren sind ein entscheidender Faktor für die Wahrung des Datenschutzes. Wir brauchen bessere Möglichkeiten, deren Möglichkeiten zu überwachen.

8. Die unvollendete Datenlöschung

Arbeitnehmer sind im Persönlichkeitsrecht gefährdet durch mangelhafte Löschungstechniken und Möglichkeiten. So schön das Gesetz auch klingt, Löschung von Mitarbeiterdaten stößt in der Praxis an ihre Grenzen. Wie kommen die Daten aus der Datenbank wieder raus? Praktisch lassen sich Daten in Datenbanken nicht löschen. Darüber hinaus gibt es das Problem der verteilten Datenspeicherung: Notebooks, Palms, Sicherungsmedien. Daten im aktiven System zu löschen, nutzt nichts, weil diese in lokalen Geräten und in Sicherungsmedien noch immer vorhanden sind. Es gibt gute Gründe, Sicherungsmedien jahrelang aufzubewahren. Auf diese Daten kann weiterhin zugegriffen werden, und sie können erneut in den Produktionskreislauf einfließen.

Wie häufig das vorkommt, zeigt ein praktischer Fall: Die Mitarbeiter der Personalabteilung haben die Vorgabe, nicht mehr genutzte Dokumente regelmäßig zu löschen. So bestehen je nach Dokumententyp zeitliche Vorgaben, ab welcher Dauer der Nichtnutzung Dokumente entweder zu archivieren oder zu löschen sind. Regelmäßig rufen Mitarbeiter in der IT-Abteilung an und bitten um Wiedereinspielung einzelner Dokumente, die gelöscht wurden und nun doch wieder benötigt werden.

Der rechtliche Anspruch auf Datenlöschung kann praktisch fast nie vollständig umgesetzt werden. Es gibt kaum Antworten darauf, wie man die Löschung sämtlicher Einzeldokumente und die Löschung von Daten auf Sicherungsmedien oder in lokalen Geräten in einem vertretbaren Aufwand umsetzen kann. Hinzu kommt, dass elektronische Dokumente über Mitarbeiter nicht nur in Datenbanken und auf File-Servern zu finden sind, sondern auch in den E-Mail-Postfächern. Vorlagen von Abmahntexten, Bewerbungsunterlagen, Berichte über An- und Abwesenheit, Schulungsteilnahmen, aber auch Informationen über Nutzungsverhalten am PC werden per E-Mail versendet. Diese Daten zu löschen, kann man praktisch nur sehr schwer sicherstellen.

9. Der externe Dienstleister

Große Risiken für das Persönlichkeitsrecht stellen die externen Dienstleister dar. Dienstleister werden für verschiedene Dinge eingebunden: Zum Beispiel die Durchführung der Gehaltsabrechnung, die Umstellung auf ein geändertes Tarifsystem (zum Beispiel Entgelt-Rahmen-Abkommen), Wirtschaftsprüfung, Hauswirtschaftsdienste, aber auch Wachdienste, technische Dienstleister. Sie erhalten Daten über die Mitarbeiter oder greifen darauf zu. Und dann? Formelle Verträge zur Sicherstellung einer Auftragsdatenverarbeitung lassen sich schnell erstellen und regeln. Aber was sind sie wert? Praktisch ist es so, dass Dienstleister erhebliche Mengen an Mitarbeiterdaten speichern und dass das ursprüngliche Unternehmen die Kontrolle über diese Daten verliert.

Es ist praktisch kaum möglich, all diese Datenspeicherungen zu kontrollieren: Weder kann man all diese Dienstleister vor Ort besuchen und überprüfen, noch lässt sich überblicken, wer tatsächlich Zugriff auf die Daten hat. Daten werden zur Erfüllung der Aufgaben des Dienstleisters auf Datenträgern übergeben, sie sind im Speicher von gemieteten Faxgeräten und Kopierern oder in geleas-

ten Fahrzeugen. Diesen Datenfluss kann man praktisch nicht kontrollieren. Kritisch sind dabei zwei Dinge: Die zunehmende Spezialisierung, die die Einbindung von unternehmensfremden Experten erfordert, und die zunehmende Elektronisierung der Arbeitswelt, die die Speicherung von Mitarbeiterdaten in immer neueren Gerätschaften nach sich zieht. Hier brauchen wir mehr und andere Antworten als den Abschluss von Verträgen zur Auftragsdatenverarbeitung.

III. Fazit

Die gesetzlichen Rahmenbedingungen zum Schutz der Beschäftigtendaten sind nur begrenzt hilfreich, um den Interessenausgleich zwischen Unternehmen und Beschäftigten herzustellen. Notwendig ist besonderer Sachverstand. Die Beantwortung von Datenschutzfragen durch Nicht-Fachleute führt in der Praxis zu Ergebnissen, die gerade den Interessenausgleich nicht gewährleisten. Durch moderne Techniken, deren Einsatzmöglichkeiten, aber auch durch die Elektronisierung von Vorgängen im Arbeitsleben ist ein faktischer Verlust von Privatheit die Folge. Zur Wahrung des Interessenausgleichs benötigt unsere Gesellschaft eine neue ethische Diskussion darüber, wie viel Information man von Beschäftigten wissen darf, sie benötigt Qualität in der Datenschutzüberwachung und neue Verpflichtungen für den Datenverwender.

Was geht?
Seriöse und unseriöse Überwachungspraktiken

Eveline Wippermann

Wenn ich mein heutiges Thema: "Was geht, was geht nicht", mit einem Satz zu beantworten hätte, würde ich sagen: "Es geht alles, was vom Gesetz her nicht verboten ist".

Allgemeine Unkenntnis führt leider leicht zu einer generellen Vorverurteilung der Überwachungspraktiken von Mitarbeitern (oder wem auch immer), auch durch seriöse Unternehmen der Sicherheitsbranche, und zu einem Ruf nach Verschärfung der eigentlich, aus meiner Sicht, voll ausreichenden Gesetzgebung.

Der Bundesverband Deutscher Detektive (BDD) hat die das Detektivgewerbe so sehr belastenden Vorfälle, insbesondere bei dem Discounter Lidl und der Deutschen Telekom, sehr sorgfältig verfolgt und analysiert. Unsere Position haben wir öffentlichkeitswirksam zum Ausdruck gebracht und uns entschieden von allen Arten unseriöser Bearbeitung distanziert.

Die Reaktion führte dann zu der zwischen dem BDD und dem Discounter Lidl getroffenen Vereinbarung zur Qualitätssicherung, sowohl im Detektivgewerbe als auch bei den Bewachungsfachkräften im Handel, letztere sind sicherlich besser bekannt unter dem Begriff "Kaufhausdetektive".

Im Ergebnis ist festzustellen, dass aus unserer Sicht die gesetzlichen Grundlagen völlig ausreichen und vielmehr Mängel an persönlicher Integrität, an fachlicher und sachlicher Qualifikation sowohl bei dem Auftraggeber, als auch bei dem Auftragnehmer zu den bekannten Fällen von Fehlverhalten geführt haben.

Wie kann man nun unseriöse Überwachungspraktiken weitgehend vermeiden? Oder anders ausgedrückt: Wie kann man die bereits angesprochene persönliche Integrität, fachliche und sachliche Qualifikation beim Auftraggeber wie beim Auftragnehmer sicherstellen? Die Beantwortung dieser Frage fällt für die jeweiligen Tätigkeitsbereiche völlig unterschiedlich aus. Der Unterschied zwischen der Bewachungsfachkraft im Handel, dem so genannten "Kaufhausdetektiv" und dem klassischen Detektiv erklärt sich wie folgt:

Aufgaben der Bewachungsfachkraft im Handel – Kaufhausdetektiv

Die im Handel eingesetzten Bewachungsfachkräfte gehören zum Wach- und Sicherheitsgewerbe, das strenge, in der Bewachungsverordnung festgeschriebene und öffentlich überprüfbare Auflagen erfüllen muss.

Bewachungsfachkräfte im Handel müssen für die Ausübung ihrer Tätigkeit eine nach § 34a der Gewerbeordnung vorgeschriebene Sachkundeprüfung vor der zuständigen Industrie- und Handelskammer ablegen. Der BDD hat zur Hilfestellung bei der Beauftragung von Wach- und Sicherheitsfirmen eine Broschüre "Anforderungsprofil für Bewachungsfachkräfte im Handel" herausgegeben, die auch von unserer Homepage kostenfrei heruntergeladen werden kann.

Sind alle diese Voraussetzungen erfüllt und die notwendigen Informationen bekannt, sollten Auftraggebern und Auftragnehmern das rechtlich abgesicherte Einsatzspektrum und damit die Möglichkeiten und Grenzen der Tätigkeiten bewusst sein, was in vielen Fällen jedoch nicht der Fall ist.

Ein ganz wesentlicher Unterschied zu den Tätigkeiten der Bewachungsfachkräfte im Handel und den klassisch arbeitenden Detektiven besteht darin, dass die Bewachungsfachkräfte in Ausübung des Hausrechts ihres Auftraggebers die Waren bewachen, um Diebstähle aufzudecken oder allein durch ihre Anwesenheit zu verhindern.

Die Aufgabe der Bewachungsfachkräfte beschränkt sich demnach allein auf die Überwachung von Kunden und gegebenenfalls auch von Mitarbeitern im Verkaufsbereich zur Verhinderung von Warendiebstahl aber keinesfalls auf die prophylaktische Observation ein-

zelner Mitarbeiter zum Beispiel im Warenlager, Kassenbereich oder Verkaufsraum.

Letzteres ist bei bestimmten Voraussetzungen beziehungsweise fallbezogen die Aufgabe von klassisch arbeitenden Detektiven. Der Fall Lidl hat aber auch gezeigt, dass die Trennung dieser Aufgaben zwischen den so genannten Kaufhausdetektiven und den Privatdetektiven in der Öffentlichkeit weitgehend unbekannt ist.

Obwohl bei dem Discounter Lidl ausschließlich "Kaufhausdetektive" tätig waren, wurde das gesamte Detektivgewerbe durch eine undifferenzierte Berichterstattung belastet. Aus dem Grund soll die von uns geprägte neue Berufsbezeichnung "Bewachungsfachkraft im Handel" hier auf Sicht mehr Klarheit bringen.

Die gesetzlichen Voraussetzungen für klassisch arbeitende Detektive

Es stellt sich die Frage, welche Voraussetzungen der Gesetzgeber geschaffen hat, um Detektive in die Lage zu versetzen, den fachlichen und persönlichen Anforderungen nachweisbar zu entsprechen. Die Antwort ist kurz und knapp: keine.

In Deutschland gibt es bedauerlicherweise weder eine rechtlich geschützte Berufsbezeichnung noch ein rechtlich verankertes Berufsbild für Detektive. Jeder kann sich durch eine Gewerbeanmeldung und Vorlage eines einfachen Führungszeugnisses sowie eines Auszugs aus dem Gewerbezentralregister "Detektiv", "Wirtschaftsdetektiv", "Privater Ermittler" oder so, wie es ihm auch immer sinnvoll erscheint, nennen und diese Tätigkeit ausüben.

Die Wirtschaft und auch der private Bereich haben also keine rechtlich abgesicherte Grundlage, um zumindest weitgehend vermeiden zu können, dass Aufträge an unseriöse Unternehmen vergeben werden. Fast täglich erreichen den BDD Berichte aufgebrachter Auftraggeber, die an ein unseriöses Unternehmen geraten sind.

Seit dem Zusammenschluss kompetenter Detekteien im BDD im Jahr 1950, hat sich der Gesetzgeber nicht zu der von uns geforderten Regulierung des Detektivberufs durchringen können. Aus dem Grund ergeben sich zwangsläufig folgende Fragen:

- Wie kann man nun sicherstellen, aus den gegenwärtig 1.530 umsatzsteuerpflichtigen Detektivunternehmen in Deutschland ein seriös arbeitendes herauszufinden?

- Welche Rechtskenntnisse kann man dann zum Beispiel im Bereich des Datenschutzes und des Schutzes der Persönlichkeitsrechte erwarten?

- Was bleibt noch zu tun?

Aus gutem Grund fordert der BDD anerkannte Qualitätsstandards

Selbst ich habe seit 1994 viel Zeit, Fleiß und Mühen aufgebracht, um eine öffentlichrechtliche Qualifizierung und Zugangsregeln zu erreichen, aber vergeblich. Solange der Gesetzgeber keine berufliche Regulierung zulässt, bleibt aus meiner Sicht nur noch eine Möglichkeit: Der BDD muss und wird auf der Grundlage seiner Satzung und Ordnungen sowie des Berufsbildungsplans für Detektive anerkannte Qualitätsstandards etablieren.

Wir gehen davon aus, hiermit dann ein Marktregulativ schaffen zu können, an dem sich zukünftig Ausbildungseinrichtungen, die Wirtschaft aber auch der private Bereich und letztendlich die Detekteien selbst orientieren werden.

Wir gehen weiter davon aus, dass die mit Lidl getroffene Vereinbarung den Weg dahingehend öffnet, dass sich auch weitere Unternehmen der Wirtschaft unserer Initiative anschließen werden.

Unabhängig davon, was der BDD fordert, haben wir ohnehin die Messlatte für eine Mitgliedschaft recht hoch angelegt; in der Regel müssen Antragsteller auf Mitgliedschaft im BDD vor der Aufnahme- und Prüfungskommission des Verbandes eine Prüfung ablegen. Darüber hinaus führt der BDD alljährlich ein Fortbildungsseminar für seine Mitglieder durch.

Grundlagen eines jeden Detektivauftrages

Der private Ermittler, wenn er denn seriös arbeitet, wird einen Auftrag nur dann annehmen, wenn der Auftraggeber ein berechtigtes Interesse glaubhaft darlegen kann. Das Gesetz spricht nur von

"berechtigtem Interesse", nicht von "rechtlichem Interesse". Und das mit gutem Grund. Der Auftraggeber wird – von reinen Schikanefällen einmal abgesehen – immer ein irgendwie geartetes rechtlich relevantes Interesse an der Erlangung der begehrten Information haben. Rechtfertigend wirkt dies Interesse aber nur dann, wenn es auch von der Rechtsordnung als berechtigt anerkannt wird.

Das berechtigte Interesse spielt bei der Abwägung, einen Auftrag anzunehmen oder abzulehnen, demzufolge eine große Rolle. Der Detektiv muss in der Lage sein, in der Rechtsgüterabwägung zwischen berechtigten Ansprüchen des Auftraggebers und den zu schützenden Rechten der Mitarbeiter eine Entscheidung zu treffen. Diese Entscheidung muss gegebenenfalls auch vor Gericht der Anerkennung des Beweismaterials standhalten.

Auch gerade im Bereich des Datenschutzes gibt das Bundesdatenschutzgesetz (BDSG) dem Detektiv noch den notwendigen Entscheidungs- und Handlungsspielraum. Eine weitere Beschneidung der gegeben Möglichkeiten wäre fatal und würde das Recht des Täterschutzes über das Recht zur Aufklärung und Beweissicherung stellen.

Darüber hinaus muss ein Detektiv genau wissen, in welchem rechtlichen Rahmen er sich bei der Ausführung seiner Tätigkeiten bewegen darf. Auf illegalem Wege beschafftes Beweismaterial wird bei einer Rechtsgüterabwägung in der Regel vor Gericht ohnehin nicht anerkannt werden.

Zusammenfassend heißt das für jeden seriös arbeitenden Detektiv:

Als schutzwürdiges berechtigtes Interesse kommt jedes öffentliche, private, ideelle oder vermögensrechtliche Interesse in Betracht, das nicht im Widerspruch zu Recht oder Sittengrundsätzen steht und dessen Verfolgung rechtlich schutzwürdig ist. Zu berücksichtigen sind bei detektivischen Recherchen auch stets die Persönlichkeitsrechte des Betroffenen, besonders in den Bereichen

- Individualsphäre
- Privatsphäre
- Intimsphäre.

Zur fachgerechten Ausführung von detektivischen Tätigkeiten bedarf es neben der notwendigen Rechtskenntnis vor allem fundierter

Kenntnisse betriebswirtschaftlicher Abläufe, technischen Verständnisses, um Patentschriften lesen und verstehen zu können, Fachkenntnisse in den Tätigkeitsbereichen des Detektivs, wie zum Beispiel der Ermittlungstechnik und -taktik, Observationstechnik, Kriminologie und Kriminalistik sowie Fachkenntnisse in den Bereichen Technik, Ausrüstung und Berichterstattung, unabhängig vom notwendigen Talent.

Recherchen unter Legende

Häufig wird, um illegale, kriminelle Handlungen aufklären zu können, unter Legende gearbeitet. Solche verdeckten Ermittlungen sind oftmals notwendig und grundsätzlich auch zulässig. Die wahre Identität eines Detektivs darf verschwiegen werden, er darf eine falsche Identität vorspiegeln, wenn dieses für die jeweiligen Ermittlungen notwendig ist.

Das heißt, Detektiven ist durchaus erlaubt, den wahren Anlass eines Gespräches zu verschweigen und den Gesprächspartner zur Sache zu hören, ohne dass der Gesprächspartner den Zusammenhang zum vorliegenden Fall bemerken muss. In solchen Fällen eine Gesprächsstrategie zu entwickeln, die die Wahrheit trifft, ohne den tatsächlichen Grund zu verraten, ist die hohe Schule des Ermittelns. Das sich natürlich ein seriös arbeitender Detektiv stets an den Richtlinien des BDSG orientieren wird, steht völlig außer Frage.

Detektivische Recherchen im Hinblick auf das BDSG

Welche Rechtsgrundlage für die Übermittlung von personenbezogenen Daten bei der Arbeit von Detekteien in Betracht zu ziehen ist, bestimmt sich einzelfall- beziehungsweise auftragsbezogen. Die Verarbeitung erfolgt grundsätzlich im Rahmen der Vorgaben des § 28 BDSG. Da der Geschäftsbetrieb einer Detektei im Regelfall nicht in der reinen gewerbsmäßigen Erhebung und Übermittlung von Daten bestehen wird, kommt § 29 BDSG nur in Ausnahmefällen in Betracht.

Generell wird die Pflicht zur Unterrichtung des Betroffenen über die Datenerhebung in § 4 BDSG geregelt. Die für Detektive wichtige Ausnahmeregelung ist in § 33 Abs. 2 Satz 1 Nr. 3 BDSG nachzulesen, der bekanntlich besagt:

Eine Pflicht zur Benachrichtigung besteht nicht, wenn die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, geheim gehalten werden müssen.

Über die Praxis der Detektivarbeit

Wie probat Detektive tatsächlich für den Einsatz gegen die allgemeine Wirtschaftskriminalität sind, wird letztlich schon dadurch deutlich, dass inzwischen mehr als 80 % der Aufträge, die an Detekteien des BDD vergeben werden, direkt oder indirekt aus der Wirtschaft kommen. Heute werden Detekteien in allen Bereichen der Wirtschaftskriminalität eingesetzt, wie unter anderem bei

- Verletzung des Patentrechts und des Markenschutzes,
- Produkt- und Markenpiraterie, wie dem Herstellen und Inverkehrbringen von Fälschungen und Verfälschungen, beziehungsweise dem Verkauf nichtverkehrsfähiger Ware,
- Parallel- beziehungsweise Grauimporten,
- Reimport von Produkten, die für ein Drittland produziert wurden und in Nacht- und Nebelaktionen wieder nach Deutschland geschafft werden,
- Anlage- und Subventionsbetrug, den es nach Grenzöffnung besonders häufig gab, wenn Gelder zweckentfremdet verwendet werden, oder
- Computer Forensik.

Auch wird in großem Umfang bei dem Verdacht auf Versicherungsbetrug ermittelt (nicht bei Kavaliersdelikten, sondern primär im Großschadenbereich).

Mitarbeiterdelikte

Einen breiten Raum der Beauftragungen von Detekteien nehmen auch die Mitarbeiterdelikte in all ihren Erscheinungsformen ein, die Bestandteil der Thematik dieses Symposiums sind, wie

- Verstöße gegen ein vertraglich bestehendes Wettbewerbsverbot,

- Verrat von Betriebs- und Geschäftsgeheimnissen,

- Know-how-Diebstahl oder auch Diebstahl geistigen Eigentums,

- Betriebssabotage,

- unberechtigte Fehlzeiten,

- Schwarzarbeit,

- Nötigung und Erpressung oder

- Sachbeschädigung, Vandalismus oder Körperverletzung.

Auf Grund der eigenen Erfahrung zählen zu den häufigsten Mitarbeiterdelikten

- der Diebstahl,
- die Korruption,
- die Urkundenfälschung und
- die Unterschlagung beziehungsweise die Untreue.

Es könnten viele Fallbeispiele dieser häufigen Mitarbeiterdelikte vorgetragen werden, die aber den zeitlichen Rahmen sprengen würden.

Die Motive für die allgemeinen Mitarbeiterdelikte sind aus meiner Sicht sicher seltener kriminelle Energie, als eher

- menschliche Schwächen in ihren Vielfältigkeiten,
- übersteigerte materielle Ansprüche (mein Haus, mein Auto, mein Boot),
- persönliche Geltungssucht,
- Spielleidenschaft sowie
- negativer Einfluss von Partnern.

Sucht und Alkoholismus sind die weiteren hauptsächlichen Motive für den Griff in die Kasse, um es einmal symbolisch auszudrücken.

Bei der Betrachtung der allgemeinen Mitarbeiterdelikte wird doch deutlich, dass die bekannten Arbeitsordnungen in den Unternehmen häufig nicht ausreichen, beziehungsweise im Alltag untergehen, anstatt Mitarbeiterdelikte zu verhindern. Aus dem Grund sind vielerorts Präventivmaßnahmen vonnöten:

Dazu zählt zum Beispiel ein gut funktionierendes Kontrollsystem, das ausreichende Funktionstrennungen, Transparenz und nachvollziehbare Arbeitsabläufe beinhaltet. Dies ist unabhängig vom notwendigen 4-Augenprinzip bei bedeutenden Einkaufs- oder Verkaufsverhandlungen. Darüber hinaus sollten im Rahmen regelmäßiger Fortbildungsmaßnahmen die Mitarbeiter stets für ein korrektes, ethisch einwandfreies Verhalten sensibilisiert werden. Führungskräfte, die Entscheidungen treffen und Verantwortung tragen, müssen sich auf ethische Grundsätze stützen können – schon, um der ihnen obliegenden Vorbildfunktion gerecht werden zu können.

Art der Bearbeitung und Voraussetzungen

Die Aufklärung von Wirtschafts- und Mitarbeiterdelikten erfordert natürlich unterschiedliche Bearbeitungsmethoden, die stets dem Erfordernis entsprechend angepasst werden müssen – natürlich unter den bereits erwähnten rechtlichen Rahmenbedingungen.

- **Ermittlungen**

  Je nach Auftragslage können ein genaues Aktenstudium, Datenbankrecherchen, betriebswirtschaftliche Auswertungen, Nutzung aller öffentlich zugänglichen Register, Ermittlungen im geschäftlichen beziehungsweise im nachbarschaftlichen Umfeld oder Ermittlungen bei dem Betroffenen (der Zielperson) erforderlich sein.

- **Observation**

  Für die spätere Beweisführung ist eine Observation in bestimmten Fällen unerlässlich und unterstützend sehr wichtig – in der Regel aber erst, nachdem man Detailkenntnisse durch Ermittlungen erlangt hat, um dann eine Observation gezielt und effektiv einsetzen zu können.

- **Videoüberwachung**

  Wenn ein konkreter Verdacht besteht, beispielsweise auf Diebstahl durch einen Mitarbeiter, ist die Aufklärung oft nur durch eine direkte Überwachung – im Einvernehmen mit dem jeweiligen Betriebsrat – durch eine zeitlich begrenzte Videodokumentation möglich. Sei es zum Beispiel bei dem direkten Griff in eine Kasse, bei dem Lagerdiebstahl oder bei der bereits erwähnten Sabotage.

  Die Aufzeichnungsgeräte sind in solchen Fällen so auszurichten, dass natürlich nur der infrage kommende Bereich videotechnisch abgedeckt wird. Sanitär- und Umkleidebereiche, wie man es aus der Presse entnehmen konnte, sind natürlich tabu. In jedem Fall sind die schutzwürdigen Interessen der Mitarbeiter in vollem Umfang zu berücksichtigen.

- **Taschenkontrolle**

  Es ist sicher allgemein bekannt, dass der Anteil des Waren- und Werkzeugdiebstahls, der durch Betriebsangehörige begangen wird, recht hoch ist. In solchen Fällen sind natürlich sichtbar angebrachte Kameras kein abschreckendes Mittel, weil sie leicht zu umgehen sind.

  Erfahrungsgemäß sind in solchen Fällen sporadische Taschenkotrollen eine geeignete abschreckende Maßnahme, zum Beispiel bei Verwendung eines Drehkreuzes mit Zufallsgenerator. Taschenkontrollen werden im Allgemeinen sogar von der überwiegenden Zahl der Mitarbeiter eines Betriebes begrüßt, damit dadurch die Spreu vom Weizen getrennt werden kann.

- **Einschleusung**

  Eine weitere Möglichkeit, Mitarbeiterdelikte aufzuklären, ist die Einschleusung eines Detektivs in den Betrieb des Auftraggebers, wenn auch hier die zuständigen Entscheidungsträger, wie auch der Betriebsrat, gemeinsam zugestimmt haben.

  Im Fall der Einschleusung in den eigenen Betrieb gelten die gleichen datenschutzrechtlichen Voraussetzungen wie für jeden detektivischen Einsatz. Das heißt, es muss ein berech-

tigtes Interesse des Arbeitgebers vorliegen, das schwerer wiegt, als die schutzwürdigen Interessen des jeweiligen Arbeitnehmers.

Bei der Einschleusung in ein für den Auftraggeber fremdes Unternehmen, muss in der Regel davon ausgegangen werden, dass eine solche unzulässig ist und gegen das BDSG verstößt, also kein rechtlich relevantes Interesse vorliegt und Daten weder erhoben, noch später an den Auftraggeber weitergegeben werden dürfen. Darüber hinaus ist eine solche Einschleusung auch ein Eingriff in das allgemeine Persönlichkeitsrecht der Mitarbeiter und ebenso ein Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb des Mitbewerbers.

Eine andere Bewertung kommt nur in Betracht, wenn erhebliche Straftaten zum Beispiel gegen einen Mitbewerber begangen wurden oder ein besonders hohes öffentliches Interesse vorhanden ist, das dann in besonderer Weise einer Abwägung bedarf.

Ist ein Beschäftigtendatenschutzgesetz wirklich vonnöten?

Die bestehenden Gesetze des Datenschutz- und des Arbeitsrechts bieten insbesondere Arbeitnehmern einen erheblichen umfassenden Schutz, sofern umsichtig nach diesen gehandelt wird.

Wenn nun zum Teil Rechtsunsicherheit besteht und Arbeitnehmer sowie Arbeitgeber nicht wissen sollten, welche ihre Rechte sind, fehlt es aus meiner Sicht an der notwendigen Aufklärung und sicher nicht an einem Beschäftigtendatenschutzgesetz.

Eine gezielte Aufklärungsarbeit ist in jedem Fall einer Überregulierung vorzuziehen, wenngleich eine Überregulierung in unserer Behördenkultur, um nicht Behördendiktatur zu sagen, keine Seltenheit ist.

Vor allem aber sollte bei allem Regulierungseifer vermieden werden, dass Datenschutz zum Täterschutz wird, denn weit sind wir davon ohnehin nicht mehr entfernt. Aufklärung soll doch in jedem Fall gewährleistet sein, damit die vielen illegalen, kriminellen Handlungen die Allgemeinheit und den Fiskus nicht noch mehr belasten.