Der geplante Einsatz des Systems SAP R/3 - ein Verstoß gegen das BDSG?

Rechtsgutachten

erstattet im Auftrage des Gesamtbetriebsrats der Firma Digital Equipment GmbH

von Prof. Dr. Wolfgang Däubler, Bremen

A Sachverhalt

I. Die geplante Maßnahme

Die Digital Equipment GmbH Deutschland (im folgenden: GmbH) ist eine hundertprozentige Tochtergesellschaft der Firma Digital Equipment Corporation mit Sitz in USA (im folgenden: Corporation).

Die Corporation beabsichtigt, ihr Auftragsabwicklungssystem weltweit zu zentrieren und hierdurch Synergien zu nutzen. Dies soll durch Einführung des Systems SAP R/3 geschehen. Dabei soll der zentrale Rechner in Merrimack (USA) installiert werden. Die einzelnen Niederlassungen (darunter auch die deutsche GmbH) geben ihre Daten über PC's ein, die direkt mit dem Rechner verbunden sind und mangels eigener größerer Speicherkapazität als "dumme Terminals" bezeichnet werden.

Je nach eingesetztem Modul wird eine unterschiedliche Zahl von personenbezogenen Daten der Kunden wie der Mitarbeiter 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. Wie weit der Datenvorrat reicht oder reichen kann, ist den vorliegenden Unterlagen nicht zu entnehmen; für die rechtliche Würdigung kommt es hierauf aber nicht entscheidend an, da beispielsweise schon mit sehr wenigen Daten jedenfalls unter Heranziehung von sog. Zusatzwissen Aussagen zu Verhalten und Leistung einzelner Beschäftigter möglich sind. Auch stellen die Regeln über den grenzüberschreitenden Datenschutz nicht darauf ab, welches Quantum an personenbezogenen Daten eine Staatsgrenze überschreitet.

In Deutschland sollen die Module SD (Vertrieb) und FI (Finance) verwendet werden. Ab 28.8.1995 ist ein Pilotbetrieb geplant,

der drei Monate dauert und drei ausgewählte Kunden mit Echtdaten erfassen soll. Der generelle Einsatz ist für die Zeit ab 1.1.1996 geplant.

Die Einführung des Systems SAP soll weltweit etwa 330 Mio. US Dollar kosten; das Budget für Deutschland beträgt für das Finanzjahr 1995 2,2 Mio US Dollar. Die jährlichen Betriebskosten von ca. 200 Mio. US Dollar weltweit sollen durch das Wegfallen anderer Systeme eingespart werden.

In den Arbeitsverträgen der Mitarbeiter der GmbH wird nicht auf die grenzüberschreitende Übermittlung von Daten Bezug genommen. Soweit Ausnahmen vorliegen sollten, ist dies im vorliegenden Zusammenhang ohne Bedeutung, da das geplante System nur dann adäquat funktionieren kann, wenn in bezug auf alle Beteiligten eine ausreichende Rechtsgrundlage existiert.

Sämtliche Arbeitsverhältnisse unterliegen - da mit einer GmbH deutschen Rechts abgeschlossen - dem deutschen Arbeitsrecht.

II. Der Entwurf eines Vertrages zwischen der Corporation und der GmbH

In einem "Interoffice Memorandum" vom 30.6.1995 wird eine Datenschutzvereinbarung vorgeschlagen, deren Partner die GmbH und die Corporation sein sollen. In der Präambel wird darauf verwiesen, daß personenbezogene Daten von Mitarbeitern in Zukunft zwischen der GmbH und der Corporation ständig ausgetauscht würden. Weiter heißt es:

> "Zur Verbesserung des Datenschutzes bei diesem grenzüberschreitenden Verkehr vereinbaren die Parteien die folgenden Datenschutzmaßnahmen, die eventuelle Risiken für die betroffenen Kunden und Mitarbeiter bei diesen Datenübermittlungen mindern sollen."

Nach § 1 des Vertragsentwurfs sollen die übermittelten Daten denselben Schutz wie nach BDSG erfahren. § 2 sieht deshalb eine

strikte Zweckbindung vor; die Daten "werden ausschließlich zum Zweck der beschleunigten und effektiveren Auftragsabwicklung spezifischer Kundenaufträge übermittelt. Jede zweckwidrige Verwendung ist der Corporation untersagt."

§ 3 sieht eine Auskunftspflicht der Corporation sowohl gegenüber dem einzelnen Betroffenen wie gegenüber der GmbH vor. Sie erstreckt sich auf folgende Angaben:

> "- Die zu seiner Person gespeicherten Daten, auch soweit sie sich auf Herkunft und Empfänger beziehen,
>
> - den Zweck der Speicherung
>
> und
>
> - Personen und Stellen, an die seine Daten regelmäßig übermittelt werden, wenn seine Daten automatisiert verarbeitet werden."

§ 4 gibt die dem BDSG entsprechenden Rechte auf Berichtigung, Sperrung und Löschung unrichtiger bzw. in ihrer Richtigkeit umstrittener Daten. Diese Korrekturansprüche stehen allerdings nur der GmbH zu; nach § 10 Abs. 2 Satz 2 des Entwurfs kann diese jedoch jederzeit und ohne Zustimmung der Corporation ihre Rechte an einen Betroffenen abtreten. Unter welchen Voraussetzungen dies zu geschehen hat, ist nicht behandelt.

§ 5 sieht eine Benachrichtigungspflicht der GmbH gegenüber den Betroffenen vor, die sich auf die Datenübermittlung ins Ausland sowie die eingeräumten Rechte bezieht. Die GmbH kann verlangen, daß eine entsprechende Benachrichtigung auch durch die Corporation selbst erfolgt.

§ 6 regelt die Datensicherung und bestimmt insbesondere, daß als unbefugte Dritte auch solche Personen gelten, die zwar bei der Corporation beschäftigt sind, die aber auf das System im

Rahmen ihrer arbeitsvertraglichen Aufgabe nicht zugreifen dürfen.

§ 7 sieht Kontrollrechte der GmbH gegenüber der Corporation vor. Letztere hat jederzeit nicht nur Auskunft zu erteilen, sondern auch in sämtliche Unterlagen und in Archive, in welchen sich die betreffenden Daten befinden, Einsicht zu gewähren. Weiter wird bestimmt:

> "Die GmbH hat ferner das Recht, jederzeit vor Ort eine Besichtigung des Systems vorzunehmen und, sofern die in Abs. 1 genannte Auskunft und Einsicht nicht ausreichend ist, selber Untersuchungen und Maßnahmen am System vorzunehmen, um ihren Verpflichtungen nach dem Bundesdatenschutzgesetz nachzukommen."

Während das Recht auf Auskunft und Einsicht nach § 10 Abs. 2 Satz 2 des Entwurfs an die einzelnen Betroffenen abtretbar ist, gilt dies nicht für das Besichtigungsrecht nach § 7 Abs. 2.

Für den Fall einer Zuwiderhandlung gegen die Vereinbarung verspricht die Corporation die Zahlung einer Vertragsstrafe in Höhe von 10.000 DM (§ 8). Auch übernimmt nach § 9 die Corporation die gesamtschuldnerische Haftung für die Erfüllung der Verpflichtungen nach dem Bundesdatenschutzgesetz, was allerdings wohl nur im Sinne eines Einstehens für Schadensersatzpflichten zu verstehen ist, da andernfalls die in § 10 Abs. 2 Satz 2 vorgesehene Abtretbarkeit von Rechten der GmbH schwerlich verständlich wäre.

Kontrollmöglichkeiten des betrieblichen Datenschutzbeauftragten oder der Aufsichtsbehörde sind nicht erwähnt. Dasselbe gilt für die Rechte des Gesamtbetriebsrats.

III. Entwurf einer Betriebsvereinbarung

Im Gesamtbetriebsrat existiert der Entwurf einer Gesamtbetriebsvereinbarung zur Einführung des Systems SAP R/3. Er enthält sehr viele Regelungen, die - wie die Hardware-

Konfiguration und die Software-Konfiguration - keinen unmittelbaren Einfluß auf die datenschutzrechtlichen Fragen haben. Hintergrund ist das dem Betriebsrat zustehende Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG; auch dürfte wegen der Änderung der Arbeitsbedingungen die Voraussetzung einer Betriebsänderung nach § 111 BetrVG erfüllt sein.

Nr. 11 des Entwurfs nennt die personenbezogenen Daten, die im System gehalten werden. Nr. 13 sieht eine Information und Beteiligung der Mitarbeiter vor. Er bestimmt im einzelnen:

> "Mitarbeiter, deren Arbeitsbereich sich durch den Einsatz von SAP R/3 verändert, sind rechtzeitig und umfassend vor der Einführung zu unterrichten.
>
> Änderungen in der organisatorischen und ablaufmäßigen Einordnung der Aufgaben sind den Mitarbeitern ausführlich zu erläutern. Die Unterrichtung muß so rechtzeitig erfolgen, daß Anregungen und Vorschläge der jeweiligen Mitarbeiter berücksichtigt werden können. Bei Aufgabenänderungen ist darauf zu achten, daß die Möglichkeiten für eine Verbesserung der Arbeitssituation genutzt werden."

Von Interesse ist im vorliegenden Zusammenhang Nr. 16, der die Kontrollrechte des Gesamtbetriebsrats regelt. Dort heißt es im einzelnen:

> "Zur Wahrnehmung seiner Überwachungsrechte hat der GBR das Zugangsrecht zum SAP R/3-System (durch Definition eines eigenen Benutzerprofils) und den jeweiligen Einzelanwendungen (Masken/Programme). Die verantwortlichen SAP R/3-Systembetreuer sind verpflichtet, den Beauftragten des GBR (max. zwei benannte Personen) Auskunft zu geben. Dies gilt besonders für
>
> - Einsicht in die Protokolldatei und weitere Systemunterlagen und Aushändigung dieser Unterlagen zu Überprüfungszwecken und Aufklärung von Verstößen gegen die Gebote des Datenschutzes.
>
> - Anzeigemöglichkeit aller Benutzer inklusive ihrer Zugriffsrechte

- Anzeigemöglichkeit aller Tabellen inklusive ihrer Eigenschaften (z.B. Sperrkennziffer, Mandantenkennung etc.) inklusive Datum letzter Änderung und ihrer Dokumentation

- Alle verwendeten Reports (ABAP's) inklusive Datum letzter Änderung und ihrer Dokumentation

- Information über die aktuelle Systemauslegung (wie Benutzerstamm, Infotypen mit Datenfeldern, Dokumentation, DAP R/3-Version, Datenbankversion, Betriebssystemversion)

Soweit erforderlich, erhalten die betreuenden Betriebsratsmitglieder die Möglichkeit, an Schulungen des SAP R/3-Systems teilzunehmen, um Aufgaben nach dieser Betriebsvereinbarung wahrnehmen zu können."

IV. Die Fragestellung

Der Gesamtbetriebsrat möchte wissen, ob die vorgesehene grenzüberschreitende Übermittlung von Daten sich mit dem BDSG vereinbaren läßt. Sollte sich insoweit kein universelles Verbot ergeben, wäre zu fragen, inwieweit durch vertragliche Ausgestaltungen des Datenflusses ein Zustand geschaffen werden kann, der rechtliche Bedenken ausschließt.

B Rechtliche Beurteilung

1. Anwendbarkeit des BDSG

Eine wichtige, wenngleich selten gestellte Vorfrage besteht darin, ob und in welchem Umfang das BDSG überhaupt auf Vorgänge wie die hier zu untersuchenden anwendbar ist. Würde sich der ganze Vorgang beispielsweise nach US-amerikanischem Recht bestimmen, wären andere Beurteilungsmaßstäbe zugrundezulegen.

In der Literatur besteht auf der einen Seite Übereinstimmung darüber, daß der grenzüberschreitende Datenverkehr immer wichtiger wird.

> S. nur Schapper in: Klebe-Roth (Hrsg.), Informationen ohne Grenzen, Hamburg 1987, S. 191/192; Wohlgemuth BB 1991, 340

Bemerkenswert ist auch, daß 90 % der Datentransfers innerhalb multinationaler Konzerne erfolgt.

> Sautner, EDV und Recht (Wien) 1995, 82

Auf der anderen Seite sind klare Kriterien dafür, wann ein nationales Datenschutzrecht eingreift, nicht ersichtlich. So wird etwa für den privaten Sektor einerseits der Standpunkt vertreten, für den gesamten Prozeß der Datenverarbeitung sei im Prinzip das Recht des Aufenthaltsorts des Betroffenen maßgebend,

> so Rigaux, La loi applicable à la protection des individus à l'égard du traitement automatisé de données à caractère personnel, Revue critique de droit international privé 1980, 443 ff.

was im konkreten Fall zur Folge hätte, daß auch die Datenverarbeitung in den USA in bezug auf die in Deutschland tätigen Beschäftigten dem BDSG unterliegen würde. Auf der anderen Seite

wird der Standpunkt vertreten, maßgebend sei das Recht des Orts, wo die Datenverarbeitung stattfinde.

> S. die Nachweise bei Ellger, Der Datenschutz im grenzüberschreitenden Datenverkehr. Eine rechtsvergleichende und kollisionsrechtliche Untersuchung, Baden-Baden 1990, S. 587 ff.

Daneben existieren Auffassungen, die allein auf das Recht des angerufenen Gerichts (Lex fori) sowie darauf abstellen wollen, welche Rechtsordnung den besten Schutz personenbezogener Daten gewährleistet.

> S. den Überblick bei Bergmann, Grenzüberschreitender Datenschutz, Baden -Baden 1985, S. 230 ff.

In der Literatur ist man sich deshalb im wesentlichen einig darüber, daß es derzeit keine überzeugende kollisionsrechtliche Lösung gibt, die Aussicht hätte, allgemeine Anerkennung zu finden.

> Bergmann, a.a.O., S. 235; Ellger, a.a.O., S. 595 f.; Korff RDV 1994, 212

Die allgemeine Tendenz geht deshalb dahin, lediglich eine einseitige Kollisionsnorm des Inhalts zu entwickeln, daß der räumliche Geltungsbereich des BDSG bestimmt wird. Dieses soll immer dann Anwendung finden, wenn die speichernde Stelle ihren Sitz im Inland hat,

> Ellger, a.a.O., S. 609

oder wenn und soweit ein Teil der Datenverarbeitung im Inland erfolgt.

> Bergmann, a.a.O., S. 245

Dies wird u.a. mit der Erwägung gerechtfertigt, beim BDSG handele es sich nicht um "neutrales" Privatrecht, das lediglich

den Rahmen für einen frei ausgehandelten Interessenausgleich zwischen Privaten schaffe; vielmehr handele es sich um sog. ordnungsrelevantes Recht, das einen bestimmten Regelungserfolg sicherstellen wolle; dies mache nicht zuletzt die Einschaltung der Aufsichtsbehörde sowie die Existenz von Straf- und Ordnungswidrigkeitentatbeständen deutlich.

So Ellger, a.a.O., S. 604

Ähnlich wie dies im Betriebsverfassungsrecht allgemein anerkannt ist,

näher Däubler, in: Däubler-Kittner-Klebe-Schneider (Hrsg.), Betriebsverfassungsgesetz mit Wahlordnung, Kommentar für die Praxis, 4. Aufl., Köln 1994, Einleitung Rn 201 ff.

geht man auch im Datenschutzrecht davon aus, daß deutsches Recht alle Vorgänge erfaßt, die sich auf deutschem Territorium abspielen, daß es gleichzeitig jedoch keine Anwendung auf Vorgänge findet, die sich außerhalb der deutschen Grenzen vollziehen.

Eine solche Sicht wird durch Art. 4 Abs. 1 der EG-Richtlinie über den Datenschutz bestätigt, die am 24. Juli 1995 verabschiedet wurde.

Vgl. etwa die Pressemitteilung der Gesellschaft für Datenschutz und Datensicherung (GDD) vom 31. Juli 1995

Danach findet das jeweilige einzelstaatliche Recht Anwendung, wenn die speichernde Stelle ("Verantwortlicher" genannt) eine Niederlassung im Hoheitsgebiet des betreffenden Mitgliedstaats besitzt oder wenn ein in einem Drittstaat niedergelassenes Unternehmen "zum Zwecke der Verarbeitung personenbezogener Daten auf automatisierte oder nichtautomatisierte Mittel zurückgreift, die im Hoheitsgebiet des betreffenden Mitgliedstaats belegen sind." Nach ihrem Art. 32 Abs. 1 Satz 1 ist die Richtlinie zwar erst innerhalb eines Zeitraums von drei Jahren umzu-

setzen, doch ist sie schon heute für die Interpretation des nationalen Rechts zu berücksichtigen: Dies folgt aus dem in Art. 5 EGV niedergelegten Prinzip des gemeinschaftsfreundlichen Verhaltens sowie daraus, daß der EuGH die mitgliedstaatlichen Gerichte sogar verpflichtet, rechtlich nicht verbindliche Empfehlungen als Auslegungshilfen heranzuziehen.

So EuGH NZA 1991, 283; zustimmend BAG DB 1993, 443, 444

Im konkreten Fall bedeutet dies, daß das BDSG in bezug auf die Eingabe in die bei der GmbH befindlichen Terminals Anwendung findet, jedoch nicht auf die Datenverarbeitung in den USA erstreckt werden kann. Die Daten erleiden also - kollisionsrechtlich gesprochen - einen Statutenwechsel.

II. Die Vorgaben des BDSG für die Datenübermittlung ins Ausland, insbesondere in die USA

1. Anwendbare Vorschriften

Das BDSG hat den grenzüberschreitenden Datenverkehr nur an zwei Stellen ausdrücklich erwähnt.

- Für den öffentlichen Bereich hat § 17 BDSG eine relativ eingehende Regelung getroffen. Danach wird eine Weitergabe an ausländische öffentliche oder private Stellen nach den gleichen Grundsätzen behandelt, die für die Übermittlung personenbezogener Daten an nichtöffentliche Stellen im Inland gelten. In einer Reihe von Fällen ist der Betroffene zu unterrichten. Nach § 17 Abs. 2 muß die Übermittlung unterbleiben, wenn sie gegen den Zweck eines deutschen Gesetzes verstoßen würde. Schließlich verlangt § 17 Abs. 4 BDSG, den Empfänger der Daten darauf hinzuweisen, daß er sie nur zu dem Zweck verarbeiten oder nutzen darf, zu dessen Erfüllung sie ihm übermittelt wurden.

- Für den hier interessierenden privaten Bereich existiert keine vergleichbare Regelung. Mittelbar kommen die Besonderheiten der Übermittlung über die Grenze nur in § 3 Abs. 9 Satz 2 BDSG zur Geltung, wonach eine im Ausland befindliche Person oder Stelle auch dann "Dritter" ist, wenn sie die Daten im Auftrage der speichernden Stelle verarbeitet oder nutzt. Anders ausgedrückt: Eine Auftragsdatenverarbeitung, die die Verantwortung für die Einhaltung des BDSG beim Auftraggeber beläßt, ist nur innerhalb des Territoriums der Bundesrepublik möglich; bei Überschreitung der Grenzen ist zwingend eine "Übermittlung" anzunehmen.

Für die Anforderungen, der eine solche Übermittlung genügen muß, enthält das BDSG keine spezifischen Regeln. Man wendet deshalb die allgemeinen Vorschriften an, die für eine Übermittlung im Inland gelten.

> Allgemeine Meinung; vgl. nur Bergmann, a.a.O., S. 83; Ellger, a.a.O., S. 434; Schapper CR 1987, 86

Da die Übermittlung nach der Legaldefinition des § 3 Abs. 5 zur "Verarbeitung" von Daten gehört, bestimmt sich die Zulässigkeit nach § 4 Abs. 1 BDSG. Danach sind drei Fälle denkbar:

- Die Übermittlung kann mit Einwilligung des Betroffenen erfolgen, deren nähere Voraussetzungen in § 4 Abs. 2 BDSG geregelt sind.

- Das BDSG läßt die Übermittlung zu. Hier ist insbesondere an § 28 Abs. 1 Satz 1 Nr. 1 (Zweckbestimmung eines Vertragsverhältnisses) sowie an § 28 Abs. 1 Satz 1 Nr. 2 und an § 28 Abs. 2 Nr. 1 lit. a zu denken, wonach berechtigte Interessen der speichernden Stelle bzw. Dritter oder öffentliche Interessen eine Übermittlung rechtfertigen, sofern kein Grund zu der Annahme besteht, daß schutzwürdige Interessen des Betroffenen entgegenstehen bzw. überwiegen.

- Schließlich ermöglicht § 4 Abs. 1 BDSG eine Datenverarbeitung auch dann, wenn sie "eine andere Rechtsvorschrift erlaubt".

2. Auslegungsgrundsätze

Die Tatsache, daß mit Ausnahme der Vorschrift über die Auftragsdatenverarbeitung dieselben Bestimmungen für den innerstaatlichen wie für den grenzüberschreitenden Datentransfer gelten, bedeutet nicht, daß diese den spezifischen Umständen nicht Rechnung tragen könnten, die sich bei der transnationalen Übermittlung ergeben. So wird insbesondere das "schutzwürdige Interesse" des Betroffenen einer Weitergabe häufiger entgegenstehen, wenn am Zielort weder Datenschutz noch Datensicherung existieren. Soweit ersichtlich, besteht hierüber auch keine Meinungsverschiedenheit.

Im einzelnen ist zunächst danach zu fragen, ob die ausländische Rechtsordnung einen zumindest gleichwertigen Datenschutz wie das deutsche Recht gewährt. Dabei sind ohne Rücksicht auf die Bezeichnung als "Datenschutznorm" ("data protection", "protection des données") alle diejenigen gesetzlichen und richterrechtlichen Normen zu berücksichtigen, die den Vorgang der Datenverarbeitung betreffen. Mit Recht wurde weiter auch darauf verwiesen, daß die Einflußmöglichkeiten der Arbeitnehmerseite, wie sie etwa in Deutschland § 87 Abs. 1 Nr. 6 BetrVG sicherstellt, ebenfalls in die vergleichende Betrachtung eingehen müssen.

Simitis CR 1991, 176

Von Bedeutung ist weiter auch, ob die im Ausland geltenden Vorschriften ernst genommen werden oder nicht.

Kilian RdA 1978, 713

Bloße Empfehlungen oder Selbstverpflichtungen einzelner Unternehmen sind ohne Bedeutung, da sie jederzeit ohne Rechtsverstoß wieder rückgängig gemacht werden können.

Ellger, a.a.O., S. 209

Läßt sich aufgrund der vorliegenden Informationen nicht klären, in welchem Umfang verbindliche Regeln bestehen, so ist davon auszugehen, daß kein angemessenes Schutzniveau existiert.

So ausdrücklich die Checkliste der Aufsichtsbehörden für grenzüberschreitenden Datenverkehr, wiedergegeben in DuD 1993, 712

Bei der Beurteilung der Gleichwertigkeit ist weiter nicht nur auf das materielle Recht zu schauen, sondern auch die Frage einzubeziehen, inwiefern Aufsichtsinstanzen zentraler oder dezentraler Natur existieren, die Verstöße im einzelnen aufzudekken vermögen.

Besteht in einem fremden Staat kein oder jedenfalls kein angemessener Datenschutz, so stellt die Übermittlung von Daten dorthin einen in seiner Tragweite schwer einschätzbaren, potentiell umfassenden Eingriff in das Recht auf informationelle Selbstbestimmung dar.

Ellger, a.a.O., S. 140; Wohlgemuth BB 1991, 340

Der Betroffene kann nicht mehr beurteilen, was mit seinen Daten im einzelnen geschieht, zu welchen Zwecken sie verwendet, ob sie an beliebige Dritte weitergegeben oder veröffentlicht werden usw. Die Datei wird potentiell zum "Selbstbedienungsladen"; in der Literatur ist davon die Rede, es handele sich um eine umfassende "Verarbeitungsfreigabe"

so Wohlgemuth BB 1991, 340 unter Berufung auf Simitis,

an anderer Stelle findet sich die Aussage, der einzelne werde "datenmäßig vogelfrei".

So Schapper, in: Klebe-Roth, a.a.O., S. 200

Aber auch dann, wenn die Verarbeitungsvoraussetzungen als solche im wesentlichen dem deutschen Recht entsprechen, ergeben sich für den Betroffenen eine Reihe gravierender Nachteile. Zum einen kann die Datentransparenz leiden, wenn unklar ist, wo sich im einzelnen der Datenempfänger befindet - dies insbesondere dann, wenn er seinerseits berechtigt ist, die Daten unter bestimmten Voraussetzungen an andere Personen weiterzugeben. Wichtiger ist, daß normalerweise die Kontrollrechte versagen, die im Inland existieren: Die Aufsichtsbehörde hat keinen Zugriff auf die im Ausland gespeicherten Daten, der betriebliche Datenschutzbeauftragte wird seine Kompetenz im Regelfall gleichfalls nicht hierauf erstrecken können. Auch der Betriebsrat wird zumindest Schwierigkeiten haben, einen entsprechenden Auskunftsanspruch durchzusetzen. Der Betroffene selbst hat bei der Wahrung seiner Rechte das Problem, die speichernde Stelle oft nicht zu kennen und wegen Sprachproblemen mit ihr ggf. nur unter Schwierigkeiten kommunizieren zu können.

Dazu insgesamt Bergmann, a.a.O., S. 78; Gola-Wronka, Handbuch zum Arbeitnehmerdatenschutz. Rechtsfragen und Handlungshilfen für die betriebliche Praxis, 2. Aufl., Köln 1994, S. 207; Wohlgemuth BB 1991, 340

Eine grenzüberschreitende Übermittlung von Daten ist für den Betroffenen unter diesen Umständen sehr viel belastender; dies ist bei der Handhabung der in § 4 Abs. 1 BDSG in bezug genommenen Vorschriften zu beachten.

3. Die Situation in den USA

Wie eine neuere Untersuchung ergab,

Welske CR 1993, 297 ff.

kann der Datenschutz in den USA nicht als dem deutschen gleichwertig qualifiziert werden.

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" (Polygraph) beschränkt und nicht etwa ausgeschlossen; im übrigen dürfen vorhandene Informationen nicht zu einer Diskriminierung insbesondere wegen Rasse und Geschlecht verwendet werden.

Welske CR 1993, 303

Ansonsten bestehen keine bundesrechtlichen Grenzen in bezug auf die Sammlung, Speicherung und Nutzung von Arbeitnehmerdaten.

Auf einzelstaatlicher Ebene ist die Situation nur unwesentlich besser. Trotz Bestimmungen über die Handhabung von Personalakten, die in einigen Staaten existieren, ist die Art der Datenerhebung, der Umfang und die Dauer der Speicherung weiterhin völlig frei. Dem Arbeitgeber ist es nicht untersagt, quasi beliebige Daten zu sammeln und sie für andere als die der Erhebung zugrundeliegenden 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.

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.

Die Erklärung von 181 US-Unternehmen, sich freiwillig an die OECD-Richtlinien zum Datenschutz zu halten,

mitgeteilt bei Ellger, a.a.O., S. 209

vermag daran nichts zu ändern.

Ein rechtlich relevantes "Datenschutzgefälle" würde auch dann bestehen, wenn man nicht das BDSG, sondern beispielsweise die Datenschutzkonvention des Europa-Rats und die OECD-Richtlinien als Maßstab nehmen würde.

Dafür Bergmann-Möhrle-Herb, Kommentar zum BDSG, Stuttgart u.a., Loseblatt (Stand: März 1995), § 28 Rn 150

Auch bei einem solchen großzügigeren Maßstab wäre die Gleichwertigkeit nicht erreicht. Dasselbe gilt dann, wenn man mit Art. 25 der EG-Datenschutzrichtlinie lediglich ein "angemessenes" Schutzniveau voraussetzt; auch dieses kann nicht als gegeben anerkannt werden.

III. Rechtfertigung durch Einwilligung der betroffenen Mitarbeiter?

1. Die Fragestellung

Die spezifischen Probleme, die sich durch ein "Datenschutzgefälle" ergeben, könnten möglicherweise dadurch auf einfache Art ausgeräumt werden, daß der einzelne Arbeitnehmer in die Übermittlung seiner Daten ausdrücklich einwilligt. Zum Teil wird in der Literatur hierin ein wichtiger Ausweg gesehen,

So Drews DuD 1994, 68

während andernorts hervorgehoben wird, diesem Weg komme trotz einiger Versuche multinationaler Unternehmen kaum Bedeutung zu.

Wohlgemuth BB 1991, 341

2. Formelle Voraussetzungen der Einwilligung

a) Zeitpunkt

Von einer Einwilligung im Sinne des § 4 BDSG kann nur dann die Rede sein, wenn die Erklärung vor dem Datenverarbeitungsvorgang abgegeben wurde. Insoweit hat der Gesetzgeber die Terminologie des § 183 BGB übernommen.

Gola-Wronka, a.a.O., S. 126; Kroll, Datenschutz im Arbeitsverhältnis, Königstein/Ts. 1981, S. 166; Tinnefeld-Ehmann, Einführung in das Datenschutzrecht, München 1992, S. 103 u.a.

Eine nachträglich erteilte Zustimmung hat keine legalisierende Wirkung.

b) Klare Reichweite der Einwilligung

Die rechtfertigende Wirkung der Einwilligung reicht nur so weit wie der Wille des Erklärenden. Dabei werden relativ hohe Anforderungen gestellt. Eine Blankoeinwilligung, die den Umfang der erfaßten und/oder verwendeten Daten dem Ermessen des Adressaten überläßt, ist unwirksam.

Kroll, a.a.O., S. 175; Simitis, in: Simitis-Dammann-Geiger-Mallmann-Walz, Kommentar zum Bundesdatenschutzgesetz, Baden-Baden, Loseblatt (Stand: Juli 1994) § 4 Rn 55; Tinnefeld-Ehmann, a.a.O., S. 104

Der Arbeitnehmer muß wissen, um welche Angaben es sich handelt, ob sie bei ihm oder bei Dritten erhoben werden, für welche

Zwecke sie verwendet, und ob sie ggf. an Dritte weitergegeben werden. Maßgebend für diese Beschränkung der Dispositionsfreiheit ist die Erwägung, daß das Persönlichkeitsrecht keine "Selbstentäußerung" verträgt, daß auch freiwillige Einschränkungen für den Betroffenen in ihren Wirkungen überschaubar bleiben müssen. Konsequenterweise gilt der Grundsatz der Zweckbindung auch hier; nur in dem vom Betroffenen gewollten Rahmen darf die Verarbeitung erfolgen.

> Baumann DVBl 1984, 615; Kroll, a.a.O., S. 178; Wohlgemuth, Datenschutz für Arbeitnehmer, 2. Aufl., Neuwied 1988, Rn 198

c) Informationspflicht des Arbeitgebers

Nach § 4 Abs. 2 Satz 1 BDSG muß der Betroffene auf den Zweck der Speicherung und einer vorgesehenen Übermittlung sowie auf Verlangen auf die Folgen der Verweigerung der Einwilligung hingewiesen werden. Der Gesetzgeber will nur die "informierte" Einwilligung anerkennen.

> Ellger, a.a.O., S. 219, 445

Angesichts der Übermittlung ins Ausland besteht insoweit eine gesteigerte Hinweispflicht, die dem Betroffenen Umfang und Konsequenzen der beabsichtigten Datenverarbeitung vor Augen führt.

> Bergmann-Möhrle-Herb, a.a.O., § 4 Rn 50

Dabei ist selbstredend vorausgesetzt, daß zugleich die personenbezogenen Daten benannt werden, um die es geht; andernfalls wäre die "Belehrung" ohne Bedeutung.

> Bergmann-Möhrle-Herb, a.a.O., § 4 Rn 47; Ordemann-Schomerus-Gola, BDSG, Kommentar, 5. Aufl., München 1992, § 4 Anmerkung 5.4.

Fehlt sie, ist die Einwilligung unwirksam, da dann eine wesentliche gesetzliche Voraussetzung nicht erfüllt ist.

Tinnefeld-Ehmann, a.a.O., S. 104; Wohlgemuth, Datenschutzrecht. Eine Einführung mit praktischen Fällen, 2. Aufl., Neuwied u.a. 1993, Rn 121; a.A. Dörr RDV 1992, 167

d) Schriftform

Nach § 4 Abs. 2 Satz 2 BDSG bedarf die Einwilligung im Regelfall der Schriftform. Dies setzt die Unterschrift des Betroffenen unter eine Erklärung voraus (§ 126 BGB). Wird dieser Form nicht Genüge getan, ist die Einwilligung unwirksam.

Dörr RDV 1992, 168; Tinnefeld-Ehmann, S. 105 u.a.

Schon diese formalen Voraussetzungen machen deutlich, daß die Einwilligung aus Arbeitgebersicht ein schwer zu handhabendes Mittel darstellt. Der Aufwand, um die Einwilligungserklärungen zu erreichen, wäre beträchtlich. Ein Einsatz von Arbeitnehmern am System SAP R/3 wäre nur möglich, wenn vorher eine auf umfassender Information basierende Einwilligung erteilt wäre. Auch hat der Arbeitgeber keine Möglichkeit, die Einwilligung in jedem Einzelfall zu erzwingen; ein Arbeitnehmer mit starker Stellung (die sich z.B. aus einem verstärkten Kündigungsschutz ergeben kann) ist durchaus in der Lage, "nein" zu sagen und so ggf. die Inbetriebnahme oder Fortführung des Systems zu blockieren, sofern er nicht unschwer durch einen Arbeitskollegen ersetzt werden kann.

3. Mitbestimmungspflichtigkeit der Aufforderung zur Einwilligung

An alle Arbeitnehmer oder an eine Arbeitnehmergruppe mit der Frage heranzutreten, ob sie ihre Einwilligung in eine bestimmte Datenübermittlung geben wollen, stellt überdies einen Vorgang dar, der der Mitbestimmung des Betriebsrats nach § 94 BetrVG unterliegt. Obwohl höchstrichterliche Entscheidungen zu dieser Frage nicht ersichtlich sind, steht die ganz überwiegende Auffassung in der Literatur auf dem Standpunkt, daß auch eine sol-

che Einzelfrage unter den Begriff des Personalfragebogens im Sinne des § 94 Abs. 1 BetrVG fällt.

> Fitting-Auffarth-Kaiser-Heither, Handkommentar zum BetrVG, 17. Aufl., München 1992, § 94 Rn 10; Gitter-Henker ZTR 1990, 409; Kilian RdA 1978, 205; Klebe, in: Däubler-Kittner-Klebe-Schneider, a.a.O., § 94 Rn 27; Küpferle-Wohlgemuth, Personaldatenverarbeitende Systeme. Rechtsprobleme und Argumentationsmöglichkeiten aus der Sicht der Beschäftigten, Köln 1987, Rn 165 f., 217 ff.; Wohlgemuth, Arbeitnehmerdatenschutz, a.a.O., Rn 685; ders. BB 1991, 341; Däubler, Gläserne Belegschaften? Datenschutz für Arbeiter, Angestellte und Beamte, 3. Aufl., Köln 1993, Rn 373; ders., Das Arbeitsrecht 1, 14. Aufl., Reinbek 1995, Rn 1029; wohl auch MünchArbR-Blomeyer § 97 Rn 18; a.A, nur Kraft, in: Fabricius-Kraft-Thiele-Wiese-Kreutz, Gemeinschaftskommentar zum BetrVG, Bd. 2, 4. Aufl., Neuwied 1990, § 94 Rn 16; MünchArbR-Matthes § 339 Rn 14

In der Tat kann es keinen Unterschied machen, wie zahlreich die an die Arbeitnehmer oder eine bestimmte Gruppe gerichteten Fragen sind.

4. Inhaltliche Schranken

Schließlich ist zweifelhaft, ob die von einem Arbeitnehmer abgegebene Einwilligung überhaupt wirksam ist, weil er sich typischerweise nicht in einer Situation befindet, in der er ohne Vermeidung von Nachteilen "nein" sagen kann. In der Literatur wird daraus u.a. die Konsequenz gezogen, das Einverständnis des Arbeitnehmers könne lediglich die Verarbeitung von Angaben rechtfertigen, die für das konkrete Arbeitsverhältnis objektiv erforderlich seien.

> Simitis, in: Simitis u.a., a.a.O., § 4 Rn 27 mwN

Andere vertreten den Standpunkt, daß eine formularmäßig erteilte oder auf gleichförmigen Fragen beruhende Einwilligung nur dann wirksam ist, wenn sie unter Abwägung der beiderseitigen Interessen der Billigkeit entspricht.

Vgl. Bergmann-Möhrle-Herb, a.a.O., § 28 Anlage 6 unter 4.2., die Unbilligkeit nach § 9 AGB-Gesetz annehmen, wenn im Ausland kein vergleichbarer Datenschutz besteht und die deshalb im Arbeitsverhältnis, wo das AGB-Gesetz keine Anwendung findet, unmittelbar zur Konsequenz einer Unbilligkeit kommen müßten; Däubler, Gläserne Belegschaften? Rn 138 ff.

Im Ergebnis kann diese Frage allerdings dahinstehen, da im konkreten Fall weder eine Initiative der Geschäftsleitung zur Erlangung der Einwilligungen noch ein an den Betriebsrat gerichteter Antrag ersichtlich ist, einer derartigen Aktion seine Zustimmung zu erteilen.

IV. Rechtfertigung durch den Arbeitsvertrag?

1. Die Problematik

Nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG ist das Übermitteln personenbezogener Daten "im Rahmen der Zweckbestimmung eines Vertragsverhältnisses" zulässig. Dies gilt - wie oben ausgeführt - auch für Fälle von grenzüberschreitender Übermittlung. So ist es beispielsweise allgemein akzeptiert, daß als Folge eines Überweisungsauftrags zugunsten eines ausländischen Gläubigers 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 auch Arbeitnehmerdaten auch bei rein innerstaatlichen Konzernen grundsätzlich nicht an andere Konzerngesellschaften übermittelt werden dürfen. Auch eine Rechtfertigung nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG scheidet nach ganz überwiegender Auffassung aus, da es angesichts der gesetzgeberischen Entscheidung für die "Informationseinheit Unternehmen" kein "berechtigtes" Interesse

des Arbeitgebers darstellt, Daten von einem Konzernunternehmen an ein anderes übermitteln zu können.

> Freise-Wohlgemuth DVR 1982, 288; Gola-Wronka, a.a.O., S. 204; Kroll, a.a.O., S. 115 ff.; Wohlgemuth BB 1991, 341 und BB 1992, 283 mwN; a.A. nur Zöllner, Daten- und Informationsschutz im Arbeitsverhältnis, Köln-Berlin u.a. 2. Aufl., 1983, S. 49

Erst recht überschreitet es daher den vom Arbeitsvertrag gezogenen Verarbeitungsrahmen, wenn Daten im Rahmen eines multinationalen Konzerns an ein ausländisches Konzernunternehmen übermittelt werden sollen.

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

2. Der Ausnahmetatbestand

Beim rein innerstaatlichen Konzern wird dann eine Ausnahme gemacht, wenn sich das Arbeitsverhältnis nicht auf das Arbeitgeberunternehmen beschränkt, sondern Rechtsbeziehungen des einzelnen Arbeitnehmers auch zur Konzernspitze hergestellt werden.

> Zu einem solchen konzerndimensionalen Arbeitsverhältnis s. Däubler, Arbeitsrecht 2, 10. Aufl., Reinbek 1995, S. 666 ff. mwN

In diesen Fällen existiert eine vertragliche oder vertragsähnliche Beziehung zu allen Konzernunternehmen, in denen ein Arbeitseinsatz in Betracht kommt.

Dieselbe Position wird in der Literatur nun auch in bezug auf grenzüberschreitende Konzerne vertreten. Wird der Arbeitnehmer einvernehmlich auch für Auslandseinsätze vorgesehen, hält sich der damit verbundene Datenfluß innerhalb des vertraglich Vereinbarten und ist deshalb durch § 28 Abs. 1 Satz 1 Nr. 1 BDSG gedeckt.

> Ebenso Bergmann, a.a.O., S. 84; Bergmann-Möhrle-Herb § 28 Anlage 6 unter 5.2.2; Däubler, Gläserne Belegschaften? Rn

254; Drews DuD 1994, 68; Ellger, a.a.O., S. 201; Ordemann-Schomerus-Gola, a.a.O., § 28 Anm. 8.2.; Schapper, in: Klebe-Roth, a.a.O., S. 199; Wohlgemuth BB 1991, 342

Dasselbe wird dann angenommen, wenn bei der Einstellung deutlich erkennbar ist, daß die Personaldatenverarbeitung in einem anderen Land zentralisiert ist.

Bergmann, a.a.O., S. 84; Bergmann-Möhrle-Herb § 28 Anlage 6 unter 5.3; Ellger, a.a.O., S. 199; Ordemann-Schomerus-Gola, a.a.O., § 28 Anm. 8.2.

Eine solche vertragliche Legitimierung deckt ersichtlich nicht den Fall, der hier zur Debatte steht: Beim Abschluß des Arbeitsvertrags war für die Betroffenen nicht absehbar, daß Daten über ihr Arbeitsverhalten in eine weltweit für alle Aktivitäten des Konzerns zuständige ausländische Datenbank eingespeist würden. Die Tatsache, daß man einen Arbeitsvertrag mit einem (nationalen oder internationalen) Konzern schließt, enthält nach allgemeiner Auffassung nicht die stillschweigende Ermächtigung, Daten von einem Konzernteil in einen anderen zu transferieren: Andernfalls wäre der Unternehmensbezug des BDSG gegenstandslos.

Im konkreten Fall mag es einzelne Beschäftigte geben, die ein sog. konzerndimensionales Arbeitsverhältnis besitzen; nach den verfügbaren Informationen ist dies allenfalls eine kleine Minderheit, so daß das geplante System nicht auf der Grundlage einer Datenübermittlung nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG betrieben werden kann.

Ergänzend sei darauf hingewiesen, daß auch im Rahmen konzerndimensionaler Arbeitsverhältnisse keine beliebige Datenübermittlung zulässig wäre. Zwar ist es nicht möglich, den Vorbehalt zugunsten der "schutzwürdigen Interessen des Betroffenen" aus der Nr. 2 in die Nr. 1 des § 28 Abs. 1 Satz 1 BDSG hineinzuprojizieren, da der Vertrag die Verarbeitungsmöglichkeiten abschließend umschreibt.

Bergmann, a.a.O., S. 86 f.; Däubler, Gläserne Belegschaften? Rn 254; Drews DuD 1991, 513

Dies bedeutet jedoch nicht, daß damit jede arbeitsvertragliche Abmachung zulässig wäre: Diese muß sich vielmehr eine Billigkeitskontrolle gefallen lassen.

Däubler, Arbeitsrecht 2, a.a.O., S. 118 f., 123

Dies bedeutet, daß Abmachungen keine rechtliche Anerkennung verdienen, mit denen der Arbeitgeber ausschließlich eigene Interessen durchsetzt. Dies wäre aber der Fall, würde man eine Überspielung von Daten in ein Land ermöglichen, wo praktisch beliebig mit ihnen verfahren werden könnte. Von "billigem Interessenausgleich" könnte nur dann die Rede sein, wenn auch in einem solchen Fall für ein ausreichendes Maß an Datenschutz gesorgt wäre, was den Umständen nach nur durch vertragliche Bindungen des Arbeitgebers und des ausländischen Unternehmens möglich wäre.

Ähnlich (wenn auch ohne den Ausweg über vertragliche Abmachungen) Wohlgemuth BB 1991, 342; auf die Fürsorgepflicht des Arbeitgebers stützen sich Bergmann-Möhrle-Herb, a.a.O., § 28 Anlage 6 unter 5.2.2; Gola-Wronka, a.a.O., S. 207

Da solche kompensatorischen Verträge an anderer Stelle eine größere Rolle spielen, sollen sie dort behandelt werden.

V. Rechtfertigung der Datenübermittlung mit berechtigten Interessen des Arbeitgebers nach § 28 Abs. 1 Satz 1 Nr.2 BDSG?

1. Anwendbarkeit des § 28 Abs. 1 Satz 1 Nr. 2 BDSG neben vertraglichen Rechtsbeziehungen?

Im Rahmen der Speicherung (deren Zulässigkeit sich gleichfalls nach § 28 Abs. 1 Satz 1 BDSG bestimmt), aber auch im vorliegenden Zusammenhang ist streitig, ob sich der Arbeitgeber für die Übermittlung von Daten nicht nur auf den Arbeitsvertrag, sondern auch auf die Generalklausel des § 28 Abs. 1 Satz 1 Nr. 2 BDSG berufen darf, wonach die Übermittlung zulässig ist, "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 oder Nutzung überwiegt." Einen vergleichbaren Tatbestand enthält § 28 Abs. 2 Nr. 1 lit. a, wonach die Übermittlung auch dann zulässig ist, "soweit es zur Wahrung berechtigter Interessen eines Dritten oder öffentlicher Interessen erforderlich ist" und "kein Grund zu der Annahme besteht, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat."

Die Rechtsprechung steht auf dem Standpunkt, daß trotz vertraglicher Beziehungen auch die Generalklausel des "berechtigten Interesses" als Grundlage für die Speicherung und Übermittlung von Daten herangezogen werden kann.

> So zum BDSG 1977 BGH NJW 1984, 436; BAG EzA § 87 BetrVG 1972 Kontrolleinrichtung Nr. 15 (S. 135).

Auch die Mehrheit in der Literatur hat sich dieser Auffassung angeschlossen.

> Bergmann-Möhrle-Herb § 28 Anlage 6 unter 5.5; Ehmann, Beilage 1/1985 zu NZA S. 5; Ellger, a.a.O., S. 102; Sproll ZIP 1984, 30; a.A. Däubler, Gläserne Belegschaften? Rn 185; Ordemann-Schomerus-Gola, § 28 Anm. 2.2; Wohlgemuth, Datenschutz für Arbeitnehmer, Rn 246, 461; ders., BB 1991, 341

Die besseren Argumente dürften gleichwohl für den Vorrang des vertraglich vereinbarten Zwecks sprechen. Durch den Abschluß eines Vertrages wird ein "Verarbeitungsrahmen" geschaffen, wird bewußt und gewollt bestimmt, was den Beteiligten erlaubt und

was ihnen verboten sein soll. Diese Festlegung darf nicht nachträglich dadurch korrigiert werden, daß pauschal auf die "berechtigten Interessen" einer Seite zurückgegriffen und eine Gegenindizierung lediglich am Maßstab "schutzwürdiger Belange" der anderen Seite vorgenommen wird. Wollte man dies tun, so wäre nicht nur der Wille der Beteiligten überspielt, sondern auch der Gedanke der Zweckbindung verletzt: Die zu bestimmten vertragskonformen Zwecken erhobenen Daten könnten für ganz andere Zwecke gespeichert (und dann ausgewertet) werden.

Dennoch soll im folgenden die Position der Rechtsprechung zugrundegelegt werden, da es nicht um die Entscheidung einer wissenschaftlichen Kontroverse, sondern allein darum geht, den rechtlichen Rahmen für praktisches Verhalten zu bestimmen: Dieser wird aber bis auf weiteres durch die Rechtsprechung gezogen.

2. Die Voraussetzungen des § 28 Abs. 1 Satz 1 Nr. 2 BDSG im einzelnen

Erste Voraussetzung für eine Übermittlung ist, daß sie "zur Wahrung berechtigter Interessen" des Arbeitgebers erforderlich ist. Dies wird man im vorliegenden Zusammenhang ohne großes Zögern bejahen können: 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" konstituieren können, 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. Im vorliegenden Zusammenhang besteht jedoch Grund zu einer solchen Annahme: Die personenbezogenen Daten der Betroffenen werden in die USA übermittelt, wo bei weitem kein vergleichbarer Datenschutz existiert und wo auch

eine Kontrolle durch Aufsichtsbehörde, betrieblichen Datenschutzbeauftragten, Betriebsrat und einzelnen Arbeitnehmer faktisch ausscheidet. Eine schwerere Beeinträchtigung schutzwürdiger Interessen im datenschutzrechtlichen Sinne ist kaum vorstellbar. Im Ergebnis ist man sich deshalb auch im wesentlichen darüber einig, daß § 28 Abs. 1 Satz 1 Nr. 2 BDSG eine grenzüberschreitende Datenübermittlung allenfalls dann rechtfertigen kann, wenn durch Vertrag sichergestellt wird, daß auch im Ausland ein äquivalentes Maß an Datenschutz praktiziert wird.

> S. statt aller Bergmann-Möhrle-Herb § 28 Anlage 6 unter 5.5.; Däubler, Gläserne Belegschaften? Rn 254a; Ordemann-Schomerus-Gola § 28 Anm. 8.1; Ungnade-Gorynia WM-Sonderbeilage 7/1983, S. 17; Wohlgemuth BB 1991, 342

Derselben Auffassung ist offensichtlich auch die GmbH, da andernfalls der vorgelegte Vertragsentwurf mit der Corporation nicht recht verständlich wäre.

3. Wahrung "schutzwürdiger Interessen" durch Vertrag?

Die Frage, ob "schutzwürdige Interessen" der Betroffenen überhaupt durch Vertrag gesichert werden können, wird durchaus unterschiedlich eingeschätzt. Ein beträchtlicher Teil der Literatur lehnt eine solche Lösung ab und hält die Datenübermittlung deshalb definitiv für unzulässig. Im einzelnen werden dazu hauptsächlich drei Argumente vorgetragen.

(1) Die deutschen Aufsichtsbehörden können nicht kontrollieren, ob im Ausland dem Vertrag entsprechend verfahren wird.

> Bergmann, a.a.O., S. 220; Simitis CR 1991, 177; Wohlgemuth BB 1991, 342

(2) Der Vertrag gibt dem Betroffenen keine ausreichenden Rechte. Typischerweise ist er selbst nicht Vertragspartei,

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

ein Vertrag zugunsten Dritter sei normalerweise nicht gewollt.

So Ellger, a.a.O., S. 444

Die Beteiligten hätten die Möglichkeit, den Vertrag jederzeit an neue Informationsbedürfnisse der Konzernspitze anzupassen

so Ellger, a.a.O., S. 204

oder ihn aufzuheben oder zu kündigen.

Wohlgemuth BB 1991, 342

Auch hätte der deutsche Arbeitgeber kein Eigeninteresse daran, die datenschutzrechtlichen Befugnisse seiner Beschäftigten gegen eine mächtige ausländische Konzernspitze durchzusetzen.

Ellger, a.a.O.,. S. 204

(3) Die Daten unterliegen dem Zugriff durch die Behörden des anderen Landes. Dies kann zu einer Gefährdung der Datensicherheit, aber auch zu anderen Unzuträglichkeiten führen.

Vgl. Simitis CR 1991, 177; Wohlgemuth BB 1992, 284

Das erste Argument ist sicherlich zutreffend; ohne Zustimmung ausländischer Instanzen kann eine deutsche Behörde im Ausland keine Funktionen wahrnehmen. Auch eine vertragliche Erstreckung ihrer Kompetenzen kommt nicht in Betracht. Insofern besteht die Notwendigkeit, andere Kontrollmechanismen vorzusehen, die dieses Defizit auszugleichen vermögen.

Das zweite Argument ist sehr viel problematischer. Als Vertragspartei kommen zwar in der Tat nur die betroffenen Konzern-

unternehmen in Betracht, doch kann ihnen niemand verbieten, entgegen dem bisher Üblichen eine echten Vertrag zugunsten Dritter im Sinne des § 328 Abs. 1 BGB abzuschließen: Sie können den betroffenen Arbeitnehmern das Recht einräumen, die vom BDSG vorgesehenen Ansprüche auch gegenüber der ausländischen Konzerngesellschaft geltend zu machen. § 328 Abs. 2 läßt es überdies zu, im Vertrag vorzusehen, daß die Rechte der "Dritten" nicht ohne deren Zustimmung aufgehoben werden können. Macht man davon Gebrauch, ist auch die Gefahr gebannt, daß die Vertragsparteien ihre Abmachung aus Opportunitätsgründen jeweils an veränderte Umstände anpassen oder ihn kündigen bzw. aufheben.

Werden keine unentziehbaren Rechte eingeräumt, besteht gleichfalls nicht die Gefahr, daß der Vertrag über die Köpfe der Betroffenen hinweg verändert oder gar gekündigt oder aufgehoben wird. Etwas Derartiges wäre zwar rechtlich möglich, für die beteiligten Unternehmen jedoch in keiner Weise wünschenswert: Mit dem Wegfall des die "schutzwürdigen Interessen" der Betroffenen wahrenden kompensatorischen Vertrages würde die Datenübermittlung ins Ausland unzulässig. Notfalls könnte sie im Wege der einstweiligen Verfügung untersagt werden.

Das dritte Argument ist seinerseits wieder schlüssig, doch spielt es in der Praxis so gut wie keine Rolle. Niemand nimmt etwa Anstoß daran, daß einzelne Geschäftsreisende ihren Laptop samt Disketten ins Ausland mitnehmen, obwohl sie dem Zugriff ausländischer Staatsgewalten ausgesetzt sind, gegen den man sich nur schwer zur Wehr setzen könnte. Ein im Ausland angesiedeltes Konzernunternehmen ist demgegenüber in der Lage, sich gegen einen unangemessenen oder rechtswidrigen Zugriff der ausländischen Behörden auf seine Datenvorräte zu schützen. Die Zeiten, in denen eine willkürlich vorgehende Staatsgewalt bei einem ausländischen Unternehmen mal "Haussuchung" macht und dabei einige Betriebsgeheimnisse erbeutet, sind längst vorbei; in der Realität wird alles versucht, um Investoren nicht vom eigenen Standort abzuschrecken. Auch muß man im vorliegenden Zusam-

menhang berücksichtigen, daß eine (theoretische) Gefahr allenfalls für technische Daten, nicht aber für Daten der in Deutschland tätigen Arbeitnehmer besteht. Daß sich der FBI für sie interessieren könnte ist denkbar fernliegend; außerdem untersteht auch er grundsätzlich rechtsstaatlichen Sicherungen.

Die Argumente der Gegner einer "Vertragslösung" vermögen daher nicht zu überzeugen. Den schutzwürdigen Interessen des bzw. der Betroffenen kann durch eine entsprechende Vertragsgestaltung in vollem Umfang Rechnung getragen werden. Legt man dies zugrunde, sind die Voraussetzungen des § 28 Abs. 1 Satz 1 Nr. 2 BDSG eindeutig erfüllt; schon der Grundsatz der Bindung des Richters an das Gesetz schließt es aus, in einem solchen Fall eine Übermittlung ins Ausland gleichwohl zu blockieren. Davon ganz abgesehen würde es an den Bedürfnissen der Unternehmenspraxis völlig vorbeigehen, wollte man trotz vertraglicher Sicherungen ein Stop-Schild an der Grenze anbringen: Umgehungsstrategien wären vorprogrammiert wie etwa die, manuell erhobene Daten in ein weniger streng vorgehendes Nachbarland zu verbringen und von dort aus - dann ohne jegliche vertragliche Sicherungen! - in den vorgesehenen Zentralrechner zu überspielen.

4. Anforderungen an den Vertrag im einzelnen

Um die "schutzwürdigen Interessen" der Betroffenen zu wahren, muß der zwischen dem deutschen Arbeitgeber und dem ausländischen Datenempfänger geschlossene Vertrag einen äquivalenten Schutz wie das BDSG sicherstellen und überdies zusätzliche Mechanismen vorsehen, die einen Ausgleich für die wegfallenden Kontrollbefugnisse der Aufsichtsbehörde darstellen.

Notwendig ist zunächst, daß dasselbe inhaltliche Schutzniveau wie nach BDSG festgeschrieben wird. Dies bedeutet, daß keine umfassenderen Verarbeitungsmöglichkeiten eröffnet werden als sie auch bei einem rein innerstaatlichen Sachverhalt zulässig wären.

Zum zweiten ist dafür zu sorgen, daß die Informations- und Kontrollrechte des einzelnen entsprechend §§ 33 ff. BDSG eine vertragliche Festschreibung erfahren. Dabei ist Gleichwertigkeit nur dann gegeben, wenn die Betroffenen nicht den Umweg über den deutschen Arbeitgeber gehen müssen, sondern sich direkt an die ausländische speichernde Stelle wenden können. Der Weg dorthin darf nicht mit wesentlichen organisatorischen oder sprachlichen Schwierigkeiten verbunden sein.

Auch die betriebliche Interessenvertretung muß die Möglichkeit haben, die Einhaltung der vertraglichen Verarbeitungsbschränkungen wirksam zu kontrollieren. Dies wird im Einzelfall durch eine entsprechende Einschaltung in das System möglich sein, doch kann es auch erforderlich werden, eine Besichtigung vor Ort vorzunehmen. Dieselben Möglichkeiten müssen auch dem betrieblichen Datenschutzbeauftragten zustehen.

Die den Kontrollinstanzen eingeräumten Rechte müssen so ausgestaltet sein, daß sie nicht gegen den Willen ihrer Träger entzogen werden können. § 328 Abs. 2 läßt Derartiges ausdrücklich zu.

Wird rechtswidriges Verhalten der ausländischen speichernden Stelle nicht korrigiert (trotz entsprechender Aufforderung durch einen Betroffenen wird z.B. eine ersichtlich falsche Angabe nicht gelöscht), so wäre es wenig sinnvoll, ein Gerichtsverfahren im anderen Land anzustrengen. Dieses wäre nur unter großen Schwierigkeiten in Gang zu setzen, im Falle der USA außerordentlich teuer und überdies mit der Hypothek behaftet, daß unklar bleibt, ob der geschlossene Vertrag durch das ausländische Gericht anerkannt und seiner Entscheidung zugrundegelegt wird. Sinnvoller ist es deshalb, für jeden Fall der Zuwiderhandlung eine Vertragsstrafe vorzusehen. Das Vorliegen eines Verstoßes zu prüfen, müßte Sache eines Schiedsgerichts sein, dessen Entscheidungen in der Bundesrepublik nach §§ 1025 ff. ZPO anerkannt werden. Würde man eine solche Instanz nicht einschalten, bestünde die Gefahr, daß der

Verstoß bestritten wird und dann doch ein normales gerichtliches Verfahren stattfinden muß, für das u.U. kein inländischer, sondern nur ein ausländischer Gerichtsstand zur Verfügung steht. Wenig sinnvoll ist es, die Vertragsstrafe der inländischen Arbeitgebergesellschaft zuzusprechen, da sie wirtschaftlich mit der Konzernspitze identisch ist, so daß eine solche Sanktion eher symbolische als praktische Bedeutung besitzt.

5. Überprüfung des vorliegenden Entwurfs

Der vorliegende Entwurf wird den Erfordernissen der Gleichwertigkeit nur teilweise gerecht.

Keinerlei Bedenken erweckt die materiell-rechtliche Seite: Die Bezugnahme auf das BDSG in § 1 sowie die eindeutige Festlegung eines bestimmten Verwendungszwecks in § 2 entsprechen den hier skizzierten Anforderungen in vollem Umfang. Die eigentliche Schwierigkeit liegt in den Kontrollrechten sowie in den Sanktionen.

Die Auskunftsrechte nach § 3 stehen richtigerweise sowohl dem einzelnen Betroffenen als auch der GmbH zu. Bedenken erweckt jedoch demgegenüber § 4, der die Rechte auf Berichtigung, Sperrung und Löschung ausschließlich der GmbH einräumt. Zwar können diese nach § 10 Abs. 2 Satz 2 an einzelne Betroffene abgetreten werden, doch ist nicht ersichtlich, daß die GmbH dazu nach dem Vertrag oder auf anderer Rechtsgrundlage verpflichtet wäre. Denkbar ist deshalb, daß von den Rechten des § 4 kein effektiver Gebrauch gemacht wird, weil die Konzernleitung in den USA der deutschen Unternehmensleitung von entsprechenden Maßnahmen deutlich abgeraten hat. Aus diesem Grund ist es notwendig, das Modell des § 3 auf die Gegenstände des § 4 zu übertragen und den einzelnen Betroffenen entsprechend BDSG das Recht einzuräumen, ggf. Berichtigung, Sperrung oder Löschung direkt von der speichernden Stelle in den USA verlangen zu können.

Der Gesamtbetriebsrat ist im Vertragsentwurf nicht erwähnt, obwohl er in der Praxis eine zentrale Rolle als Kontrollorgan für die Einhaltung datenschutzrechtlicher Vorschriften besitzt. Es müßte daher eine Vorschrift entsprechend Ziffer 16 des Betriebsvereinbarungsentwurfs aufgenommen werden, doch bleibt es den Beteiligten selbstredend unbenommen, etwas Derartiges nicht im Vertrag zwischen GmbH und Corporation, sondern in einer (Gesamt-)Betriebsvereinbarung festzuschreiben. Notwendig wäre allerdings eine Ergänzung im Sinne des § 7 Abs. 2 des Vertragsentwurfs: Die dort vorgesehene Besichtigung "vor Ort" sollte auch dem Gesamtbetriebsrat ermöglicht werden. Entsprechende Rechte sollte der betriebliche Datenschutzbeauftragte erhalten, der im Vertragsentwurf keine Erwähnung gefunden hat.

Was die Sanktionen betrifft, so ist die in § 8 des Entwurfs vorgesehene Vertragsstrafe zu begrüßen. Insbesondere ist anzuerkennen, daß sie auch für den Fall der verspäteten Erfüllung von Verpflichtungen durch die Corporation vorgesehen ist. Gleichzeitig fehlt jedoch ein Schiedsgericht, das das Vorliegen der Zuwiderhandlung im Streitfalle feststellt und eine Entscheidung trifft, die vollstreckt werden kann. Der verwirkte Betrag sollte im übrigen entweder (ganz oder teilweise) dem Betroffenen zufallen oder aber für soziale Zwecke verwendet werden.

Schließlich fehlt eine Festlegung des Inhalts, daß die den einzelnen eingeräumten Rechte nicht ohne deren Zustimmung entzogen werden können.

Wird der vorgelegte Vertragsentwurf entsprechend revidiert, wären die datenschutzrechtlichen Bedenken aus § 28 Abs. 1 Satz 1 Nr. 2 BDSG ausgeräumt. Die Inbetriebnahme des Systems hinge nur noch davon ab, daß der nach § 87 Abs. 1 Nr. 6 zur Mitbestimmung berufene Gesamtbetriebsrat seine Zustimmung erteilt.

VI. Gestattung der grenzüberschreitenden Übermittlung durch Betriebsvereinbarung?

Teilt man die hier vertretene Auffassung, daß Vertragspartner nicht auf § 28 Abs. 1 Satz 1 Nr. 2 BDSG zurückgreifen können, weil der Vertrag den Verarbeitungsrahmen abschließend umschreibt, so stellt sich das Problem, ob durch Betriebsvereinbarung die Datenübermittlung ermöglicht werden könnte: Da Einwilligung und Arbeitsvertrag aus unterschiedlichen Gründen ausscheiden, läge hier die einzige Möglichkeit, um überhaupt datenschutzrechtliche Hindernisse zu überwinden.

1. Die Betriebsvereinbarung als "andere Rechtsvorschrift" im Sinne des § 4 Abs. 1 BDSG?

Betriebsvereinbarungen können "Erlaubnisnormen" im Sinne des § 4 Abs. 1 BDSG sein. Wie sich aus § 77 Abs. 4 BetrVG ergibt, haben sie normative Wirkung und stellen von daher eine "Vorschrift" dar. Irgendwelche formalen Qualifikationen wie Gesetz, Verordnung usw. stellt § 4 Abs. 1 BDSG nicht auf, so daß insoweit keinerlei Probleme entstehen.

> Für Behandlung der Betriebsvereinbarung als Erlaubnisnorm auch BAG AP Nr. 15 zu § 87 BetrVG 1972 Überwachung; Buschmann, in: Däubler-Kittner-Klebe-Schneider, § 83 Rn 19; Gola-Wronka, a.a.O., S. 68 f. jeweils mwN

2. Einschränkung des BDSG

Umstritten ist demgegenüber die Frage, ob Betriebsvereinbarungen die Verarbeitungsmöglichkeiten, die das BDSG eröffnet, nicht nur konkretisieren, sondern auch zugunsten des Arbeitgebers erweitern können. Das BAG hat dies im Grundsatz bejaht,

> BAG AP Nr. 15 zu § 87 BetrVG 1972

die Literatur hat dem mit großer Mehrheit widersprochen.

S. etwa die Nachweise bei Walz, in: Simitis-Dammann-Geiger-Mallmann-Walz, § 4 Rn 16; Latendorf-Rademacher CR 1989, 1105; Wohlgemuth CR 1988, 1005

Teilt man die in der Literatur herrschende Auffassung, ist auch dieser Weg zur Legalisierung eines grenzüberschreitenden Datenschutzes verschlossen. Schließt man sich dem BAG an, so ist zu beachten, daß auch die Betriebspartner den "grundgesetzlichen Wertungen, zwingendem Gesetzrecht und den sich aus allgemeinen Grundsätzen des Arbeitsrechts ergebenden Beschränkungen" unterliegen (so BAG a.a.O.). Dies bedeutet, daß insbesondere das informationelle Selbstbestimmungsrecht zu beachten ist, das Eingriffe nur im überwiegenden Arbeitgeberinteresse zuläßt.

Näher Däubler, Gläserne Belegschaften? Rn 113 ff.

Außerdem unterliegen Betriebsvereinbarungen einer gerichtlichen Billigkeitskontrolle.

BAG AP Nr. 142 zu § 242 BGB Ruhegehalt; BAG AP Nr. 5 zu § 57 BetrVG (1952), ständige Rechtsprechung

Legt man dies zugrunde, so kann mit Rücksicht auf das Arbeitgeberinteresse an der Rationalisierung des Unternehmens durch Einführung eines neuen Auftragsabwicklungssystems zwar eine grenzüberschreitende Datenübermittlung im vorliegenden Umfang legalisiert werden, gleichzeitig muß die Betriebsvereinbarung jedoch Sorge dafür tragen, daß auch die berechtigten Interessen der Arbeitnehmer beachtet werden. Würde man lediglich die Handlungsspielräume des Arbeitgebers erweitern, läge eine ersichtliche Unbilligkeit vor, die zur Unwirksamkeit der getroffenen Abmachung führen würde.

Vgl. den Fall BAG AP Nr. 26 zu § 611 BGB Fürsorgepflicht, wo eine Betriebsvereinbarung ausschließlich festlegte, daß der Arbeitgeber nicht für eingestellte Fahrzeuge der Arbeitnehmer haften sollte.

Auch in bezug auf Betriebsvereinbarungen nach § 87 Abs. 1 Nr. 6 BetrVG hat das BAG entsprechende Grundsätze herausgearbeitet.

So hat es das BAG auf der einen Seite zugelassen, ein gewisses Maß an "Überwachungsdruck" zu legalisieren, sofern gleichzeitig "kompensatorische Mechanismen" vorgesehen werden, die dafür sorgen, daß sich der einzelne Arbeitnehmer nicht vor einem Übermaß an Datenauswertung oder vor unsachlichen Reaktionen zu fürchten braucht. Im Zusammenhang mit der Speicherung und Auswertung von Fehlzeiten hat dies das BAG wie folgt konkretisiert (BAG EzA § 87 BetrVG 1972 Kontrolleinrichtung Nr. 15 (S. 139):

> "Diesem Überwachungsdruck kann in unterschiedlicher Weise und mit unterschiedlicher Wirkung begegnet werden. Solche Krankenläufe können überhaupt ausgeschlossen oder nur unter bestimmten Voraussetzungen für zulässig erklärt werden, die so gestaltet sein können, daß sie nur in Ausnahmefällen möglich sind und daher eine generelle Furcht vor einer lückenlosen Überwachung des 'Krankheitsverhaltens' nicht aufkommen lassen. Möglich ist es auf der anderen Seite auch, das aus den Erkenntnissen der Krankenläufe folgende Reagieren des Arbeitgebers zu regeln, und so dem Arbeitnehmer die Sicherheit zu geben, daß aus seinem Krankheitsverhalten keine unzutreffenden Schlüsse gezogen und keine nicht berechtigten und nicht einsichtigen Reaktionen hergeleitet werden. Welche dieser möglichen Maßnahmen allein oder in Verbindung zueinander die Einigungsstelle wählt, liegt in ihrem Ermessen, ebenso wie die Betriebspartner vereinbaren können, mit welchen Maßnahmen sie den aufgezeigten Gefahren begegnen wollen."

Vergleichbares gilt im vorliegenden Zusammenhang: Wird einerseits die Möglichkeit zur Datenübermittlung in gewissem Umfang erweitert, muß auf der anderen Seite eine deutliche Sicherung dagegen geschaffen werden, daß der vorher bestehende Schutzstandard nicht unterschritten wird. Im Ergebnis ist daher eine die grenzüberschreitende Datenübermittlung gestattende Betriebsvereinbarung nur dann unter Billigkeitsgesichtspunkten nicht zu beanstanden, wenn sie in ähnlicher Weise wie dies oben geschildert wurde, für einen äquivalenten Schutz sorgt.

VII. Zusammenfassung

Die mit dem System SAP R/3 verbundene Übermittlung von mitarbeiterbezogenen Daten in die USA läßt sich nicht auf eine Einwilligung der Betroffenen stützen.

Auch die Arbeitsverträge können eine solche Form von Datenübermittlung nicht legitimieren.

Nach Rechtsprechung und herrschender Lehre ist eine Berufung auf ein "berechtigtes Interesse" zur Datenübermittlung nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG auch dann zulässig, wenn vertragliche Beziehungen zu dem Betroffenen bestehen. Voraussetzung für eine Datenübermittlung ist allerdings, daß nicht schutzwürdige Interessen des Betroffenen überwiegen.

Die Übermittlung von Daten in ein Land, das keinen angemessenen Datenschutz gewährleistet, und wo die praktische Durchsetzung von Rechten große Schwierigkeiten machen würde, verletzt schutzwürdige Interessen des Betroffenen. Dem kann nur dadurch begegnet werden, daß auf vertraglicher Ebene ein äquivalenter Schutz wie nach BDSG geschaffen wird.

Der äquivalente Schutz setzt nicht nur voraus, daß vergleichbare materiellrechtliche Regeln befolgt werden; wichtig ist daneben auch, daß die Einhaltung des Vereinbarten in gleicher Weise wie bei einem innerstaatlichen Tatbestand kontrolliert werden kann.

Die Individualrechte nach §§ 33 ff. BDSG müssen den Betroffenen auch gegenüber der ausländischen speichernden Stelle zustehen. Auch dem Betriebsrat sind Kontrollrechte bis hin zu einer Besichtigung vor Ort einzuräumen. Damit wird ein Ausgleich dafür geschaffen, daß die Aufsichtsbehörde keinen Zugang zu der ausländischen speichernden Stelle besitzt.

Als Sanktionen für Verstöße sollte eine Vertragsstrafe vorgesehen werden, die nicht einem Konzernunternehmen zugutekommt. Da Streit über das Vorliegen einer Pflichtverletzung nie auszuschließen ist, sollte ein Schiedsgericht eingesetzt werden, dessen Entscheidungen schnell ergehen und die für vollstreckbar erklärt werden können.

Hält man § 28 Abs. 1 Satz 1 Nr. 2 BDSG für nicht anwendbar, so kommt es im Anschluß an die Rechtsprechung des BAG in Betracht, die grenzüberschreitende Datenübermittlung durch Betriebsvereinbarung zuzulassen. Diese unterliegt allerdings einer Billigkeitskontrolle; im Ergebnis muß sie in gleicher Weise für die Wahrung der schutzwürdigen Interessen der Betroffenen sorgen.