Ulf Brühann

Selbstregulierungsinstrumente zur Liberalisierung des Datenexports

1. Warum Datenexportregeln?

Alle Studien zum Datenschutz belegen, dass die Entwicklung zur Informationsgesellschaft eine weltweite Welle von Datenschutzregeln ausgelöst hat. Die vorerst jüngste Übersicht dieser Art wurde von der internationalen Anwaltsfirma White & Case LLP auf dem Global Privacy Symposium in New York am 30. 4. 2002 vorgelegt (http://www.whitecase.com/report_global_ privacy.pdf). 15 Länder wurden einer vergleichenden Analyse ihrer Datenschutzsysteme unterzogen. Alle hatten gesetzliche Regelungen, und in acht von ihnen wurden Änderungen vorbereitet. »Es gibt eine anhaltende Flut von gesetzlichen und anderen Vorschriften, die die Nutzung von Wirtschaftsdaten von Unternehmen reguliert.« »Dies betrifft alle Wirtschaftsbereiche, aber die Tatsache, dass es sich um einen weltweiten Trend handelt, heißt nicht, dass die Regelungen einheitlich oder mindestens konform wären. Für multinationale Unternehmen bedeutet die Notwendigkeit der Beachtung aller dieser Regeln ständige Wachsamkeit und besondere Aufmerksamkeit.« Soweit die Vorstellung der Ergebnisse der Studie (http://www.whitecase.com/pr_wc_ privacy_law_survey.html).

Die Informationsgesellschaft hat aber nicht nur Aktivität des Gesetzgebers ausgelöst. Internationale Organisationen wie der Europarat und die OECD haben die Anwendbarkeit ihrer allgemeinen Instrumente auf die Verarbeitung personenbezogener Daten insbesondere im Internet und elektronischen Handel überprüft. Der Europarat hat beispielsweise eine Empfehlung verabschiedet zum Datenschutz auf dem Internet (http://www.legal.coe.int/dataprotection/Default.asp?fd=general&fn=InstrumentsE.htm). Die Ministerkonferenz der OECD hat auf ihrer Tagung 1998 in Ottawa aus einer detaillierten Überprüfung die Schlussfolgerung gezogen, dass die allgemeinen Datenschutzprinzipien auch für den elektronischen Handel volle Anwendung finden und beschlossen, die notwendigen Schritte einzuleiten, um sicherzustellen, dass die Leitlinien der OECD zum Datenschutz in globalen Netzwerken effektiv angewandt werden (Declaration on the protection of privacy on global networks made by OECD Ministers at the Conference »A borderlesss world: Realising the potential of global electronic commerce«, 7 – 9 October 1998, Ottawa, Canada, DSTI/ICC/REG(98)10/FINAL v. 22.12.1998).

Darüber hinaus ist der Datenschutz zu einem der wesentlichen Bereiche geworden, für den sich die interessierten Kreise der Wirtschaft über die Notwendigkeit von Selbstregulierungselementen verständigt haben. Schon im sogenannten Bangemann-Bericht wurde die Verbindung geknüpft zwischen einem wirksamen Datenschutz und der effektiven Entwicklung des elektronischen Handels. Diese Gruppe Vertreter europäischer Industrie unter dem Vorsitz des Vizepräsidenten der Kommission, Dr. Martin Bangemann, ver-

abschiedete einen Bericht an den Europäischen Rat, in dem festgestellt wird dass der Datenschutz eine der wesentlichen Voraussetzungen ist für die Akzeptanz der Dienste der Informationsgesellschaft und deren wirtschaftliche Entwicklung (»The Group believes that without the legal security of a Union-wide approach, lack of consumer confidence will certainly undermine the rapid development of the information society. Given the importance and sensitivity of the privacy issue, a fast decision from Member States is required on the Commission's proposed Directive setting out general principles of data protection.« http://europa.eu. int/ISPO/infosoc/backg/bangeman.html).

Im Transatlantischen Wirtschaftsdialog (TABD) wurde ausdrücklich bekräftigt, dass effektive Datenschutzregeln für die Entwicklung des elektronischen Handels erarbeitet werden sollten (»Industry should continue to develop mechanisms for privacy protection parallel to the evolution of electronic commerce«, http://www.tabd.org/recommendations/Berlin99.pdf).

Im Weltweiten Wirtschaftsdialog wurden bereits erste Entwürfe für ein Selbstregulierungsinstrument mit weltweiter Anwendbarkeit diskutiert (http://consumerconfidence.gbde.org/protection.html).

Auch die G8 haben eine »Okinawa Charter on Global Information Society« angenommen, in der die Entwicklung effektiver und sinnvoller Instrumente zum Schutz personenbezogener Daten angemahnt wird und eine gemischte Arbeitsgruppe »Digital Opportunity Task Force« (DOT) eingesetzt, die Vertreter von Regierungen, Wirtschaft und Wissenschaft auf weltweiter Basis zusammenbringt (http://www.dotforce.org/reports/it1.html).

Fast alle dieser Instrumente enthalten Regelungen zum Datenexport. Ziel dieser Regelungen ist, den Export von geschützten personenbezogenen Daten aus dem räumlichen und sachlichen Geltungsbereich des jeweiligen Schutzinstruments heraus zu beschränken und nur zuzulassen, soweit sonstige Garantien für den Schutz der Daten nach der Übermittlung in einen ungeschützten Empfängerbereich sichergestellt sind.

Es ist ein Paradox der Entwicklung zur Informationsgesellschaft, dass sie sowohl den Grund für eine solche Regelung als auch die Schwierigkeit seiner Durchsetzung verstärkt hat. Daten können ohne größere Schwierigkeiten und Kosten auf im Ausland gelegene Verarbeitungsmittel übertragen, dort frei von den Anforderungen des inländischen Datenschutzes weiterverarbeitet und wieder in das Inland reimportiert werden. Inländische Kontrollinstanzen betonen die Schwierigkeiten einer grenzüberschreitenden Durchsetzung inländischer Datenschutzgrundsätze und reagieren oft defensiv, indem sie sich für die grenzüberschreitenden Verarbeitungsvorgänge oft nicht für zuständig halten. Die Gründe für eine solche Internationalität der Datenströme können vielfältiger Art sein, insbesondere von Gesichtspunkten der Kosten für die Arbeitsfaktoren in einem Drittland beeinflusst sein, so dass in diesen Fällen nicht automatisch eine Absicht der Umgehung der nationalen Regeln unterstellt werden kann. Wird es möglich, die Anwendung nationaler Regeln durch Nutzung der Möglichkeiten der dezentralen Struktur der Datenverarbeitung in der Informationsgesellschaft und insbesondere des Internet zu vermeiden, so

verliert die Territorialität der Verarbeitung ihre Bedeutung bei der Kontrolle und vor allem der Durchsetzung der Einhaltung der Regeln. Daraus entwickel sich aber ein Problem der generellen Akzeptanz inländischer Datenschutzanforderungen, wenn im übrigen ausländische Unternehmen, die nicht denselben Zwängen unterliegen, ohne Schwierigkeiten Daten im Inland erheben oder sich sonst übermitteln lassen können und mit inländischen Unternehmen in direkten Wettbewerb treten können. Schließlich weist auch der menschenrechtliche Ansatz des Datenschutzes, der keinen Unterschied nach Nationalität zulässt, in dieselbe Richtung.

Angesichts dieses Befundes, nämlich der aus guten Gründen in vielen Staaten bestehenden rechtlichen Beschränkungen des internationalen Datentransfers, ist die Rolle von Selbstregulierungsinstrumenten der Wirtschaft zu untersuchen. Es liegt auf der Hand, dass solche Instrumente im Hinblick auf ihre Charakteristik der Freiwilligkeit nicht geeignet sind, Beschränkungen, die auf rechtlichen Instrumenten beruhen, abzubauen: Gesetze können nur durch ebensolche modifiziert werden.

Dennoch sollte Platz für Selbstkontrollinstrumente innerhalb des gegenwärtigen, durch die Existenz rechtlicher Instrumente charakterisierten Systems sein. Verhaltenskodices könnten erstens die Anwendung allgemeiner Datenschutzprinzipien im Hinblick auf bereichsspezifische Verarbeitungen präzisieren. Verhaltenskodices könnten zweitens den Gesetzgeber veranlassen, die Regelungsdichte zu senken, indem sie den Mangel an Datenschutz durch staatliche Maßnahmen in Drittstaaten kompensieren.

Beide Fälle haben unterschiedliche Ausgangspunkte und Zielsetzungen und benötigen deshalb ein unterschiedliches Instrumentarium. Im ersten Fall ergänzen Selbstkontrollinstrumente bestehende rechtliche Regeln im innerstaatlichen Bereich. Sie können sie deshalb voraussetzen, brauchen sie nicht zu wiederholen und können sich ganz auf die Einzelfragen bei der Anwendung der Prinzipien im Hinblick auf die Besonderheiten der Wirtschaftsbereiche konzentrieren. Auch die Durchsetzung der freiwilligen Regeln könnte in diesem Fall den gesetzlichen Grundsätzen folgen. Wenn die freiwilligen Regeln die Anwendung der allgemeinen rechtlichen Grundsätze präzisieren, könnten sie auch an ihren Durchsetzungsmechanismen teilnehmen.

Ganz anders die Regeln zur Kompensation mangelnder verbindlicher staatlicher Datenschutzregeln in einem Drittland. Sie müssen alle wesentlichen Elemente eines kompletten Datenschutzsystems enthalten und darüber hinaus selbst Mechanismen für ihre Durchsetzbarkeit schaffen, insbesondere den betroffenen Personen die Geltendmachung ihrer Rechte ermöglichen. Außerdem könnten sie zusätzliche bereichsspezifische Regeln wie oben beschrieben enthalten.

Dieser Fall ist im Zusammenhang mit Artikel 26 der Richtlinie 95/46/EG zu untersuchen, während der erste Fall davon zu unterscheiden ist und in Artikel 27 behandelt wird.

2. Welche Exportdatenregeln?

Zunächst darf nicht vergessen werden, dass der Datenverkehr innerhalb der gegenwärtig 15 Mitgliedstaaten der Gemeinschaft sowie den Staaten des EWR (Norwegen, Island, Liechtenstein) auf der Basis der Garantie eines **gleichwertigen** Schutzniveaus durch Harmonisierung der Datenschutzgesetze in allen diesen Ländern durch die Richtlinie 95/46/EG selbst bereits liberalisiert ist. Artikel 1 Abs. 2 der Richtlinie sieht ausdrücklich vor, dass die Mitgliedstaaten den freien Verkehr personenbezogener Daten zwischen ihnen nicht aus Gründen des Datenschutzes beschränken oder untersagen.

Die EU-Datenschutzrichtlinie eröffnet grundsätzlich drei Wege zur Liberalisierung des internationalen Datenverkehrs: erstens die inländische oder gemeinschaftliche Anerkennung der Existenz eines **angemessenen** Datenschutzniveaus seitens des Datenimporteurs, zweitens die inländische oder gemeinschaftliche Anerkennung der Erbringung angemessener Garantien für den Schutz der Daten nach ihrer Übermittlung seitens des Datenexporteurs, und drittens die Feststellung einer Situation, in der nach Einschätzung in der Richtlinie selbst das Risiko für die Privatsphäre der betroffenen Person auch nach der Übermittlung typischerweise gering ist.

2.1

Die besonderen Situationen, in denen die Richtlinie das Risiko für die Privatsphäre des Einzelnen auch nach Übermittlung als gering ansieht, können in diesem Zusammenhang vernachlässigt werden, weil sie nicht auf die Existenz von Selbstregulierungsinstrumenten abstellen.

2.2

Die Angemessenheit des Datenschutzes in einem Drittstaat, in dem der Empfänger der übermittelten Daten niedergelassen ist, ist anhand der in Artikel 25 Abs. 2 der Richtlinie genannten Merkmale des konkreten Transfers und des Schutzes im Drittland durch allgemeine Rechtsnormen, sektorelle Rechtsnormen, Standesregeln und Sicherheitsmaßnahmen zu beurteilen.

2.3

Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten der Personen sowie hinsichtlich der Ausübung der damit verbundenen Rechte kann auch der für die Übermittlung Verantwortliche beibringen. Die Richtlinie erwähnt insbesondere entsprechende Vertragsklauseln, lässt aber damit auch andere Möglichkeiten offen.

Es ist deshalb zu fragen, welche Rolle Selbstregulierungsinstrumente zur Liberalisierung des internationalen Datenverkehrs nach den beiden letztgenannten Möglichkeiten spielen können.

3. Wann können freiwillige Selbstkontrollen anerkannt werden?

3.1 Selbstregulierungsinstrumente als Teil eines angemessenen Datenschutzsystems im Drittland?

Aus dem erwähnten Artikel 25 Abs. 2 der Richtlinie 95/46/EG ergibt sich, dass auch nichtgesetzliche Maßnahmen in einem Drittland bei der Prüfung der Angemessenheit berücksichtigt werden können, sofern diese Regeln effektiv befolgt und durchgesetzt werden. Die Beurteilung ihrer Angemessenheit erfolgt nach denselben objektiven Kriterien, nach denen auch die Angemessenheit gesetzlicher und sonstiger Vorschriften bemessen wird.

In den bisherigen Entscheidungen zur Angemessenheit hat die Europäische Kommission zur materiellen Ausfüllung regelmäßig auf die von der Gruppe für den Schutz der Rechte von Personen bei der Verarbeitung personenbezogener Daten entwickelten Grundsätze Bezug genommen. Diese durch Artikel 29 der Richtlinie 95/46/EG eingesetzte Gruppe mit beratender Funktion, an deren Beschlussfassung auch Vertreter der deutschen öffentlich bestellten Datenschutzbeauftragten teilnehmen, ist unabhängig und hat u.a. den Auftrag, zum Schutzniveau in der Gemeinschaft und in Drittländern gegenüber der Kommission Stellung zu nehmen. In der Arbeitsunterlage »Übermittlungen personenbezogener Daten an Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU« (WP 12) vom 24.7. 1998 (http:// europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp12de.pdf) hat sie einen funktionalen Ansatz für die Beurteilung der Angemessenheit des Schutzniveaus in Drittländern entwickelt. Ausgangspunkt ist die Tatsache, dass Datenschutzregeln nur dann zum Schutz der Grundrechte und -freiheiten, und insbesondere der Privatsphäre, beitragen können, wenn sie in der Praxis befolgt werden. Deswegen muss jede ernsthafte Analyse des Datenschutzniveaus zwei Elemente umfassen: den Regelungsinhalt und die Durchsetzung der Regeln.

Ausgehend von einer Analyse der Risiken für die Privatsphäre des Einzelnen nach Übermittlung seiner personenbezogenen Daten in ein Drittland und unter Berücksichtigung der international anerkannten Grundsätze des Datenschutzes[1] entwickelte die Gruppe einen Kern inhaltlicher Prinzipien sowie Anforderungen an ihre effektive Durchsetzung.

Diese materiellen Grundsätze enthalten die Zweckbestimmung und -bindung, Datenqualität und -verhältnismäßigkeit, Transparenz, Sicherheit, Auskunfts-, Widerspruchs- und Berichtigungsrechte, Drittlandtransfers sowie gegebenenfalls sensitive Daten, Direktmarketing und automatisierte Entscheidungen.

Die Effektivität der Durchsetzung soll daran gemessen werden, ob erstens eine gute Befolgungsrate gewährleistet wird, ob zweitens den einzelnen betroffenen Personen Unterstützung und Hilfe zuteil wird und ob drittens eine angemessene Entschädigung bei Verstoß gegen die Bestimmungen gewährleistet wird.

Dieser funktionale Ansatzpunkt erlaubt eine Analyse des jeweiligen Schutzsystems in einem Drittland unabhängig von seiner Art und Rechtsnatur. Er ist deshalb auch grundsätzlich auf Selbstregulierungsinstrumente anwendbar. Artikel 25 Abs. 2 der Richtlinie nennt selbst »Standesregeln« als mögliches Element der Angemessenheit des Schutzniveaus in einem Drittland. Allerdings ist deren Charakteristikum, dass sie durch staatliche Maßnahmen im Drittstaat abgesichert und für eine repräsentative Anzahl von Empfängern von Daten einer Berufsgruppe oder eines Wirtschaftsbereichs verbindlich sind.

Der US-Safe Harbor erfüllt diese Voraussetzungen. Die Mitgliedstaaten unterstützten einstimmig einen entsprechenden Vorschlag einer Entscheidung der Kommission über die Angemessenheit des durch den Safe Harbor erbrachten Datenschutzes, die am 27.6.1998 angenommen wurde (http://europa.eu.int/comm/internal_market/en/dataprot/news/decision_de.pdf). Das System ist offen für alle im Inland niedergelassenen Organisationen, die ihm beitreten wollen und die Voraussetzungen erfüllen (insbesondere der Aufsicht mindestens einer staatlichen Behörde unterliegen, die Befugnisse zur Sicherstellung der Einhaltung der Regeln hat und diese effektiv einsetzt). Es basiert auf der freiwilligen Akzeptanz von Verhaltensregeln durch solche Organisationen, ohne dass sie die Regeln abändern oder für die Vergangenheit aufsagen können. Zur Sicherstellung angemessener Maßnahmen zur Durchsetzung ist zwingend vorgesehen: eine (externe oder interne) periodische Überprüfung der internen Verfahren zur Datenverarbeitung (z.B. in Form eines Audits), ein privates System der Streitschlichtung, das für den Einzelnen leicht zugänglich und kostengünstig sein muss sowie die Existenz einer staatlichen Aufsichtsbehörde, der alle ungelösten Konfliktfälle über die Einhaltung der Regeln vorgelegt werden können und die wirksame Sanktionen im Fall der Nichtbeachtung verhängt. Darüber hinaus müssen die Unternehmen Ersatz im Fall des Eintritts eines auf einer Verletzung der Regeln beruhenden Schadens gewährleisten.

Unternehmensregeln, wie sie beispielsweise von der DaimlerChrysler AG erarbeitet und den Aufsichtsbehörden in Deutschland zur Genehmigung vorgelegt worden sind, unterscheiden sich von den Safe-Harbor-Regeln in mehrfacher Hinsicht. Zunächst sind sie für eine weltweite Anwendung konzipiert und nicht in das Rechtssystem eines bestimmten Drittstaates eingebettet. Diese Besonderheit erschwert nicht nur die Zuordnung des Schutzsystems zu einem bestimmten Drittstaat, wie dies in Artikel 25 Abs. 1, 2 der Richtlinie 95/46/EG vorausgesetzt wird, sondern führt ferner zu Schwierigkeiten bei der Rückbindung der Kontrolle der Einhaltung der Regeln in ein staatliches Sanktionssystem. Außerdem führt es zu Unsicherheiten über die Verbindlich-

keit der Regeln, insbesondere wenn sie von nationalen Vorschriften in positiver oder negativer Hinsicht abweichen. Ferner stehen die Unternehmensregeln nur den selbständigen Unternehmen als Teile eines bestimmten Konzerns zur Verfügung, nicht aber den Unternehmen eines gesamten Wirtschaftsbereichs, geschweige denn allen Organisationen, die ihnen beitreten wollen. Allein aus diesen Gründen können solche Regeln nicht die »Angemessenheit« des Schutzniveaus eines Drittstaates (welchen?) begründen. Aus denselben Gründen scheint eine Einordnung der Unternehmensregeln unter den in Artikel 25 Abs. 2 der Richtlinie enthaltenen Begriff der »Standesregeln« nicht möglich.

3.2 Selbstregulierungsinstrumente als Garantien des Exporteurs?

In Artikel 26 Abs. 2 der Richtlinie ist vorgesehen, dass die zuständigen Behörden in den Mitgliedstaaten einzelne Übermittlungen in ein Drittland ohne angemessenes Schutzniveau genehmigen können, wenn der Exporteur der Daten (nota bene nicht das Drittland oder der dortige Empfänger oder Importeur der Daten) ausreichende Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten der Personen sowie hinsichtlich der Ausübung der damit verbundenen Rechte beibringt. Diese Garantien können ausdrücklich – aber nicht ausschließlich – durch entsprechende Vertragsklauseln erbracht werden. Damit sind zunächst zweiseitige Verträge angesprochen, in denen sich der Datenimporteur gegenüber dem Datenexporteur verpflichtet, auf die weitere Verarbeitung der übermittelten Daten einen bestimmten Datenschutzstandard anzuwenden und in denen Garantien im Hinblick auf die Durchsetzung der Verpflichtungen des Importeurs der Daten sowie der Rechte der betroffenen Personen enthalten sind, die den oben genannten von der Gruppe für den Schutz der Rechte von Personen bei der Verarbeitung personenbezogener Daten entwickelten Datenschutzgrundsätzen entsprechen.

Die Richtlinie schließt aber nicht aus, dass der Datenexporteur andere Arten von Garantien erbringt, soweit sie diesen Anforderungen an angemessenen Inhalt und Durchsetzung Genüge tun. In diesem Zusammenhang könnten Selbstregulierungsinstrumente eine **wesentliche und neue Rolle** spielen. Unternehmensregeln könnten als interne Regelungen von den jeweiligen nach Gesellschaftsrecht zuständigen Organen für die Organisationen im oder sogar außerhalb des Konzerns verbindlich gemacht werden. Auch wenn keine zweiseitige vertragliche Verpflichtung mit dem Importeur besteht, könnte das jeweilige exportierende Konzernunternehmen im Grundsatz mittels (ggfs. eines Bündels) dieser einseitigen, aber verbindlichen Selbstverpflichtung seitens des Empfängers der Daten Garantien erbringen, sofern diese den Erfordernissen eines angemessenen Schutzstandards genügen. Zum Nachweis dürfte die Vorlage des verbindlichen Beschlusses der zuständigen Organe der Gesellschaft, an die die Daten übermittelt werden, ausreichen.

3.2.1 Angemessenheitsprüfung der Datenschutzprinzipien

Relativ unproblematisch erscheint ebenfalls die Prüfung der Angemessenheit des Inhalts der Datenschutzprinzipien: sie sind an den allgemeinen Anforderungen an die Angemessenheit des Schutzniveaus zu messen. Die auf den Datenimporteur anwendbaren Unternehmensregeln müssen Grundsätze enthalten über die Zweckbestimmung und -bindung, Datenqualität und -verhältnismäßigkeit, Transparenz, Sicherheit, Auskunfts-, Widerspruchs- und Berichtigungsrechte, Weiterübermittlungen an Dritte sowie gegebenenfalls sensitive Daten, Direktmarketing und automatisierte Entscheidungen.

3.2.2 Durchsetzungsmechanismen

Die Effektivität der Durchsetzung muss daran gemessen werden, ob erstens eine gute Befolgungsrate gewährleistet wird, ob zweitens den einzelnen betroffenen Personen Unterstützung und Hilfe zuteil wird und ob drittens eine angemessene Entschädigung bei Verstoß gegen die Bestimmungen gewährleistet wird (siehe Arbeitsunterlage »Übermittlungen personenbezogener Daten an Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU« (WP 12) vom 24.7.1998, aaO., S. 12 ff.)

3.2.2.1 Allgemeine Befolgung

Eine allgemeine gute Befolgungsrate könnte insbesondere durch organisationelle und technische Maßnahmen in den Unternehmen, aber auch durch die regelmäßige Kontrolle der Verfahren der Datenverarbeitung im Hinblick auf die Einhaltung der Unternehmensregeln, etwa durch interne oder externe Auditierung, sichergestellt werden. Die Bestellung eines internen Konzerndatenschutzbeauftragten zur Überwachung der Einhaltung der Unternehmensregeln, insbesondere wenn er durch ein Netzwerk an Datenschutzkoordinatoren unterstützt wird und Stichproben vornehmen kann, ist ebenfalls ein entscheidender Beitrag in diesem Zusammenhang. Am wichtigsten erscheint jedoch die Art und Weise der Durchsetzung von Sanktionen im Fall der Nichteinhaltung der Unternehmensregeln. Neben der Änderung der nicht konformen Praxis kommt es auch gerade darauf an, dass eine »Strafe« ausgesprochen werden kann, die sich auf das künftige Verhalten des Unternehmens auswirkt, indem schon die bloße Möglichkeit einen Anreiz für die Einhaltung der Unternehmensregeln bietet. In diesem Zusammenhang erscheint es nicht ausreichend, Verstöße gegen die Unternehmensregeln der Geschäftsleitung des betroffenen Unternehmens sowie der Konzernleitung mit einer Stellungnahme des Konzerndatenschutzbeauftragten zu unterbreiten. Deshalb könnte im Fall eines letztlich unlösbaren Konflikts ein gewisses Maß externer Publizität sowie eine unabhängige Stelle vorgesehen werden, die ein Gericht, eine

Schiedsstelle oder die zuständige Datenschutzkontrollbehörde sein und die Sanktionen aussprechen könnte. Ohne derartige Sanktionsmöglichkeiten ist schwer zu vermitteln, wie ohne ein effektives System externer Überprüfung ein hohes Niveau allgemeiner Einhaltung der Regeln sichergestellt werden kann.

3.2.2.2 Hilfe und Unterstützung der betroffenen Person

Hilfe und Unterstützung der betroffenen Personen kann durch die Einrichtung interner und externer Stellen gewährt werden, an die sich der Einzelne wenden kann, wenn sein Anliegen einer behaupteten Verletzung der Unternehmensregeln nicht auf andere Weise gütlich beigelegt werden konnte. Im Rahmen der internen Verfahren kann die Einräumung einer Kompetenz des Konzerndatenschutzbeauftragten zur Anhörung von Beschwerden und zur Ermittlung des Sachverhalts eine wesentliche Garantie sein. Darüber hinaus sollte eine unabhängige Stelle bestehen, die im Konfliktfall den Sachverhalt untersuchen und eine verbindliche Lösung vorschlagen kann.

3.2.2.3 Schadensersatz

Eine angemessene Entschädigung müsste für den Fall gewährt werden, dass betroffenen Personen infolge eines Verstoßes gegen die Unternehmensregeln ein (finanzieller oder immaterieller) Schaden entstanden ist. Ein entsprechender Antrag kann von den Datenschutzkoordinatoren und dem Konzerndatenschutzbeauftragten behandelt werden. Wichtig ist aber auch hier, dass für die Durchsetzung im Konfliktfall die Einschaltung einer unabhängigen Stelle möglich ist, deren Entscheidungen zu respektieren das Unternehmen verbindlich anerkannt hat.

3.2.2.4 Haftung des Datenexporteurs

Während es der Datenimporteur ist, der die notwendigen Maßnahmen zur Sicherstellung der Einhaltung der Verhaltensregeln treffen oder dulden muss, kann der Datenexporteur eine gleichwertige Rolle bei der Sicherstellung der Hilfe und Unterstützung der betroffenen Person sowie der Entschädigung spielen. Der Datenexporteur könnte die Verpflichtung übernehmen, die betroffenen Personen bei der Durchsetzung ihrer Rechte gegenüber dem Datenimporteur zu unterstützen oder für die Schadensersatzleistung selbst an die Stelle des Datenimporteurs zu treten. Dies ist allerdings nur adäquat, solange der Datenexporteur als solventes Unternehmen diese Verpflichtung auch effektiv honorieren kann.

4. Wie können Unternehmensregeln anerkannt werden?

Nach Artikel 26 Abs. 2 der Richtlinie 95/46/EG bedürfen alle Übermittlungen von Daten, die auf der Grundlage von durch den Exporteur beigebrachten Garantien erfolgen sollen, der Genehmigung durch die zuständige Stelle in dem Mitgliedstaat, in dem der Datenexporteur niedergelassen ist. Eine etwaige informelle Stellungnahme der zuständigen Behörde zu den Unternehmensregeln ist natürlich möglich und für das Unternehmen im Hinblick auf die Beurteilung zukünftiger Anträge zur Genehmigung von Einzelübermittlungen von Daten hilfreich.

Jede Genehmigung durch eine nationale Stelle ist nach Artikel 26 Abs. 3 der Europäischen Kommission und den Mitgliedstaaten mitzuteilen, denen damit die Möglichkeit eröffnet werden soll, eine Stellungnahme in Bezug auf den Schutz der Grundrechte und -freiheiten und insbesondere der Privatsphäre abzugeben. Die damit ermöglichte Harmonisierung der Praxis liegt letztlich im Interesse der Mitgliedstaaten selbst. Sie erlaubt es, künstliche Verkehrsverlagerungen zu Mitgliedstaaten mit einer großzügigen Genehmigungspraxis entgegenzuwirken und damit zu verhindern, dass eine strengere Praxis in manchen Mitgliedstaaten durch Ausnutzen der innergemeinschaftlichen Datenverkehrsfreiheit weitgehend unterlaufen könnte.

Ein eventuelles Ergebnis dieser Information könnte bereits sein, dass die zuständigen Behörden in den übrigen Mitgliedstaaten, in denen konzernangehörige Unternehmen niedergelassen sind, eine einheitliche Genehmigungspraxis entwickeln. Allerdings machen die bisherigen Erfahrungen eine solche zufällige und freiwillige Harmonisierung nicht sehr wahrscheinlich.

Wahrscheinlicher ist die Möglichkeit, dass die Mitgliedstaaten und die Kommission nach Ergebnis und Begründung verschiedene Stellungnahmen abgeben und dass davon zumindest eine einen »hinreichend begründeten Widerspruch« im Sinne des Artikel 26 Abs. 3 geltend macht. Für diesen Fall ist vorgesehen, dass die Kommission die »geeigneten Maßnahmen« nach dem Verfahren des Artikel 31 Abs. 2 einleitet. Diese kann feststellen, dass für die mitgeteilte Übermittlung unter Berücksichtigung der gebotenen Garantien die Genehmigung nicht zu erteilen ist, oder – wahrscheinlicher – die Bedingungen oder zusätzlichen Garantien aufführen, die erforderlich sind, um eine rechtmäßige Genehmigung der in Frage stehenden Übermittlung erteilen zu können (Brühann, in: Grabitz/Hilf, Kommentar zum EU Vertrag II, Verbraucher- und Datenschutzrecht A 30, Art. 26, Rn. 18). Diese Entscheidung hat Wirkung für alle Mitgliedstaaten der Gemeinschaft und muss von ihnen umgesetzt werden, soweit sie nach ihrer Rechtsordnung nicht mit unmittelbarer Wirkung ausgestattet ist. Allerdings bezieht sich die Entscheidung der Kommission nur auf die mit der Genehmigung vorgelegte Einzelübermittlung. Sie bringt deshalb noch nicht die Rechtssicherheit, dass zukünftige Übermittlungen unter Zugrundelegung der der Entscheidung angepassten Unternehmensregeln durch konzernangehörige Unternehmen aus allen Mitgliedstaaten automatisch zulässig wären. Auch verfahrensmäßig wäre eine Genehmigung jeder einzel-

nen Übermittlung durch die zuständigen Behörden der Mitgliedstaaten weiterhin erforderlich. In diesem Verfahren wären die Mitgliedstaaten nicht verpflichtet, selbst bei Vorliegen der Voraussetzungen, eine Genehmigung tatsächlich zu erteilen, da die Möglichkeit der Genehmigung in Artikel 26 Abs. 2 für die Mitgliedstaaten nicht zwingend, sondern fakultativ ist (»ein Mitgliedsstaat kann…«). Insoweit bleibt der Harmonisierungseffekt dieser Entscheidung der Kommission unvollständig.

Nach Artikel 26 Abs. 4 kann allerdings die Kommission mit verbindlicher Wirkung für alle Mitgliedstaaten bestimmen, dass bestimmte »Standardvertragsklauseln« ausreichende Garantien gemäß Artikel 26 Abs. 2 bieten. Zu prüfen ist, ob Verhaltensregeln von Unternehmen als solche »Standardvertragsklauseln« angesehen werden können oder ob diese Möglichkeit es der Kommission auch erlauben würde, mit Wirkung für die gesamte Gemeinschaft andere als vertragliche Garantien, nämlich Unternehmensregeln, als angemessen anzuerkennen.

Unternehmensregeln werden in der Regel als einseitige Rechtsakte, beispielsweise durch Beschluss, der selbständigen Organisationseinheiten in dem Konzern entsprechend den für die Beschlussfassung geltenden Bestimmungen insbesondere des Gesellschaftsrechts geschaffen. Als solche sind sie nicht als »Vertragsklauseln« anzusehen, weil ihnen das Element der wechselseitigen Verpflichtung, das Synallagma, fehlt. Demgegenüber könnten die Unternehmen jedoch mehrseitige Verträge mit dem Inhalt von Unternehmensregeln schließen, in denen alle teilnehmenden Konzernunternehmen durch ihre Unterschrift gemeinsam und gegenseitig versprechen, die Unternehmensregeln einzuhalten. In diesem Fall wäre durch die Verpflichtung der Konzernunternehmen auf ein gemeinsames Ziel ein Vertragsverhältnis entstanden, das die Möglichkeit für die Kommission eröffnet, eine für die Gemeinschaft verbindliche Anerkennung des Schutzniveaus vorzunehmen. Nach dem Sinn und Zweck der Vorschrift des Artikel 26 Abs. 4 erscheint es aber auch vertretbar, den Verweis auf den Abs. 2 in einem umfassenderen Sinne auszulegen, dass nämlich alle dort genannten Garantien auch Gegenstand einer Entscheidung nach Artikel 26 Abs. 4 durch die Kommission sein können. Gründe des Datenschutzes, die dagegen sprechen könnten, sind nicht ersichtlich, der Umweg über die Konstruktion eines mehrseitigen Vertrages führt zum selben Ergebnis und es besteht ein mehrfach geäußertes Bedürfnis der Wirtschaft, durch eine einzige Entscheidung auf Ebene der Gemeinschaft die Anerkennung der Unternehmensregeln für alle in Europa niedergelassenen konzernangehörigen Unternehmen zu erwirken.

Darüber hinaus hätte erst die Entscheidung der Kommission über die Angemessenheit des Schutzniveaus der Unternehmensregeln eine wesentliche verfahrensmäßige Erleichterung zur Folge. Inhalt dieser Entscheidung könnten die Unternehmensregeln als solche sein, so dass die Notwendigkeit der Genehmigung der darauf gestützten nachfolgenden Einzelübermittlungen entfiele. Damit wäre ihre Anerkennung auch in den Mitgliedstaaten sichergestellt, die die Möglichkeit der Einzelgenehmigungen nach Artikel 26 Abs. 2

nicht vorsehen, und damit eine vollständige Harmonisierung der Praxis im Sinne einer erheblichen Verbesserung des internationalen Datenschutzes im Sinne der europäischen Bürger erreicht.

[1] Insbesondere das »Übereinkommen No. 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten« des Europarats v. 28.1.1981 sowie die »Leitlinien zum Schutz der Privatsphäre und grenzüberschreitender Fluss personenbezogener Daten« der OECD v. 23.9.1980. Darüber hinaus sei auf die Instrumente der UN und ihrer Unterorganisationen hingewiesen.