Die Kritik an dieser Regelung wiegt schwer. Es kann füglich bezweifelt werden, ob durch die Möglichkeit der Arbeit nach der Berufsschule die Betriebe, etwa im Handwerk, bereit sein werden, die Zahl der Ausbildungsplätze zu vermehren. Kein Zweifel besteht aber, daß durch die Arbeit nach dem Berufsschultag die schulische Bildung erheblich beeinträchtigt wird. Im dualen Ausbildungssystem wird die Ausbildung in der Berufsschule in den Hintergrund gedrängt und etwa häusliche Nacharbeit im Anschluß an den Berufsschulunterricht, wenn das Gelernte noch frisch im Gedächtnis haftet, wird praktisch unmöglich gemacht. Soweit Arbeitgeber vermehrt von dieser Möglichkeit Gebrauch machen sollten, wird dies insgesamt auf die Qualität des Berufsschulunterrichts durchschlagen, da wie erwähnt, mehr als 70 % der Berufsschulpflichtigen über 18 Jahre alt sind.

Auch die betrieblichen Verwerfungen dürfen nicht unterschätzt werden, wenn künftig in den Betrieben „unterschiedliches Recht" für jüngere und ältere Berufsschulpflichtige besteht.

Abhilfe können hier, jedenfalls in größeren Betrieben mit Betriebsrat, Betriebsabsprachen oder **Betriebsvereinbarungen** schaffen, wenn diese Regelungen vorsehen, auch Ältere nach dem Berufsschulunterricht von der Arbeitspflicht zu befreien. Unter Umständen muß aber z. B. bei einer Betriebsvereinbarung gemäß § 87 Abs. 1 Nr. 2 BetrVG die ausfallende Arbeitszeit auf andere Tage verlegt werden. Lediglich die tatsächliche Berufsschulzeit wird nämlich nach § 7 BBiG auf die Arbeitszeit angerechnet.

Beschäftigungsverbot bei gefährlichen Arbeiten

Neu gefaßt wurden die Regelungen über Beschäftigungsverbote bei gefährlichen Arbeiten in § 22 JArbSchG. Der Katalog bezieht sich insbesondere auf Arbeiten, die mit Unfall- oder Gesundheitsgefahren verbunden sind oder die die physische oder psychische Leistungsfähigkeit der Jugendlichen übersteigen oder bei denen man schädlichen Einwirkungen bestimmter Arbeitsstoffe ausgesetzt ist.

Beurteilung der Arbeitsbedingungen

Neu eingefügt wurde eine sinnvolle Regelung, wonach vor Beginn der Beschäftigung und bei wesentlicher Änderung der Arbeitsbedingungen der **Arbeitgeber verpflichtet** ist, zunächst die mit der Beschäftigung verbundenen **Gefährdungen** zu beurteilen, wie § 28 a JArbSchG nunmehr bestimmt. Ferner sind dann die Jugendlichen nicht nur bei Beginn der Beschäftigung, sondern auch bei wesentlicher Änderung der Arbeitsbedingungen über die Unfall- und Gesundheitsgefahren und über Maßnahmen zur Abwendung dieser Gefahren zu unterweisen.

Bußgeldvorschriften

Die Bußgeldbestimmungen sind ergänzt und der **Bußgeldrahmen** ist **erhöht** worden. Das Risiko, Kinder als billige Arbeitskräfte zu gebrauchen und zu mißbrauchen, ist höher geworden. Gleichwohl stehen und fallen die Schutzbestimmungen des Jugendarbeitsschutzgesetzes mit einer wirksamen Überwachung durch die Gewerbeaufsichtsämter, die jedenfalls in der Vergangenheit nur im geringen Maße in der Lage waren, die gebotenen Kontrollen in angemessenem Umfang und gebotener Regelmäßigkeit durchzuführen.

Michael Schoden,
DGB-Bundesvorstand, Abt. Arbeits-, Sozial- und Mitbestimmungsrecht

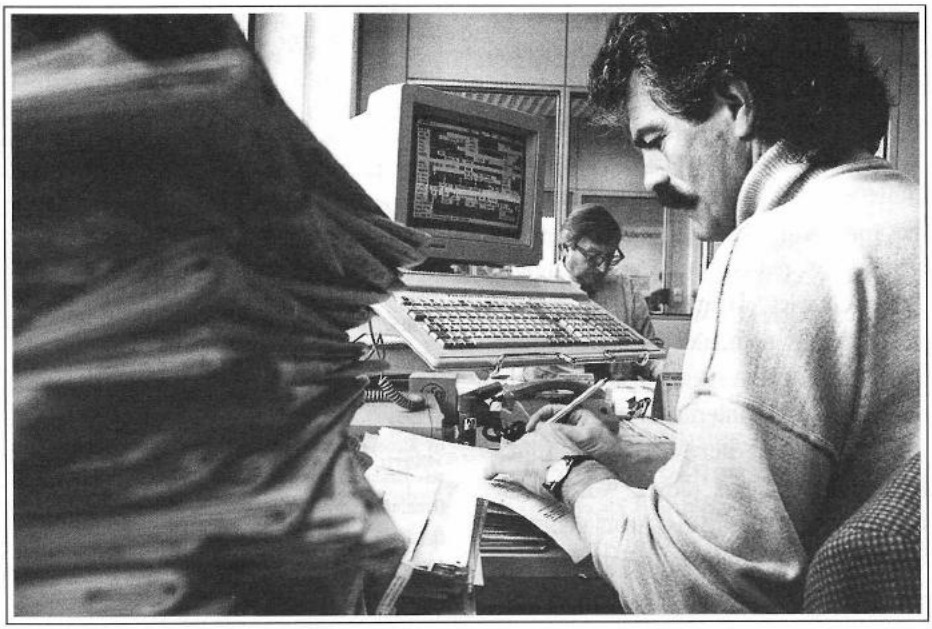
Betriebsräten fällt in der Praxis die Kontrollle, ob die Schutzbestimmungen des Bundesdatenschutzgesetzes (BDSG) eingehalten werden, nicht leicht. Erst recht gilt dies im Fall der grenzüberschreitenden Übermittlung von Arbeitnehmerdaten. Am Beispiel einer deutschen Computerfirma zeigt der Verfasser, daß durch entsprechende Vereinbarungen die schutzwürdigen Belange der Arbeitnehmer gewahrt werden können.

Die deutsche Firma, welche eine hundertprozentige Tochter einer US-amerikanischen Corporation ist, beabsichtigt, ihr Auftragsabwicklungssystem weltweit zu konzentrieren und hierdurch Synergien zu nutzen. Dies soll durch Einführung des Systems SAP R/3 geschehen. Der zentrale Rechner soll in den USA installiert werden. Die einzelnen Niederlassungen, darunter auch die deutsche GmbH, geben ihre Daten über PCs ein, die direkt mit dem Rechner verbunden sind. Mangels größerer eigener Speicherkapazität werden sie als „dumme Terminals" bezeichnet.

Je nach eingesetztem Modul wird eine unterschiedliche Zahl von personenbezogenen Daten der Mitarbeiter wie der Kunden in das System eingegeben. So erfolgt beispielsweise eine Identifizierung von Vertriebsbeauftragten, Einkäufern, Administratoren und Benutzern; zu diesen „Stammdaten" kommen dann die Angaben hinzu, die die einzelnen akquirierten und abgewickelten Aufträge betreffen. Insoweit läßt sich von den USA aus genau feststellen, wer wieviele Aufträge in welcher Art und Weise abgewickelt hat.

Die Einführung des Systems SAP R/3 soll weltweit etwa 330 Mio. US-Dollar kosten; davon fallen in Deutschland etwa 3 Mio. US-Dollar an. Die jährlichen Betriebskosten sollen sich auf etwa 200 Mio. US-Dollar weltweit belaufen; die Konzernspitze ist der Auffassung, daß die

Grenzüberschreitender Datenschutz — Handlungsmöglichkeiten des Betriebsrats



In vielen Staaten existiert kein dem deutschen Datenschutzrecht vergleichbarer Schutzstandard — von daher ist gerade eine Kontrolle der Übermittlung von Arbeitnehmerdaten ins Ausland dringendst geboten.

bisher praktizierten unterschiedlichen Systeme mit sehr viel mehr Aufwand verbunden sind.

Überlegungen dieser Art sind heute an der Tagesordnung. Im Zeitalter der Globalisierung ist es nachgerade selbstverständlich, daß die Konzernleitung einen umfassenden Überblick über das haben will, was in den jeweiligen ausländischen Niederlassungen geschieht. Auch die Vereinheitlichung der EDV-Programme ist dabei ein naheliegendes Ziel, da es nicht nur Kosten sparen kann, sondern auch die Auswertung und Steuerung des Verhaltens der einzelnen Niederlassungen erleichtert[1]. Etwa 90 % der Datentransfers von einem Land in ein anderes finden deshalb innerhalb multinationaler Unternehmen oder Konzerne statt.[2]

Wann ist die Datenübermittlung ins Ausland zulässig?

Die Übermittlung von Daten ins Ausland wirft insbesondere dann Probleme auf, wenn dort kein vergleichbarer Schutzstandard wie nach dem BDSG besteht. Im Extremfall könnten Dateien dort zum „Selbstbedienungsladen" werden, aus dem sich jeder Interessierte holen kann. In der Praxis droht dies in dieser Form schon deshalb nicht, weil die Firmen selbst aus Konkurrenzgründen darauf achten, daß etwa mit den Kundenlisten pfleglich umgegangen wird. In bezug auf die Arbeitnehmerdaten muß dies nicht der Fall sein: Hier wäre eine weltweite Personalpolitik denkbar, die sich auf die Auswertung einer Unzahl arbeitsbezogener Vorgänge stützt, deren Ablauf sich unschwer durch Abfrage im System rekonstruieren läßt. Insofern besteht ein dringendes Interesse daran, die grenzüberschreitende Übermittlung von Arbeitnehmerdaten zu kontrollieren und Mißbräuche für Zwecke der Kontrolle zu vermeiden.

Wer die Bestimmungen des BDSG durchgeht, könnte den Eindruck gewinnen, Datenverarbeitung finde allein innerhalb der deutschen Grenzen statt. Nur an relativ versteckter Stelle — in § 3 Abs. 9 Satz 2 BDSG — ist davon die Rede, daß eine sogenannte Auftragsdatenverarbeitung nur innerhalb des Geltungsbereichs des BDSG möglich ist. Werden die deutschen Grenzen überschritten, ist der Beauftragte automatisch „Dritter", an den Daten nur unter den allgemeinen Voraussetzungen übermittelt werden können[3]. Im übrigen finden sich keine Bestimmungen.

In Literatur und Rechtsprechung ist man sich einig, daß das Schweigen des BDSG nicht etwa als Votum für generelle Unzulässigkeit verstanden werden kann. Vielmehr werden grundsätzlich dieselben Vorschriften angewandt, die für Inlandssachverhalte gelten. Soweit dort auf „schutzwürdige Belange" des Betroffenen abgestellt wird, ist selbstredend zu berücksichtigen, daß diese durch eine grenzüberschreitende Übermittlung sehr viel nachhaltiger beeinträchtigt sein können.

---

1) Siehe bereits Schapper, in: Klebe-Roth (Hrsg.), Informationen ohne Grenzen, Hamburg 1987, S. 191 f.

2) Sautner, EDV und Recht (österreichische Zeitschrift) 1995, 82

3) Näher dazu Däubler, Gläserne Belegschaften? Datenschutz für Arbeiter, Angestellte und Beamte, 3. Aufl., Köln 1993, Rn. 250 ff. m. w. N.

Einwilligung des Betroffenen als Rechtfertigung?

Nach § 4 Abs. 1 BDSG ist eine Datenübermittlung dann zulässig, wenn der Betroffene einwilligt. Diese Voraussetzung ist bei Arbeitnehmerdaten in aller Regel schon aus formellen Gründen nicht erfüllt: Nach § 4 Abs. 2 Satz 2 BDSG bedarf die Einwilligung der Schriftform. Auch ein schriftlich geschlossener Arbeitsvertrag reicht hierfür nicht aus, da die Einwilligungserklärung „im äußeren Erscheinungsbild der Erklärung" hervorzuheben ist (§ 4 Abs. 2 Satz 3 BDSG), was — soweit ersichtlich — in der Praxis so gut wie nie vorkommt. Wollte der Arbeitgeber anläßlich der Einführung eines neuen Systems nachträglich die Einwilligung einholen, könnte er dies nur mit Zustimmung des Betriebsrats tun: § 94 BetrVG deckt auch Fälle ab, in denen der Arbeitnehmer nur nach einer einzigen Sache gefragt wird[4]. Im Ergebnis kommt es daher gar nicht auf die weitere Frage an, ob ein Arbeitnehmer überhaupt über den nötigen eigenständigen Entscheidungsspielraum verfügt, der für eine Einwilligung und damit für eine Erweiterung der dem Arbeitgeber zustehenden Verarbeitungsmöglichkeiten erforderlich ist[5].

Rechtfertigung durch den Arbeitsvertrag?

Nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG ist das Übermitteln personenbezogener Daten außerdem „im Rahmen der Zweckbestimmung eines Vertragsverhältnisses" zulässig. Dies gilt — wie bereits erwähnt — auch für Fälle von grenzüberschreitender Übermittlung. So ist es beispielsweise allgemein akzeptiert, daß als Folge eines Überweisungsauftrags zugunsten einer ausländischen Firma auch personenbezogene Daten übermittelt werden, und dasselbe gilt dann, wenn ein Reisevertrag geschlossen und die Fluggesellschaft sowie das Hotel am ausländischen Zielort eine Reihe von personenbezogenen Angaben erhalten.

Im Arbeitsverhältnis liegen die Dinge insoweit anders, als das BDSG streng unternehmensbezogen ist und deshalb Arbeitnehmerdaten auch bei rein innerstaatlichen Konzernen grundsätzlich nicht an andere Konzerngesellschaften übermittelt werden dürfen[6]. Erst recht überschreitet es daher den vom Arbeitsvertrag gezogenen Verarbeitungsrahmen, wenn Daten im Rahmen eines multinationalen Konzerns an ein ausländisches Konzernunternehmen übermittelt werden sollen[7]. Ausnahmen können sich bei einem sog. konzerndimensionalen Arbeitsverhältnis ergeben, das von vornherein auf Einsätze bei verschiedenen nationalen Niederlassungen ausgerichtet ist[8]. Damit ist aber in der Praxis jedenfalls nicht der Regelfall erfaßt. Selbst dann, wenn eine solche Konstellation gegeben ist, unterliegt der Arbeitsvertrag im übrigen inhaltlich einer Billigkeitskontrolle[9]. An dieser würde eine Klausel scheitern, die den Arbeitgeber ermächtigt, ohne Bindung an irgendwelche datenschutzrechtliche Grundsätze mit den Arbeitnehmerdaten zu verfahren.

Berechtigte Interessen des Arbeitgebers unter Wahrung schutzwürdiger Belange des Arbeitnehmers

§ 28 Abs. 1 Satz 1 Nr. 2 BDSG ermöglicht die Übermittlung personenbezogener Daten, „soweit es zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und kein Grund zu der Annahme besteht, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Verarbeitung überwiegt".

Ob sich ein Arbeitgeber seinen Arbeitnehmern gegenüber auch auf diese Rechtsgrundlage berufen kann oder ob der Vertrag den „Verarbeitungsrahmen" abschließend umschreibt, ist umstritten. Die Rechtsprechung wendet beide Vorschriften nebeneinander an[10], die Literatur ist gespalten[11]. Obwohl an sich die besseren Argumente für einen Vorrang des Vertrages sprechen, soll hier die „arbeitgeberfreundlichere" Position der Rechtsprechung zugrunde gelegt werden; in betrieblichen Auseinandersetzungen wird sich die Geschäftsleitung immer darauf berufen.

Erste Voraussetzung für eine Übermittlung ist, daß sie „zur Wahrung berechtigter Interessen" des Arbeitgebers erforderlich ist. Dies läßt sich meist (und auch beim

---

4) Ebenso Fitting/Kaiser/Heither/Engels, Kommentar zum BetrVG, 18. Aufl., München 1996, § 94 Rn. 10; Klebe, in: Däubler/Kittner/Klebe, Kommentar zum BetrVG, 5. Aufl., Köln 1996, § 94 Rn. 27; Däubler, Das Arbeitsrecht 1, 14. Aufl., Reinbek 1995, Rn. 1029; Wohlgemuth, Datenschutz für Arbeitnehmer, 2. Aufl., Neuwied 1988, Rn. 685.

5) Dazu näher Däubler, Gläserne Belegschaften? Rn. 136 ff.

6) Klebe, in: Däubler/Klebe/Wedde, Bundesdatenschutzgesetz. Basiskommentar, Köln 1996, § 3 Rn. 22; Gola-Wronka, Handbuch zum Arbeitnehmerdatenschutz. Rechtsfragen und Handlungshilfen für die betriebliche Praxis, 2. Aufl., Köln 1994, S. 204; Kroll, Datenschutz im Arbeitsverhältnis, Königstein/Ts. 1981, S. 115 ff.; Wohlgemuth BB 1992, 283 m. w. N.; a. A. nur Zöllner, Daten- und Informationsschutz im Arbeitsverhältnis, 2. Aufl., Köln/Berlin u. a. 1983, S. 49.

7) Vgl. Gola-Wronka, a. a. O., S. 206; Wohlgemuth BB 1991, 342.

8) Zu einem solchen konzerndimensionalen Arbeitsverhältnis s. Däubler, Arbeitsrecht 2, 10. Aufl., Reinbek 1995, S. 666 ff. mwN. Zur hier relevanten Problematik ebenso Bergmann, Grenzüberschreitender Datenschutz, Baden-Baden 1985, S. 84; Bergmann-Möhrle-Herb, Datenschutzrecht, Handkommentar (Loseblatt — Stand März 1995) § 28 Anlage 6 unter 5.2.2.

9) Däubler, Arbeitsrecht 2, S. 118 ff., 123; eingehend U. Preis, Vertragsgestaltung im Arbeitsrecht, Neuwied 1995.

10) So zum BDSG 1977 BGH NJW 1984, 436; BAG EzA § 87 BetrVG 1972 Kontrolleinrichtung Nr. 15.

11) Wie die Rechtsprechung Bergmann-Möhrle-Herb § 28 Anlage 6 unter 5.5; Ehmann, Beilage 1/1985 zu NZA S. 5; Ellger, Der Datenschutz im grenzüberschreitenden Datenverkehr. Eine rechtsvergleichende und kollisionsrechtliche Untersuchung, Baden-Baden 1990, S. 102; Sproll ZIP 1984, 30; a. A. Däubler, Gläserne Belegschaften? Rn. 185; Ordemann-Schomerus-Gola, Bundesdatenschutzgesetz, 5. Aufl., München 1992, § 28 Anm. 2. 2; Wohlgemuth, Datenschutz für Arbeitnehmer, Rn. 246, 461.

oben wiedergegebenen Sachverhalt) bejahen: Es ist durchaus „berechtigt", in diesem Sinne ein neues Auftragsabwicklungssystem einzuführen und dadurch Synergieeffekte zu erzielen. Dabei kann dahingestellt bleiben, ob auch solche Arbeitgebermaßnahmen ein „berechtigtes Interesse" begründen, die im Ergebnis nicht zu rationellerem Arbeiten im Unternehmen führen.

Das eigentliche Problem liegt in der zweiten Voraussetzung. Es darf kein Grund zu der Annahme bestehen, daß das „schutzwürdige Interesse" des Betroffenen an dem Ausschluß der Verarbeitung oder Nutzung überwiegt. Dabei ist zu beachten, in welchem „Zustand" sich die Daten nach der Übermittlung in ein anderes Land befinden.

Nimmt man das Beispiel der USA, so kann weder von einem gleichwertigen noch auch nur von einem angemessenen Datenschutz die Rede sein[12]. Auf Bundesebene existieren nur Regeln für einzelne Bereiche wie z. B. den Finanzsektor oder die Telekommunikation. Was den Arbeitnehmerdatenschutz betrifft, so ist lediglich die Erhebung von Daten mit Hilfe eines Lügendetektors beschränkt (aber nicht etwa ausgeschlossen!). Im übrigen dürfen vorhandene Informationen nicht zu einer Diskriminierung insbesondere wegen Rasse und Geschlecht verwendet werden[13]. Ansonsten existieren keine bundesrechtlichen Grenzen in bezug auf die Sammlung, Speicherung und Nutzung von Arbeitnehmerdaten. Für den Arbeitgeber entsteht so ein Reich der unbegrenzten Möglichkeiten.

Auf einzelstaatlicher Ebene ist die Situation nur unwesentlich besser. Trotz Bestimmungen über die Handhabung von Personalakten, die in einigen Staaten existieren, sind die Art der Datenerhebung, der Umfang und die Dauer der Speicherung auch insoweit völlig frei. Dem Arbeitgeber ist es nicht untersagt, quasi beliebige Daten zu sammeln und sie für andere als die der Erhebung zugrunde liegenden Zwecke zu verwenden. Auch die Rechtsprechung zum Persönlichkeitsschutz kann dies nicht verhindern. Erst recht fehlen Instanzen, die die bescheidenen Normen durchsetzen könnten. Auch ist nicht bekannt, daß sich Arbeitnehmervertretungen in nennenswertem Umfang um Datenschutz gekümmert hätten; dabei ist zu berücksichtigen, daß in der Privatwirtschaft nur noch rund 10 % aller Beschäftigten von einer Gewerkschaft vertreten werden[14].

Das „Datenschutzgefälle" ist unter diesen Umständen evident.

Die Übermittlung von Arbeitnehmerdaten in ein solches Land würde schutzwürdige Belange der Betroffenen verletzen.

Unzulässigkeit der Übermittlung oder Schaffung von vertraglichen Lösung

Ein Teil der Literatur steht auf dem Standpunkt, angesichts solcher Umstände sei Datenübermittlung unter Berufung auf § 28 Abs. 1 Satz 1 Nr. 2 BDSG generell unzulässig. Auch eine vertragliche Abmachung zwischen dem deutschen Arbeitgeber und dem ausländischen Unternehmer könnte hier keinen Ausgleich schaffen. Ein solcher Vertrag gewähre dem einzelnen keine ausreichenden Rechte[15]; auch hätten die Beteiligten die Möglichkeit, den Vertrag ohne Einschaltung des einzelnen jederzeit an neue Informationsbedürfnisse der Konzernspitze anzupassen[16], ihn aufzuheben oder zu kündigen[17]. Außerdem hätten die deutschen Aufsichtsbehörden keine Möglichkeit, um die Einhaltung eines solchen Vertrages im Ausland zu kontrollieren[18].

Dies sind gewichtige Einwände, die jedoch mehr den Inhalt des Vertrages als einen solchen Weg schlechthin betreffen: Soweit es möglich ist, die Rechte des einzelnen umfassend abzusichern und auch eine effiziente Kontrolle zu etablieren, sind „schutzwürdige Belange" der Arbeitnehmer nicht mehr verletzt. Schon vom Wortlaut des § 28 Abs. 1 Satz 1 Nr. 2 BDSG her besteht daher kein Anlaß, bei einem generellen Verbot zu bleiben. Davon ganz abgesehen: die Globalisierung der Wirtschaft ist eine Realität, die man gestalten muß, der man sich aber nicht durch Verbote entziehen kann. Kein Betriebsrat könnte es ernsthaft durchhalten, in einer Situation wie der eingangs geschilderten das gesamte System trotz erheblichen Einsparungspotentials unter Berufung auf einige Stimmen zum deutschen Datenschutzrecht zu blockieren.

Anforderungen an einen Vertrag

Schutzwürdige Belange der betroffenen Arbeitnehmer sind nicht schon dann gewahrt, wenn sich die ausländische Konzernspitze bereit erklärt, das Schutzniveau des BDSG (oder vergleichbarer Vorschriften) zu wahren. Vielmehr „lebt" der Arbeitnehmerdatenschutz entscheidend von seinen Kontrollrechten. Diese stehen nach §§ 33—35 BDSG einmal dem Betroffenen selbst zu. Zum zweiten haben (relativ) unabhängige Instanzen wie der betriebliche Datenschutzbeauftragte und der Betriebsrat die Möglichkeit, die Einhaltung des bestehenden Rechts wie auch

12) Eingehend Welske CR 1993, 297 ff.

13) Welske CR 1993, 303.

14) Vgl. Gould, A Primer on American Labor Law, 3. Aufl., Cambridge/Mass. und London/England 1993, S. VII, der den Organisationsgrad einschließlich des öffentlichen Dienstes mit 15 % beziffert.

15) So Bergmann, a. a. O., S. 85, 220; Simitis, in: Simitis-Dammann- Mallmann-Reh, Kommentar zum BDSG 1977, 3. Aufl., Loseblatt, § 24 Rn. 50.

16) Ellger, a. a. O., S. 204.

17) Wohlgemuth BB 1991, 342.

18) Bergmann, S. 220; Simitis CR 1991, 177; Wohlgemuth BB 1991, 342.

getroffener Vereinbarungen zu überwachen. Schließlich existiert eine Aufsichtsbehörde, deren Sanktionsgewalt allerdings eher bescheiden ist[19]. Ihre Kompetenzen können schon aus völkerrechtlichen Gründen nicht auf Vorgänge erstreckt werden, die sich im Ausland abspielen. Insoweit muß daher auf vertraglicher Basis eine Kompensation geschaffen werden, also beispielsweise die Zahlung einer Vertragsstrafe für jeden Fall der Verletzung datenschutzrechtlicher Grundsätze durch den ausländischen Datenverarbeiter, d. h. im konkreten Fall durch die US-amerikanische Konzernspitze. Nur wenn allen diesen Anforderungen Rechnung getragen ist, läßt sich eine Übermittlung mit den schutzwürdigen Belangen der betroffenen Arbeitnehmer in Einklang bringen.

Ein wichtiger Beispielsfall

Im folgenden ist eine Datenschutzvereinbarung (DV) zwischen der deutschen Tochtergesellschaft und der amerikanischen Mutter sowie (in den relevanten Auszügen) die dazugehörige Gesamtbetriebsvereinbarung abgedruckt. Sie ist in dieser Form von allen Beteiligten Mitte 1996 unterzeichnet worden und wird seither ohne größere Probleme praktiziert. Einzelne Bestimmungen sind Ergebnisse eines Kompromisses, der in einer Einigungsstelle gefunden wurde. Eine Reihe von Einzelpunkten bedürfen deshalb der Erläuterung.

● Keine großen Probleme ergaben sich bei der Übernahme des Schutzniveaus des BDSG (§ 1 Abs. 1 DV) und bei der in § 2 der Datenschutzvereinbarung festgelegten Zweckbindung.

● Weniger selbstverständlich ist die Garantie der Individualrechte nach den §§ 3 und 4 DV. Die Betriebsratsseite hatte zunächst gefordert, den in Deutschland Beschäftigten einen unmittelbaren Anspruch gegen die amerikanische Muttergesellschaft einzuräumen. Für diese wäre es angesichts der völlig anderen Arbeitsbeziehungen in den USA ein schwer zu verdauender Brocken gewesen, könnte jeder in Deutschland Beschäftigte sie zu einem bestimmten Verhalten zwingen oder jedenfalls Rechenschaft von ihr verlangen.

Der Kompromiß bestand darin, zwar einen Anspruch auf Auskunft, Berichtigung, Sperrung und Löschung einzuräumen, seine Geltendmachung jedoch an die Einschaltung der deutschen GmbH zu binden (§ 3 Abs. 2, § 4 Abs. 2 DV).

Um zu verhindern, daß einzelne Ersuchen einfach nicht bearbeitet werden, sehen § 3 Abs. 3 DV und § 4 Abs. 2 Satz 2 DV eine bestimmte Frist vor. Wird sie nicht eingehalten, wäre dies ein eindeutiger Verstoß gegen die Vereinbarung, der Sanktionen auslösen würde.

Bei der Festlegung der Individualrechte wurde auf § 328 Abs. 2 BGB Bezug genommen. Er besagt, daß bei einem Vertrag zugunsten Dritter eine Begünstigung in der Weise erfolgen kann, daß das eingeräumte Recht nur mit Zustimmung des Dritten wieder entzogen werden darf (§ 3 Abs. 4 und § 4 Abs. 5 DV). Damit soll dem in der Literatur genannten Einwand Rechnung getragen werden, der Vertrag zwischen Arbeitgeber und Konzernspitze könne jederzeit zu Lasten des Betroffenen verändert werden[20].

● Keine Meinungsverschiedenheiten ergaben sich zum Problem der Datensicherung (§ 5 DV). Hervorzuheben ist nur die in § 5 Abs. 1 Satz 2 DV erfolgende Konkretisierung, daß „unbefugt" auch Mitarbeiter der Corporation sind, die ihrer arbeitsvertraglichen Aufgabe nach nicht auf das System zugreifen dürfen.

● Entscheidender Punkt ist die Kontrolle der Einhaltung des BDSG-Standards durch unabhängige Instanzen. Insoweit müssen Datenschutzvereinbarung und Gesamtbetriebsvereinbarung zusammen gesehen werden.

Der Vorstand einer hundertprozentigen Tochtergesellschaft ist nicht unbedingt die geeignete Instanz, um irgendwelche Rechte gegenüber der Muttergesellschaft durchzusetzen. Von daher muß er gegebenenfalls zu einem Einschreiten gezwungen werden können; auch sind unabhängige Instanzen wie der Gesamtbetriebsrat einzuschalten. Zu beachten war allerdings, daß es für die Muttergesellschaft aus optischen Gründen schwer erträglich gewesen wäre, hätten plötzlich drei GBR-Mitglieder aus Deutschland im Vorzimmer des Präsidenten angeklopft und um Einsicht in die dort erfolgende Datenverarbeitung gebeten: Was man den eigenen amerikanischen Beschäftigten nicht gewährt, wird man den aus der fernen „Provinz" anreisenden Interessenvertretern schwerlich einräumen wollen. Die Regelungen des Vertrages haben dem ausreichend Rechnung getragen.

Nach Nr. 15 der Gesamtbetriebsvereinbarung hat der Gesamtbetriebsrat Zugriffsrechte auf das System, ohne jedoch selbst Daten eingeben zu können. Allerdings ist die Zahl der Mitglieder, die diese Befugnis haben, auf zwei beschränkt. Die GmbH bestimmt einen Ansprechpartner.

Nach § 6 DV hat nicht nur die GmbH, sondern auch ihr betrieblicher Datenschutzbeauftragter ein umfassendes Kontrollrecht, das auch vor Ort, d. h. in den USA ausgeübt werden kann. Besteht ein Verdacht auf Datenmißbrauch, ist nach § 6 Abs. 5 DV eine unverzügliche Kontrolle in den USA durchzuführen. Dem Gesamtbetriebsrat steht insoweit ein Antragsrecht zu. Außerdem kann er bis zu zwei unter-

19) Überblick bei Däubler, in: Däubler/Klebe/Wedde, Erläuterungen zu § 38 und bei Walz, in: Simitis-Dammann-Geiger-Mallmann-Walz, Kommentar zum BDSG, 4. Aufl., Erläuterungen zu § 38.

20) Ellger, S. 204; Wohlgemuth BB 1991, 342.

nehmensangehörige Personen benennen, die gemeinsam mit dem betrieblichen Datenschutzbeauftragten die Kontrolle durchführen und die in den USA als dessen Mitarbeiter auftreten.

Bleibt der betriebliche Datenschutzbeauftragte untätig (weil er z. B. keinen Verdacht auf Datenmißbrauch annimmt), so geht das Kontrollrecht auf eine Dreierkommission über, die aus einem namentlich bestimmten Richter der Arbeitsgerichtsbarkeit und je einem Vertreter der deutschen GmbH und des Gesamtbetriebsrats besteht. Sie könnte dann vor Ort die erforderlichen Untersuchungen vornehmen.

● Bei jedem Vertrag können Meinungsverschiedenheiten entstehen, ob denn nun seinen Bestimmungen Rechnung getragen ist oder nicht. Nr. 15 Abs. 2 der Gesamtbetriebsvereinbarung sieht vor, daß in solchen Fällen eine innerbetriebliche Einigungsstelle entscheidet. Dies wirkt zwar nicht gegenüber der amerikanischen Corporation, doch kommt es darauf nicht entscheidend an. Die in § 7 DV als Sanktion für Vertragsverletzungen vorgesehene Vertragsstrafe von 20 000 DM ist vielmehr nach Nr. 16 Abs. 3 der Gesamtbetriebsvereinbarung (auch) von der deutschen GmbH zu bezahlen. Insofern vermeidet man das für alle Beteiligten schwierige direkte Vorgehen gegen die Muttergesellschaft. Zwar ist ein deutscher Gerichtsstand in § 9 Abs. 3 DV vorgesehen, doch wäre es mit Sicherheit der einfachere Weg, die Vertragsstrafe gegen die deutsche GmbH effektiv umzusetzen.

● Ein letzter Punkt betrifft die Frage, unter welchen Voraussetzungen eine Kündigung zulässig ist, die die weitere Datenübermittlung ggf. unzulässig macht. Hier ist zu differenzieren:

Die Datenschutzvereinbarung ist nur aus wichtigem Grund kündbar; wird sie gekündigt, ist von diesem Zeitpunkt an nach ihrem § 8 die weitere Datenübermittlung unzulässig.

Die Gesamtbetriebsvereinbarung ist nach ihrer Nr. 18 mit einer Frist von 6 Monaten ordentlich kündbar. Kommt es jedoch wegen eines groben Verstoßes gegen die aus der Gesamtbetriebsvereinbarung folgenden Pflichten zu einer außerordentlichen Kündigung durch den Gesamtbetriebsrat, so endet die Befugnis zur Übermittlung einen Monat ab Zugang der Kündigung (Nr. 16 Abs. 2 der Gesamtbetriebsvereinbarung).

Würdigung

Der hier wiedergegebene Vertrag widerlegt die These, auf einem solchen Wege sei kein dem BDSG entsprechender Schutz erreichbar. Gleichzeitig muß man aber berücksichtigen, daß im konkreten Fall drei wesentliche Bedingungen vorlagen, die eine recht weitgehende vertragliche Gestaltung ermöglichen:

● Der Betriebsrat hätte die Einführung des Systems über sein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG blockieren, jedenfalls erheblich hinauszögern können. Dies hätte die Strategie der Konzernleitung zunichte gemacht, die nun einmal weltweit dasselbe System einführen wollte. Ein Ausscheren der Deutschen hätte mit Sicherheit erhebliche Kosten verursacht.

● Der Konzernleitung ging es ersichtlich ausschließlich um eine rationellere Bewältigung der Geschäftsabläufe, nicht um die Kontrolle der Beschäftigten. Insoweit war sie bereit, für den Fall des Datenmißbrauchs relativ weitgehende Sanktionen zu akzeptieren.

● In der deutschen GmbH ist es in der Vergangenheit zu Arbeitsniederlegungen gekommen, die dazu geführt haben, daß den Forderungen der betrieblichen Interessenvertretung auch dann ein hoher Stellenwert zukommt, wenn im konkreten Fall ein Streik nicht ernsthaft in Betracht gezogen wird.

Die Übertragung auf andere Unternehmen ist daher nicht immer einfach. Doch es besteht kein Grund zur Zurückhaltung: Warum sollte das Beispiel nicht Schule machen?

Prof. Dr. Wolfgang Däubler, Bremen

Literaturempfehlung

● Däubler; Das Fernsprechgeheimnis des Arbeitnehmers; AiB 3/1995, S. 149

● Däubler:; Gläserne Belegschaften? Datenschutz für Arbeiter, Angestellte und Beamte; 3. Aufl.; Köln 1993

● Däubler/Klebe/Wedde; Bundesdatenschutzgesetz. Basiskommentar; Köln 1996

● Schierbaum; Datenschutz bei Auftragsdatenverwaltung; Computer-Fachwissen 3/1997, S. 25