

# Datenschutz und Arbeitnehmer

## SAP-Fachtagung 2008 SAP im betrieblichen Spannungsfeld

### I. Einleitung:

Sie haben in den vergangenen zwei Tagen viel gehört über SAP und auch über SAP und Datenschutz. Ich will an Ihrem letzten Seminartag heute den Bogen etwas weiter spannen und über den Arbeitnehmerdatenschutz insgesamt sprechen, über die Gefahren, die in der heutigen Arbeitswelt für das Persönlichkeitsrecht jedes Einzelnen bestehen.

Das im Grundgesetz verankerte allgemeine Persönlichkeitsrecht ist die Grundlage des Datenschutzes. Der Datenschutz soll die Würde, Privatsphäre und Handlungsfreiheit der Individuen gewährleisten. Ohne einen geschützten Raum, in dem man unbeobachtet reflektieren und sich mit anderen austauschen kann, kann es keine freie demokratische Gesellschaft geben. Dies gilt auch für die Arbeitswelt. Deshalb ist es das Ziel meines Vortrags, Sie – als Personalrat, als Betriebsrat, als Datenschutzbeauftragter oder schlicht als Arbeitnehmer – zu sensibilisieren für die Gefahren, die bestehen und Ihnen Mut zu machen, durch Dienst- oder Betriebsvereinbarungen, durch persönliches Engagement das Selbstbestimmungsrecht der Beschäftigten über ihre Daten zu schützen und vor mannigfachen Begehrlichkeiten zu verteidigen.

Persönlichkeitsrechte und Datenschutz sind im Arbeitsverhältnis in vielfältiger Weise bedroht:

Während eines Berufslebens sammelt sich über jeden Berufstätigen umfangreiches Datenmaterial bei Arbeitgebern an. Sie erhalten bei der Bewerbung Angaben über Schulbildung, berufliche Ausbildung, bisherige Tätigkeiten etc.. Diese Angaben werden mit der Zeit immer weiter ergänzt, zum Beispiel durch Leistungsbewertungen und Beurteilungen, Gehaltsdaten, Fehlzeiten, Krankmeldungen und Urlaubdaten. Zudem werden mittels Arbeitszeiterfassungssystemen Daten über die An- bzw. Abwesenheit erhoben und in Arbeitszeitkonten erfasst. Digitale Telefonanlagen registrieren die Telefonate, und bei der Nutzung des Internets fallen Daten über E-Mails und das Surfverhalten an. Computer und Kassensysteme ermöglichen die direkte Erfassung von Leistungsparametern – z.B. zu den von einer Schreibkraft eingegebenen Zeichen und zur Fehlerhäufigkeit. Immer mehr Arbeitsplätze werden durch Videokameras überwacht. Außerdem können Controllingverfahren die Leistung und das Verhalten überwachen und bewerten.

Ich könnte hier noch viele Beispiele nennen, aber ich werde im Weiteren noch genauer auf einzelne Bereiche der Gefährdungen eingehen.

Die Gefahr liegt darin, dass informationstechnische Systeme, die eine immer größere Überwachungsichte ermöglichen, schleichend Besitz von unserem beruflichen und privaten Alltag ergriffen haben. Wir sind dabei, uns an immer umfassendere Kontrollen und an permanente Überwachung zu gewöhnen.

Die bislang zielgerichtete Überwachung von Arbeitnehmern wird zunehmend ungezielt und zeitlich und räumlich allgegenwärtig – mit einem Wort: sie wird ubiquitär. Hintergrund dieser Überwachung ist weniger der böse Wille der Arbeitgeber, vielmehr stecken dahinter in der Regel vielfältige andere Zwecke und – ganz banal – die technische Entwicklung. Die Zwecke

liegen vor allem in der Rationalisierung der Betriebsabläufe durch Automation sowie in der Erhöhung der Produktionssicherheit wie allgemein der Sicherheit angesichts neuer Risiken. Auf den Punkt gebracht: Der Einsatz von IT für Kontrollzwecke wird immer billiger, einfacher in der Anwendung, komplexer, intelligenter und vernetzter.

Hierzu möchte ich Ihnen **einige Beispiele** nennen:

## **II. Gefahren für die Persönlichkeitsrechte am einzelnen Arbeitsplatz:**

### **Auf dem Weg zum gläsernen Mitarbeiter:**

Ich will mit einem Beispiel aus den USA beginnen, das zeigt, wohin die Entwicklung bei der Überwachung des Arbeitsalltags im Betrieb auch bei uns führen kann, wenn man nicht rechtzeitig die Notbremse zieht.

Microsoft lässt sich derzeit ein System zur Erfassung der Leistungsfähigkeit von Arbeitnehmern patentieren. Dabei sollen Körperfunktionen permanent gemessen und dauerhaft gespeichert werden. Körperfunktionen eines Menschen verändern sich unter Stress. Beispielsweise bei der stressbeladenen Arbeit am PC. Sensoren, die am Körper des Mitarbeiters befestigt werden und permanent eine Vielzahl von Körperfunktionen messen, sollen künftig für eine bessere Kommunikation zwischen Mensch und Maschine sorgen. Der Softwarekonzern will sich ein komplexes Kommunikations- und Überwachungssystem patentieren lassen. Die Sensoren am Körper des Arbeitnehmers leiten ihre Messdaten per Funk an einen zentralen Rechner weiter. Kameras beobachten jede Geste. Ob jemand lächelt oder seine Stirn in Falten zieht – alles wird erfasst und abgespeichert und wie beim Lügendetektortest mit den jeweiligen Normalwerten des Nutzers abgeglichen.

Weichen die gemessenen Werte von den Durchschnittswerten ab, "weiß" der zentrale Rechner: "Hier gibt es ein Problem!" Dann fragt er nach und bietet dem gestressten Arbeitnehmer automatisch seine Hilfe an. Lässt sich das Problem auf diesem Weg nicht lösen, kann der Überwachungsrechner in seiner Datenbank nach einem anderen Mitarbeiter suchen, der eine ähnliche Aufgabe irgendwann bereits erledigt hat, und bittet ihn um Hilfe. Die Mitarbeiter sollen durch permanente Überwachung entlastet werden und im Ergebnis stressfreier arbeiten. So steht es zumindest im Patentantrag. Doch das ist nur die eine Seite der Medaille. Die andere Seite ist, dass alle Überwachungsdaten in einer zentralen Datenbank gespeichert werden und zu persönlichen Gesundheits- und Leistungsprofilen verarbeitet werden können. Das geplante Kontrollsystem produziert ganz nebenbei, was sich ein jeder Arbeitgeber wünscht: Den gläsernen Mitarbeiter.

In Deutschland kann ein Arbeitgeber nicht nach eigenem Belieben Software zur Überwachung seiner Arbeitnehmer einführen. Unser Betriebsverfassungsgesetz sagt, dass bei der „Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung von Arbeitnehmern zu überwachen“, der Betriebsrat ein zwingendes Mitbestimmungsrecht hat. Und der Betriebsrat wird es sich hierzulande genau überlegen, ob er der totalen Überwachung aller Arbeitnehmer wirklich zustimmt.

### **Gesundheitsdaten im Arbeitsleben:**

Das genannte Beispiel des verkabelten Mitarbeiters hat ja – Gott sei Dank – noch keinen Einzug in unseren Arbeitsalltag gefunden und dazu wird es hoffentlich auch nie kommen. Doch sind die Begehrlichkeiten von Arbeitgebern, möglichst viel über den Gesundheitszustand ihrer Mitarbeiter zu wissen, groß. Dabei ist die Verarbeitung von Gesundheitsdaten datenschutzrechtlich besonders kritisch; für diese Daten gelten rechtlich strengere Maßstäbe als für sons-

tige personenbezogene Daten. Entgegen der gängigen Rechtsprechung durch die Arbeitsgerichte werden allerdings z.B. Bewerberinnen nach wie vor gefragt, ob eine Schwangerschaft vorliege.

Die **Entwicklung in der Gesundheitsforschung** beeinflusst auch den Arbeitnehmerdatenschutz. Neue Diagnosemöglichkeiten und molekulargenetische Untersuchungsmethoden gewinnen zunehmend Bedeutung für das Arbeitsverhältnis. Prädikative Gentests zielen darauf ab, genetische Faktoren zu identifizieren, die zu einem späteren Zeitpunkt mit erhöhter Wahrscheinlichkeit zu einer Erkrankung führen können. Die genetischen Untersuchungen werden heute überwiegend nicht mehr als aufwändige individuelle Labortests durchgeführt, sondern mittels sog. Biochips, die mehrere hundert Gensequenzen in Minutenschnelle auswerten können. Praktische und finanzielle Schranken verlieren so mehr und mehr an Bedeutung für solche Tests. Arbeitgeber sind verständlicherweise daran interessiert, vorzugsweise leistungsfähige und gesunde Arbeitnehmer einzustellen. Schon deshalb wird sich der Druck zur Durchführung genetischer Untersuchungen auf Bewerber verstärken.

Der Arbeitgeber könnte seine Bewerber auf bestimmte Gendefekte testen und so ihre Anfälligkeiten für bestimmte Krankheiten herausfinden, auch wenn dies nach der Rechtsprechung unzulässig ist.

Generell ist es dem Arbeitgeber lediglich gestattet, dem Bewerber Fragen zu stellen, die für den jeweiligen konkreten Arbeitsplatz relevant sind. Soweit dabei der Gesundheitszustand berührt ist, muss sich der Arbeitgeber allerdings auf Fragen nach wesentlichen Beeinträchtigungen der Leistungsfähigkeit oder des Einsatzes des Arbeitnehmers durch akute oder ansteckende Krankheiten oder nach geplanten Operationen beschränken. Das Fragerecht umfasst regelmäßig nicht Angaben zu genetischen Dispositionen. Die Frage eines Betriebsarztes etwa im Rahmen einer Einstellungsuntersuchung nach „schweren Krankheiten bei Familienmitgliedern“ stellt eine simple Form von genetischer Diagnostik dar und braucht nicht beantwortet zu werden.

### **Internet- und E-Mail-Nutzung am Arbeitsplatz:**

Die meisten Beschäftigten haben heute Zugang zum Internet am Arbeitsplatz. Jede E-Mail und jeder Aufruf einer Webseite am Arbeitsplatz hinterlässt Spuren in den betrieblichen IT-Systemen. Während diese Daten bei der häuslichen Nutzung nur beim Anbieter des entsprechenden Dienstes anfallen, erhält beim dienstlichen Surfen zusätzlich der Arbeitgeber Kenntnis vom Surfverhalten – bisweilen mit erheblichen Konsequenzen für den Arbeitnehmer.

Da Unternehmens- und Verwaltungsnetze üblicherweise stärker abgesichert sind als private Systeme, werden hier sogar mehr Daten erfasst und automatisiert ausgewertet. Die Auswertung umfasst bisweilen sogar die Inhalte der Kommunikation. Immer wieder wenden sich Betroffene – häufig zu Recht – an die Datenschutzaufsichtsbehörden, weil sie befürchten, der Chef lese die E-Mails mit. Manchen Arbeitgebern scheint nicht klar zu sein, dass selbst bei **rein dienstlicher Nutzung des Internets** eine lückenlose Überwachung von E-Mails oder dem Surfverhalten nicht zulässig ist, weil damit die ständige Kontrolle des Arbeitnehmers verbunden wäre und eine derartige automatisierte Vollkontrolle als schwerwiegender Eingriff in das Persönlichkeitsrecht der Beschäftigten nicht zulässig ist. Der Arbeitgeber darf aber eine stichprobenhafte und zeitnahe Auswertung der Protokolldaten vornehmen, wobei das Verfahren möglichst transparent zu gestalten ist.

Soweit Beschäftigten **die private Nutzung von Internet und E-Mail** erlaubt ist, sind zudem die Vorgaben des Telekommunikationsrechts zu beachten. So hat der Arbeitgeber das Fernmeldegeheimnis zu wahren, wenn er dem Arbeitnehmer die private Nutzung des betrieblichen

E-Mail-Systems oder auch des Diensttelefons gestattet hat. Die Überwachung wäre dann sogar eine Straftat.

Da der Arbeitgeber ein berechtigtes Interesse daran hat, Missbrauch oder gar strafbare Handlungen nicht nur im dienstlichen Bereich, sondern auch bei der privaten Nutzung des dienstlichen Internet-Zugangs zu unterbinden, kann er die private Nutzung an bestimmte Bedingungen hinsichtlich des Zeitrahmens, der zugelassenen Bereiche und regelmäßig durchzuführender Kontrollen knüpfen. Entsprechende Regelungen sollten in einer Betriebs- bzw. Dienstvereinbarung – am besten mit der Personalvertretung – verbindlich festgelegt werden. Die Beschäftigten sollten die Kenntnisnahme schriftlich bestätigen. Wenn ein Mitarbeiter die erforderlichen und festgelegten Kontrollmaßnahmen nicht akzeptiert, muss er die private Nutzung unterlassen. Es gibt keinen Anspruch, das Internet und die E-Mail privat am Arbeitsplatz nutzen zu können.

Eine Protokollierung darf ohne Einwilligung nur erfolgen, wenn sie zu Zwecken der Datenschutzkontrolle, der Datensicherung, zur Sicherung des ordnungsgemäßen Betriebs oder zu Abrechnungszwecken erforderlich ist. Die Verwendung der Protokolldaten zu anderen Zwecken ist unzulässig.

### **Videüberwachung am Arbeitsplatz:**

Videüberwachung des öffentlichen Raumes oder aber auch in Firmen ist heute weit verbreitet. Sie soll dem Schutz von Objekten vor Vandalismus, Diebstahl oder anderer Eigentumsdelikten oder aber dem Schutz von Personen dienen. In der Regel ist es nicht Sinn und Zweck der Videüberwachung, die Beschäftigten zu beobachten und zu kontrollieren. Doch ist beides oftmals deckungsgleich. So werden in Kreditinstituten oder Parkhäusern, in Kassenbereichen von Warenhäusern oder Museen – quasi nebenbei – auch die Mitarbeiter überwacht. Ob beiläufig oder zielgerichtet bezweckt, für beides gilt, dass die Videoaufzeichnung des Arbeitnehmerverhaltens nur in engen Grenzen zulässig ist.

Unabhängig davon, nach welchen Regeln des Bundesdatenschutzgesetzes (BDSG) die Zulässigkeit einer Videüberwachung zu beurteilen ist, ob nach § 6b BDSG, der die Überwachung öffentlich zugänglicher Räume, also Räumen mit Publikumsverkehr, regelt oder nach den generellen Erhebungs-, Verarbeitungs- und Nutzungstatbeständen des § 28 BDSG: Der zentrale Wertungsmaßstab bei der Beurteilung der Zulässigkeit einer Videüberwachung ist immer die Verhältnismäßigkeit. Die Überwachung muss sich als erforderlich darstellen, d.h. es dürfen keine objektiv zumutbaren Alternativen zur Videüberwachung gegeben sein. Daneben muss auch die Mittel-Zweck-Relation gewahrt sein, d.h. Videüberwachung darf nicht im Zusammenhang mit geringfügigen Verstößen eingesetzt werden, z.B. um ein bestehendes Rauchverbot zu überprüfen.

Wenn eine Videüberwachung von **öffentlich zugänglichen Räumen** aus Sicherheitsbedürfnissen nach § 6b BDSG zulässig ist und dieser Bereich gleichzeitig Arbeitsplätze von Mitarbeitern umfasst – wie z.B. der Bereich einer Bank –, so werden die Mitarbeiter die Videüberwachung als arbeitsplatzimmanent hinnehmen müssen. In diesen Fällen, in denen die Mitarbeiter nicht der eigentliche Beobachtungsgegenstand sind, ist eine Auswertung der Beobachtungsergebnisse zum Zweck einer mitarbeiterbezogenen Leistungs- und Verhaltenskontrolle allerdings unzulässig. So würde die Auswertung der zum Schutz gegen Überfälle gerechtfertigten Videüberwachung einer Bank zwecks Kontrolle des Mitarbeiterverhaltens mit der Datenerhebung und –speicherung unvereinbar sein, während die Videüberwachung in einem Kaufhaus ggf. auch legitimerweise zum Schutz vor Diebstählen durch den Mitarbeiter eingesetzt wird.

Die Zwecke der Überwachung müssen im Vorhinein konkret festgelegt werden, d.h. dokumentiert und in einem Verfahrensverzeichnis jedem Interessierten offengelegt werden (§ 4g Abs. 2 BDSG).

Im Allgemeinen wird Arbeit jedoch nicht in öffentlich zugänglichen Räumen verrichtet, so dass die gesetzlichen Regelungen zur Videoüberwachung für den Arbeitsplatz im Allgemeinen nicht gelten. Hier darf die Videoüberwachung nur eingesetzt werden, wenn sie zur Gewährleistung der Sicherheit erforderlich ist, wobei das Verhältnismäßigkeitsprinzip und die Persönlichkeitsrechte der Beschäftigten berücksichtigt werden müssen. Dabei hat das Bundesarbeitsgericht anerkannt, dass schon die Möglichkeit der jederzeitigen Überwachung einen Druck auf den Arbeitnehmer erzeugt, der mit seinem Anspruch auf Wahrung seiner Persönlichkeitsrechte regelmäßig nicht zu vereinbaren ist. Das Bundesarbeitsgericht zieht daraus den Schluss, dass die Videoüberwachung von Arbeitsplätzen nur durch besondere Sicherheitsinteressen des Arbeitgebers ausnahmsweise gerechtfertigt ist. Generell ist von den folgenden Grundsätzen auszugehen, die sich in der Rechtsprechung entwickelt haben:

- Das einen Eingriff in das Persönlichkeitsrecht rechtfertigende schutzwürdige Interesse des Arbeitgebers, etwa zum Schutz vor Verlust von Firmeneigentum durch Diebstahl etc., muss vor Beginn der Videoüberwachung durch konkrete Anhaltspunkte und Verdachtsmomente belegt sein. Eine vage Vermutung oder ein pauschaler Verdacht gegen alle Beschäftigte reicht nicht aus.
- Eine an sich zulässige Videoüberwachung ist grundsätzlich offen mittels einer sichtbaren Anlage nach vorheriger Information der Belegschaft durchzuführen.
- Eine Überwachung durch verdeckte Kameras ist als „ultimo ratio“ nur zulässig, wenn das die einzige Möglichkeit darstellt, berechtigte schutzwürdige Interessen des Arbeitgebers zu wahren.
- Die Videoüberwachung unterliegt der Mitbestimmung des Betriebsrates oder der Personalvertretung. Zu beachten ist hier jedoch, dass eine an sich unzulässige Videoüberwachung durch die Zustimmung des Betriebs- oder Personalrats nicht legitimiert wird.
- Die durch eine rechtswidrige Überwachung gewonnenen Erkenntnisse unterliegen einem Verwertungsverbot.

### **Chipausweise im Arbeitsalltag:**

In fast allen Bereichen des Arbeitslebens sind heutzutage kontaktlose Betriebs- oder Chipausweise im Einsatz. Sie dienen zum einen der Zeiterfassung, aber oftmals auch zugleich als Zutrittsschlüssel. Ganz nebenbei lassen sich so nicht nur das Kommen und Gehen protokollieren, sondern auch das Betreten und Verlassen einzelner Räume. Über den Karteneinsatz können dabei leicht betriebsinterne Bewegungsprofile der einzelnen Mitarbeiter entstehen. In manchen Unternehmen dient der Ausweis auch als Zahlungsmittel in der Kantine, als Karte für das digitale Signieren von elektronischen Dokumenten oder als Berechtigungskarte für Serviceangebote des Arbeitgebers. Dadurch entstehen in der Kantine Konsumprofile, in Freizeiteinrichtungen Interessenprofile und im Intranet Tätigkeitsprofile.

Gegen die Einführung dieser Systeme ist grundsätzlich nichts einzuwenden. Allerdings ist das zweckfremde Nutzen und Zusammenführen all dieser Daten nicht zulässig – aber möglich. Und der Reiz, diese vorhandenen Daten auch zu nutzen, ist für manch einen Arbeitgeber groß. Bei der Einführung von Chipausweisen sollte daher unbedingt darauf geachtet werden, dass in einer Betriebsvereinbarung/ Dienstvereinbarung die möglichst dezentrale Speicherung der Daten festgelegt wird und detaillierte Zugriffskonzepte geregelt werden.

### **Biometrie am Arbeitsplatz:**

Einen ähnlichen Effekt wie der kontaktlose Chip hat der Einsatz von Biometrie am Arbeitsplatz. Mit Fingerabdruck-, Iris-, Stimm- oder Gesichtserkennung wird das lästige Zücken des Betriebsausweises überflüssig. Zugleich erfolgt eine sichere Identifizierung des Beschäftigten beim Betreten des Arbeitsplatzes, beim Einloggen ins Firmennetz oder beim Betreten eines Sicherheitsbereiches. Auch bei der Bezahlung in Kantinen findet man heute schon Biometriesysteme.

Der Einsatz von Biometrie birgt ähnliche Gefahren wie der kontaktlose Chip. Verstärkt werden diese noch durch eine in der Regel lebenslange Bindung des biometrischen Merkmals an die Person. Es besteht die Gefahr der – evtl. heimlichen – dauerhaften Überwachung, der Ansammlung umfangreicher Datenbestände und der Bildung von Verhaltensprofilen. Des Weiteren können aus den biometrischen Merkmalsdaten sogenannte Überschussinformationen gewonnen werden, das sind z.B. Informationen über Krankheiten, die entweder direkt aus dem biometrischen Merkmal, also z.B. der Iris des Auges, erkannt werden können oder nach der Statistik aller Wahrscheinlichkeit nach auftreten werden.

Aus Datenschutzgesichtspunkten sollte darauf geachtet werden, dass biometrische Merkmale nicht in Datenbanken gespeichert werden, sondern nur auf der Chipkarte.

Eine weitere Anwendung findet sich in der Verknüpfung von Biometrie und Videotechnik. Der Weg eines Mitarbeiters kann bei entsprechender Kameradichte vom Erreichen des Geländes bis zum Verlassen automatisiert und lückenlos verfolgt werden. Personen werden dabei anhand hinterlegter Fotos automatisch identifiziert. Beispiel für die Absicherung durch modernste Zugangstechnik ist eine Großbank in der Schweiz: Der Zugang zum Gebäude einschließlich Tiefgarage sowie die Hauptgänge in der Bank sind videoüberwacht. Bei der Zufahrt in die Tiefgarage werden die Autokennzeichen automatisch gescannt und nach automatisierter Überprüfung wird die Zufahrt freigegeben. Fahrstuhlbenutzung, Etagen- und Bürotüren sowie Zugang zum PC sind biometrisch abgesichert. Die Beschäftigten benötigen weder Schlüssel noch Pin's oder Passwörter.

Man kann sich hier so einiges an Datenmissbrauchsmöglichkeiten vorstellen. In diesem Fall war Grundlage für die Installation allerdings ein detailliertes Datenschutz- und Datensicherheitskonzept und eine direkte Einbindung der Mitarbeitervertretung bei allen Entscheidungen die Technik betreffend.

Mit diesen Beispielen will ich es bewenden lassen. Ich hoffe, es ist mir gelungen, Ihnen einige der besonders gravierenden Gefährdungen plastisch darzulegen. Hier sind Sie, meine Damen und Herren, gefordert, die Persönlichkeitsrechte der Beschäftigten zu schützen.

### **III. Personaldatenflüsse im Konzern – national und international:**

Personaldaten werden heutzutage automatisiert verarbeitet und können per Knopfdruck in die ganze Welt versandt werden. Sie können sich vorstellen, meine Damen und Herren, dass für dieses Szenario dringend datenschutzrechtliche Grenzen eingehalten werden müssen.

#### **Personaldatenübermittlungen im Konzern - national:**

In großen Konzernen finden oft Datenflüsse von Mitarbeiterdaten statt. Dabei geht es in der Regel um den Zugriff des Mutterkonzerns auf Daten der Töchter, um eine konzernweite einheitliche Personalverwaltung oder auch um den konzernweiten Zugriff auf die Mitarbeiterdaten im Rahmen von konzernumfassenden Personaldatenpools.

Das Datenschutzrecht kennt das Phänomen der Unternehmensverflechtungen nicht. Es gibt aus datenschutzrechtlicher Sicht grundsätzlich kein Konzernprivileg. Das hat nachhaltige Auswirkungen auf Unternehmen, die zwar rechtlich selbständig, wirtschaftlich aber mehr oder weniger eng miteinander verbunden sind. Die rechtlich selbständigen Unternehmen innerhalb eines Konzerns sind im Verhältnis zueinander eigenständige Dritte. Jede Datenweitergabe ist daher eine Datenübermittlung an Dritte, auch wenn sie den Beteiligten noch so sehr als interne Angelegenheit vorkommt. Dies gilt natürlich auch für Arbeitnehmerdaten, mag der Konzern auch eine konzerneinheitliche Personalpolitik anstreben.

Wenn die Konzernmutter die gesamte Personalverwaltung für alle selbstständigen Konzerntöchter eigenverantwortlich erledigen will, hat das zur Konsequenz, dass die gesetzlichen Voraussetzungen für eine Übermittlung von Daten an Dritte eingehalten werden müssen:

- Zum einen ist der Datenfluss zulässig, wenn der Beschäftigte seine **Einwilligung** erteilt (§ 4 Abs. 1 BDSG).
- Zum anderen können die Daten weitergegeben werden, wenn es der **Zweckbestimmung des Vertragsverhältnisses** dient (§ 28 Abs. 1 S. 1 Nr. 1 BDSG). Der Zweck des jeweiligen Arbeitsverhältnisses bestimmt hier die Verarbeitungsgrenzen. Wenn der Arbeitsvertrag dem Arbeitgeber z.B. auch den Einsatz des Mitarbeiters in anderen konzernangehörigen Firmen gestattet, wäre es auch zulässig, die für die entsprechende Personalentscheidung maßgebenden Personaldaten zu der „Ersatzfirma“ oder in den „Human-Resources-Datenpool“ zu übermitteln. Dies diene dann der Zweckbestimmung des Arbeitsverhältnisses.
- Eine Übermittlung könnte auch zur **Wahrung berechtigter Interessen der verantwortlichen Stelle** zulässig sein (§ 28 Abs. 1 S. 1 Nr. 2 BDSG). Hier kann es jedoch nicht darum gehen, durch die Hintertür ein Konzernprivileg einzuführen. Es reicht also nicht der Wunsch nach einer konzernweiten Personalsteuerung, um Personaldaten zwischen den Töchtern und dem Mutterkonzern zu transferieren. Das geforderte „berechtigte“ Interesse muss mehr beinhalten und ist immer auch in Bezug zu setzen zu dem Schutzinteresse des Beschäftigten an der Vertraulichkeit seiner Daten. Bei der Abwägung können besondere Verträge und Konzernregelungen eine Rolle spielen. Dann, wenn das datenempfangende Konzernunternehmen Befugnisse und Funktionen erhält, die an sich nur dem direkten Arbeitgeber zustehen, z.B. bei der Zentralisierung der Personalverwaltung in einem Konzern, kann die Übermittlung gerechtfertigt sein, wenn die beteiligten Konzernunternehmen besondere Maßnahmen zugunsten der Beschäftigten treffen, so dass das Ergebnis der Abwägung doch noch zugunsten der berechtigten Interessen des Konzernunternehmens ausfällt. Welche Maßnahmen das sein können, muss im Einzelfall entschieden werden. In Betracht kommt z.B. ein konzernweites Datenschutzkonzept, das einheitliche Standards zur Gewährleistung und Durchsetzung der Datenschutzrechte der Betroffenen fest-schreibt. Der Verarbeitungsverlauf muss für die betroffenen Beschäftigten transparent sein. Nach Auffassung der Datenschutzaufsichtsbehörden muss vor allem die durch die Übermittlung herbeigeführte Diversifizierung der Verantwortlichkeiten dadurch kompensiert werden, dass der Arbeitgeber umfassend Ansprechpartner für den Arbeitnehmer bleibt, d.h. auch für die Erfüllung seiner Rechte auf Auskunft, Löschung, Berichtigung und Sperrung seiner Daten und das zusätzlich zu denjenigen Unternehmen, an welche die Daten übermittelt wurden.

Regelung durch Betriebsvereinbarung:

Da die konzerninternen Datenflüsse regelmäßig auf der Grundlage automatisierter Datenverarbeitung erfolgen, unterliegen sie der Mitbestimmung nach dem BetrVG (§ 87 Abs. 1 Nr. 6). Auf Grund ihres normativen Charakters stellen Konzern, Gesamt- oder Betriebsvereinbarungen zwischen Arbeitgebern und Betriebsräten formal gesehen Rechtsvorschriften i. S. des BDSG dar und können damit Erlaubnisnormen für eine Datenverarbeitung sein. Dabei müssen sie sich aber auch, wenn sie einen konzerninternen Datenfluss legitimieren wollen, an die Grundsätze des Datenschutzes halten. Sie dürfen zwar vom BDSG abweichen, doch nur insoweit, wie sie die dort getroffenen Regelungen durch Schutzverordnungen ersetzen, die den im jeweiligen Unternehmen spezifischen Beschäftigungsbedingungen besser angepasst sind, allerdings mindestens auch so weitreichend sind. Sie dürfen, wenn sie eine Datenverarbeitung wirksam legitimieren wollen, das durch das BDSG gewährleistete Schutzniveau nicht unterschreiten.

#### Personaldatenfluss im Rahmen einer Auftragsdatenverarbeitung:

Die vorgenannten Ausführungen zu § 28 BDSG sind dann nicht relevant, wenn es sich um eine Auftragsdatenverarbeitung handelt.

Eine Auftragsdatenverarbeitung wird für die Fälle angenommen, in denen die technische Abwicklung der Datenverarbeitung auf einen Dritten – den Auftragnehmer – übertragen wird, während die inhaltliche Verantwortung für die Aufgabenerfüllung beim Auftraggeber verbleibt.

Die Auftragsdatenverarbeitung hat für den Konzern den Vorteil, dass es sich bei den Datenflüssen nicht um Übermittlungen handelt, sondern um eine quasi „interne Angelegenheit“. Konzerne machen daher gerne Gebrauch. Betreibt ein Konzernunternehmen z.B. ausschließlich die Datenverarbeitung für die übrigen Konzernfirmen als Dienstleistungsunternehmen, so wird das als Auftragsdatenverarbeitung qualifiziert.

Für das Unternehmen ist diese Rechtsform allerdings nicht immer von Vorteil und vor allem datenschutzrechtlich nicht so regelfrei, wie das oft angenommen wird. So hat eine Auftragsdatenverarbeitung etwa zur Konsequenz, dass der Auftragnehmer bei der Verarbeitung bestimmte Grenzen beachten muss und der Auftraggeber den Auftragnehmer kontrollieren können muss.

Wenn in einem Konzern etwa das Mutterunternehmen für die angeschlossenen Töchter eine zentrale Personalverwaltung im Sinne einer Auftragsdatenverarbeitung betreiben will, müsste sichergestellt sein, dass die Töchter den Mutterkonzern bei dieser Verarbeitung kontrollieren können, da die Tochterunternehmen die eigentlich Verantwortlichen für die Personaldaten ihrer Beschäftigten sind. Dies dürfte in der Praxis bereits wegen des Machtgefälles kaum vorstellbar sein. Auch müssten die jeweiligen betrieblichen Datenschutzbeauftragten der Tochterkonzerne die Einhaltung der Vorschriften des Datenschutzes beim Mutterkonzern sicherstellen. Dies bedeutet, dass die betrieblichen Datenschutzbeauftragten bei der Auswahl eines Auftragnehmers und bei der Auftragsvergabe regelmäßig unter Datensicherungsgesichtspunkten zu beteiligen wären und über eine Aufstellung der verschiedenen Auftragsdatenverarbeitungsverträge ihres Unternehmens verfügen bzw. davon in anderer Weise unmittelbar Kenntnis erlangen können müssten.

Entsprechendes würde sich aus den Kontroll- und Unterrichtsrechten der Mitarbeitervertretung ergeben, die auch im Falle der Auftragsdatenverarbeitung von Personaldaten bestehen und vom Arbeitgeber gegenüber dem Auftragnehmer gewährleistet werden müssen (§ 80 Abs. 1 Nr. 1 und Abs. 2 BetrVG bzw. § 68 Abs. 1 Nr. 1 und Abs. 2 BPersVG).

Alternativ könnte man sich für den Bereich der Personalverwaltung vorstellen, dass die jeweiligen Arbeitsverträge direkt mit der datenverarbeitenden Stelle (also in unserem Beispiel dem Mutterkonzern) geschlossen werden. Dies hat dann allerdings auch unter Umständen weitreichende Folgen im Falle von Kündigungen etc.. Vertragspartner des Beschäftigten wäre in diesem Fall nicht das selbstständige Tochterunternehmen, sondern allein der Mutterkonzern.

### **Datenflüsse in Unternehmen im Rahmen von Personalinformationssystemen – Beispiel Skill - Datenbank:**

Fast alle Unternehmen benutzen heute automatisierte Systeme für die Verwaltung ihrer Personaldaten. Durch derartige Systeme wird das Verhalten der Beschäftigten immer lückenloser registriert, bisweilen sogar, ohne dass die Betroffenen dies merken.

In sog. Skill – Datenbanken werden Kenntnisse, Erfahrungen und Kompetenzen von Mitarbeitern, z.T. konzernweit, verwaltet. Sie werden zu unterschiedlichen Zwecken erstellt. Teilweise dienen sie der optimalen Rekrutierung von Führungskräften oder generell der Vergabe von Beförderungstellen im Konzern. Sie dienen auch dazu, mit wenig zeitlichem und finanziellem Aufwand den richtigen Mitarbeiter an für den Konzern optimaler Stelle zu platzieren oder geeignete Projektteams zu bilden. Die Anliegen sind aus Sicht der Unternehmen verständlich, doch darf es nicht dazu kommen, dass hierdurch gläserne Mitarbeiter geschaffen werden und anhand der Skill–Profile interne und externe Leistungsbeurteilungen getroffen werden.

Es ist immer im Auge zu behalten, dass Mitarbeiterqualifikationen, insbesondere wenn sie in sehr detaillierter Form vorliegen, hochsensible Informationen sind und daher einen besonderen Schutz erfordern. Am datenschutzfreundlichsten sind Systeme, die auf Freiwilligkeit beruhen. Besonders zu begrüßen sind dabei Datenbanken, in denen die Mitarbeiter sich selber ein Profil anlegen unter Nutzung von Parametern, die vom Unternehmen vorgegeben werden. Sie verwalten ihre Profile selber, aktualisieren, berichtigen, löschen oder sperren ihre Profildaten mit der Konsequenz, dass sie beim Sperren ihres Profils bei der weiteren Suche nach geeigneten Personen für die Besetzung von Stellen oder Projekten nicht mehr berücksichtigt werden.

Bei nicht freiwilliger Aufnahme in derartige Tools hängt es vom Einzelfall ab, was zulässig ist und was nicht. Sollen Skill – Datenbanken verwendet werden, um potentiellen Kunden die Qualifikation der Mitarbeiter nachzuweisen, kommt grundsätzlich nur die Übermittlung solcher Daten in Betracht, aus denen der Kunde keine Rückschlüsse auf die Identität des Mitarbeiters ziehen kann.

### **Personaldatenfluss bei international agierenden Unternehmen:**

Noch schwieriger zu realisieren ist der Datenschutz in international agierenden Unternehmen. Wenn etwa die Gehaltsabrechnung für die Mitarbeiter einer deutschen Niederlassung in Singapur erstellt wird, die Arbeitnehmerdaten auf einem Computer in Indien gespeichert werden oder der E-Mail Server der Firma in San Francisco betrieben wird.

Angesichts der dramatisch gesunkenen Übertragungskosten spielt es wirtschaftlich so gut wie keine Rolle mehr, wo die Datenverarbeitung stattfindet. Die elektronische Datenverarbeitung hat eine weltweite Dimension erreicht. Den Arbeitnehmern sind diese Dimensionen in aller Regel nicht bewusst. Unbeschadet der sinkenden technischen Schwellen und der praktisch zu vernachlässigenden Übertragungskosten hat es allerdings erhebliche datenschutzrechtliche Konsequenzen, wo die Datenverarbeitung stattfindet.

### Konzernproblematik:

Besonders zu beachten ist auch bei transnational agierenden Unternehmen, dass es **kein Konzernprivileg** gibt. Auch konzernweit geltende Unternehmensregelungen ändern daran nichts. Der Datenaustausch zwischen selbstständigen Töchtern und dem Mutterkonzern ist eine Übermittlung von Daten. Im grenzüberschreitenden Datenverkehr ist danach zu unterscheiden, ob es sich um eine Datenübermittlung innerhalb des Europäischen Binnenmarktes oder in Drittstaaten handelt.

### Datenübermittlung innerhalb des europäischen Binnenmarktes:

Innerhalb der Mitgliedstaaten der Europäischen Union existiert ein vergleichbar hohes Datenschutzniveau, so dass es letztlich für den Betroffenen nicht entscheidend ist, ob seine Gehaltsdaten in Berlin, Warschau oder Lissabon verarbeitet werden. Datenübermittlungen innerhalb des europäischen Binnenmarktes sind unter denselben Voraussetzungen zulässig wie Übermittlungen im Inland.

### Datenübermittlung in Drittstaaten:

Für die Frage, ob eine Datenübermittlung in ein Drittland zulässig ist, kommt es entscheidend darauf an, ob bei der empfangenden Stelle im Drittland ein angemessenes Datenschutzniveau gewährleistet ist. Bisher hat die Europäische Kommission lediglich für einige wenige Länder wie Kanada, die Schweiz oder Argentinien entsprechende Feststellungen getroffen. Für den Rest der Welt muss im Einzelfall geprüft werden, ob ausnahmsweise trotzdem ein angemessenes Schutzniveau angenommen werden kann. Hierfür gibt es gesetzlich geregelte Ausnahmetatbestände (§4c BDSG):

### Angemessenes Schutzniveau – Ausnahmen:

1. Ein Tatbestand des gesetzlichen Ausnahmekatalogs ist die **Einwilligung** des Betroffenen (§4 c Abs. 1 Nr. 1 BDSG)
2. Die Übermittlung kann auch dann zulässig sein, wenn die an dem Datenfluss beteiligten Stellen bestimmte **Standardvertragsklauseln ohne Änderungen** verwenden. Diese Standardvertragsklauseln enthalten rechtlich durchsetzbare Verpflichtungserklärungen und darauf gegründete Garantien des Datenexporteurs und des Datenimporteurs und gleichzeitig Schutzgarantien für die Betroffenen. Ihre Anerkennung als ausreichende Garantien ist nach Art. 26 Abs. 4 der EG-Datenschutzrichtlinie allein der Europäischen Kommission vorbehalten. Die Standardvertragsklauseln können von allen Unternehmen verwendet werden. Es bedarf dann keiner zusätzlichen Genehmigung mehr, wenn sie unverändert vom Unternehmen übernommen werden.
3. Das BDSG sieht darüber hinaus die Möglichkeit einer **Ausnahmegenehmigung durch die zuständige Datenschutzaufsichtsbehörde** vor (§ 4c Abs. 2 BDSG). Die Erteilung einer solchen Genehmigung kann erfolgen, wenn die verantwortliche Stelle ausreichende Garantien zugunsten des Betroffenen vorweist. Als Grundlage solcher ausreichender Garantien nennt das Gesetz Vertragsklauseln oder verbindliche Unternehmensregelungen.

- Vertragsklauseln:

Unter Vertragsklauseln versteht das BDSG allein die von der verantwortlichen Stelle selbst erstellten Vertragsklauseln, nicht dagegen Standardvertragsklauseln nach Art. 26 Abs. 4. der EG-Richtlinie. Solche vertraglichen Verpflichtungen sind nur dann ausreichende Garantien, wenn der durch sie verbürgte Schutz des Betroffenen nach Abschluss des Vertrages nicht mehr zur Disposition der Stellen steht, die die Daten übermitteln und sie empfangen.

- Verbindliche Unternehmensregelungen:

Mit der Einführung verbindlicher Unternehmensregelungen trägt das Gesetz der Situation Rechnung, dass Teilunternehmen international tätiger Unternehmen in Ländern ohne angemessenes Datenschutzniveau operieren und dabei das Verhältnis der Teilunternehmen untereinander nicht von Vertragsklauseln bestimmt wird. Als Antwort hierauf gehen internationale Konzerne zunehmend dazu über, für alle Teilunternehmen standortunabhängig verbindliche Verhaltenskodizes auf den Gebieten des Datenschutzes und der Datensicherheit zu erlassen.

Verbindliche Unternehmensregelungen oder – entsprechend der inzwischen auf EU-Ebene eingebürgerten englischsprachigen Bezeichnung – **Binding Corporate Rules (BCR)** stellen grundsätzlich einen Unterfall vertraglicher Vereinbarungen dar.

Für die Ausgestaltung solcher Unternehmensregelungen ist ausschlaggebend, dass sie in einer rechtlich verbindlichen, alle Konzernunternehmen und Unternehmens-teile gleichermaßen verpflichtenden Weise beschlossen werden und dass dies nach innen in Form von Handlungsanweisungen der jeweiligen Arbeitgeber gegenüber allen Arbeitnehmern umgesetzt wird, beispielsweise mithilfe einer Betriebsvereinbarung.

Die sog. Artikel 29-Gruppe – eine internationale Datenschutzgruppe, die die Europäische Kommission berät – hat sich mehrfach mit diesem Thema beschäftigt.

Im Jahre 2005 wurden zwei Arbeitspapiere erstellt, die europaweit von den Datenschutzbehörden als Hilfsmittel genutzt werden können. Zum einen wurde eine Muster-Checkliste für Anträge auf Genehmigung von Datenübermittlungen in Drittstaaten erstellt (WP 108 vom 14. April 2005). Den Unternehmen wird darin erläutert, welche Unterlagen in der Regel hierfür bei der zuständigen Datenschutzaufsichtsbehörde vorzulegen sind. In einem weiteren Arbeitspapier wurde ein Verfahren zur Kooperation innerhalb Europas zur Anerkennung von BCR festgelegt (WP 107 vom 14. April 2005). Da die Verfahrensweise sich in der Praxis als kompliziert und zeitaufwändig erwiesen hat, hat die Artikel 29-Gruppe Empfehlungen für ein Standardantragsverfahren erarbeitet, um ein vereinfachtes Verfahren wie bei den Standardvertragsklauseln zu erreichen (WP 133 vom 10. Januar 2007).

*(Die Papiere finden Sie auf der Homepage der EU-Kommission [http://ec.europa.eu/justice\\_home/fsj/privacy/index\\_de.htm](http://ec.europa.eu/justice_home/fsj/privacy/index_de.htm)).*

### Sondersituation Vereinigte Staaten von Amerika:

Die Vereinigten Staaten von Amerika gehören eigentlich auch zu den Staaten ohne angemessenes Datenschutzniveau. Die EU hat allerdings mit den Vereinigten Staaten eine besondere

Abmachung über einen sog. "sicheren Hafen" (Safe Harbour Agreement) getroffen. Bei Unternehmen, die sich zur Einhaltung der im Abkommen festgelegten Prinzipien bekennen und ihre Praxis entsprechend überprüfen lassen, wird ein angemessenes Datenschutzniveau angenommen. Die Einhaltung der Verpflichtung wird durch unabhängige Wirtschaftsprüfungsgesellschaften kontrolliert, und Verstöße können durch die Federal Trade Commission des US-Handelsministeriums mit erheblichen Bußgeldern geahndet werden. Ein wesentliches Manko des Safe-Harbour-Systems besteht allerdings darin, dass wichtige Branchen nicht in den Anwendungsbereich des Abkommens fallen, wie etwa die Banken und die Telekommunikationsunternehmen.

#### Auftragsdatenverarbeitung im internationalen Bereich:

Aktuell gewinnt die Frage an Bedeutung, wie beim „Outsourcing“ der Datenverarbeitung, also bei der Vergabe der Erfassung, Speicherung und Auswertung personenbezogener Daten an externe Firmen, der Datenschutz gewährleistet werden kann. Soweit die Datenverarbeitung nur innerhalb der Europäischen Union vergeben werden soll, ist dies datenschutzrechtlich unproblematisch. Anders sieht es allerdings beim Outsourcing in die sog. Drittstaaten aus. So bemühen sich derzeit viele datenschutzrechtlich weniger entwickelte Staaten um Datenverarbeitungsaufträge europäischer Unternehmen. Theoretisch besteht hier zwar die Möglichkeit, die Outsourcing - Partner vertraglich auf die Gewährleistung des Datenschutzes zu verpflichten; allerdings bleibt fraglich, wie die Einhaltung dieser Verpflichtungen effektiv kontrolliert werden soll.

#### IV. Regelungen zum Arbeitnehmerdatenschutz:

Es gibt bis heute bedauerlicherweise keine speziellen gesetzlichen Regelungen zum Arbeitnehmerdatenschutz. Arbeitnehmer und Arbeitgeber sind daher im Wesentlichen darauf angewiesen, sich an der lückenhaften und im Einzelfall für die Betroffenen nur schwer zu erschließenden einschlägigen Rechtsprechung zu orientieren.

Auch der Ansatz der Einwilligung – ein ansonsten durchaus sinnvoller Ansatz, der die Datenverarbeitung außerhalb gesetzlicher Regelungen nur zulässt, wenn der Betroffene eingewilligt hat – ist im Arbeitsverhältnis nur sehr eingeschränkt sinnvoll. Eine Einwilligung nach dem Bundesdatenschutzgesetz setzt eine freie Entscheidung voraus. Wegen seiner Abhängigkeit kann der Arbeitnehmer jedoch im Regelfall nicht wirklich frei von Zwang entscheiden. Welcher Arbeitnehmer wird sich in der heutigen Zeit der hohen Arbeitslosenzahlen schon seinem Chef entgegenstellen, um seine Privatsphäre zu schützen. Im Regelfall wird die Furcht vor Repressalien hier größer sein. Ein anderer Aspekt ist der, dass der Arbeitnehmer die Tragweite seiner Einwilligung zur Nutzung eines neuen informationstechnischen Systems, einer Software oder eines neuen Verfahrens oftmals gar nicht erkennt. Ihm ist gar nicht bewusst, dass hier sein informationelles Selbstbestimmungsrecht tangiert wird. Welcher Beschäftigte weiß schon Bescheid über die genauen Datenflüsse bei der Einführung und dem Betrieb von Personalverwaltungssystemen oder Personalinformationssystemen oder beim Einsatz von Videotechnik am Arbeitsplatz und die damit verbundenen Risiken für die Persönlichkeitsrechte.

Hier sind die Interessenvertretungen eines Unternehmens gefragt. Die Einführung automatisierter Systeme unterliegt in weiten Bereichen der Mitbestimmung des Betriebs- oder Personalrats. Das Betriebsverfassungsgesetz verpflichtet Arbeitgeber und Betriebsrat, „die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern“. Hierzu gehört auch das Recht auf informationelle Selbstbestimmung.

Mitbestimmungsrechte bestehen etwa, wenn eine Einrichtung eingeführt wird, mit der sich das Verhalten oder die Leistung der Mitarbeiter kontrollieren oder messen lässt. Die Möglichkeit der Verhaltens- oder Leistungskontrolle muss dabei nicht der eigentliche Sinn und Zweck der Einführung des Verfahrens sein; es reicht aus, dass – sozusagen als Nebenprodukt – eine solche Verhaltens- oder Leistungskontrolle ermöglicht wird. So müssen Betriebs- oder Personalräte zustimmen, wenn Arbeitnehmer das Internet nutzen sollen und wenn ein System zur Kommunikation mittels E-Mail oder ein Controllingssystem eingeführt wird. Für die Einführung solcher Systeme sind Regelwerke zu erstellen, die ausführlich beschreiben, wie die Systeme zu nutzen sind und welche Konsequenzen ein Missbrauch zur Folge hat.

In vielen Unternehmen achten die Arbeitnehmervertretungen mit Argusaugen auf die Gewährleistung des Arbeitnehmerdatenschutzes. Diese Kontrolle entfällt aber regelmäßig, wenn ein Betrieb wegen seiner geringen Größe oder aus anderen Gründen keinen Betriebsrat hat. Auch betriebliche Datenschutzbeauftragte leisten wertvolle Hilfestellung. In manchen Unternehmen fehlt allerdings auch diese unternehmensinterne Kontrollinstanz, sei es, weil die Voraussetzungen für die Bestellung eines Datenschutzbeauftragten nicht gegeben sind (§ 4f BDSG), sei es, weil ein solcher entgegen den gesetzlichen Vorgaben nicht ernannt worden ist. In diesen Fällen sind die Beschäftigten darauf angewiesen, den Beteuerungen der Unternehmensleitung zu glauben. Zwar kann sich jedermann an die zuständige Datenschutzaufsichtsbehörde wenden, falls er vermutet, dass gegen Datenschutzbestimmungen verstoßen wird. Im betrieblichen Alltag sind allerdings – wohl aus der verständlichen Angst vor Repressalien – nur wenige Mitarbeiter zu diesem Schritt bereit.

Um den Schutz der informationellen Selbstbestimmung und damit der Persönlichkeit eines jeden Beschäftigten im Arbeitsleben nicht von all diesen Unwägbarkeiten abhängig zu machen, fordern Datenschützer und Gewerkschaften seit vielen Jahren gesetzliche Regelungen zum Arbeitnehmerdatenschutz. Angesichts stetig wachsender technischer Möglichkeiten muss klar geregelt werden, welche Daten Unternehmen über ihre Beschäftigten erheben dürfen, wie sie damit verfahren müssen und wozu sie die Daten nutzen dürfen. Die Achtung des Grundrechts auf informationelle Selbstbestimmung der Arbeitnehmer zählt ebenso zu guten und fairen Arbeitsbedingungen wie Chancengleichheit oder gerechte Bezahlung. Beschäftigtendatenschutz erhöht zudem die Motivation, trägt und fördert die Arbeitszufriedenheit und bedeutet damit auch für die Unternehmen einen nicht zu unterschätzenden Standortvorteil.

Obwohl der Deutsche Bundestag entsprechende Forderungen wiederholt mit großen, fraktionsübergreifenden Mehrheiten unterstützt hat, haben die verschiedenen Bundesregierungen – von schwarz-gelb über rot-grün bis zu schwarz-rot – bislang keine erkennbaren Aktivitäten auf diesem Gebiet entwickelt. In ihrer Stellungnahme zu meinem letzten Tätigkeitsbericht hat sich die Bundesregierung dahingehend geäußert, dass sie die Auffassung des BfDI, ein Gesetz zum Schutze der Arbeitnehmerdaten sei notwendig, teile. „Allerdings solle vor einer nationalen Kodifikation die weitere Entwicklung in Europa bei der Schaffung des harmonisierten Gemeinschaftsrahmens zum Arbeitnehmerdatenschutz abgewartet werden.“

Leider kommen auch auf europäischer Ebene die bereits vor Jahren begonnenen Vorarbeiten für eine europäische Arbeitnehmerdatenschutzrichtlinie nicht voran. Auf meine Anfrage in Brüssel in der letzten Woche nach dem Stand einer europäischen Gesetzgebung auf dem Gebiet des Arbeitnehmerdatenschutzes bekam ich von der zuständigen Stelle die Antwort: „It is a thing on which we speak a lot but we never see.“ Die europäische Kommission, Generaldirektion Beschäftigung, arbeite nicht länger an einem Entwurfsvorschlag, der bereits vor einiger Zeit wieder aus dem Legislativprogramm genommen worden sei.

Ich glaube, ich muss diese Aussagen nicht weiter kommentieren. Die Aussichten für einen verbesserten Arbeitnehmerdatenschutz, gestützt auf gesetzliche Regelungen, sehen in naher Zukunft schlecht aus.

Da die technologische Entwicklung und deren Einzug in die Arbeitswelt mit all ihren Risiken und Gefahren für den Datenschutz des Einzelnen nicht halt machen wird, ist es umso wichtiger, dass die Interessenvertretungen hier für die Arbeitnehmer ihre Stimme erheben und im Rahmen ihrer Möglichkeiten aktiv werden. Der Bundesdatenschutzbeauftragte und die Kollegen aus den Ländern werden Sie hierin nach Kräften unterstützen.