kann einem Unternehmen nicht den Erfolg am Markt garantieren, aber sie kann dafür Sorge tragen, daß Unternehmen ein attraktives und innovatives Umfeld zur Verfügung steht. Mit den neuen Bedeutungen des Wissens verbindet sich deshalb für die Politik die Notwendigkeit, Prioritäten neu zu setzen und Investitionen in neue Bahnen zu lenken. Neue Wachstumstheorie hin oder her: Wer den ökonomischen Erfolg will, muß in Bildung und Wissenschaft investieren. Viele Fragen, die sich an die Modernisierung unseren Schulen, Hochschulen und Forschungseinrichtungen stellen, lassen sich nicht mit Geld beantworten. Dennoch: Gute Lehrer und leistungsfähige Labors haben ihren Preis. Wer nicht bereit ist, diesen zu zahlen, zahlt später doppelt.

8. Mit der Wissensgesellschaft verbindet sich auch die Chance einer Renaissance der Ethik.

Wissen fordert das Gewissen, und umgekehrt. In der Vergangenheit wurde diese Partnerschaft oft einseitig aufgekündigt. Wohin aber Rationalität ohne Moral führen kann, hat unser 20. Jahrhundert reichlich und grausam bewiesen. Zu Recht ist auch die technologische Entwicklung Gegenstand kritischer ethischer Reflexion. Problematisch verlief die Entwicklung jedoch dort, wo eine spekulative Moral vergaß, auf sicherem Wissen aufzubauen, und wo Mutmaßungen höheren Anspruch als Gewißheiten reklamierten. Das Ergebnis war eine Ethik des Verzichtes und der Verweigerung. Genauso notwendig ist aber eine Ethik der Ermöglichung, die uns zwingt, von unseren Begabungen, von unserem Wissen und von unseren Potentialen aktiven und verantwortlichen Gebrauch zu machen. In unserer Welt geschieht nicht zu viel, sondern zu wenig. Wir nehmen noch zuviel hin. Eine solche Ethik der Ermöglichung kapituliert nicht vor dem Nichtwissen, sondern macht Wissen und seinen verantwortlichen Gebrauch zur Pflicht. Die Entwicklung zur Wissensgesellschaft fordert daher auch ein neues Selbstbewußtsein der Geistes- und Sozialwissenschaften. Obwohl in unserer Gesellschaft die Nachfrage nach Orientierungswissen groß ist, herrscht in unseren philosophischen Fakultäten oft nur Selbstzweifel. Mit bedauerlichen Schulterzucken wird darauf hingewiesen, die einstige eigene „Deutungsmacht" sei an die Naturwissenschaften, insbesondere die Biologie, übergegangen. Orientierungswissen ist aber nicht eine Frage der vorherrschenden Disziplin, sondern die Bereitschaft zum interdisziplinären Dialog. Interdisziplinarität und Dialog sind deshalb auch die wichtigsten Ziele dieses Kongresses.

9. Der Übergang zur Wissensgesellschaft verbessert die Chancen für eine Reform des Bildungs- und Wissenschaftssystems.

Die Bildungsdebatten der Vergangenheit waren stets ideologisch aufgeladen. Schule sollte verändert werden, damit sich die Gesellschaft verändert. Die jetzt notwendige Bildungsdebatte hat die Chance, daß ihr ideologische Schlachten dieser Art erspart bleiben. Wohl auch deshalb, weil sich unsere Gesellschaft geändert hat, ohne daß Schule, ohne daß Bildung und Erziehung bislang angemessen auf diese Veränderungen reagierten. Schule gerät wieder in den Blick als das, was sie ist: Ort der Heran-Bildung junger Menschen zu Persönlichkeiten und damit Fundament für die Heraus-Bildung persönlicher Lebenschancen.

Sind die Schulen erst einmal von der Last befreit, alle möglichen gesellschaftlichen Ziele realisieren zu müssen, können sie sich wieder ganz den Kindern und Jugendlichen zuwenden. Angesichts der Tatsache, daß im internationalen Vergleich deutsche Lehrer erheblich weniger Zeit für ihre Schüler haben als beispielsweise ihre Schweizer Kollegen, ist dieser Hinweis alles andere als polemisch. Dies ist auch kein Vorwurf an die Lehrer, sondern eher Beleg für die Tatsache, daß wir uns alle zu lange zu wenig um die Schule gekümmert haben. Eine Bildungsreform, die damit beginnt, Schule und Bildung ins Zentrum der Öffentlichkeit zu rücken, tut not. Mit Blick auf die Hochschulen ist dieser Schritt jetzt getan. Die Novelle des Hochschulrahmengesetzes ist eine Reform mit weitreichender Wirkung. Sie macht Schluß mit der unsinnigen Situation, daß die öffentliche Hand angesichts leerer Kassen den Hochschulen Finanzmittel nicht zur Verfügung stellen kann, aber gleichzeitig den Hochschulen durch ein vorgegebenes bürokratisches Korsett verwehrt, daraus in eigener Verantwortung Konsequenzen zu ziehen. Daß die Hochschulen selbst lieber Geld statt Selbständigkeit forderten, hat sie nicht gerade zu brillanten Vordenkern der Reform gemacht. Doch jetzt, zweihundert Jahre nach Humboldt, besteht die Chance zum Neuanfang – nicht in Freiheit und Einsamkeit, aber in Freiheit und Eigenverantwortung. Die Chancen der Wissensgesellschaft sind kein Phantom und auch kein ungedeckter Wechsel auf eine unklare Zukunft. Phasen des Übergangs bedeuten immer Verflüssigung des Bestehenden. Sie bedeuten damit immer auch, daß Neues entsteht und gestaltet werden kann. Dies mitzugestalten ist unser Ziel.

Prof. Dr. Wolfgang Däubler, Bremen*

Grenzüberschreitender Datenschutz – Handlungsmöglichkeiten des Betriebsrats**

Betriebsräten fällt in der Praxis die Kontrolle, 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

* Der Autor ist Professor für Arbeitsrecht, Handels- und Wirtschaftsrecht an der Universität Bremen.

** Der Beitrag erscheint als Nachdruck zu der Veröffentlichung in der Zeitschrift Arbeitsrecht im Betrieb 5/97, S. 258 ff.

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 Kunde 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 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 bedienen 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.

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 wird, 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

---

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

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

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

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. S.283 m. w. N.; a. A. nur Zöllner, Daten- und Informationsschutz im Arbeitsverhältnis, 2. Aufl., Köln/Berlin u.a. 1983, S. 49.

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 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 einer 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]

---

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

8 Zu einem solchen konzerndimensionalen Arbeitsverhältnis s. Däubler, Arbeitsrecht 2, 10. Aufl., Reinbek 1995, S. 666 ff. m. w. N. 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, S. 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, S. 30; a. A. Däubler, Gläserne Belegschaften? Rn. 185; Gola-Schomerus, Bundesdatenschutzgesetz, 6. Aufl., München 1997, § 28 Anm. 2.2; Wohlgemuth, Datenschutz für Arbeitnehmer, Rn. 246, 461.

12 Eingehend Welske CR 1993, S. 297 ff.

13 Welske CR 1993, S. 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, S. 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, S. 342.

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

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

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, S. 342.

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 solle das Beispiel nicht Schule machen?

Betriebsvereinbarung

(Datum)

Zwischen der Geschäftsführung (nachfolgend GF) und dem Gesamtbetriebsrat (nachfolgend GBR) der ... GmbH wird über die Einführung und den Betrieb der Anwendung SAP R/3 und ihrer einzelnen Module folgende Betriebsvereinbarung geschlossen.

1. Gegenstand

1.1 Diese Betriebsvereinbarung beschreibt und regelt die EDV-mäßige Erfassung, Speicherung, Auswertung, Löschung und Weitergabe von Daten des SAP Systems R/3 und der dazu verwendeten Komponenten (siehe Auflistung der aktuellen einzelnen Systeme und deren Komponenten in Anlage 1).

1.2 Sie bezieht die Betriebsvereinbarung „EDV-Gesamtsystem" Version 3.4 vom ... ausdrücklich mit ein.

2. Geltungsbereich

2.1 Diese Betriebsvereinbarung gilt für alle Mitarbeiter der ... GmbH, soweit sie nicht leitende Angestellte i. S. v. § 5 Abs. 3 BetrVG sind.

2.2 Sie regelt die allgemeine, GmbH-weite Einführung, Anwendung und Änderung und/oder Erweiterung der Basissoftware und der einzelnen Anwendungsprogramme (Module) von SAP R/3 und der hierzu erforderlichen Hardwarekonfiguration einschließlich der notwendigen Systemprogramme.

3. Betriebsorganisatorischer Zweck

3.1 Das SAP R/3-System dient der Erfassung, Auslieferung und Berechnung von Aufträgen. Materialplanung und Debitorenbuchhaltung sind ebenfalls Teil der Funktionalität von SAP R/3, die bei diesem System zum Einsatz kommt.

3.2 Sämtliche personenbezogenen Daten werden ausschließlich zum Zweck der effektiveren betriebswirtschaftlichen und kaufmännischen Geschäftsentwicklung (unter Ausschluß des Personalwesens) genutzt. Jede andere Verwendung ist untersagt.

4. Verarbeitung der Daten im Ausland, Installationsort

4.1 Die systemtechnische Verarbeitung der Daten in SAP R/3 erfolgt ausschließlich in den USA. Das System ist zur Zeit in ... installiert. Über Änderungen wird der GBR unverzüglich informiert.

4.2 Zur Regelung der Auslandsverarbeitung schließt die deutsche ... GmbH mit der amerikanischen ... Corporation eine Vereinbarung ab. Die Vereinbarung wird dieser BV als Anlage 2 beigefügt.

5. Hardwarekonfiguration

...

6. Softwarekonfiguration

...

7. Verknüpfung mit anderen Systemen

...

8. Dokumentation

...

9. Organisatorischer Ablauf

...

10. Technische und organisatorische Vorkehrungen für den Datenschutz

...

11. Personenbezogene Daten

Folgende personenbezogene Daten werden in SAP R/3 gehalten:

- SAP-User-ID (Benutzeridentifikation)
- Vertriebsbeauftragter:
  = Badge-Nummer des Vertriebsbeauftragten
- Credit & Collection und Cash Application:
  = Name des Credit & Collection- und Cash Application-Sachbearbeiters
  = Telefonnummer und Location des C&C- und Cash Appl.-Sachbearbeiters
  = Cost Center des C&C- und Cash Appl.-Sachbearbeiters

- Administratoren:
  - = Name des Administrators (hat Pointer zum Auftrag)
  - = Telefonnummer und Location des Administrators
  - = Cost Center des Administrators
- Finance
  - = Name des Finance-Sachbearbeiters (Revenue, Intercompany und Closing)
  - = Telefonnummer und Location des Finance-Sachbearbeiters
  - = Cost Center des Finance-Sachbearbeiters
- Benutzer:
  - = Name des Benutzers, der nur lesenden Zugriff auf Business-Daten erhält
  - = Telefonnummer und Location des Enquiry-Benutzers
  - = Cost Center des Enquiry-Benutzers

12. Report

...

13. Informationen und Beteiligung der Mitarbeiter

13.1 Die GmbH wird die betroffenen Mitarbeiterinnen und Mitarbeiter rechtzeitig vor Einführung des SAP R/3-Systems darüber informieren, welche personenbezogenen Daten ins Ausland übermittelt werden, und daß ihnen sämtliche Rechte, die ihnen das Bundesdatenschutzgesetz gewährt, auch nach dem Datenschutzvertrag, abgeschlossen zwischen der GmbH und der Corporation, zustehen. Außerdem ist der GBR zuvor davon in Kenntnis zu setzen. Neu eintretende Mitarbeiter werden entsprechend informiert.

13.2 Falls Änderungen in der organisatorischen und ablaufmäßigen Einordnung der Aufgaben anfallen, so sind diese 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 Möglichkeit für eine Verbesserung der Arbeitssituation genutzt werden.

14. Qualifizierung

...

15. Kontrollrechte des Gesamtbetriebsrats

Zur Wahrnehmung seiner Überwachungsrechte hat der GBR das Zugangsrecht (nur lesend) zum SAP R/3-System und den jeweiligen Einzelanwendungen (Masken/Programme). Die Geschäftsführung benennt dem GBR eine verantwortliche Person, die dem GBR die erforderlichen Auskünfte und Informationen gibt. Der GBR benennt dazu maximal 2 Vertreter.

Ist zwischen Arbeitgeber und GBR streitig, ob die Corporation ihre Verpflichtung aus dem Datenschutzvertrag verletzt hat, entscheidet eine innerbetriebliche Einigungsstelle, die nach den Regeln des § 76 BetrVG gebildet wird. Jede Seite benennt zwei Mitglieder dieser Einigungsstelle.

16. Verhältnis zum Datenschutzvertrag, außerordentliche Kündigung

Die Betriebsvereinbarung endet, wenn der Datenschutzvertrag außerordentlich gekündigt oder geändert wird. In diesem Falle besteht keine Nachwirkung.

Die GmbH haftet dem GBR für die Einhaltung des Datenschutzvertrages. Wird die Betriebsvereinbarung wegen eines groben Verstoßes gegen die in ihr begründeten Pflichten von Seiten des GBR außerordentlich gekündigt, dürfen personenbezogene Daten der Arbeitnehmer (Abschnitt 11) nach Ablauf eines Monats ab Zugang der Kündigung nicht mehr an die Corporation übermittelt werden.

Die GmbH haftet auch für die von der Corporation verwirkte Vertragsstrafe und für weitere Kosten des Verfahrens. Die Vertragsstrafe wird für soziale Zwecke verwendet. Kommt eine Einigung zwischen Arbeitgeber und GBR über die Verwendung der Vertragsstrafe nicht zustande, kann jede Seite einen Vorschlag einbringen. Über die Frage, welcher Einrichtung die Vertragsstrafe zufällt, entscheidet das Los. Muß im Rahmen einer Einigungsstelle entschieden werden, trifft die Einigungsstelle auch die Bestimmung über die Verwendung der verwirkten Vertragsstrafe.

Die in § 3 des Datenschutzvertrages begründeten Ansprüche der Arbeitnehmer gegen die Corporation auf Auskunft stehen auch dem GBR als betriebsverfassungsrechtliche Ansprüche zu. Der GBR kann diese Ansprüche gegenüber dem Arbeitgeber geltend machen.

17. Weitere Anlage

...

18. Inkrafttreten

Diese Vereinbarung tritt mit ihrer Unterzeichnung in Kraft. Sie gilt, bis das System eingestellt wird.

Die Betriebsvereinbarung ist mit einer Frist von sechs Monaten kündbar. Sie wirkt nach.

Vereinbarung zum grenzüberschreitenden Verkehr mit personenbezogenen Daten (Datenschutzvereinbarung)

zwischen
Corporation/USA
– nachfolgend „Corporation" genannt –
und
GmbH/Deutschland
– nachfolgend „GmbH" genannt –

Präambel

Die Corporation beabsichtigt, ihre interne betriebswirtschaftliche und kaufmännische Geschäftsabwicklung (unter Ausschluß des Personalwesens) weltweit zu zentralisieren und hierdurch Synergien zu nutzen. Sie wird daher in den USA die Anwendung von SAP R/3 (nachfolgend das System genannt) installieren, um es weltweit im Rahmen des Konzernverbundes zu nutzen.

Die GmbH wird als Nutzer dieses Systems alle zu seiner Etablierung notwendigen sachlichen und persönlichen Daten ihrer Mitarbeiter an die Corporation übermitteln. Diese speichert die Daten in der Datenbank des Systems. Nach Inbetriebnahme des Systems werden die genannten Daten zwischen der GmbH und der Corporation ständig ausgetauscht.

Um den Datenschutz auch bei einem solchen grenzüberschreitenden Informationsverkehr sicherzustellen, treffen die Parteien die folgende Vereinbarung. Sie sind sich darüber einig, daß diese Vereinbarung auf freiwilliger Grundlage und nicht in Erfüllung einer Rechtspflicht geschlossen wird. Sie werden die übernommenen Verpflichtungen jedoch gewissenhaft erfüllen.

§ 1 Vertragsgegenstand

(1) Die Corporation verpflichtet sich gegenüber der GmbH sicherzustellen, daß die betroffenen Mitarbeiter (nachfolgend „Betroffene" genannt) durch die Übermittlung ihrer Daten in das Ausland keinerlei Rechtsnachteile erleiden und denselben Schutz genießen, den das deutsche Bundesdatenschutzgesetz vom 20. Dezember 1990 (nachfolgend „Bundesdatenschutzgesetz" genannt) gewährt.

(2) Daten im Sinne des Abs. 1 sind Angaben über persönliche oder sachliche Verhältnisse eines Betroffenen, die im System gespeichert, übermittelt oder auf andere Weise weiterverarbeitet werden (nachfolgend „personenbezogene Daten"). Gleichgestellt sind Angaben, die auf bestimmte Personen beziehbar sind.

(3) Um das Ziel des Abs. 1 zu erreichen, räumt die Corporation der GmbH und den Betroffenen insbesondere die nachfolgend genannten Rechte ein.

§ 2 Verwendungszweck

Sämtliche personenbezogenen Daten, die die GmbH im Rahmen der Errichtung und Nutzung des Systems an die Corporation übermittelt, werden ausschließlich zum Zweck der effektiveren internen und betriebswirtschaftlichen und kaufmännischen Geschäftsabwicklung (unter Ausschluß des Personalwesens) genutzt. Jede andere Verwendung ist der Corporation untersagt.

§ 3 Auskunftsrechte

(1) Die Corporation wird jedem Betroffenen, dessen personenbezogene Daten an sie übermittelt werden, auf dessen Verlangen Auskunft erteilen über

- 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.

Soweit die GmbH dies verlangt, erhält auch sie die Auskünfte nach Satz 1.

(2) Die Auskunft ist bei der GmbH zu beantragen. Die GmbH wird das Auskunftsersuchen von Betroffenen unverzüglich an die Corporation weiterleiten.

(3) Die Auskunft wird bei Standardanfragen, die über vorab definierte Reports abgedeckt werden können, innerhalb von 1 Woche nach Eingang des Ersuchens bei der GmbH schriftlich erteilt und ist unentgeltlich. Alle anderen Anfragen werden innerhalb von 4 Wochen beantwortet.

(4) Die den betroffenen Arbeitnehmern eingeräumten Rechte können nicht ohne ihre Zustimmung eingeschränkt oder aufgehoben werden (§ 328 Abs. 2 BGB).

§ 4 Berichtigung, Sperrung, Löschung

(1) Die Corporation wird auf Verlangen des Betroffenen unverzüglich die auf ihn/auf sie bezogenen oder beziehbaren Daten berichtigen, sperren oder löschen, sofern dies nach dem Bundesdatenschutzgesetz, insbesondere nach § 35 BDSG, verlangt werden kann.

(2) Berichtigung, Löschung oder Sperrung sind bei der GmbH zu beantragen. Ein Verlangen, das bei der GmbH eingeht, wird ohne inhaltliche Änderung unverzüglich an die Corporation weitergeleitet. Innerhalb von zwei Wochen nach Eingang erfolgt eine schriftliche Stellungnahme. Die Corporation wird dem Mitarbeiter schriftlich bekanntgeben, in welcher Form Daten berichtigt, gesperrt oder gelöscht werden. Die Schriftform gilt auch dann als erfüllt, wenn die Bestätigung über das konzerninterne elektronische Kommunikationssystem erfolgt.

(3) Die Ansprüche nach Abs. 1 können auch von der GmbH geltend gemacht werden, sofern der Betroffene sie hierzu ermächtigt.

(4) Falls bei Anwendung des § 35 BDSG eine Berichtigung, Sperrung oder Löschung aus technischen oder rechtlichen Gründen nicht oder nicht mehr möglich ist, wird die Korrektur in einem Folgesystem durchgeführt. Außerdem werden die Stellungnahme und der Sachverhalt in einer Systemtabelle mit Referenz zum Mitarbeiternamen und Badgenummer hinterlegt.

(5) Die den betroffenen Arbeitnehmern eingeräumten Rechte können nicht ohne ihre Zustimmung eingeschränkt oder aufgehoben werden (§ 328 Abs. 2 BGB).

§ 5 Datensicherung

(1) Die Corporation verpflichtet sich, die ihr übermittelten personenbezogenen Daten streng vertraulich zu behandeln und gegen den Zugriff Unbefugter zu sichern. Als unbefugt gelten nicht nur Dritte, sondern auch diejenigen Mitarbeiter der Corporation, die auf das System nicht im Rahmen ihrer arbeitsvertraglichen Aufgabe und im Rahmen des § 2 zugreifen dürfen.

(2) Die Corporation wird alle konzernweiten Sicherheitsstandards zur Datensicherung und Zugangskontrolle einhalten.

§ 6 Kontrollverfahren

(1) Die Corporation wird der GmbH auf deren Wunsch jederzeit umfassend Auskunft zu allen Fragen auch technischer Art gewähren, die mit der Erfassung und Verarbeitung personenbezogener Daten im Rahmen des Systems zusammenhängen.

(2) Die Corporation wird der GmbH jederzeit unverzüglich Einsicht gewähren in sämtliche Unterlagen und sonstige Archive, in denen sich die personenbezogenen Daten befinden oder die mit dem System in Zusammenhang stehen. Dies bezieht sich auch auf den zentralen Speicher.

(3) Die GmbH hat ferner das Recht, das System jederzeit vor Ort zu besichtigen und selbst Untersuchungen und Maßnahmen vorzunehmen, sofern nach ihrer Ansicht trotz der gemäß Abs. 1 und 2 gewonnenen Informationen die Notwendigkeit besteht, die Einhaltung des Bundesdatenschutzgesetzes zu überprüfen.

(4) Unter den gleichen Voraussetzungen stehen dieselben Rechte dem betrieblichen Datenschutzbeauftragten der GmbH zu. Dieser ist verpflichtet, regelmäßig (mindestens einmal pro Jahr) die Einhaltung des Bundesdatenschutzgesetzes auch vor Ort in den USA zu überwachen.

(5) Bei Verdacht auf Datenmißbrauch führt der betriebliche Datenschutzbeauftragte auf Antrag des Gesamtbetriebsrats unverzüglich eine Kontrolle in den USA durch.

Der betriebliche Datenschutzbeauftragte bedient sich bei seiner Überwachungstätigkeit im Rahmen dieser Bestimmung (Abs. 5) der Hilfe und Unterstützung von bis zu zwei vom Gesamtbetriebsrat benannten unternehmensangehörigen Personen, die mit ihm zusammen vor Ort die Überwachungstätigkeit ausüben sollen. Im Verhältnis der GmbH zu Dritten treten diese Personen als Mitarbeiter des betrieblichen Datenschutzbeauftragten auf.

(6) Wird das in Abs. 5 vorgesehene Kontrollverfahren innerhalb eines Monats nach Antrag des GBR (§ 5 Abs. 5) tatsächlich nicht in der gesetzlich und vertraglich (§ 6 Abs. 2) vorgeschriebenen Form durchgeführt, geht das Kontrollrecht auf Herrn X., Richter am Arbeitsgericht, als Vorsitzenden einer Kontrollkommission über. Herrn X. werden schon jetzt entsprechende Vollmachten erteilt. Herr X. wird demnächst für den Fall seiner Verhinderung einen geeigneten Richter aus der Arbeitsgerichtsbarkeit als Vertreter für den Fall der Verhinderung bestellen. Der Vorsitzende dieser Kontrollkommission bittet die GmbH und den GBR, ihm jeweils eine Person ihres Vertrauens zur Unterstützung zu benennen.

§ 7 Sicherung der Vertragserfüllung (Vertragsstrafe)

Die Corporation wird für jeden Fall des festgestellten Datenmißbrauchs eine Vertragsstrafe in Höhe von DM 20000, – zahlen.

§ 8 Dauer, Kündigung

Diese Vereinbarung gilt für unbestimmte Zeit. Sie ist nur aus wichtigem Grund kündbar. Mit Wirksamkeit der Kündigung wird die vertragsgegenständliche Datenübertragung ins Ausland unzulässig. Vorher zulässigerweise übermittelte Daten können noch nach Beendigung der Vereinbarung nach ihren Regeln verarbeitet und genutzt werden.

§ 9 Ergänzende Bestimmungen

(1) Sollte eine Bestimmung dieser Vereinbarung unwirksam sein oder werden, so berührt dies die Wirksamkeit der übrigen Bestimmungen nicht. Die Parteien werden in einem solchen Fall eine Vereinbarung treffen, die dem wirtschaftlichen Zweck der unwirksamen Bedingung möglichst nahe kommt.

(2) Auf diesen Vertrag findet deutsches Recht Anwendung.

(3) Als Gerichtsstand für Klagen von Arbeitnehmern der GmbH gegen die Corporation wird München vereinbart.

(4) Soweit diese Vereinbarung Lücken aufweist, findet ergänzend das Bundesdatenschutzgesetz Anwendung.

(5) Maßgebend ist allein die deutschsprachige Fassung der vorliegenden Vereinbarung.

(6) Änderungen und Ergänzungen dieses Vertrages einschließlich dieser Klausel bedürfen der Schriftform.

Dr. Peter Münch, Halle*

Wem hilft der Katalog der Sicherheitsanforderungen gemäß § 87 TKG?

1. Die Vorgabe des Gesetzgebers

Nach § 87 Abs. 1 des Telekommunikationsgesetzes – TKG – vom 25. Juli 1996 war durch die Regulierungsbehörde in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) ein Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen zu erstellen. Dieser soll dem Stand der Technik entsprechen, internationalen Maßstäben gerecht werden und eine angemessene Standardsicherheit erfüllen helfen. Der Katalog war mit Verbraucher- und Wirtschaftsverbänden abzustimmen und dem Bundesbeauftragten für den Datenschutz zur Stellungnahme vorzulegen.

Im § 87 Abs. 2 TKG wird für lizenzpflichtige Betreiber von Telekommunikationsanlagen gefordert, eine Sicherheitskonzeption zu erstellen, welche der Regulierungsbehörde vorzulegen ist. Darüber hinaus ist ein Sicherheitsbeauftragter zu benennen.

Von der im § 87 Abs. 3 angekündigten Rechtsverordnung zu technisch-organisatorischen Schutzmaßnahmen wird zunächst Abstand genommen, „... solange die Betreiber die Gefährdungen sachgerecht beurteilen und entsprechende Vorsorgemaßnahmen treffen", wie es im „Katalog von

* Der Autor ist selbständiger Datenschutz- und Datensicherheitsberater und Mitglied des Vorstandes der GDD e.V., Bonn.