Informationstechnik
und Recht

8

Alfred Büllesbach (Hrsg.)

# Datenverkehr ohne Datenschutz?

## Eine globale Herausforderung

Verlag
Dr. Otto Schmidt
Köln

der bisherigen Rechtslage möglich ist. Diese Frage resultiert natürlich einerseits aus wirtschaftlichen Interessen, stellt sich aber andererseits auch aus dem Blickwinkel des Kunden, der zunehmend optimierte Serviceleistungen verlangt, die häufig erst aufgrund der Zusammenführung von Einzelinformationen möglich werden.

Unübersichtlich für grenzüberschreitend tätige Unternehmen und unpraktikabel ist die zergliederte und wenig homogene Zuständigkeit der jeweiligen nationalen Aufsichtsbehörden und die hieraus resultierende Unterschiedlichkeit der Reaktionsformen. Es müssen hierbei im Sinne der Vereinheitlichung von Wirtschaftsräumen noch viele Anstrengungen unternommen werden.

Besonders bedeutsam im Hinblick auf den auch vertrieblich bedingten Datenverkehr mit Nicht-EU-Mitgliedsstaaten ist die sogenannte Drittstaatenproblematik. In diesem Zusammenhang erscheint die Erarbeitung von Maßnahmen der Selbstregulierung auf der Basis der Ausnahmentatbestände des Art. 26 der Datenschutzrichtlinie derzeit die pragmatischste Herangehensweise zu sein, die im übrigen den Trend zu staatlicher Deregulierung beim Aufbau eigener Problemlösungskompetenz bestätigt.



# Übermittlung von Arbeitnehmerdaten ins Ausland

Wolfgang Däubler



*Literaturübersicht*

*Baumann*, DVBl. 1984, 615; *Bergmann*, Grenzüberschreitender Datenschutz, Baden-Baden 1985; *Bergmann/Möhrle/Herb*, Kommentar zum BDSG, Stuttgart u. a., Loseblatt (Stand: 30. 6. 1999); *Büllesbach*, RDV 1997, 239; *Dammann/Simitis*, EG-Datenschutzrichtlinie, Kommentar, Baden-Baden 1997; *Däubler*, AiB 1997, 259 ff; *ders.*, Arbeitsrecht 2, 11. Aufl., Reinbek 1998; *ders. dd*, AuR 1990, 11; *ders.*, Das Arbeitsrecht 1, 15. Aufl., Reinbek 1998; *ders.*, Gläserne Belegschaften? Datenschutz für Arbeiter, Angestellte und Beamte, 3. Aufl., Köln 1993, Rz. 21, 173 ff; *ders.*, in: Däubler/Kittner/Klebe (Hrsg.), Betriebsverfassungsgesetz mit Wahlordnung, Kommentar für die Praxis, 6. Aufl., Köln 1998; *ders.*, Zivilrecht 1, Reinbek 1997; *Däubler/Klebe/Wedde*, Bundesdatenschutzgesetz, Basiskommentar, Köln 1996; *Dörr*, RDV 1992, 167; *Drews*, DuD 1994, 68; *Ehmann*, Beilage 1/1985 zu NZA, S. 5; *Ehmann-Sutschet*, RDV 1997, 11; *Einwag*, RDV 1990, 1; *Ellger*, CR

1993, 9; *ders.*, Der Datenschutz im grenzüberschreitenden Datenverkehr. Eine rechtsvergleichende und kollisionsrechtliche Untersuchung, Baden-Baden 1990; *Finkin*, ZVglRWiss 94 (1995), 109 ff; *Fitting/Kaiser/Heither/Engels*, Handkommentar zum BetrVG, 19. Aufl., München 1998; *Freise/Wohlgemuth*, DVR 1982, 288; *Geis*, NJW 1997, 288; *Gitter/Henker*, ZTR 1990, 409; *Gola/Schomerus*, BDSG, Kommentar, 6. Aufl., München 1997; *Gola/Wronka*, Handbuch zum Arbeitnehmerdatenschutz. Rechtsfragen und Handlungshilfen für die betriebliche Praxis, 2. Aufl., Köln 1994; *Gounalakis/Mand*, CR 1997, 502; *Jaspers*, RDV 1996, 18; *Kilian*, RdA 1978, 205; *Kraft*, in: Fabricius u. a., Gemeinschaftskommentar zum BetrVG, Bd. 2, 6. Aufl., Neuwied 1998; *Kroll*, Datenschutz im Arbeitsverhältnis, Königstein/Ts. 1981; *Küpferle/Wohlgemuth*, Personaldatenverarbeitende Systeme. Rechtsprobleme und Argumentationsmöglichkeiten aus der Sicht der Beschäftigten, Köln 1987; *Mütsch*, DuD 1994, 189; *Napier*, RDV 1990, 216 ff; *Palm*, CR 1998, 65 ff; *U. Preis*, Grundfragen der Vertragsgestaltung im Arbeitsrecht, Neuwied u. a. 1993; *Riemann*, CR 1997, 752; *ders.*, CR 1997, 752; *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; *Rüttgers*, CR 1996, 55; *Schaar*, CR 1996, 172 f; *Schapper*, in: Klebe/Roth, Informationen ohne Grenzen, Köln 1987; *Schild*, EuZW 1996, 553; *Schwartz*, Iowa Law Review 80 (1995) 471 ff; *Schwartz/Reidenberg*, Data Privacy Law, Charlottesville 1996; *Simitis*, CR 1991, 177; *ders.*, in: Simitis/Dammann/Geiger/Mallmann/Walz, Kommentar zum Bundesdatenschutzgesetz, Baden-Baden, Loseblatt (Stand: April 1998); *ders.*, in: Simitis/Dammann/Mallmann/Reh, Kommentar zum BDSG 1977, 3. Aufl.; *ders.*, NJW 1997, 284; *Sproll*, ZIP 1984, 30; *Taeger*, EWS 1995, 69; *Tinnefeld/Ehmann*, Einführung in das Datenschutzrecht, 3. Aufl., München 1998; Ungnade/*Gorynia*, WM-Sonderbeilage 7/1983, S. 17; *Wedde*, RDV 1996, 7; *Weichert*, Datenschutz-Nachrichten Heft 4/5-1996; *Welske*, CR 1993, 297 ff; *Wohlgemuth*, BB 1991, 341; *ders.*, BB 1992, 283 mwN; *ders.*, Datenschutz für Arbeitnehmer, 2. Aufl., Neuwied 1988; *ders.*, Datenschutzrecht. Eine Einführung mit praktischen Fällen, 2. Aufl., Neuwied u. a. 1993; *Zöllner*, Daten- und Informationsschutz im Arbeitsverhältnis, Köln–Berlin u. a. 2. Aufl. 1983.

# 1. Grenzüberschreitender Datenverkehr

## 1.1 Allgemeine Situation

Daß personenbezogene Daten immer häufiger in andere Länder übermittelt werden, ist eine im Grunde triviale Feststellung. Je größer der Anteil der Informationstechnologie am Wertschöpfungsprozeß ist und je stärker dieser eine globale Dimension hat, um so intensiver wird der grenzüberschreitende Datenverkehr sein. Dabei geht es nicht allein darum, daß Daten gewissermaßen im Schlepptau von Gütern und Dienstleistungen von einem in ein anderes





Land transferiert werden. Informationen sind vielmehr zu einem eigenständigen Handelsgut geworden, zu einer Ware, für die auch in anderen Ländern Interesse besteht. Eine detaillierte Analyse des Käuferverhaltens ist für ausländische Unternehmen nicht weniger interessant als für inländische. Schon vor acht Jahren wurde darüber berichtet, eine Wirtschaftsauskunftei biete 8 Mio. Firmenprofile aus 12 EG-Staaten an[1] – inzwischen dürften die Dimensionen sicherlich keine bescheideneren geworden sein.[2] Einen besonderen Anreiz bietet es, daß dank Internet und Telekommunikation die Kosten sinken und so die Möglichkeit besteht, auf die preiswerteren Dienste ausländischer Rechenzentren zurückzugreifen.[3] Im Einzelfall kann es sogar zweckmäßig sein, Arbeitsvorgänge im Inland vom Ausland aus steuern zu lassen.[4]

Die landläufige Vorstellung, die im Staat A generierten Daten würden – einem mit Birnen beladenen Lkw vergleichbar – auf dem direkten Wege in den Staat B gebracht, erweist sich immer häufiger als Irrtum. Zu Recht wurde in der Literatur darauf hingewiesen, daß der Weg von einem zu einem anderen Hamburger Internet-Anschluß über die USA führt[5] – wobei offenbleiben kann, ob sich nachträglich nicht nur die „Reiseroute", sondern auch der Inhalt des Übermittelten rekonstruieren läßt. Die Datenautobahn kennt ersichtlich keine Schlagbäume, auch vor Schengen fürchtet sich dort niemand.

## 1.2 Arbeitnehmerdaten

Arbeitnehmerdaten sind von dieser Entwicklung in großem Umfang erfaßt. Ein multinationaler Konzern, der Vertrieb und Kundendienst weltweit nach einem einheitlichen System strukturiert[6], wird dabei ersichtlich nicht ohne Übermittlung von Arbeitnehmerdaten auskommen. Dasselbe gilt dann, wenn die Personalverwaltung in gewissem Umfang zentralisiert wird oder ein Personenaustausch zwischen Niederlassungen in verschiedenen Ländern erfolgt.

1 *Einwag*, RDV 1990, 1.
2 *Büllesbach*, RDV 1997, 239.
3 *Taeger*, EWS 1995, 69.
4 *Wedde*, RDV 1996, 7 berichtet von einem (konventionellen) Kraftwerk in Deutschland, das von vergleichsweise bescheiden entlohnten Mitarbeitern in Polen gesteuert wird.
5 *Schaar*, CR 1996, 172 f.
6 S. den bei *Däubler*, AiB 1997, 259 ff. eingehend dargestellten Fall.

Die Entsendung von Mitarbeitern ins Ausland spielt auch außerhalb von Konzernen eine erhebliche Rolle.

Im folgenden soll die Zulässigkeit der grenzüberschreitenden Übermittlung speziell dieser Art von Daten untersucht werden. Hintergrund ist einmal die Überlegung, daß die über Beschäftigte gespeicherten Daten sehr vielfältigen Lebensbereichen entnommen sind und deshalb im Extremfall ein Persönlichkeitsprofil ermöglichen können.[7] Zum zweiten besteht die Besonderheit, daß in Form der betrieblichen Interessenvertretung eine vom Arbeitgeber unabhängige Stelle existiert, die über die Einhaltung datenschutzrechtlicher Grundsätze zu wachen hat. Durch Gesetz oder Vertrag festgelegte Regeln haben daher eine erhöhte Chance, in der Praxis Beachtung zu finden.

Die Zulässigkeit soll nach dem derzeit (noch) geltenden Recht, anschließend nach der EG-Richtlinie zum Datenschutz[8] diskutiert werden, deren Umsetzung möglicherweise noch einige Zeit in Anspruch nehmen wird. Zunächst ist allerdings eine kollisionsrechtliche Vorfrage zu klären: Inwieweit ist (heutiges oder künftiges) deutsches Recht überhaupt anwendbar, wenn Daten zB in die USA „exportiert" oder aus Japan nach Deutschland „importiert" werden?

## 2. Anwendbarkeit des deutschen Datenschutzrechts

### 2.1 Ausgangspunkt

Obwohl die „Auslandsberührung" in kaum einem anderen Gebiet so leicht herstellbar ist wie bei der Datenübermittlung, steckt das Kollisionsrecht insoweit noch in den Kinderschuhen. Die Meinungen sind höchst unterschiedlich, ohne daß sich ein Grundstock an gemeinsamen Überzeugungen herausgebildet hätte.

So wird etwa auf der einen Seite auf das Recht des Aufenthaltsorts des Betroffenen abgestellt[9], während andere den Standpunkt vertreten, maßgebend sei allein das Recht des Orts, wo die Datenverarbeitung stattfinde.[10] Wieder andere wollen das Recht des angerufenen Gerichts (lex fori) oder auch die Rechtsordnung entscheiden lassen, die den besten Schutz personenbezogener Daten gewährleistet.[11]

Da ersichtlich eine allseits akzeptierte Kollisionsnorm fehlt[12], beschränkt man sich darauf, allein den Anwendungsbereich des BDSG zu bestimmen und so nur eine einseitige Norm aufzustellen. Deutsches Datenschutzrecht soll immer dann Anwendung finden, wenn die speichernde Stelle ihren Sitz im Inland hat[13] oder wenn und soweit ein Teil der Datenverarbeitung im Inland erfolgt.[14] Dies läßt sich u. a. mit der Erwägung rechtfertigen, daß es sich beim BDSG nicht um „neutrales" Privatrecht handelt, das lediglich den Rahmen für einen frei ausgehandelten Interessenausgleich zwischen Individuen schafft. Vielmehr geht es um einen wichtigen Teil der Wirtschaftsordnung, durch den ein bestimmter Regelungserfolg sichergestellt werden soll. Deutlich wird dies nicht zuletzt an der Einschaltung der Aufsichtsbehörde sowie an der Existenz von Straf- und Bußgeldtatbeständen.[15] Datenschutzrecht ist somit „zwingendes Recht" im Sinne des Art. 34 EGBGB, das alle Vorgänge erfassen will, die sich auf deutschem Territorium abspielen. Insoweit ist es dem Betriebsverfassungsrecht ähnlich, für das nach allgemeiner Auffassung derselbe Grundsatz gilt.[16]

### 2.2 Einzelfragen

Im Ergebnis stimmt damit Art. 4 Abs. 1 der EG-Richtlinie[17] überein. 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 auto-

7 Näher *Däubler*, Gläserne Belegschaften, Rz. 21, 173 ff.
8 Richtlinie 95/46/EG des *Europäischen Parlaments* und des *Rates* vom 24. 10. 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. vom 23. 11. 1995, Nr. L 281/31, abgedruckt auch bei *Däubler/Klebe/Wedde*, S. 321 ff. Zu ihr die interessante „Außenansicht" von *Schwartz*, Iowa Law Review 80 (1995) 471 ff.
9 So *Rigaux*, 443 ff.
10 S. die Nachweise bei *Ellger*, S. 587 ff.
11 S. den Überblick bei *Bergmann*, S. 230 ff.
12 *Bergmann*, (Fn. 11), S. 235; *Ellger*, (Fn. 10), S. 595 f.; *Korff*, RDV 1994, 212.
13 *Ellger*, (Fn. 10), S. 609.
14 *Bergmann*, (Fn. 11), S. 245.
15 *Ellger*, (Fn. 10), S. 604.
16 BAG, DB 1978, 451; weitere Nachweise bei *Däubler*, in: Däubler/Kittner/Klebe (Hrsg.), Einl. Rz. 201 ff.
17 S. o. (Fn. 8).

matisierte oder nichtautomatisierte Mittel zurückgreift, die im Hoheitsgebiet des betreffenden Mitgliedstaats belegen sind"[18].

Die Frage, ob in Deutschland gespeicherte Daten in ein anderes Land übermittelt werden dürfen, richtet sich daher bis auf weiteres nach dem BDSG. Dasselbe gilt für den „Import" personenbezogener Daten sowie ihre Weiterverarbeitung im Inland. Keine Anwendung findet es auf Vorgänge außerhalb der deutschen Grenzen; was nach einem (zulässigen) Export oder vor einem (zulässigen) Import geschieht, interessiert das BDSG nicht. Insoweit greifen ausländische Rechtsordnungen ein.

Für bereichsspezifische Regelungen des Datenschutzes wie zB die §§ 68 bis 77 SGB X gilt nichts Abweichendes. Die Erstreckung auf einzelne Vorgänge im Ausland, die Zurücknahme des Geltungsanspruchs im Inland sowie die Einführung einer freien Wahl des anwendbaren Rechts bedürften ausdrücklicher gesetzlicher Bestimmung.

Die Tatsache, daß das Datenschutzrecht unter Art. 34 EGBGB fällt, macht die Frage gegenstandslos, ob man nicht einzelne Teile den entsprechenden Sachmaterien zuordnen und den für diese geltenden Kollisionsregeln unterstellen muß. Das auf den Bankvertrag anwendbare Recht hätte danach auch über den Schutz der der Bank anvertrauten Daten, das Arbeitsstatut über den Arbeitnehmerdatenschutz entschieden.[19]

## 3. Zulässigkeit des „Datenexports" nach dem BDSG

### 3.1 Rechtfertigungsmöglichkeiten

Das geltende BDSG enthält keine spezifischen Regeln für eine Übermittlung personenbezogener Daten ins Ausland, soweit es um den nichtöffentlichen Bereich geht.[20] Nach allgemeiner Meinung wendet man deshalb die Vorschriften an, die für entsprechende Vor-

18 Einzelheiten bei *Dammann/Simitis*, Erl. zu Art. 4.
19 Dazu *Däubler*, AuR 1990, 11.
20 Zum öffentlichen Bereich s. § 17 BDSG und dazu *Palm*, CR 1998, 65 ff. Anders § 8 des Gesetzentwurfs von Bündnis '90 / DIE GRÜNEN für ein neues BDSG, BT-Drucksache 13/9082.





gänge im Inland gelten.[21] Da die Übermittlung nach der Legaldefinition des § 3 Abs. 5 BDSG zur „Verarbeitung" von Daten gehört, bestimmt sich die Zulässigkeit nach § 4 Abs. 1 BDSG. Danach sind in bezug auf Arbeitnehmerdaten drei Fälle denkbar:

- Die Übermittlung erfolgt mit Einwilligung des Betroffenen; die näheren Voraussetzungen finden sich in § 4 Abs. 2 BDSG.
- § 28 Abs. 1 Satz 1 Nr. 1 BDSG läßt die Übermittlung im Rahmen der Zweckbestimmung eines Vertragsverhältnisses zu. Insoweit könnte der Arbeitsvertrag eine geeignete Rechtsgrundlage darstellen.
- In Betracht kommt weiter eine Rechtfertigung mit berechtigten Interessen der speichernden Stelle (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG) oder mit berechtigten Interessen eines Dritten oder mit öffentlichen Interessen (§ 28 Abs. 2 Nr. 1 lit. a BDSG). Beides setzt jedoch voraus, daß kein Grund zu der Annahme besteht, daß schutzwürdige Interessen des Betroffenen überwiegen bzw. entgegenstehen.

Sämtliche genannten Voraussetzungen werfen Interpretationsprobleme auf.

### 3.2 Einwilligung des Arbeitnehmers

Von einer die Übermittlung rechtfertigenden Einwilligung kann nur dann die Rede sein, wenn den formellen und materiellen Voraussetzungen des § 4 Abs. 2 BDSG Rechnung getragen ist. Danach gilt folgendes:

Die Einwilligung muß vor dem in Frage stehenden Datenverarbeitungsvorgang liegen; der Gesetzgeber hat insoweit die Terminologie des § 183 BGB übernommen.[22] Eine nachträglich erteilte Zustimmung hat keine legalisierende Wirkung.

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

21 S. statt aller *Bergmann*, (Fn. 11), S. 83; *Ellger*, (Fn. 10), S. 434; *Riemann*, CR 1997, 752; *Schapper*, CR 1987, 86.
22 *Gola/Wronka*, S. 126; *Kroll*, S. 166; *Tinnefeld/Ehmann*, S. 214 u. a.

überläßt, ist unwirksam.[23] Der Arbeitnehmer muß wissen, um welche Angaben es sich handelt, für welche Zwecke sie verwendet und an welchen Personenkreis sie weitergegeben werden. Maßgebend für diese Beschränkung der Dispositionsfreiheit ist die Erwägung, daß das Persönlichkeitsrecht keine „Selbstentäußerung" verträgt und 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.[24]

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 zulassen.[25] Angesichts einer Übermittlung ins Ausland besteht insoweit eine gesteigerte Hinweispflicht, die dem Betroffenen Umfang und Konsequenzen der beabsichtigten Datenverarbeitung vor Augen führt.[26] Dabei ist selbstredend vorausgesetzt, daß zugleich die personenbezogenen Daten benannt werden, um die es geht; andernfalls wäre die „Belehrung" ohne Bedeutung.[27] Fehlt sie, ist die Einwilligung unwirksam, da dann eine wesentliche gesetzliche Voraussetzung nicht erfüllt ist.[28]

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.[29] Die Richtlinie ist insoweit großzügiger als sie auch eine konkludente Erklärung zuläßt.[30]

Schon diese formalen Voraussetzungen machen deutlich, daß die Einwilligung aus Arbeitgebersicht ein schwer zu handhabendes

23 *Kroll*, (Fn. 22), S. 175; *Simitis*, in: Simitis/Dammann/Geiger/Mallmann/Walz, § 4 Rz. 55; *Tinnefeld/Ehmann* (Fn. 22), S. 212. S. a. OLG Karlsruhe, RDV 1997, 180.

24 *Baumann*, DVBl. 1984, 615; *Kroll*, (Fn. 22), S. 178; *Wohlgemuth*, Datenschutz für Arbeitnehmer, Rz. 198.

25 *Ellger*, (Fn. 10), S. 219, 445; *Tinnefeld/Ehmann* (Fn. 22), S. 212.

26 *Bergmann/Möhrle/Herb*, § 4 Rz. 50.

27 *Bergmann/Möhrle/Herb*, (Fn. 26), § 4 Rz. 47; *Gola/Schomerus*, § 4 Anm. 5.4.

28 Vgl. *Tinnefeld/Ehmann*, (Fn. 22), S. 212; *Wohlgemuth*, Datenschutzrecht, Rz. 121; aA *Dörr*, RDV 1992, 167.

29 *Dörr*, RDV 1992, 168.

30 Dazu *Dammann/Simitis* (Fn. 18), Art. 2 Rz. 22.





Mittel darstellt. Da zahlreiche Systeme nur dann sachgerecht funktionieren können, wenn alle Beteiligten in gleicher Weise erfaßt werden, kann schon das Ausscheren einiger weniger den gewollten Erfolg zunichte machen. Dazu kommt ein betriebsverfassungsrechtliches Hindernis: An alle Arbeitnehmer oder an eine Arbeitnehmergruppe mit der Frage heranzutreten, ob sie ihre Einwilligung in eine bestimmte Datenübermittlung geben wollen, stellt 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 solche Einzelfrage unter den Begriff des Personalfragebogens im Sinne dieser Vorschrift fällt.[31] In der Tat kann es keinen Unterschied machen, wie zahlreich die an die Arbeitnehmer oder eine bestimmte Gruppe gerichteten Fragen sind.

Schließlich kann zweifelhaft sein, 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.[32] Zumindest wird man hier dieselben Maßstäbe wie bei der Inhaltskontrolle von Arbeitsverhältnissen anlegen müssen: Soweit eine entsprechende arbeitsvertragliche Abmachung wegen „Unbilligkeit" unwirksam wäre[33], muß dies auch für eine vom Arbeitsvertrag als solchem abgekoppelte selbständige Einwilligung mit identischem Inhalt gelten. Letztlich kann dies jedoch dahinstehen, da diesem Weg trotz einiger Versuche multinationaler Unternehmen kaum praktische Bedeutung zukommen dürfte.[34]

31 *Fitting/Kaiser/Heither/Engels*, § 94 Rz. 10; *Gitter/Henker*, ZTR 1990, 409; *Kilian*, RdA 1978, 205; *Klebe*, in: Däubler/Kittner/Klebe, (Fn. 16), § 94 Rz. 27; *Küpferle/Wohlgemuth*, Rz. 165 f., 217 ff.; *Wohlgemuth*, BB 1991, 341; *Däubler*, (Fn. 7), Rz. 373; *Däubler*, Das Arbeitsrecht 1, Rz. 1029; wohl auch *MünchArbR-Blomeyer*, § 97 Rz. 18; aA nur *Kraft*, in: Fabricius u. a., § 94 Rz. 15; *MünchArbR-Matthes* § 339 Rz. 14.

32 Überlegungen hierzu auch bei *Rüttgers*, CR 1996, 55; *Taeger*, EWS 1995, 71; *Weichert*, S. 11. Art. 2 lit. h der Richtlinie verlangt eine „ohne Zwang" abgegebene Willenserklärung.

33 Ähnlich *Tinnefeld/Ehmann*, (Fn. 22), S. 219. Zur Inhaltskontrolle gegenüber Arbeitsverträgen *Däubler*, Arbeitsrecht 2, Rz. 127 ff.; *U. Preis*, S. 237 ff.

34 *Wohlgemuth*, BB 1991, 341.

### 3.3 Rechtfertigung durch den Arbeitsvertrag?

Der Rückgriff auf § 28 Abs. 1 Satz 1 Nr. 1 BDSG ist vermutlich der häufigste Weg zur Legalisierung der grenzüberschreitenden Datenübermittlung. So ist es beispielsweise allgemein akzeptiert, daß als Folge eines Überweisungsauftrags zugunsten eines ausländischen Gläubigers auch personenbezogene Daten weitergegeben 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 Arbeitsrecht liegen die Dinge insoweit anders, als das Arbeitsverhältnis wie auch das BDSG unternehmensbezogen sind und deshalb auch bei rein innerstaatlichen Konzernen Arbeitnehmerdaten grundsätzlich nicht an andere Konzerngesellschaften übermittelt werden dürfen. Nach ganz überwiegender Meinung scheidet auch eine Rechtfertigung mit einem überwiegenden Arbeitgeberinteresse nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG aus, da es angesichts der gesetzgeberischen Entscheidung für die „Informationseinheit" Unternehmen kein „berechtigtes" Interesse des Arbeitgebers darstelle, Daten von einem Konzernunternehmen an ein anderes zu übermitteln.[35] Verständlicherweise fordert deshalb auch der *Bundesverband der deutschen Industrie* eine Privilegierung der konzerninternen Datenverarbeitung in einem zu novellierenden BDSG.[36] Erst recht ist der vom Arbeitsvertrag gezogene Verarbeitungsrahmen überschritten, wenn Daten im Rahmen eines multinationalen Konzerns an ein ausländisches Konzernunternehmen übermittelt werden sollen.[37]

Beim rein innerstaatlichen Konzern wird dann eine Ausnahme gemacht, wenn sich das Arbeitsverhältnis nicht auf das Arbeitgeberunternehmen beschränkt, sondern Rechtsbeziehungen auch zwischen einzelnem Arbeitnehmer und Konzernspitze bestehen.[38] In diesen Fällen existiert eine vertragliche oder vertragsähnliche Beziehung zu allen Konzernunternehmen, in denen ein Arbeitseinsatz in Betracht kommt.

35 *Freise/Wohlgemuth*, DVR 1982, 288; *Gola/Wronka*, (Fn. 22), S. 204; *Klebe*, in: Däubler/Klebe/Wedde, BDSG, § 3 Rz. 22; *Kroll*, (Fn. 22), S. 115 ff.; *Wohlgemuth*, BB 1991, 341 und BB 1992, 283 mwN; aA nur *Zöllner*, S. 49.

36 Mitgeteilt bei *Jaspers*, RDV 1996, 18.

37 Vgl. *Gola/Wronka*, (Fn. 22), S. 206; *Wohlgemuth* BB 1991, 342.

38 Zu einem solchen konzerndimensionalen Arbeitsverhältnis s. *Däubler*, Arbeitsrecht 2, (Fn. 33), Rz. 1384 ff. mwN.





In der Literatur wird dieselbe Position 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.[39] Dasselbe wird dann angenommen, wenn bei der Einstellung deutlich erkennbar war, daß die Personaldatenverarbeitung in einem anderen Land zentralisiert ist.[40] In der Vergangenheit wird diese Voraussetzung in aller Regel nicht vorgelegen haben oder jedenfalls nicht beweisbar sein; bei künftigen Einstellungen kann dies allerdings anders werden.[41] Auch in solchen Fällen ist freilich zu beachten, daß der Inhalt von Arbeitsverträgen einer gerichtlichen Billigkeitskontrolle unterliegt.[42] An dieser würden „Übermittlungsklauseln" scheitern, die der ausländischen Konzernspitze praktisch freie Verfügung über die Daten des Arbeitnehmers einräumen würden.

### 3.4 Rechtfertigung mit berechtigten Interessen des Arbeitgebers nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG?

#### 3.4.1 Berechtigtes Interesse?

Ob neben § 28 Abs. 1 Satz 1 Nr. 1 BDSG auch Nr. 2 derselben Vorschrift herangezogen werden kann, wird durchaus unterschiedlich beurteilt.[43] Im vorliegenden Zusammenhang soll dies nicht vertieft werden, da die Rechtsprechung auch bei Vorliegen vertraglicher Beziehungen auf die Generalklausel des „berechtigten Interesses" als

39 Ebenso *Bergmann*, (Fn. 11), S. 84; *Bergmann/Möhrle/Herb*, (Fn. 26) § 28 Anlage 6 unter 5.2.2; *Däubler*, (Fn. 7), Rz. 254; *Drews*, DuD 1994, 68; *Ellger*, (Fn. 10), S. 201; *Gola/Schomerus*, (Fn. 27), § 28 Anm. 8.2.; *Schapper*, in: Klebe/Roth, S. 199; *Weichert*, Datenschutz-Nachrichten Heft 4/5–1996 S. 11; *Wohlgemuth*, BB 1991, 342.

40 *Bergmann*, (Fn. 11), S. 84; *Bergmann/Möhrle/Herb*, (Fn. 26), § 28 Anlage 6 unter 5.3; *Ellger*, (Fn. 10), S. 199; *Gola/Schomerus*, (Fn. 27), § 28 Anm. 8.2.

41 Vgl. *Simitis*, CR 1991, 177, wonach eine Übermittlungsklausel unschwer in den Arbeitsvertrag aufgenommen werden kann.

42 S. o. (Fn. 31).

43 Dafür *Bergmann/Möhrle/Herb*, (Fn. 26), § 28 Anlage 6 unter 5.5; H. *Ehmann*, Beilage 1/1985 zu NZA, S. 5; *Ellger*, (Fn. 10), S. 102; *Sproll*, ZIP 1984, 30; dagegen *Däubler*, (Fn. 7), Rz. 185; *Gola-Schomerus*, (Fn. 22), § 28 Anm. 2.2; *Wohlgemuth*, Datenschutz für Arbeitnehmer, Rz. 246, 461; *ders.*, BB 1991, 341.

Grundlage für die Speicherung und Übermittlung von Daten zurückgreift.[44]

§ 28 Abs. 1 Satz 1 Nr. 2 BDSG setzt als erstes voraus, daß die Übermittlung „zur Wahrung berechtigter Interessen" der speichernden Stelle, d.h. hier des Arbeitgebers, erforderlich ist. Dies wird man im Regelfall ohne großes Zögern bejahen können: Es ist durchaus „berechtigt" in diesem Sinne, ein Personalinformationssystem oder ein neues Auftragsabwicklungssystem einzuführen und dadurch Synergieeffekte zu erzielen.

### 3.4.2 Schutzwürdige Belange des Arbeitnehmers verletzt?

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. Letzteres ist dann der Fall, wenn im Land des Datenempfängers kein Datenschutz existiert oder wenn dieser nicht gleichwertig ist.[45] Bei der Beurteilung der Gleichwertigkeit ist dabei nicht nur das materielle Datenschutzrecht in Form von Gesetzen und ständiger Rechtsprechung zu beachten; vielmehr kommt es entscheidend auch darauf an, ob unabhängige Kontrollinstanzen vorhanden sind, die für die Einhaltung der inhaltlichen Vorgaben sorgen.[46] Bloße „Selbstverpflichtungen" und Verhaltenskodizes reichen nicht aus.

### 3.4.3 Wahrung durch vertragliche Abmachungen mit dem Datenempfänger?

Würde man diesen Anforderungen schematisch Rechnung tragen, wäre die Datenübermittlung in zahlreiche Länder, insbesondere auch in die USA[47], unzulässig. Angesichts wachsender internatio-

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

45 So *Geis*, NJW 1997, 288; *Taeger*, EWS 1995, 72.

46 *Simitis*, (Fn. 41), 176 verlangt deshalb, daß eine „kollektive Einwirkung der Arbeitnehmer auf Verarbeitungsabsichten des Arbeitgebers" möglich ist, da nur so ein Äquivalent zu den Mitbestimmungsrechten nach §§ 87 Abs. 1 Nr. 6, 94 BetrVG bestehe.

47 Zur dortigen Rechtslage im Datenschutz s. *Welske*, CR 1993, 297 ff. Die historische Entwicklung ist dargestellt bei *Tinnefeld/Ehmann*, (Fn. 22), S. 36 ff. Zu einem Diskussionspapier der US National Telecommunication and Information Administration (NTIA) s. die zusammenfassende Wiedergabe in CR 1998, 191. Zum (bescheidenen) Schutz der Arbeitnehmerpersönlichkeit im allgemeinen s. *Finkin*, ZVglRWiss 94 (1995), 109 ff.





naler Arbeitsteiligkeit läßt sich eine solche Position jedoch nicht ernsthaft aufrechterhalten. Zahlreiche Autoren[48] sowie die Aufsichtsbehörden befürworten deshalb eine sog. Vertragslösung: Die grenzüberschreitende Datenübermittlung ist auch in solche Länder zulässig, sofern durch Vertrag sichergestellt ist, daß im Empfängerstaat ein äquivalentes Maß an Datenschutz praktiziert wird.

Obwohl diese Position im Vordringen ist[49], sieht sie sich immer noch einer Reihe von Einwendungen ausgesetzt. Ihnen kann jedoch durch entsprechende Vertragsgestaltung Rechnung getragen werden.

#### *3.4.3.1 Fehlende Kontrollmöglichkeit*

Der erste Einwand geht dahin, die deutschen Aufsichtsbehörden könnten nicht kontrollieren, ob der Datenschutzvertrag auch wirklich im Ausland eingehalten werde.[50] Dies trifft sicherlich zu, da es ein Eingriff in fremde Souveränitätsrechte wäre, wollte eine deutsche Behörde in den USA oder in der Schweiz nach dem Rechten sehen. Entsprechende Kompetenzerweiterungen wären nur auf völkerrechtlicher Grundlage, insbesondere durch Abschluß eines Verwaltungsabkommens möglich. Dennoch scheitert die Vertragslösung nicht an diesem Einwand: Vernünftigerweise wird ja nicht Identität, sondern Gleichwertigkeit des Schutzes verlangt, so daß der Vertrag dafür sorgen muß, daß private Instanzen eine vergleichbare Kontrollkompetenz eingeräumt erhalten. Dies ist in der Weise möglich, daß man beispielsweise dem Betriebsrat oder dem betrieblichen Datenschutzbeauftragten entsprechende Befugnisse einräumt.

#### *3.4.3.2 Schwächen der vertraglichen Rechtsgestaltung*

Ein zweiter Einwand stützt sich auf die Schwächen der Rechtsform „Vertrag". Der Betroffene sei selbst in der Regel nicht Vertragspar-

48 S. statt aller *Bergmann/Möhrle/Herb*, (Fn. 26), § 28 Anlage 6 unter 5.5; *Däubler*, (Fn. 7), Rz. 254a; *Geis*, (Fn. 45), 289; *Napier*, RDV 1990, 216 ff.; *Gola/Schomerus*, § 28 Anm. 8.1; *Taeger*, EWS 1995, 72; *Ungnade/Gorynia*, WM-Sonderbeilage 7/1983, S. 17; *Weichert*, Datenschutz-Nachrichten Heft 4/5–1996, S. 12.

49 *Riemann*, CR 1997, 752.

50 *Bergmann*, (Fn. 11), S. 220; *Simitis*, (Fn. 41), 177; *Wohlgemuth*, BB 1991, 342.

tei[51], ein Vertrag zugunsten Dritter nicht gewollt[52] oder (so das englische Recht) nicht möglich.[53] Auch könnten die Beteiligten den Vertrag jederzeit an neue Informationsbedürfnisse der Konzernspitze anpassen[54] oder ihn kündigen.[55] Schließlich hätte der deutsche Arbeitgeber kein Eigeninteresse daran, die datenschutzrechtlichen Befugnisse seiner Beschäftigten gegenüber einer mächtigen ausländischen Konzernspitze durchzusetzen.[56]

Auch hier lassen sich einigermaßen „wasserdichte" Lösungen entwickeln, die diesen Einwänden Rechnung tragen. Das hier speziell interessierende deutsche Recht läßt den Abschluß eines echten Vertrages zugunsten Dritter zu: Nach § 328 Abs. 1 BGB kann man den betroffenen Arbeitnehmern das Recht einräumen, die vom BDSG vorgesehenen Ansprüche auch gegenüber der ausländischen Konzerngesellschaft geltend zu machen. § 328 Abs. 2 BGB gestattet es überdies, 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. Selbst wenn keine unentziehbaren Rechte eingeräumt werden, besteht gleichwohl keine Gefahr, daß der Vertrag über die Köpfe der Betroffenen hinweg verändert oder gar 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 Vertrages würde die Datenübermittlung ins Ausland unzulässig. Notfalls könnte sie im Wege der einstweiligen Verfügung untersagt werden.

*3.4.3.3 Zugriff ausländischer Behörden*

Schließlich wird zu bedenken gegeben, daß die im Ausland gespeicherten Daten dem Zugriff der dortigen Behörden ausgesetzt sind. Dies könne zu einer Gefährdung der Datensicherheit, aber auch zu

51 So *Bergmann*, (Fn. 11), S. 85, 220; *Simitis*, in: Simitis/Dammann/Mallmann/Reh, § 24 Rz. 50.
52 So *Ellger*, (Fn. 10), S. 444.
53 Vgl. *Napier*, (Fn. 48).
54 So *Ellger*, (Fn. 10), S. 204.
55 *Wohlgemuth*, (Fn. 50).
56 *Ellger*, (Fn. 10), S. 204.





anderen Unzuträglichkeiten führen.[57] Ein solcher Einwand ist gleichfalls nur auf den ersten Blick überzeugend. Niemand nimmt etwa Anstoß daran, daß einzelne Geschäftsreisende ihren Laptop samt Disketten ins Ausland mitnehmen, obwohl sie dem Zugriff ausländischer Staatsgewalten ausgesetzt sind, gegen die sie sich nur schwer zur Wehr setzen könnten. Ein im Ausland angesiedeltes Konzernunternehmen ist im Vergleich zu einem Fluggast sehr viel besser 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" machte und dabei Betriebsgeheimnisse erbeutete, sind längst vorbei. In der Realität wird alles versucht, um Investoren nicht vom eigenen Standort abzuschrecken. Auch muß man im vorliegenden Zusammenhang berücksichtigen, daß eine (theoretische) Gefahr allenfalls für technische Daten, nicht aber für Daten der in Deutschland tätigen Arbeitnehmer besteht. Daß sich das FBI für sie interessieren könnte, ist denkbar unwahrscheinlich; außerdem untersteht auch dieses im Prinzip rechtsstaatlichen Sicherungen.

### 3.5 Anforderungen an die „Vertragslösung" im einzelnen

Um die „schutzwürdigen Interessen" der Betroffenen zu wahren, muß der zwischen dem deutschen Arbeitgeber und dem ausländischen Datenempfänger geschlossene Vertrag einen dem deutschen Recht äquivalenten Datenschutz sicherstellen und überdies zusätzliche Mechanismen vorsehen, die einen Ausgleich für die wegfallenden Kontrollbefugnisse der Aufsichtsbehörde darstellen. Dies führt zu bestimmten Vorgaben für die Vertragsgestaltung.

- Durch die Übermittlung ins Ausland dürfen keine umfassenderen Verarbeitungsmöglichkeiten eröffnet werden, als sie 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 wünschenswert, daß die Betroffenen nicht den Umweg über den deutschen Arbeitgeber gehen müssen, sondern sich direkt an die ausländische spei-

57 Vgl. *Simitis*, (Fn. 41); *Wohlgemuth*, BB 1992, 284.

chernde 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 Verarbeitungsbeschränkungen 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 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 BGB läßt Derartiges ausdrücklich zu.
- Wird rechtswidriges Verhalten der ausländischen speichernden Stelle nicht korrigiert (trotz entsprechender Aufforderung durch einen Betroffenen wird zB 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 ein dortiges Gericht anerkannt und seiner Entscheidung zugrunde gelegt wird. Sinnvoller ist es deshalb, für jeden Fall der Zuwiderhandlung eine Vertragsstrafe vorzusehen. Das Vorliegen eines Verstoßes zu prüfen, müßte Sache eines Schiedsgerichts oder eines deutschen staatlichen Gerichts sein[58]. Ohne eine solche Instanz bestünde die Gefahr, daß der Verstoß bestritten wird und dann doch ein normales gerichtliches Verfahren stattfinden muß, für das uU kein inländischer, sondern nur ein ausländischer Gerichtsstand zur Verfügung steht. Mit der Vertragsstrafe müßte die speichernde Stelle im Inland belastet werden, da sie wirtschaftlich mit der Konzernspitze identisch ist und ihr gegenüber in der Regel keine Durchsetzungsprobleme bestehen.

Eine entsprechende Musterabmachung ist an anderer Stelle veröffentlicht worden.[59] Die hier entwickelten Grundsätze gelten

58 *Napier*, (Fn. 48).
59 *Däubler/Klebe/Wedde*, BDSG, (Fn. 8), Anhang 2.





auch für die „Durchleitung" von Daten durch ein Land ohne gleichwertiges Schutzniveau, es sei denn, dort wäre jeder Zugriff auf die Daten ausgeschlossen.[60]

## 4. Zulässigkeit des „Datenimports"

Wenig Aufmerksamkeit hat bislang die Frage erfahren, inwieweit Daten ins Inland überspielt werden dürfen, die in einer Weise erhoben wurden, die mit unserem Rechtsverständnis schwer in Einklang zu bringen ist. Dies mag damit zusammenhängen, daß durch solche Vorgänge in der Regel ausländische und keine deutschen Staatsbürger betroffen sind, und daß sich überdies Vorgänge schwer klären lassen, die sich irgendwann in einem anderen Land vollzogen haben. Dennoch wäre es inkonsequent, wollte man die Datenerhebung im Inland nach § 28 Abs. 1 Satz 2 BDSG an die Beachtung von Treu und Glauben und eines rechtmäßigen Verfahrens binden, während man auf der anderen Seite den „Import" auch solcher Daten zuließe, die ohne Rücksicht auf Bank- und Steuergeheimnis oder gar mit Hilfe eines Lügendetektors erhoben wurden.[61] Das Verbringen in den Geltungsbereich des BDSG ist daher dann unzulässig, wenn die Erhebung unter Verstoß gegen Grundauffassungen des deutschen Rechts erfolgt ist (Art. 6 EGBGB). Eine schlichte Erstrekkung des § 28 Abs. 1 Satz 2 scheidet dagegen aus.

## 5. Zur künftigen Rechtslage nach der EG-Datenschutzrichtlinie

### 5.1 Übermittlung innerhalb der EU

Sobald die Datenschutzrichtlinie von allen Mitgliedstaaten umgesetzt ist, gilt das Territorium der EU datenschutzrechtlich als „In-

60 Die hier skizzierten Grenzen gelten auch dann, wenn man Betriebsvereinbarungen als weitere mögliche Rechtsgrundlage für Datentransfers anerkennt.
61 Zur Auslegung des § 28 Abs. 1 Satz 2 BDSG s. *Wedde*, in: Däubler/Klebe/Wedde, (Fn. 8), § 28 Rz. 47 ff.; zum teilweisen (wenn auch nicht völligen) Verbot in den USA, Arbeitnehmer mit Hilfe eines Lügendetektors zu befragen, s. *Welske*, CR 1993, 297 ff.

land". Ob von Hamburg nach München oder von Hamburg nach Marseille übermittelt wird, macht dann keinerlei Unterschied mehr aus. Allerdings ist der Umsetzungstermin (24. 10. 1998) von der Bundesrepublik und einigen anderen Mitgliedstaaten nicht eingehalten worden. Dem Sinn der Richtlinie entsprechend gilt dann der freie Datenfluß zunächst nur zwischen jenen Staaten, die den Vorgaben des EG-Rechts Rechnung getragen haben.

Die Länder des Europäischen Wirtschaftsraumes (Norwegen, Island, Liechtenstein) sind gleichfalls einbezogen.

### 5.2 Übermittlung in Drittstaaten

#### 5.2.1 ... mit angemessenem Schutzniveau

Nach Art. 25 Abs. 1 der Richtlinie ist die Übermittlung in einen Drittstaat nur dann zulässig, wenn dieser über ein „angemessenes" Schutzniveau verfügt. Die bisher zugrunde gelegte „Gleichwertigkeit" wird nicht mehr verlangt.[62] Ob man „Angemessenheit" mit „funktionaler Äquivalenz" gleichstellen kann[63], erscheint zweifelhaft, da dies doch wieder auf die nicht gewollte Gleichwertigkeit hinausläuft.

Die Formel von der „Angemessenheit" ist ersichtlich ein politischer Kompromiß[64], der den Sinn hat, eine Abkoppelung der EU von weltweiten Datenströmen zu verhindern.

Welches Maß an Abweichung vom EG-Standard tolerierbar ist und die Angemessenheit nicht in Frage stellt, erscheint unklar. Bisweilen wird der Standpunkt vertreten, uU könne es nicht genügen, lediglich den Standard der Datenschutzkonvention des Europarats zu praktizieren.[65] Andere sehen größere Spielräume, die nach politischen Gesichtspunkten ausgefüllt würden.[66] Auch ist bei der Konkretisierung die staatliche Schutzpflicht in bezug auf das informationelle Selbstbestimmungsrecht des Betroffenen zu berücksichtigen, die grundsätzlich auch im Rahmen von grenzüberschreitenden

62 *Dammann/Simitis*, (Fn. 18), Art. 25 Rz. 8; *Gounalakis/Mand*, CR 1997, 502; *Taeger*, EWS 1995, 79; kritisch dazu *Ellger*, CR 1993, 9.
63 So *Simitis*, NJW 1997, 284.
64 *Mütsch*, DuD 1994, 189; *Riemann*, CR 1997, 754.
65 *Ellger*, CR 1994, 567.
66 *Riemann*, (Fn. 63).





Sachverhalten besteht.[67] Die Richtlinie bietet selbst nur zwei Anhaltspunkte.

Zum einen soll nach ihrem Art. 25 Abs. 2 auf die Umstände bei einer einzelnen Datenübermittlung oder einer bestimmten Kategorie von Datenübermittlungen abgestellt werden. Dies bedeutet, daß ein bestimmtes Drittland uU wegen eines bereichsspezifischen Datenschutzes in einzelnen Sektoren durchaus ein angemessenes Schutzniveau gewährleistet, während es in anderen Bereichen dieses Prädikat nicht verdient.[68]

Zum zweiten sieht Art. 25 Abs. 3–6 ein Verfahren vor, wie die Mitgliedstaaten zu einer einheitlichen Handhabung kommen. Soweit Bedenken gegen die Angemessenheit des Schutzniveaus in einem Drittstaat bestehen, sind diese in einen Konsultationsprozeß einzubringen, an dessen Ende eine verbindliche Festlegung durch die Kommission steht. Diese hat zugleich die Aufgabe, zum „geeigneten Zeitpunkt" Verhandlungen mit dem Drittstaat einzuleiten, um auf diesen im Sinne einer stärkeren Homogenisierung der Anforderungen einzuwirken. Daß man insoweit Druck auf Handelspartner ausüben kann[69], mag im Einzelfall sicherlich richtig sein; einen großen Partner wie die USA, Kanada oder Japan zu einer Annäherung an den europäischen Standard zu veranlassen, dürfte auch mit einem starken Euro im Rücken kaum möglich sein. Die Gefahr, daß um des lieben Friedens willen die Anforderungen an die Angemessenheit immer mehr gesenkt werden, ist allerdings nicht sehr groß, da Art. 26 selbst in bezug auf Drittstaaten mit nicht angemessenem Schutzniveau eine Übermittlung in beträchtlichem Umfang zuläßt.

#### 5.2.2 ... ohne angemessenes Schutzniveau

Nach Art. 26 Abs. 1 lit. a der Richtlinie reicht zum einen die Einwilligung des Betroffenen aus. Diese muß „ohne jeden Zweifel" vorliegen, was auch bei konkludenter Erklärung (etwa durch Erteilung eines Überweisungsauftrags oder Buchung einer Reise) möglich ist.[70] Von der ausdrücklichen unterscheidet sich die konkludente Willenserklärung nur insoweit, als im ersten Fall die Sprache,

67 *Palm*, CR 1998,69.
68 *Dammann/Simitis*, (Fn. 18), Art. 25 Rz. 9.
69 So *Ellger*, (Fn. 64), 566.
70 *Riemann*, (Fn. 65), 755.

im zweiten andere Mittel der Kommunikation benutzt werden.[71] Die Frage der Eindeutigkeit kann in beiden Fällen auftauchen, sie hat nichts mit dem benutzten Medium zu tun. Welche Anforderungen an eine wirksame Einwilligung zu stellen sind, bestimmt das nationale Recht; insoweit kann und wird es bei den oben skizzierten Grundsätzen bleiben.[72]

Eine zweite Ausnahme besteht nach Art. 26 Abs. 1 lit. b und c dann, wenn die Übermittlung im Rahmen eines Vertrages erfolgt. Lit. b setzt dabei die Erfüllung eines mit dem Betroffenen geschlossenen Vertrages, lit. c den Abschluß oder die Erfüllung eines Vertrages zwischen der speichernden Stelle und einem Dritten voraus, der im Interesse des Betroffenenen vereinbart wurde. Entsprechendes gilt für vorvertragliche Beziehungen.

Art. 26 Abs. 1 lit. d–f der Richtlinie sehen weitere Ausnahmen (etwa zur Wahrung eines wichtigen öffentlichen Interesses) vor, die im gegebenen Zusammenhang von geringerer Bedeutung sind.[73]

Für Arbeitnehmerdaten ändert sich durch diese Tatbestände zunächst nur wenig. Wie bisher dürfte die Einwilligung in der Praxis von geringer Bedeutung sein und die vertragliche Ermächtigung lediglich beim konzerndimensionalen Arbeitsverhältnis ernsthaft als Rechtsgrundlage in Betracht kommen.

Die bisher im deutschen Recht praktizierte Möglichkeit des § 28 Abs. 1 Satz 1 Nr. 2 BDSG, d. h. die Legitimation durch ein überwiegendes Arbeitgeberinteresse, ist in die Richtlinie nicht aufgenommen worden.[74] Statt dessen sieht ihr Art. 26 Abs. 2 vor, daß eine Übermittlung oder (realistischer) eine Kategorie von Übermittlungen in ein Drittland ohne angemessenes Schutzniveau genehmigt wird, „wenn der für die Verarbeitung Verantwortliche ausreichende Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten der Personen sowie hinsichtlich der Ausübung der damit verbundenen Rechte bietet". Solche Garantien könnten sich insbesondere aus „entsprechenden Vertragsklauseln" ergeben.[75] Als „Auffangtatbestand" ist daher die „Vertragslösung" ausdrücklich festgeschrieben worden, wird jedoch anders als bisher nicht ohne staatliche Zustimmung möglich sein. In der Literatur wird an sie insbesondere die Anforderung gestellt, daß für ihre Beachtung in der Praxis gesorgt wird.[76]

71 Dazu *Däubler*, Zivilrecht 1, Rz. 580.
72 Ebenso *Geis*, (Fn. 48), S. 291.
73 Dazu *Dammann/Simitis*, (Fn. 18), Art. 26 Rz. 8 ff.
74 *Ehmann-Sutschet*, RDV 1997, 11.
75 Dazu *Geis*, (Fn. 48), S. 291; *Riemann*, CR 1997, 755; *Schild*, EuZW 1996, 553.





Ähnlich wie im Rahmen der Angemessenheitsprüfung ist auch hier eine Koordination zwischen den Mitgliedstaaten vorgesehen; letztlich befindet nach Art. 26 Abs. 4 die Kommission darüber, ob bestimmte Standardvertragsklauseln ausreichende Garantien enthalten. Wie das Wörtchen „ausreichend" zu handhaben ist, läßt sich dem Richtlinientext nicht entnehmen. Wichtig ist, daß nach dem Wortlaut auch die Ausübung der mit den Grundrechten und Grundfreiheiten verbundenen Rechte gesichert sein muß; die bloße Übernahme von materiellem Datenschutzrecht ohne gleichzeitige Kontrollinstanz wäre daher mit Sicherheit nicht genügend.

### 5.3 Ein Umsetzungsversuch

Der Gesetzentwurf von BÜNDNIS 90/DIE GRÜNEN[77] trägt im hier interessierenden Bereich den Vorgaben der Richtlinie nicht voll Rechnung; erst recht kann nicht von einer Ausschöpfung der vorhandenen Spielräume im Sinne von konsequenterem Datenschutz die Rede sein.[78]

§ 50 des Entwurfs enthält eine Sonderregelung zum Arbeitnehmerdatenschutz. Nach Abs. 4 dieser Vorschrift ist eine Übermittlung nur zulässig, wenn der Empfänger ein rechtliches Interesse darlegt oder die Art und Zielsetzung der dem Beschäftigten übertragenen Aufgaben dies erfordern. Ob das letztere auch dann gelten soll, wenn durch Vernetzung zahlreiche Zugriffsmöglichkeiten für Dritte eröffnet werden, ist weder dem Wortlaut noch der Begründung zu entnehmen. Datenschutz „nach Maßgabe der Arbeit" erinnert allerdings ein wenig an den inzwischen abgeschafften arbeitsschutzrechtlichen Grundsatz, wonach der Gesundheitsschutz eine unübersteigbare Schranke an der „Natur des Betriebes" findet.[79]

76 *Dammann/Simitis*, Art. 26 Rz. 18 ff. Insoweit besteht Übereinstimmung mit dem oben III 4 und 5 Gesagten.
77 BT-Drucksache 13/9082.
78 Dies soll nicht die in anderen Zusammenhängen bestehenden Verdienste des Entwurfs schmälern.
79 § 120a GewO wurde durch das Arbeitsschutzgesetz von 1996 aufgehoben, das keinen entsprechenden Vorbehalt kennt.

Die speziellen Fragen der grenzüberschreitenden Datenübermittlung in Drittländer sind in § 8 des Entwurfs angesprochen. Sein Abs. 2 übernimmt weithin wörtlich die (sehr diffusen) Kriterien des Art. 25 Abs. 2 der Richtlinie für die Bestimmung des „angemessenen" Datenschutzniveaus, spricht allerdings pauschal von „der" Datenübermittlung, während die Richtlinie daneben auch eine „Kategorie von Datenübermittlungen" erwähnt. Die Richtlinie läßt also bewußt eine bereichsspezifische Differenzierung zu, was zB im Hinblick auf die Rechtslage in den USA höchst vernünftig ist.[80] Der Fall, daß die Kommission entsprechend Art. 25 Abs. 6 der Richtlinie die Angemessenheit feststellt, ist nicht erwähnt.

Bei der Datenübermittlung in Länder ohne angemessenes Datenschutzniveau werden in § 8 Abs. 4 des Entwurfs die Zulässigkeitsvoraussetzungen des Art. 26 Abs. 1 der Richtlinie nur in verwässerter Form übernommen. Während etwa die Richtlinie davon spricht, die Übermittlung müsse „für die Erfüllung eines Vertrages zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen erforderlich" sein, und bei der Durchführung von vorvertraglichen Maßnahmen einen „Antrag" des Betroffenen voraussetzt, geht es nach § 8 Abs. 4 Nr. 2 des Entwurfs schlicht darum, daß die Übermittlung „im Rahmen eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses" erforderlich sein muß. Statt von der „Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht" (Art. 26 Abs. 1 lit. d der Richtlinie) ist in § 8 Abs. 4 Nr. 4 von der „Geltendmachung eines rechtlichen Interesses" die Rede. Würde dies alles Gesetz, wäre ein Verfahren vor dem *EuGH* geradezu vorprogrammiert, das die Bundesrepublik als Land mit einer der längsten Datenschutztraditionen in der EU auf die ungewohnte Anklagebank bringen würde. Wenigstens ist bei der Genehmigungsfähigkeit von Vertragslösungen die Richtlinie eins zu eins übernommen worden.[81]

Die in Art. 26 der Richtlinie zugelassenen Ausnahmen müssen keinen generellen Charakter tragen. Der Einleitungssatz enthält vielmehr einen Vorbehalt zugunsten „entgegenstehender Regelungen für bestimmte Fälle" im innerstaatlichen Recht.[82] Der deutsche Ge-

80 Zum unterschiedlichen Datenschutz in einzelnen Lebensbereichen nach dem Recht der USA s. *Schwartz/Reidenberg*, Data Privacy Law, Charlottesville 1996.

81 Vgl. Art. 26 Abs. 2 der Richtlinie und § 8 Abs. 5 des Entwurfs.

82 *Dammann/Simitis*, (Fn. 18), Art. 26 Rz. 4.





setzgeber hätte also die Möglichkeit, den Transfer von Arbeitnehmerdaten restriktiver zu regeln, insoweit beispielsweise eine generelle Genehmigungspflicht bei Übermittlung in Staaten ohne angemessenes Schutzniveau vorzusehen. Gerade wer Sonderregeln für abhängig Beschäftigte will, müßte auch dies in Erwägung ziehen.