EUROPÄISCHE KOMMISSION
GENERALDIREKTION XV
BINNENMARKT UND FINANZDIENSTLEISTUNGEN
Freier Verkehr von Informationen; Gesellschaftsrecht und finanzielle Informationen
Freier Verkehr von Informationen, Datenschutz und damit zusammenhängende Internationale Aspekte

GD XV D/5025/98
WP 12

Gruppe für den Schutz der Rechte von Personen bei der Verarbeitung personenbezogener Daten

Arbeitsunterlage:

Übermittlungen personenbezogener Daten an Drittländer : Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU

Von der Arbeitsgruppe am 24. Juli 1998 angenommen

Inhaltsverzeichnis

Einführung

Ziel diese Arbeitsunterlage ist es, die bislang geleistete Arbeit der nach Artikel 29 der Datenschutzrichtlinie[1] eingesetzten Arbeitsgruppe von EU-Datenschutzbeauftragten zu einer allgemeinen Übersicht über ihre Ansichten zu sämtlichen zentralen Fragen zusammenzufassen, die sich aus der Übermittlung personenbezogener Daten in Drittländer im Zusammenhang mit der Anwendung der Datenschutzrichtlinie der EU (95/46/EG) ergeben. Der Aufbau folgt dabei dem System, wie es für internationale Übermittlungen personenbezogener Daten in Artikel 25 und 26 der Richtlinie vorgesehen ist. (Der Wortlaut dieser Artikel ist als Anhang 2 beigefügt.)

In Artikel 25 Absatz 1 ist der Grundsatz aufgeführt, daß die Mitgliedstaaten die Übermittlung in ein Drittland nur gestatten, wenn das betreffende Drittland ein angemessenes Schutzniveau gewährleistet. In Absatz 2 wird darauf verwiesen, daß „die Angemessenheit ... unter Berücksichtigung aller Umstände beurteilt" wird. Nach Absatz 6 kann die Kommission feststellen, daß bestimmte Länder ein angemessenes Schutzniveau gewährleisten. **Kapitel 1** dieses Papiers ist dieser zentralen Frage des angemessenen Schutzniveaus gewidmet. Zunächst wird erklärt, was unter „angemessen" zu verstehen ist, und danach ein Rahmen für die Frage vorgestellt, wie die Angemessenheit des Schutzes im konkreten Fall beurteilt werden kann.

In Kapitel 2 und 3 wird dieser Ansatz weiterverfolgt. **Kapitel 2** beschäftigt sich mit Übermittlungen in Länder, die das Übereinkommen Nr. 108 des Europarates ratifiziert haben, während **Kapitel 3** Fragen im Zusammenhang mit Übermittlungen behandelt, bei denen der Schutz personenbezogener Daten hauptsächlich oder vollständig über Mechanismen der freiwilligen Selbstkontrolle und nicht auf gesetzlichem Wege erfolgt.

Fehlt das angemessene Schutzniveau im Sinne von Artikel 25 Absatz 2, so ist in Artikel 26 Absatz 2 der Richtlinie die Möglichkeit von Ad-hoc-Maßnahmen vorgesehen, die insbesondere vertraglicher Art sein und zur Festlegung angemessener Garantien führen können, auf deren Basis die betreffende Übermittlung erfolgen kann. In **Kapitel 4** des vorliegenden Beitrags werden die Umstände geprüft, unter denen vertragliche Lösungen geeignet erscheinen, und Empfehlungen zur möglichen Form und zum Inhalt dieser Lösungen gegeben.

Kapitel 5 beschäftigt sich mit der dritten und letzten Situation, die in der Richtlinie vorgesehen ist, d. h. bestimmten Fällen nach Artikel 26 Absatz 1, in denen vom Erfordernis des „angemessenen Schutzniveaus" praktisch abgewichen werden kann. Der

---

[1] Siehe **WP 4 (5020/97)** „Erste Leitlinien für die Übermittlung personenbezogener Daten in Drittländer -Mögliche Ansätze für eine Bewertung der Angemessenheit", von der Arbeitsgruppe am 26. Juni 1997 angenommene Diskussionsgrundlage;

WP 7 (5057/97) Arbeitsunterlage: „Beurteilung der Selbstkontrolle der Wirtschaft: Wann ist sie ein sinnvoller Beitrag zum Niveau des Datenschutzes in einem Drittland?", von der Arbeitsgruppe am 14. Januar 1998 angenommen;

WP 9 (5005/98) Arbeitsunterlage: „Erste Überlegungen zur Verwendung vertraglicher Bestimmungen im Rahmen der Übermittlungen personenbezogener Daten an Drittländer", von der Arbeitsgruppe am 22. April 1998 angenommen.

genaue Umfang dieser Ausnahmen wird unter Zuhilfenahme von Beispielen von Fällen geprüft, in denen diese Möglichkeit genutzt werden kann bzw. dies nicht möglich erscheint.

Im abschließenden **Kapitel 6** finden sich Bemerkungen zu Verfahrensfragen, die sich in Verbindung mit der Beurteilung der Angemessenheit (bzw. des Mangels an Angemessenheit) des Schutzniveaus und der Erzielung eines gemeinschaftsweit einheitlichen Ansatzes zu diesen Fragen ergeben.

Als Anhang 1 sind mehrere anschauliche Fallstudien beigefügt, mit denen demonstriert werden soll, wie der im vorliegenden Dokument beschriebene Ansatz in der Praxis umgesetzt werden könnte.

KAPITEL 1: BEWERTUNG DER ANGEMESSENHEIT DES SCHUTZES

(1) Was ist ein „angemessenes Schutzniveau“?

Sinn und Zweck des Datenschutzes ist es, Personen, deren Daten verarbeitet werden, Schutz zu gewährleisten. Erreicht wird dies durch eine Kombination von dem Betroffenen eingeräumten Rechten und bestimmten Pflichten für die Stellen, bei denen die Daten verarbeitet werden oder in deren Zuständigkeit die Verarbeitung der Daten fällt. Die in der Richtlinie 95/46/EG verankerten Pflichten und Rechte orientieren sich an den Festlegungen des Übereinkommens Nr. 108 des Europarates, die sich wiederum kaum von den diesbezüglichen Leitlinien der OECD (1980) oder der UNO (1990) unterscheiden. Dementsprechend kann davon ausgegangen werden, daß zum Inhalt von Datenschutzvorschriften weitgehend Einigkeit besteht, die weit über die fünfzehn Mitgliedstaaten der Gemeinschaft hinausgeht.

Mit Datenschutzvorschriften werden die Rechte des Einzelnen aber nur dann geschützt, wenn sie auch in die Praxis umgesetzt werden. Daher ist nicht nur der Inhalt der für die Übermittlung personenbezogener Daten in Drittländer geltenden Vorschriften, sondern auch das System zu betrachten, mit dem die Durchsetzung der Regeln gesichert werden soll. In Europa ist es bislang so, daß die Datenschutzvorschriften gesetzlich festgeschrieben werden und bei Nichteinhaltung Strafen auferlegt werden können bzw. dem einzelnen das Recht auf Wiedergutmachung eingeräumt wird. Darüber hinaus sind in derartigen Gesetzen zusätzliche verfahrensrechtliche Mechanismen wie die Einrichtung von Kontrollstellen vorgesehen, denen Überwachungsaufgaben und die Verfolgung von Beschwerden obliegen. Die Verfahrensaspekte spiegeln sich auch in der Richtlinie 95/46/EG wider, die Bestimmungen über Haftung, Sanktionen, Rechtsbehelfe, Kontrollstellen und Meldung bei der Kontrollstelle enthält. Außerhalb der Gemeinschaft sind derartige verfahrensrechtliche Mittel zur Sicherung der Einhaltung der Datenschutzvorschriften weniger üblich. Die Parteien des Übereinkommens Nr. 108 sind zur gesetzlichen Verankerung der Grundsätze des Datenschutzes verpflichtet, doch sind zusätzliche Mechanismen wie eine Kontrollstelle nicht vorgesehen. In den OECD-Leitlinien wird lediglich „ihre Berücksichtigung“ in der Landesgesetzgebung angemahnt, und es fehlen verfahrensrechtliche Mittel, mit denen gesichert würde, daß die Leitlinien tatsächlich zu einem wirksamen Schutz des Einzelnen führen. In den später verabschiedeten Leitlinien der UNO sind andererseits Bestimmungen über Kontrolle und Sanktionen enthalten, was zeigt, daß sich weltweit die Erkenntnis durchsetzt, daß auf die ordnungsgemäße Umsetzung von Datenschutzvorschriften nicht verzichtet werden kann.

Vor diesem Hintergrund wird deutlich, daß die Analyse des angemessenen Schutzniveaus ohne die Einbeziehung der beiden folgenden Grundelemente sinnlos ist: Inhalt der geltenden Vorschriften und Mittel zur Sicherung ihrer wirksamen Anwendung.

Geht man von der Richtlinie 95/46/EG aus und berücksichtigt dabei die Bestimmungen weiterer internationaler Dokumente zum Datenschutz, so sollte es möglich sein, für den Datenschutz einen „Kern“ von „inhaltlichen“ Grundsätzen und „verfahrensrechtlichen“ bzw. mit der „Durchsetzung im Zusammenhang stehenden“ Erfordernissen herauszuarbeiten, deren Einhaltung als Mindestanforderung an eine Situation gilt, in der von einem angemessenen Schutzniveau gesprochen werden kann. Dabei sollte nicht starr auf bestimmte Mindestanforderungen gepocht werden, denn während die Liste in einem Fall erweitert werden muß, reicht im anderen möglicherweise ein vermindertes

Anforderungsspektrum. Bei der Bestimmung der genauen Anforderungen an einen konkreten Fall ist das Ausmaß der Gefahren, die für den Betroffenen der Datenübermittlung entstehen, ein wichtiger Faktor. Doch ungeachtet dieser Einschränkungen ist eine grundlegende Aufstellung von Mindestanforderungen in jedem Fall ein nützlicher Ausgangspunkt für eine Analyse.

(i) Inhaltliche Grundsätze

Die folgenden Grundsätze sind unbedingt zu berücksichtigen:

1) **Der Grundsatz der Beschränkung der Zweckbestimmung -** Daten sind für einen spezifischen Zweck zu verarbeiten und dementsprechend nur insofern zu verwenden oder weiter zu übermitteln, als dies mit der Zweckbestimmung der Übermittlung nicht unvereinbar ist. Die einzigen Ausnahmen von dieser Regel sind die in einer demokratischen Gesellschaft aus einem der in Artikel 13 der Richtlinie aufgeführten Gründe notwendigen Fälle. [2]

2) **Der Grundsatz der Datenqualität und -verhältnismäßigkeit** - Daten müssen sachlich richtig und, wenn nötig, auf dem neuesten Stand sein. Die Daten sollten angemessen, relevant und im Hinblick auf die Zweckbestimmung, für die sie übertragen oder weiterverarbeitet werden, nicht exzessiv seien.

3) **Der Grundsatz der Transparenz** - Natürliche Personen müssen Informationen über die Zweckbestimmung der Verarbeitung und die Identität des im Drittland des für die Verarbeitung Verantwortlichen sowie andere Informationen erhalten, sofern dies aus Billigkeitsgründen erforderlich ist. Ausnahmen sind lediglich im Einklang mit den Artikeln 11 Absatz 2[3] und 13 der Richtlinie möglich.

4) **Der Grundsatz der Sicherheit** - Der für die Verarbeitung Verantwortliche hat geeignete technische und organisatorische Sicherheitsmaßnahmen für die Risiken der Verarbeitung zu treffen. Alle unter der Verantwortung des für die Verarbeitung Verantwortlichen tätigen Personen, darunter auch Verarbeiter, dürfen Daten nur auf Anweisung des für die Verarbeitung Verantwortlichen verarbeiten.

5) **Das Recht auf Zugriff, Berichtigung und Widerspruch** - Die betroffene Person muß das Recht haben, eine Kopie aller sie betreffender Daten zu erhalten, die verarbeitet werden, sowie das Recht auf Berichtigung dieser Daten, wenn diese sich als unrichtig erweisen. In bestimmten Situationen muß sie auch Widerspruch gegen die Verarbeitung

---

[2] Artikel 13 gestattet eine Einschränkung auf den „Grundsatz der Zweckbestimmung", sofern eine solche Beschränkung für die Sicherheit des Staates, die Landesverteidigung, die öffentliche Sicherheit, die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen, ein wichtiges wirtschaftliches oder finanzielles Interesse oder den Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen notwendig ist.

[3] Artikel 11 Absatz 2 sieht vor, daß für den Fall, daß die Daten nicht bei der betroffenen Person erhoben wurden, die betroffene Person nicht informiert zu werden braucht, wenn dies unmöglich ist, unverhältnismäßigen Aufwand erfordert oder die Speicherung oder Weitergabe durch Gesetz ausdrücklich vorgesehen ist.

der sie betreffenden Daten einlegen können. Die einzigen Ausnahmen von diesen Rechten haben mit Artikel 13 der Richtlinie im Einklang zu stehen.

6) **Beschränkungen der Weiterübermittlung in andere Drittländer** - Weitere Übermittlungen personenbezogener Daten vom ursprünglichen Bestimmungsdrittland in ein anderes Drittland sind lediglich zulässig, wenn das zweite Drittland (d. h. der Empfänger der Weiterübermittlung) ebenfalls ein angemessenes Schutzniveau aufweist. Die einzigen zulässigen Ausnahmen haben mit Artikel 26 Absatz 1 der Richtlinie im Einklang zu stehen. (Diese Ausnahmen werden in Kapitel 5 untersucht.)

Beispiele weiterer, auf spezifische Arten der Verarbeitung anwendbarer Grundsätze:

1) **Sensible Daten -** Sind „sensible" Kategorien von Daten betroffen (die in Artikel 8 der Richtlinie[4] aufgelistet sind), so haben zusätzliche Sicherheitsmaßnahmen wie das Erfordernis zu gelten, daß die betroffene Person ausdrücklich in die Verarbeitung einwilligt.

2) **Direktmarketing** - Werden Daten zum Zwecke des Direktmarketings übermittelt, so muß die betroffene Person die Möglichkeit haben, sich jederzeit gegen die Verwendung ihrer Daten für derartige Zwecke zu entscheiden.

3) **Automatisierte Einzelentscheidung** - Erfolgt die Übermittlung mit dem Ziel, eine automatisierte Einzelentscheidung im Sinne von Artikel 15 der Richtlinie zu treffen, so muß die natürliche Person das Recht haben, die dieser Entscheidung zugrunde liegende Logik zu erfahren, und andere Maßnahmen müssen getroffen werden, um die berechtigten Interessen der Person zu schützen.

(ii) Verfahrensrechtlicher Mechanismus/ Durchsetzungsmechanismus

In Europa besteht weitgehend Einigkeit darüber, daß die Datenschutzgrundsätze gesetzlich verankert werden müssen. Im wesentlichen bestehen auch keine Zweifel über die Notwendigkeit der „externen Kontrolle" in Form einer unabhängigen Stelle, die Teil eines Systems zur Einhaltung des Datenschutzes ist. In anderen Teilen der Welt hingegen ist dies nicht immer der Fall.
Als Grundlage für die Beurteilung der Angemessenheit des vorhandenen Datenschutzniveaus sind zunächst die Ziele des zugrunde liegenden verfahrensrechtlichen Systems für den Datenschutz zu bestimmen; darauf aufbauend ist das Spektrum der verschiedenen in Drittländern bestehenden gerichtlichen und außergerichtlichen verfahrensrechtlichen Mechanismen zu bewerten.

Ein Datenschutzsystem verfolgt im wesentlichen drei Ziele:

1) Gewährleistung einer **guten Befolgungsrate** der Vorschriften. (Kein System kann eine 100%ige Einhaltung garantieren, aber einige sind besser als andere). Ein gutes System

[4] Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie Daten über Gesundheit oder Sexualleben und Daten, die Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßregeln betreffen.

zeichnet sich im allgemeinen dadurch aus, daß sich die für die Verarbeitung Verantwortlichen ihrer Pflichten und die betroffenen Personen ihrer Rechte und der Mittel für deren Wahrnehmung sehr stark bewußt sind. Die Existenz wirksamer, abschreckender Sanktionen ist wichtig, um die Einhaltung der Bestimmungen sicherzustellen; ebenso relevant sind natürlich auch Systeme der direkten Überprüfung durch Behörden, Buchprüfer oder unabhängige Datenschutzbeauftragte.

2) **Unterstützung und Hilfe für einzelne betroffene Personen** bei der Wahrnehmung ihrer Rechte. Der Einzelne muß seine Rechte rasch und wirksam, ohne überhöhte Kosten durchsetzen können. Dafür muß es eine Art institutionellen Mechanismus geben, der eine unabhängige Prüfung von Beschwerden ermöglicht.

3) **Gewährleistung angemessener Entschädigung** für die geschädigte Partei bei Verstoß gegen die Bestimmungen. Für dieses Schlüsselelement muß ein System unabhängiger Schlichtung vorhanden sein, das die Zahlung von Entschädigungen oder auch die Auferlegung von Sanktionen ermöglicht.

KAPITEL 2: ANWENDUNG DES ANSATZES AUF LÄNDER, DIE DAS ÜBEREINKOMMEN NR. 108 DES EUROPARATES RATIFIZIERT HABEN

Das Übereinkommen Nr. 108 ist neben der Richtlinie das einzige internationale Instrument, das auf dem Gebiet des Datenschutzes bindend ist. Die Mehrzahl der Parteien des Übereinkommens sind auch Mitgliedstaaten der Europäischen Union (die Ratifizierung ist inzwischen durch alle 15 Staaten erfolgt) bzw. Länder wie Norwegen und Island, für die die Richtlinie aufgrund des Abkommens über den Europäischen Wirtschaftsraum ohnehin gilt. Doch auch von Slowenien, Ungarn und der Schweiz ist das Übereinkommen ratifiziert worden, und insbesondere angesichts der Tatsache, daß das Übereinkommen auch Ländern offensteht, die dem Europarat nicht angehören, dürften weitere Drittländer in der Zukunft folgen. Aus diesem Grund ist die Prüfung, ob die Länder, die das Übereinkommen ratifiziert haben, ein angemessenes Schutzniveau im Sinne von Artikel 25 der Richtlinie bieten, nicht nur von rein akademischem Interesse.

Als Ausgangspunkt ist es zunächst günstig, den Wortlaut des Übereinkommens unter dem Aspekt der theoretischen Annahme eines „angemessenen Schutzniveaus", wie es in Kapitel 1 dieses Dokuments beschrieben ist, zu beleuchten.

Was den Inhalt der Grundprinzipien betrifft, so enthält das Übereinkommen praktisch die ersten fünf der sechs „Mindestanforderungen".[5] Auch das Erfordernis geeigneter Sicherungsmaßnahmen für sensible Daten ist vorgesehen, die als Angemessenheitskriterium für Fälle, in denen derartige Daten vorkommen, angesehen werden können.

Ein Mangel des Inhalts der wesentlichen Vorschriften des Übereinkommens besteht darin, daß für die Übermittlung an Länder, die nicht Vertragsparteien des Übereinkommens sind, Beschränkungen nicht vorgesehen sind. Dies birgt die Gefahr, daß ein dem Übereinkommen Nr. 108 beigetretenes Land bei der Übermittlung von Daten aus der Gemeinschaft in ein weiteres Drittland mit völlig unangemessenem Schutzniveau als „Zwischenstation" benutzt wird.

Der zweite Aspekt des „angemessenen Schutzniveaus" betrifft die bestehenden verfahrensrechtlichen Mechanismen, mit denen den Grundprinzipien Geltung verschafft werden soll. Dem Übereinkommen zufolge sind ihre Grundsätze in das innerstaatliche Recht aufzunehmen und geeignete Sanktionen und Rechtsmittel für den Fall der Verletzung festzulegen. Dies müßte für die Gewährleistung eines angemessenen Niveaus der Einhaltung der Vorschriften und der angemessenen Entschädigung für die betroffenen Personen im Falle der Nichteinhaltung der Vorschriften ausreichen (Ziel 1) und 3) eines Systems zur Einhaltung des Datenschutzes). Allerdings verpflichtet das Übereinkommen die Vertragsparteien nicht, institutionelle Mechanismen zur unabhängigen Untersuchung von Beschwerden festzulegen, obwohl die Länder, von denen die Ratifizierung vorgenommen wurde, dies in der Regel getan haben. Dies ist ein Nachteil, da

[5] Hinsichtlich des Grundsatzes der Transparenz mögen gewisse Zweifel bestehen. Artikel 8 Absatz a) des Übereinkommens kann mit der *aktiven* Pflicht zur Bereitstellung von Informationen, die den Kern von Artikel 10 und 11 der Richtlinie darstellt, kaum gleichgesetzt werden. Im übrigen sind im Übereinkommen keine konkreten Rechte zur Verwehrung der Verwendung der Daten vorgesehen, wenn diese für Zwecke des Direktmarketings eingesetzt werden sollen. Es fehlen auch Bestimmungen für automatisierte Einzelentscheidungen (Profilerstellung).

angemessene Unterstützung und Hilfe für die einzelnen betroffenen Personen bei der Wahrnehmung ihrer Rechte (Ziel 2)) ohne diese institutionellen Mechanismen möglicherweise nicht garantiert sind.

Diese kurze Analyse läßt den Schluß zu, daß von den meisten Übermittlungen personenbezogener Daten in Länder, von denen das Übereinkommen Nr. 108 ratifiziert worden ist, angenommen werden kann, daß sie gemäß Artikel 25(1) der Richtlinie unter der Bedingung statthaft sind, daß

- das betreffende Land über geeignete Mechanismen für die Gewährleistung der Einhaltung der Vorschriften, die Unterstützung betroffener Personen und die Möglichkeit einer Entschädigung (beispielsweise eine unabhängige Kontrollstelle mit entsprechenden Befugnissen) verfügt und
- das betreffende Land das Endbestimmungsland der Übermittlung und keine Zwischenstation ist, über die die Daten geleitet werden, es sei denn, es handelt sich um die Weiterübermittlung zurück in die EU oder einen anderen Bestimmungsort mit angemessenem Schutzniveau. [6]

Dies ist natürlich eine recht vereinfachte und oberflächliche Prüfung des Übereinkommens. Im Zusammenhang mit konkreten Fällen der Übermittlung von Daten in Länder, die dem Übereinkommen beigetreten sind, dürften neue, an dieser Stelle nicht in Betracht gezogene Probleme auftreten.

[6] Das Übereinkommen Nr. 108 wird derzeit einer Prüfung unterzogen, in deren Verlauf es zu Änderungen kommen kann, mit denen diese und weitere Schwierigkeiten angesprochen werden.

KAPITEL 3: ANWENDUNG DES ANSATZES AUF DIE SELBSTKONTROLLE DER WIRTSCHAFT

Einführung

Entsprechend Artikel 25 Absatz 2 der Datenschutzrichtlinie (95/46/EG) ist die Angemessenheit des Schutzniveaus, das ein Drittland bietet, unter Berücksichtigung *aller Umstände* zu beurteilen, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen. Nicht nur auf Rechtsvorschriften, sondern insbesondere auf „die dort geltenden Standesregeln und Sicherheitsmaßnahmen" wird Bezug genommen.

Im Text der Richtlinie ist daher festgelegt, daß in dem betreffenden Drittland möglicherweise geltende außergerichtliche Vorschriften berücksichtigt werden, sofern diese Regeln auch *eingehalten werden*. In diesem Zusammenhang ist auch die Rolle zu betrachten, die die Selbstkontrolle spielt.

Was ist Selbstkontrolle?

Der Begriff „Selbstkontrolle" mag nicht für jeden dieselbe Bedeutung haben. Im Sinne dieser Unterlage beinhaltet ein Selbstkontrollkodex (oder jedes andere Instrument) alle Datenschutzbestimmungen, die auf eine Vielzahl von für die Verarbeitung Verantwortlichen in einer Berufsgruppe oder einem Wirtschaftsbereich Anwendung finden und deren Inhalt ursprünglich von Angehörigen des betreffenden Wirtschaftszweiges oder der betreffenden Berufsgruppe festgelegt wurde.

Diese weit gefaßte Definition würde sowohl einen freiwilligen Datenschutzkodex am einen Ende der Skala einschließen, der von einem kleinen Wirtschaftsverband mit nur wenigen Mitgliedern entwickelt wurde, als auch den detaillierten Kodex von Standesregeln am anderen Ende, die für ganze Berufsgruppen wie Ärzte und Bankiers gelten und oft quasigerichtliche Kraft haben.

Ist das für den Kodex verantwortliche Gremium repräsentativ für den Sektor?

Wie aus diesem Kapitel hervorgeht, ist ein wichtiges Kriterium für die Beurteilung des Wertes eines Kodexes das Ausmaß, in dem seine Regeln durchgesetzt werden können. In diesem Zusammenhang ist die Frage, ob der für den Kodex zuständige Verband oder das zuständige Gremium alle Wirtschaftsteilnehmer in einem Sektor repräsentiert oder nur einen kleinen Prozentsatz von ihnen, wahrscheinlich von geringerer Bedeutung als die Stärke des Verbands im Hinblick auf seine Fähigkeit, beispielsweise seinen Mitgliedern wegen Nichterfüllung des Kodexes Sanktionen aufzuerlegen. Daneben gibt es allerdings einige Gründe, die branchen- oder berufsweite Kodizes mit klar abgegrenztem Geltungsbereich zu sehr viel nützlicheren Schutzinstrumenten machen als die, die von kleinen Unternehmensgruppierungen innerhalb von Wirtschaftssektoren entwickelt werden. Zunächst ist es eine Tatsache, daß aus der Sicht des Verbrauchers eine aufgespaltene und durch einige rivalisierende Verbände - mit jeweils eigenem Datenschutzkodex - gekennzeichnete Wirtschaft verwirrend ist. Das Nebeneinanderbestehen unterschiedlicher Kodizes schafft ein allgemeines Bild, dem es für die betroffene Person an Transparenz fehlt. Außerdem können sich insbesondere in Bereichen wie dem Direktmarketing, in denen regelmäßig personenbezogene Daten zwischen verschiedenen Unternehmen desselben Sektors ausgetauscht werden,

Situationen ergeben, in denen das Unternehmen, das die personenbezogenen Daten weitergibt, nicht demselben Datenschutzkodex unterliegt wie das Unternehmen, das die Daten erhält. Dies führt hinsichtlich der anwendbaren Regeln zu einem beträchtlichen Maß an Unsicherheit und dürfte auch die Untersuchung und Bearbeitung von Beschwerden einzelner betroffener Personen außerordentlich erschweren.

Beurteilung der Selbstkontrolle - der Ansatz

Angesichts der Vielfalt der Instrumente, die unter den Begriff der Selbstkontrolle fallen, ist klar, daß zwischen den verschiedenen Formen der Selbstkontrolle je nach ihrer tatsächlichen Auswirkung auf das Niveau des Datenschutzes bei der Übermittlung personenbezogener Daten in ein Drittland zu differenzieren ist.

Grundlage für die Bewertung bestehender Datenschutzregeln muß (unabhängig davon, ob sie aufgrund von freiwilliger Selbstkontrolle oder von Vorschriften bestehen) der in Kapitel 1 vorgestellte generelle Ansatz sein. Ein Eckpunkt dieses Ansatzes ist die Prüfung nicht nur des Inhalts des Instruments (es sollte eine Reihe wesentlicher Grundsätze enthalten), sondern auch seine Effizienz im Hinblick auf:

- eine hohe allgemeine Befolgungsrate,
- Unterstützung und Hilfe für die einzelne betroffene Person,
- und, als entscheidenden Faktor, eine angemessene Entschädigung (einschließlich ggf. Schadensersatz).

Beurteilung des Inhalts eines Instruments der Selbstkontrolle

Dies ist eine relativ leichte Aufgabe. Es geht darum, sicherzustellen, daß die erforderlichen, in Kapitel 1 dargelegten inhaltlichen Grundsätze erfüllt sind. Das ist eine objektive Beurteilung. Die Frage ist, was der Kodex enthält, und nicht, wie er erstellt wurde. Die Tatsache, daß ein Wirtschaftszweig oder eine Berufsgruppe selbst die wichtigste Rolle bei der Ausarbeitung des Inhalts des Kodexes gespielt haben, ist an sich nicht relevant, obwohl es natürlich wahrscheinlicher ist, daß der Kodex die erforderlichen wesentlichen Grundsätze des Datenschutzes genauer wiedergibt, wenn die Meinungen der betroffenen Personen und der Verbraucherorganisationen bei seiner Ausarbeitung berücksichtigt wurden.
Die Transparenz des Kodexes ist ein Schlüsselelement; insbesondere sollte der Kodex in allgemein verständlicher Sprache abgefaßt sein und konkrete Beispiele enthalten, die seine Bestimmungen veranschaulichen. Darüber hinaus sollte der Kodex die Offenlegung von Daten nicht angeschlossener Unternehmen verbieten, die nicht unter den Kodex fallen, wenn keine anderen angemessenen Schutzmaßnahmen vorgesehen sind.

Beurteilung der Effizienz eines Instruments der Selbstkontrolle

Die Bewertung der Effizienz eines bestimmten Selbstkontrollkodexes oder -instruments ist ein schwierigeres Unterfangen, das die Kenntnis der Mittel und Wege voraussetzt, durch die sichergestellt wird, daß man sich dem Kodex verpflichtet, und mit denen Probleme der Nichtbefolgung behandelt werden. Alle drei funktionellen Kriterien für die Beurteilung der Effizienz des Schutzes müssen erfüllt sein, wenn ein Selbstkontrollkodex bei der Bewertung der Angemessenheit des Schutzes berücksichtigt werden soll.

Gute Befolgungsrate

Ein Wirtschafts- oder Standeskodex wird normalerweise von einem repräsentativen Gremium des betreffenden Wirtschaftszweigs oder der betreffenden Berufsgruppe erstellt und gilt dann für die Mitglieder dieses speziellen repräsentativen Gremiums. Das Niveau der Einhaltung des Kodexes wird wahrscheinlich von der Bekanntheit seiner Existenz und seines Inhaltes unter den Mitgliedern, den zur Sicherstellung der Transparenz des Kodexes für die Verbraucher ergriffenen Schritten, mit denen ermöglicht werden soll, daß die Marktkräfte einen wirksamen Beitrag leisten, der Existenz eines Systems der externen Überprüfung (wie dem Erfordernis einer Überprüfung der Einhaltung in regelmäßigen Abständen) und, was vielleicht am wichtigsten ist, der Art und Durchsetzung von Sanktionen im Fall der Nichtbefolgung abhängen.

Wichtige Fragen sind deshalb:

- Welche Bemühungen des repräsentativen Gremiums sind erforderlich, um sicherzustellen, daß seine Mitglieder den Kodex kennen?
- Fordert das repräsentative Gremium von seinen Mitgliedern Nachweise darüber, daß sie die Bestimmungen des Kodexes umgesetzt haben? Wie oft?
- Ist ein solcher Nachweis von den angeschlossenen Unternehmen selbst vorgesehen oder kommt er von außen (z. B. von einem zugelassenen Wirtschaftsprüfer)?
- Untersucht das repräsentative Gremium mutmaßliche oder vermutete Verstöße gegen den Kodex?
- Ist die Einhaltung des Kodexes eine Voraussetzung für die Mitgliedschaft des repräsentativen Gremiums oder ist sie rein „freiwillig"?
- Welche Formen disziplinarischer Maßnahmen stehen dem repräsentativen Gremium zur Verfügung (Ausschluß u.ä.), wenn ein Mitglied nachweislich gegen den Kodex verstoßen hat?
- Besteht für eine Person oder ein Unternehmen in der betreffenden Berufsgruppe oder dem betreffenden Wirtschaftszweig auch nach Ausschluß aus dem repräsentativen Gremium die Möglichkeit zur Weiterarbeit?
- Ist die Einhaltung des Kodexes mit anderen Mitteln durchsetzbar, beispielsweise auf gerichtlichem Wege oder durch eine spezielle Stelle? Standesrechtliche Kodizes haben in einigen Ländern Gesetzeskraft. Unter bestimmten Umständen könnte es möglich sein, die Durchsetzung von Branchenkodizes über allgemeine Gesetze zu lauteren Handelspraktiken oder auch zum Wettbewerb zu bewirken.

Bei der Prüfung der vorhandenen Sanktionsarten ist es wichtig, zwischen der „die Situation abstellenden" Sanktion, die im Fall der Nichterfüllung von einem für die Verarbeitung Verantwortlichen lediglich fordert, seine Praktiken dahingehend zu ändern, daß sie dem Kodex entsprechen, und einer Sanktion, die weitergeht und den für die Verarbeitung Verantwortlichen für die Nichterfüllung tatsächlich bestraft, zu unterscheiden. Nur diese zweite Kategorie der „Strafsanktion" wirkt sich tatsächlich auf das künftige Verhalten der für die Verarbeitung Verantwortlichen aus, indem sie einen gewissen Anreiz für die Erfüllung des Kodex bietet.

Fehlen in einem Kodex tatsächlich abschreckende Strafmaßnahmen, so ist dies ein gravierender Nachteil. Ohne derartige Sanktionen ist schwer zu sehen, wie ohne ein striktes System externer Überprüfung (beispielsweise eine öffentliche oder private Stelle,

die für die Intervention im Fall der Nichteinhaltung des Kodexes zuständig ist, oder eine zwingende Vorschrift für eine regelmäßige externe Prüfung) ein hohes Niveau allgemeiner Erfüllung erreicht werden kann,.

Unterstützung und Hilfe für einzelne betroffene Personen

Von einem angemessenen und wirksamen Datenschutzsystem ist zu fordern, daß der Einzelne bei einem Problem im Zusammenhang mit den eigenen personenbezogenen Daten nicht allein gelassen wird, sondern institutionelle Hilfe erhält, um die Schwierigkeiten zu beheben. Diese institutionelle Unterstützung sollte idealerweise neutral, unabhängig und mit den erforderlichen Befugnissen für die Prüfung jeder Beschwerde einer betroffenen Person ausgestattet sein. Im Hinblick auf die Selbstkontrolle ergeben sich in diesem Zusammenhang folgende Fragen:

- Existiert ein System, das die Prüfung von Beschwerden einzelner betroffener Personen ermöglicht?
- Wie erhalten betroffene Personen Kenntnis von diesem System und den Entscheidungen im Einzelfall?
- Entstehen der betroffenen Person Kosten irgendwelcher Art?
- Wer führt die Prüfung durch? Sind die Prüfer mit den erforderlichen Befugnissen ausgestattet?
- Wer entscheidet über eine mutmaßliche Verletzung des Kodexes? Sind diese Personen unabhängig und neutral?

Die Neutralität des Schiedsmanns oder Schiedsrichters bei mutmaßlichen Verletzungen des Kodexes ist ein Schlüsselelement. Eine solche Person oder ein solches Gremium darf zum Verantwortlichen der Verarbeitung in keinem Abhängigkeitsverhältnis stehen. Allerdings reicht dies allein noch nicht aus, um die Neutralität zu gewährleisten. Im Idealfall sollte der Schiedsrichter nicht der betroffenen Berufsgruppe oder dem betroffenen Wirtschaftszweig angehören, weil zwischen dem Verantwortlichen der Verarbeitung, der gegen den Kodex verstoßen haben soll, und den der gleichen Berufsgruppe oder dem gleichen Wirtschaftszweig angehörenden Mitgliedern eindeutig eine Interessengemeinschaft besteht. Die Neutralität des Schiedsgremiums könnte durch die Einbeziehung von Vertretern der Verbraucher neben den Vertretern der Wirtschaft (in gleicher Zahl) gewährleistet werden.

Angemessene Entschädigung

Wenn nachweislich gegen den Selbstkontrollkodex verstoßen wurde, sollten der betroffenen Person Rechtsmittel offenstehen, mit deren Hilfe das Problem behoben werden muß (Berichtigung oder Löschen aller fehlerhaften Daten; Gewährleistung, daß die Verarbeitung für unvereinbare Zweckbestimmungen eingestellt wird); wenn der betroffenen Person Schaden entstanden ist, muß die Zahlung einer angemessenen Entschädigung vorgesehen sein. Dabei ist zu berücksichtigen, daß „Schaden" im Sinne der Datenschutzrichtlinie nicht nur materiellen Schaden und finanziellen Verlust einschließt, sondern darunter auch jeglicher psychischer und moralischer Schaden fällt (im Recht des Vereinigten Königreichs und der USA als „distress" bezeichnet).

Viele der Fragen im Hinblick auf die oben im Abschnitt „Gute Befolgungsrate" aufgelisteten Sanktionen sind hier von Bedeutung. Wie bereits dargelegt wurde, haben

Sanktionen eine doppelte Funktion: den Täter zu bestrafen (und somit die Einhaltung der Regeln durch den Täter und andere zu fördern) und einen Verstoß gegen die Bestimmungen abzustellen. Hier geht es hauptsächlich um die zweite Funktion. Zusätzliche Fragen wären deshalb:

- Läßt sich überprüfen, ob ein Mitglied, das nachweislich gegen den Kodex verstoßen hat, seine Praktiken geändert und das Problem beseitigt hat?
- Können Personen nach dem Kodex einen Entschädigung erhalten, und wie?
- Ist der Verstoß gegen den Kodex einem Vertragsverstoß gleichzusetzen oder auf dem Wege des öffentlichen Rechts geltend zu machen (beispielsweise Verbraucherschutz, unlauterer Wettbewerb), und kann das zuständige Gericht auf dieser Grundlage zur Leistung von Schadenersatz verurteilen?

Schlußfolgerungen

- Selbstkontrolle sollte unter Verwendung des objektiven, funktionellen Ansatzes beurteilt werden, der in Kapitel 1 dargelegt wurde.

- Ein Instrument der Selbstkontrolle, das als wirksamer Bestandteil eines „angemessenen Schutzes" anzusehen ist, muß für alle Mitglieder bindend sein, an die personenbezogene Daten übermittelt werden, und angemessene Sicherungsmaßnahmen vorsehen, wenn die Daten an Nichtmitglieder weitergeleitet werden.

- Das Instrument muß transparent sein und den grundlegenden Inhalt aller maßgeblichen Datenschutzgrundsätze enthalten.

- Das Instrument muß über Mechanismen verfügen, die ein gutes allgemeines Befolgungsniveau wirksam gewährleisten. Ein System abschreckender Strafmaßnahmen ist eine Möglichkeit, dies zu erreichen. Zwingende externe Prüfungen sind ein weiteres Mittel.

- Das Instrument muß Unterstützung und Hilfe für einzelne betroffene Personen bieten, die ein Problem im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten haben. Ein leicht zugängliches, neutrales und unabhängiges Gremium zur Anhörung von Beschwerden betroffener Personen und zur Schlichtung bei Verstößen gegen den Kodex muß deshalb eingerichtet werden.

- Das Instrument muß für den Fall der Verletzung von Vorschriften eine angemessene Entschädigung gewährleisten. Die betroffene Person muß die Möglichkeit haben, das Problem zu beseitigen und ggf. Schadensersatz zu erhalten.

KAPITEL 4 : DIE ROLLE DER VERTRAGLICHEN BESTIMMUNGEN

1. Einführung

Nach Artikel 25 Absatz 1 der Datenschutzrichtlinie (95/46/EG) gilt der Grundsatz, daß die Übermittlung personenbezogener Daten lediglich erfolgen darf, wenn das Drittland ein angemessenes Schutzniveau gewährleistet. In diesem Kapitel soll die Möglichkeit einer Ausnahme von dem Grundsatz des angemessenen Schutzniveaus nach Artikel 25 geprüft werden, die aufgrund von Artikel 26 Absatz 2 möglich ist. Diese Bestimmung erlaubt einem Mitgliedstaat eine Übermittlung oder eine Kategorie von Übermittlungen personenbezogener Daten in ein Drittland ohne angemessenes Schutzniveau, „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". Weiter wird ausgeführt, daß „diese Garantien sich insbesondere aus entsprechenden Vertragsklauseln ergeben können". Wenn die Kommission nach dem Verfahren des Artikels 31 tätig wird, so befugt Artikel 26 Absatz 4 sie ferner zu beschließen, daß bestimmte Standardvertragsklauseln ausreichende Garantien gemäß Artikel 26 Absatz 2 bieten.

Die Idee der Verwendung von Verträgen als Mittel der Regelung internationaler Übermittlungen personenbezogener Daten ist natürlich nicht erst durch die Richtlinie entstanden. Bereits 1992 waren der Europarat, die Internationale Handelskammer und die Europäische Kommission gemeinsam für eine Studie zu diesem Thema verantwortlich.[7] In jüngerer Zeit haben sich immer mehr Sachverständige und Kommentatoren in Studien und Artikeln zur Verwendung vertraglicher Bestimmungen geäußert - vielleicht, weil sie die ausdrückliche Bezugnahme in der Richtlinie festgestellt haben. Auch in der Praxis werden Verträge weiterhin als ein Mittel zur Behandlung von Datenschutzproblemen eingesetzt, die sich aus der Ausfuhr personenbezogener Daten aus bestimmten EU-Mitgliedstaaten ergeben. Seit Ende der 80er Jahre werden sie in Frankreich häufig verwendet, und in Deutschland fand jüngst das Beispiel der „BahnCard" große Beachtung, da ein Teil des Angebots auf der Einbeziehung der Citibank beruht.[8]

2. Die Verwendung von Verträgen als Grundlage für innergemeinschaftliche Datenflüsse

Vor der Prüfung der Anforderungen an vertragliche Bestimmungen im Rahmen von Datenströmen in Drittländer ist es wichtig, den Unterschied zwischen der Drittlandsituation und der Situation deutlich zu machen, bei der die Daten in der Gemeinschaft bleiben. Im letztgenannten Fall ist der Vertrag der Mechanismus, der verwendet wird, um die Aufteilung der Zuständigkeiten für den Datenschutz zu definieren

---

[7] „Model Contract to Ensure Equivalent Data Protection in the Context of Transborder Data Flow, with Explanatory Memorandum", gemeinsame Studie des Europarates, der Kommission der Europäischen Gemeinschaften und der Internationalen Handelskammer, Straßburg, 2. November 1992

[8] Vgl. Darstellung dieses Falls durch Alexander Dix auf der Internationalen Konferenz der Datenschutzbeauftragten, September 1996 in Ottawa.

und zu regeln, wenn mehr als eine Stelle an der fraglichen Datenverarbeitung beteiligt ist. Nach der Richtlinie trägt eine einzige Einheit, d. h. der „für die Verarbeitung Verantwortliche“ die Hauptverantwortung für die Erfüllung der wesentlichen Grundsätze des Datenschutzes. Die zweite Einheit, der „Auftragsverarbeiter“, ist lediglich für die Datensicherheit zuständig. Von einem „für die Verarbeitung Verantwortlichen“ wird gesprochen, wenn eine Person die Entscheidungsbefugnis über die Zweckbestimmung und die Mittel der Datenverarbeitung besitzt, während der „Auftragsverarbeiter“ lediglich die Stelle ist, die den Datenverarbeitungsdienst physisch erbringt. Die Beziehung zwischen den beiden wird durch Artikel 17 Absatz 3 der Richtlinie geregelt, der folgendes festlegt:

> *Die Durchführung einer Verarbeitung im Auftrag erfolgt auf der Grundlage eines Vertrags oder Rechtsakts, durch den der Auftragsverarbeiter an den für die Verarbeitung Verantwortlichen gebunden ist und in dem insbesondere folgendes vorgesehen ist:*
> – *der Auftragsverarbeiter handelt nur auf Weisung des für die Verarbeitung Verantwortlichen*
> – *die in Absatz 1 genannten Verpflichtungen (die materiellrechtlichen Bestimmungen zur Datensicherheit) gelten auch für den Auftragsverarbeiter, und zwar nach Maßgabe der Rechtsvorschriften des Mitgliedstaats, in dem er seinen Sitz hat.*

Dies baut auf dem allgemeinen Grundsatz nach Artikel 16 auf, demzufolge Personen, die dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter unterstellt sind, sowie der Auftragsverarbeiter selbst personenbezogene Daten nur auf Weisung des für die Verarbeitung Verantwortlichen verarbeiten dürfen (es sei denn, es bestehen hierzu gesetzliche Verpflichtungen).

Bei der Übermittlung personenbezogener Daten in Drittländer wird normalerweise auch mehr als eine Partei beteiligt sein. Hier ist die betreffende Beziehung eine Beziehung zwischen der die Daten übermittelnden Stelle (dem „Übermittler“) und der Stelle, die die Daten im Drittland entgegennimmt (dem „Empfänger“). Daher sollte der Zweck des Vertrags unter anderem darin bestehen, die Verteilung der Zuständigkeit für die Einhaltung des Datenschutzes auf die beiden Vertragsparteien festzulegen. Der Vertrag muß jedoch noch weiteren Anforderungen entsprechen: Er muß zusätzliche Sicherheiten für die betroffene Person bieten, die dadurch erforderlich werden, daß der Empfänger im Drittland keinem durchsetzbaren Regelwerk von Datenschutzbestimmungen unterliegt, das ein angemessenes Schutzniveau vorsieht.

3. Das Ziel einer vertraglichen Lösung

Im Rahmen der Drittlandübermittlungen ist deshalb der Vertrag ein Mittel, um angemessene Garantien durch den für die Verarbeitung Verantwortlichen vorzusehen, wenn Daten aus der Gemeinschaft (und somit außerhalb des durch die Richtlinie und natürlich durch das allgemeine Regelwerk des Gemeinschaftsrechts vorgesehenen Schutzes[9]) in ein Drittland übermittelt werden, in dem kein angemessenes allgemeines

[9] Die Wahrnehmung der Datenschutzrechte der Personen wird innerhalb der Gemeinschaft durch das allgemeine Regelwerk erleichtert, beispielsweise das Europäische Übereinkommen über die Übermittlung von Rechtshilfeersuchen (Straßburg 1977).

Schutzniveau vorhanden ist. Eine Vertragsbestimmung, die diese Funktion erfüllen soll, muß einen befriedigenden Ausgleich für das Fehlen eines allgemein angemessenen Schutzniveaus bieten, indem sie die wesentlichen Elemente des Schutzes enthält, die in einer bestimmten Situation nicht vorhanden sind.

4. Die spezifischen Erfordernisse einer vertraglichen Lösung

Ausgangspunkt für die Bewertung der Bedeutung der „ausreichenden Garantien" gemäß Artikel 26 Absatz 2 ist der Begriff des „angemessenen Schutzes", auf den in Kapitel 1 bereits recht ausführlich eingegangen worden ist. Er umfaßt eine Reihe von Grundsätzen des Datenschutzes und drei weitere Voraussetzungen, ohne die diese wirkungslos blieben.

(i) Die wesentlichen Datenschutzvorschriften

Das wichtigste Erfordernis der vertraglichen Lösung besteht darin, daß sie auf eine Verpflichtung der an der Übermittlung Beteiligten hinauslaufen muß, sicherzustellen, daß alle in Kapitel 1 dargelegten grundlegenden Bestimmungen des Datenschutzes bei der Verarbeitung von den in das Drittland übermittelten Daten gelten. Diese Grundsätze sind:

- Der Grundsatz der Beschränkung der Zweckbestimmung
- Der Grundsatz der Datenqualität und -verhältnismäßigkeit
- Der Grundsatz der Transparenz
- Der Grundsatz der Sicherheit
- Die Rechte auf Zugriff, Berichtigung und Widerspruch
- Beschränkungen der Weiterübermittlung an Nichtvertragspartner[10].

In bestimmten Situationen müssen zusätzliche Grundsätze, die sich auf sensible Daten, das Direktmarketing und automatisierte Entscheidungen beziehen, angewandt werden.

Der Vertrag sollte detailliert darlegen, wie der Empfänger der Datenübermittlung diese Grundsätze anzuwenden hat (d. h. Spezifizierung der Zweckbestimmungen, der Datenkategorien, Begrenzung der Speicherzeit, Sicherheitsmaßnahmen usw.). In anderen Fällen, wenn beispielsweise der Schutz in einem Drittland durch ein allgemeines Datenschutzgesetz vorgesehen ist, das der Richtlinie ähnelt, sind wahrscheinlich andere Mechanismen vorhanden, aus denen hervorgeht, auf welche Art und Weise die Datenschutzvorschriften in der Praxis Anwendung finden (Verhaltenskodexe, Notifizierung, beratende Funktion der Aufsichtsbehörde). Da dies bei vertraglichen Beziehungen nicht der Fall ist, kommt der Festlegung der Einzelheiten besondere Bedeutung zu, wenn die Übermittlung auf der Grundlage eines Vertrags erfolgt.

(ii) Den wesentlichen Vorschriften Geltung verschaffen

In Kapitel 1 sind für die Beurteilung der Effizienz eines Datenschutzsystems drei Kriterien dargelegt. Dabei handelt es sich um die Fähigkeit des Systems:

---

[10] Weiterübermittlungen personenbezogener Daten vom Empfänger an einen anderen Dritten sind lediglich zulässig, wenn Mittel gefunden werden, den betreffenden Dritten vertraglich zu binden und damit den betroffenen Personen dieselben Garantien des Datenschutzes zu gewährleisten.

- eine **gute Befolgungsrate** der Vorschriften zu bewirken,
- **Unterstützung und Hilfe für die einzelne betroffene Person** bei der Wahrnehmung ihrer Rechte zu sichern
- und - als besonders wichtiges Element - für eine **angemessene Entschädigung** des Geschädigten im Falle der Nichteinhaltung von Vorschriften zu sorgen.

Dieselben Kriterien müssen bei der Beurteilung der Effizienz einer vertraglichen Lösung gelten. Dies ist natürlich eine große, wenn auch zu bewältigende Herausforderung. Es geht darum, Mittel und Wege zu finden, um das Fehlen von Aufsichts- und Durchsetzungsmechanismen auszugleichen und der betroffenen Person, die vielleicht kein Vertragspartner ist, Hilfe, Unterstützung und letztendlich Entschädigung zu gewähren.

Jede dieser Fragen muß in allen Einzelheiten geprüft werden. Zur Erleichterung der Analyse werden sie hier in umgekehrter Reihenfolge behandelt.

Entschädigung für eine betroffene Person

Einer betroffenen Person mit Hilfe eines zwischen „Datenübermittler“ und „Datenempfänger“ abzuschließenden Vertrages die Möglichkeit des Rechtsbehelfs einzuräumen (d. h. das Recht auf eine durch einen unabhängigen Schiedsrichter beurteilte Beschwerde und gegebenenfalls das Recht auf eine Entschädigung) ist keine einfache Frage. Viel wird von der Art des gewählten Vertragsrechts sowie von dem auf den Vertrag anwendbaren einzelstaatlichen Recht abhängen. Normalerweise dürfte das anwendbare Recht das des Mitgliedstaats sein, in dem die übermittelnde Partei niedergelassen ist. Das Vertragsrecht einiger Mitgliedstaaten erlaubt die Begründung von Rechten Dritter, die in anderen Mitgliedstaaten nicht möglich ist.

Es gilt die allgemeine Regel, daß die Rechtssicherheit für die betroffene Person um so größer ist, je mehr der Empfänger im Hinblick auf seine Freiheit beschränkt ist, die Zweckbestimmungen, Mittel und Bedingungen zu wählen, unter denen er die übermittelten Daten verarbeitet. Da es ja hier um Fälle unangemessenen allgemeinen Schutzes geht, bestünde die beste Lösung darin, im Vertrag festzulegen, daß der Empfänger der Übermittlung im Hinblick auf die übermittelten Daten oder die Art und Weise, in der diese anschließend verarbeitet werden, keine eigene Entscheidungsbefugnis hat. Der Empfänger hat in diesem Fall allein nach Anweisung des Übermittlers zu handeln. So verbleibt beispielsweise die Entscheidungskompetenz über die Daten auch dann, wenn die Daten nach außerhalb der Europäischen Union übermittelt wurden, bei der Stelle, die die Übermittlung vorgenommen und ihren Sitz in der Gemeinschaft hat. Der Übermittler bleibt somit der für die Verarbeitung Verantwortliche, während der Empfänger lediglich ein Verarbeiter mit einem Subunternehmervertrag ist. Da die Aufsicht über die Daten durch eine in einem Mitgliedstaat der EU niedergelassene Aufsichtsbehörde ausgeübt wird, gilt das Recht des betreffenden Mitgliedstaats für die in dem Drittland erfolgte Verarbeitung weiter[11]. Darüber hinaus ist der für die Verarbeitung Verantwortliche weiterhin nach dem Recht des Mitgliedstaats für jeden Schaden haftbar, der in Folge einer unzulässigen Verarbeitung entstanden ist.[12]

[11] Aufgrund von Artikel 4 Absatz 1 Buchstabe a) der Richtlinie 95/46/EG.

[12] Vgl. Artikel 23 der Richtlinie 95/46/EG.

Diese Art der Übereinkunft ist der nicht unähnlich, die bei der interterritorialen Vereinbarung gefunden wurde, mit der der zuvor erwähnte Fall von BahnCard und Citibank gelöst wurde. In der vertraglichen Vereinbarung sind dabei insbesondere im Hinblick auf die Datensicherheit detaillierte Festlegungen für die Datenverarbeitung getroffen worden, die alle anderen Nutzungen der Daten durch den Empfänger der Übermittlung ausschließen. Damit wurde gesichert, daß für die im Drittland erfolgende Datenverarbeitung deutsches Recht gilt und den betroffenen Personen Rechtsbehelfe offenstehen.[13]

Natürlich wird es Fälle geben, in denen eine solche Lösung nicht möglich ist. Möglicherweise erbringt der Empfänger der Übermittlung nicht nur einen reinen Datenverarbeitungsdienst für den Verantwortlichen mit Sitz in der Europäischen Union, sondern hat die Daten beispielsweise für eine Verwendung zum eigenen Nutzen oder für eigene Zwecke gemietet oder erworben. Unter diesen Umständen muß der Empfänger über einen gewissen Handlungsspielraum verfügen, um die Daten nach seinem Belieben zu verarbeiten, wodurch er selbst zu einem Verantwortlichen für die Daten wird.

In einem derartigen Fall kann man sich nicht auf die ständige automatische Anwendbarkeit der Rechtsvorschriften eines Mitgliedstaats und die fortgesetzte Schadenshaftung des Übermittlers der Daten stützen. Andere, komplexere Mechanismen müssen gefunden werden, um der betroffenen Person angemessene Rechtsbehelfe an die Hand zu geben. Wie bereits erwähnt, ist es in einigen Rechtssystemen für Dritte möglich, Vertragsrechte geltend zu machen, so daß dies genutzt werden könnte, um über einen offenen, veröffentlichten Vertrag zwischen Übermittler und Empfänger Rechte für betroffene Personen zu begründen. Die Position dieser Personen würde weiter gestärkt, wenn sich im Rahmen des Vertrages die Parteien selbst zu einer Art verbindlichen Schlichtung für den Fall verpflichten, daß die Vertragserfüllung durch eine betroffene Person angefochten wird. In den Selbstkontrollkodizes einiger Branchen sind derartige Schlichtungsmechanismen enthalten, und die Verwendung von Verträgen in Verbindung mit derartigen Kodexen wäre sicherlich nutzbringend.

Eine weitere Möglichkeit besteht darin, daß der Übermittler zum Zeitpunkt des Eingangs der ersten Daten der betroffenen Person eine gesonderte vertragliche Vereinbarung mit ihr abschließt und darin festlegt, daß er (der Übermittler) für jeden Schaden oder jede Notlage haftbar bleibt, die dadurch entsteht, daß der Empfänger einer Datenübermittlung das vereinbarte Paket an Grundprinzipien des Datenschutzes nicht einhält. Auf diese Weise verfügt die betroffene Person gegenüber dem Übermittler bei Verstößen durch den Empfänger über Rechtsmittel. Es ist dann Sache des Übermittlers, Maßnahmen wegen Vertragsbruchs gegen den Empfänger einzuleiten und etwaige Schadensersatzleistungen, zu deren Zahlung an die betroffene Person er genötigt war, anschließend von diesem zurückzufordern.

---

[13] Obwohl für diesen Fall ein Gesetz galt, das vor der Richtlinie erlassen worden war, fand das Gesetz selbst nicht automatisch Anwendung auf alle Verarbeitungen, die durch einen in Deutschland niedergelassenen Verantwortlichen für die Datenverarbeitung kontrolliert wurden. Die Rechtsbehelfe für die betroffene Person wurden durch die Möglichkeit des deutschen Vertragsrechts geschaffen, Rechte Dritter zu begründen.

Diese ausgeklügelte dreiseitige Lösung ist vielleicht machbarer als dies scheinen mag. Der Vertrag mit der betroffenen Person könnte Teil der Allgemeinen Geschäftsbedingungen werden, zu denen beispielsweise eine Bank oder ein Reisebüro ihren Kunden Dienstleistungen anbietet. Sie hat den Vorteil der Transparenz: Die betroffene Person wird über ihre Rechte voll informiert.

Schließlich könnte als Alternative zum Vertragsabschluß mit der betroffenen Person auch vorgesehen werden, daß ein Mitgliedstaat für Schäden, die infolge der Handlungen des Empfängers der Übermittlung entstehen, eine fortgesetzte Haftpflicht der für die Verarbeitung Verantwortlichen, die Daten nach außerhalb der Gemeinschaft übermitteln, gesetzlich niederlegt.

Unterstützung und Hilfe für betroffene Personen

Eine der Hauptschwierigkeiten betroffener Personen, deren Daten in den Bereich einer ausländischen Rechtsprechung übermittelt werden, ist das Problem, daß sie nicht in der Lage sind, die Ursache des betreffenden Problems, mit dem sie zu kämpfen haben, zu finden, und deshalb nicht beurteilen können, ob die Vorschriften für den Datenschutz korrekt befolgt wurden oder ob Gründe für eine rechtliche Anfechtung bestehen.[14] Deshalb muß für ein angemessenes Schutzniveau eine Art institutioneller Mechanismus vorhanden sein, der eine unabhängige Untersuchung von Beschwerden ermöglicht.

Die Überwachungs- und Untersuchungsfunktion der Kontrollstelle eines Mitgliedstaats beschränkt sich auf die Datenverarbeitung, die im Hoheitsgebiet des Mitgliedstaats erfolgt.[15] Werden Daten in einen anderen Mitgliedstaat übermittelt, so gewährleistet ein System der gegenseitigen Unterstützung der Kontrollstellen, daß jede Beschwerde einer betroffenen Person in dem ersten Mitgliedstaat ordnungsgemäß bearbeitet wird. Erfolgt die Übermittlung in ein Drittland, besteht in den meisten Fällen eine solche Garantie nicht. Damit stellt sich die Frage, welche Art Ausgleichsmechanismus festgelegt werden kann, wenn die Datenübermittlung auf der Grundlage eines Vertrags erfolgt.

Eine Möglichkeit bestünde darin, die Aufnahme einer Vertragsklausel zu fordern, die der Kontrollstelle des Mitgliedstaats, in dem der Übermittler der Daten niedergelassen ist, ein Recht auf Einsichtnahme in die von dem Verarbeiter im Drittland vorgenommene Verarbeitung garantiert. Diese Einsichtnahme könnte in der Praxis durch einen gegebenenfalls von der Kontrollstelle ernannten Vertreter vorgenommen werden (beispielsweise eine spezialisierte Buchprüferfirma). Bei diesem Ansatz besteht allerdings das Problem, daß die Kontrollstelle im allgemeinen keine Vertragspartei ist[16] und bei der Forderung nach Zugang der Vertrag somit in einigen Rechtssystemen nicht geltend gemacht werden kann. Eine andere Möglichkeit wäre eine gesetzliche Verpflichtung des

---

[14] Auch wenn einer betroffenen Person Rechte durch einen Vertrag gewährt werden, wird sie oft nicht beurteilen können, ob ein Vertragsbruch vorliegt, und wenn, durch wen. Dafür ist ein Untersuchungsverfahren außerhalb der formellen zivilrechtlichen Verfahren erforderlich.

[15] Siehe Artikel 28 Absatz 1 der Richtlinie 95/46/EG.

[16] Die französische Delegation könnte sich Situationen vorstellen, in denen die Kontrollstelle Vertragspartner ist.

Empfängers im Drittland unmittelbar gegenüber der entsprechenden Kontrollstelle des EU-Mitgliedstaats, mit der der Empfänger der Daten einwilligt, der Kontrollstelle oder einem benannten Vertreter im Fall einer vermuteten Nichterfüllung der Grundsätze des Datenschutzes den Zugang zu erlauben. Zu dieser Verpflichtung könnte auch gehören, daß die an der Datenübermittlung Beteiligten die Kontrollstelle über jede Beschwerde unterrichten, die sie von einer betroffenen Person erhalten. Bei einer derartigen Vereinbarung wäre die Existenz einer solchen Verpflichtung eine Voraussetzung, die erfüllt sein müßte, bevor die Datenübermittlung stattfinden kann.

Unabhängig von der gewählten Lösung bleiben große Zweifel im Hinblick auf die Frage bestehen, ob es zweckmäßig, praktikabel oder hinsichtlich der Ressourcen für eine Kontrollstelle eines EU-Mitgliedstaats auch wirklich machbar ist, die Zuständigkeit für eine Untersuchung und Überprüfung der Datenverarbeitung zu übernehmen, die in einem Drittland erfolgt.

Gewährleistung einer hohen Befolgungsrate

Auch wenn keine Beschwerde oder kein Problem einer betroffenen Person vorliegt, muß man darauf vertrauen können, daß die Vertragsparteien den Vertrag tatsächlich erfüllen. Das Problem bei der vertraglichen Lösung ist die Schwierigkeit, Sanktionen für die Nichterfüllung festzulegen, die so abschreckend sind, daß von ihnen die für das Herstellen dieses Vertrauens erforderliche Wirkung ausgeht. Auch in Fällen, in denen eine tatsächliche Kontrolle über die Daten weiterhin von innerhalb der Gemeinschaft ausgeübt wird, droht dem Empfänger der Übermittlung möglicherweise keine direkte Strafe, wenn er Daten in Zuwiderhandlung gegen den Vertrag verarbeitet. Statt dessen bliebe die Haftung bei dem in der Gemeinschaft niedergelassenen Übermittler der Daten, der dann mögliche Verluste in einer gesonderten Rechtshandlung gegen den Empfänger eintreiben müßte. Eine solche indirekte Haftung ist möglicherweise nicht ausreichend, um den Empfänger zu veranlassen, den Vertrag in allen Einzelheiten zu erfüllen.

Angesichts dessen wird es wahrscheinlich in den meisten Fällen notwendig sein, eine vertragliche Lösung durch zumindest die Möglichkeit einer Art externer Überprüfung der Verarbeitungstätigkeiten des Empfängers zu ergänzen, z. B. ein Audit durch ein zuständiges Gremium oder ein spezialisiertes Prüfungsunternehmen.

5. Das Problem des vorrangigen Rechts

Eine besondere Schwierigkeit beim vertraglichen Ansatz ist die Möglichkeit, daß die allgemeinen Rechtsvorschriften des Drittlands den Empfänger einer Datenübermittlung verpflichten, unter bestimmten Umständen personenbezogene Daten gegenüber dem Staat offenzulegen (Polizei, Gerichte oder Steuerbehörden), und daß derartige gesetzliche Erfordernisse meist Vorrang vor Verträgen haben, bei denen der Verarbeiter Vertragspartei ist.[17] Für Verarbeiter in der Gemeinschaft ist diese Möglichkeit in Artikel 16 der Richtlinie angesprochen, dem zufolge Auftragsverarbeiter

[17] Das Ausmaß der staatlichen Befugnis zur Forderung der Offenlegung von Informationen ist ebenfalls ein Punkt, der bei der allgemeinen Beurteilung der Angemessenheit des Schutzniveaus in einem Drittland zu berücksichtigen ist.

personenbezogene Daten nur auf Weisung des für die Verarbeitung Verantwortlichen verarbeiten dürfen, *es sei denn, es bestehen gesetzliche Verpflichtungen.* Nach der Richtlinie müssen sich allerdings derartige Offenlegungen (die naturgemäß für Zweckbestimmungen erfolgen, die mit denen unvereinbar sind, für die die Daten erfaßt wurden) auf solche beschränken, die in demokratischen Gesellschaften aus einem der Gründe der öffentlichen Sicherheit nach Artikel 13 Absatz 1 der Richtlinie erforderlich sind. Artikel 6 des Vertrags von Amsterdam garantiert die Einhaltung der in der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten enthaltenen Grundrechte. In Drittländern mag es ähnliche Beschränkungen der Möglichkeiten des Staates, die Bereitstellung personenbezogener Daten von Unternehmen und anderen in ihrem Hoheitsgebiet tätigen Organisationen zu fordern, nicht immer geben.

Es gibt keine einfache Möglichkeit, diese Schwierigkeit zu überwinden. Damit wird lediglich illustriert, welche Grenzen der vertragliche Ansatz hat. In einigen Fällen ist ein Vertrag ein zu schwaches Instrument, um angemessene Garantien für den Datenschutz zu bieten, und Übermittlungen in bestimmte Länder sollten nicht genehmigt werden.

6. Praktische Erwägungen zur Verwendung von Verträgen

Aus der vorstehenden Analyse geht hervor, daß für jeden einzelnen Fall der Datenübermittlung eine detaillierte, den jeweiligen Erfordernissen angepaßte Lösung gefunden werden muß. Diese Notwendigkeit der Festlegung von Einzelheiten im Hinblick auf die genauen Zweckbestimmungen und die Voraussetzungen, unter denen die übermittelten Daten verarbeitet werden, schließt die Möglichkeit der Erstellung eines Mustervertrags nicht aus, macht es aber erforderlich, jeden auf diesen Mustervertrag aufbauenden Vertrag entsprechend den besonderen Umständen des Einzelfalls zu ergänzen.

Die Analyse hat zudem ergeben, daß besondere praktische Probleme bei der Untersuchung der Nichterfüllung eines Vertrags bestehen, wenn die Verarbeitung außerhalb der Europäischen Union erfolgt und von dem betreffenden Drittland keine Kontrollstelle vorgesehen ist. Diese beiden Erwägungen laufen darauf hinaus, daß es Situationen geben wird, in denen eine vertragliche Lösung geeignet ist, und andere, in denen ein Vertrag die erforderlichen „angemessenen Sicherheiten“ in keiner Weise garantieren kann.

Die notwendige detaillierte Anpassung von Verträgen an die Besonderheiten der jeweiligen Übermittlung impliziert, daß ein Vertrag besonders für Situationen geeignet ist, in denen ähnliche Datenübermittlungen wiederholt vorgenommen werden. Die Schwierigkeiten bei der Überwachung bedeuten, daß eine vertragliche Lösung dann äußerst effizient sein kann, wenn es sich bei den Vertragsparteien um bedeutende Wirtschaftsteilnehmer handelt, die bereits öffentlicher Prüfung und Regelung unterworfen sind[18]. Große internationale Netze, wie sie für Kreditkartengeschäfte und Flugbuchungen bestehen, weisen diese beiden Merkmale auf und stellen somit Situationen dar, für die Verträge sehr gut geeignet erscheinen. Unter diesen Umständen könnten sie sogar noch

[18] Im Fall von Citybank und „BahnCard“ arbeitete der Berliner Datenschutzbeauftragte mit den amerikanischen Bankaufsichtsbehörden zusammen.

durch multilaterale Vereinbarungen ergänzt werden, von denen eine größere Rechtssicherheit ausgeht.

Auch wenn die an der Übermittlung Beteiligten ein und derselben Unternehmensgruppe angehören oder Tochtergesellschaften sind, dürfte aufgrund der engen Bindungen zwischen dem Empfänger im Drittland und der Einheit mit Sitz in der Gemeinschaft eine weitaus größere Möglichkeit zur Untersuchung der Nichterfüllung des Vertrags bestehen. Unternehmensinterne Übermittlungen sind deshalb ein weiterer Bereich, in dem es ein deutliches Potential für die Entwicklung effizienter vertraglicher Lösungen gibt.

Wichtige Schlußfolgerungen und Empfehlungen

- Verträge werden in der Gemeinschaft als Mittel zur Festlegung der Aufteilung der Zuständigkeit für die Erfüllung des Datenschutzes zwischen dem für die Verarbeitung Verantwortlichen und einem beauftragten Auftragsverarbeiter verwendet. Erfolgt bei Datenflüssen in Drittländer der Abschluß eines Vertrages, so muß dieser weiteren Anforderungen entsprechen: Er muß zusätzliche Sicherheiten für die betroffene Person bieten, die dadurch erforderlich werden, daß der Empfänger im Drittland keinem durchsetzbaren Regelwerk von Datenschutzbestimmungen unterliegt, das ein angemessenes Schutzniveau vorsieht.

- Die Grundlage für die Beurteilung der Angemessenheit der Sicherheitsmaßnahmen aufgrund einer vertraglichen Lösung entspricht der Grundlage für die Beurteilung der Angemessenheit des allgemeinen Schutzniveaus in einem Drittland. Eine vertragliche Lösung muß die wichtigsten Grundsätze des Datenschutzes und die Mittel umfassen, mit denen die Grundsätze durchgesetzt werden können.

- Im Vertrag sind die Zweckbestimmungen, die Mittel und Bedingungen, unter denen die Verarbeitung der übermittelten Daten zu erfolgen hat, genau festzulegen. Dies gilt auch für die Art und Weise, in der die grundlegenden Prinzipien des Datenschutzes anzuwenden sind. Die Rechtssicherheit für die betroffene Person ist um so größer, je mehr der Vertrag den Empfänger in seiner Freiheit beschränkt, die Daten ohne Kontrolle von außen im eigenen Namen zu verarbeiten. Der Vertrag sollte deshalb möglichst als ein Mittel verwendet werden, mit dem die die Daten übermittelnde Stelle die Entscheidungsbefugnis über die in dem Drittland erfolgende Verarbeitung behält.

- Verfügt der Empfänger im Hinblick auf die Verarbeitung der übermittelten Daten in gewissem Maße über eigene Entscheidungsgewalt, so ist die Situation nicht so eindeutig, und ein einfacher Vertrag zwischen den an der Übermittlung Beteiligten reicht dann möglicherweise als Grundlage für die Wahrnehmung der Rechte durch Betroffene nicht aus. Vielleicht wird ein Mechanismus benötigt, auf dessen Grundlage der übermittelnde Beteiligte in der Gemeinschaft für alle Schäden haftbar bleibt, die sich aus der in dem Drittland erfolgten Verarbeitung ergeben können.

- Weiterübermittlungen an Gremien oder Organisationen, die nicht durch den Vertrag gebunden sind, sollten vertraglich explizit ausgeschlossen werden, sofern es nicht möglich ist, derartige beteiligte Dritte vertraglich auf die Einhaltung derselben Datenschutzgrundsätze zu verpflichten.

- Das Vertrauen in die Befolgung der Grundsätze des Datenschutzes nach der Übermittlung von Daten wird gestärkt, wenn die Einhaltung des Datenschutzes durch den Empfänger der Übermittlung einer externen Überprüfung beispielsweise durch ein spezialisiertes Audit-Unternehmen oder ein Normungs-/Zertifizierungs-Gremium unterworfen ist.

- Im Fall eines Problems einer betroffenen Person, das sich vielleicht aus einem Verstoß gegen die vertraglich garantierten Datenschutzbestimmungen ergibt, stellt sich das allgemeine Problem der Sicherstellung der ordnungsgemäßen Prüfung der Beschwerde einer betroffenen Person. Bei der Durchführung einer solchen Prüfung durch die Kontrollstellen des EU-Mitgliedstaats wird es zu praktischen Problemen kommen.

- Vertragliche Lösungen sind wahrscheinlich am besten für große internationale Netze (Kreditkartengeschäfte, Flugbuchungen) geeignet, die durch große Mengen sich wiederholender Datenübermittlungen gleicher Art und eine relativ kleine Anzahl bedeutender Wirtschaftsteilnehmer in Branchen charakterisiert sind, die bereits in wesentlichem Umfang öffentlicher Prüfung und Regelung unterworfen sind. Unternehmensinterne Datenübermittlungen zwischen verschiedenen Zweigniederlassungen derselben Unternehmensgruppe sind ein weiterer Bereich, in dem es ein beträchtliches Potential für die Verwendung von Verträgen gibt.

- Länder, in denen beim Informationszugang die Befugnisse der staatlichen Behörden über das hinausgehen, was durch die weltweit angenommenen Normen des Schutzes der Menschenrechte erlaubt ist, sind keine sicheren Bestimmungsorte für Übermittlungen auf der Grundlage von Vertragsklauseln.

KAPITEL 5: AUSNAHMEN VON DER ANFORDERUNG DER ANGEMESSENHEIT

In Artikel 26 Absatz 1 der Richtlinie ist eine begrenzte Zahl von Fällen aufgeführt, in denen Ausnahmen vom Erfordernis der Angemessenheit für Übermittlungen in Drittländer zulässig sind. Diese enggefaßten Ausnahmen betreffen überwiegend Fälle, in denen die Risiken für die betroffene Person relativ gering sind oder in denen andere Interessen (Wahrung eines wichtigen öffentlichen Interesses oder des Interesses der betroffenen Person selbst) Vorrang vor dem Recht der betroffenen Person auf den Schutz der Privatsphäre genießen. Als Ausnahmen von der allgemeinen Regel müssen sie restriktiv ausgelegt werden. Zudem können die Mitgliedstaaten im innerstaatlichen Recht festlegen, daß die Ausnahmen in bestimmten Fällen nicht gelten. Dies trifft beispielsweise zu, wenn besonders schutzbedürftige Gruppen wie Arbeitnehmer oder Patienten zu schützen sind.

Bei der ersten Ausnahme muß die betroffene Person ihre Einwilligung *ohne jeden Zweifel* gegeben haben Es sei darauf verwiesen, daß entsprechend der Definition in Artikel 2 Buchstabe h) der Richtlinie die Einwilligung ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage gegeben worden sein muß. Das Erfordernis der Kenntnis der Sachlage ist insofern besonders wichtig, als damit verlangt wird, daß die betroffene Person über das konkrete Risiko der Übermittlung der Daten in ein Land ohne angemessenes Schutzniveau ordnungsgemäß in Kenntnis gesetzt werden muß. Geschieht dies nicht, so darf die Ausnahme nicht angewandt werden. Da die Einwilligung ohne jeden Zweifel erfolgen muß, führt jeglicher Zweifel daran, ob die Einwilligung tatsächlich gegeben worden ist, ebenfalls dazu, daß die Ausnahmeregelung nicht gilt. Damit würde auch in einer Vielzahl von Fällen, in denen die Einwilligung unterstellt wird (weil die betreffende Person beispielsweise auf die Übermittlung aufmerksam gemacht wurde und keinen Einwand dagegen erhoben hat), die Ausnahmeregelung nicht greifen. Von Nutzen dürfte die Regelung dann sein, wenn der Übermittler in direktem Kontakt mit der betroffenen Person steht, die erforderlichen Informationen problemlos mitgeteilt werden können und die Einwilligung ohne jeden Zweifel erlangt wird. Dies ist z. B. bei Übermittlungen im Rahmen eines Versicherungsschutzes häufig der Fall.

Die zweite und die dritte Ausnahme beziehen sich auf Übermittlungen, die *erforderlich* sind für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen (oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person) oder zum Abschluß oder zur Erfüllung eines Vertrags, der *im Interesse der betroffenen Person* vom für die Verarbeitung Verantwortlichen mit einem Dritten geschlossen wurde oder geschlossen werden soll. Diese Ausnahmen erscheinen zunächst recht weitgefaßt, doch wie die im folgenden erörterte vierte und fünfte Ausnahme wird ihre Anwendung in der Praxis durch das Kriterium der Erforderlichkeit eingeschränkt: Die übermittelten Daten müssen ausnahmslos für die Erfüllung des Vertrages erforderlich sein. Werden also zusätzliche, nicht zu den wesentlichen Angaben zählende Daten übermittelt oder dient die Übermittlung nicht der Erfüllung des Vertrages, sondern einer anderen Zweckbestimmung (z. B. Nachfaßmarketing), gilt die Ausnahme nicht. Was die vorvertraglichen Maßnahmen betrifft, so können dies nur von der betroffenen Person initiierte Situationen sein (wie die Anforderung von Informationen zu einem speziellen Dienst) und nicht solche, die sich aus den Marketingkonzepten der für die Verarbeitung Verantwortlichen herleiten.

Ungeachtet dieser Vorbehalte werden die zweite und die dritte Ausnahme nicht ohne Wirkung bleiben. So dürften sie etwa bei Übermittlungen für die Buchung eines

Flugtickets für einen Passagier oder bei Übermittlungen personenbezogener Daten im Zusammenhang mit dem grenzüberschreitenden Zahlungsverkehr oder der Zahlung per Kreditkarte häufig angewandt werden. Die Ausnahmeregelung für Verträge „im Interesse der betroffenen Person“ (Artikel 26 Absatz 1 Buchstabe c)) deckt speziell auch die Übermittlung von Daten an den Empfänger von Bankzahlungen ab, der, obwohl betroffene Person, meist keine Vertragspartei des Verantwortlichen ist, der die Übermittlung vornimmt.

Zur vierten Ausnahme gehören zwei Komponenten, von denen sich die erste auf Übermittlungen bezieht, die für die Wahrung eines wichtigen öffentlichen Interesses erforderlich oder gesetzlich vorgeschrieben sind. Hierzu mögen bestimmte begrenzte Übermittlungen zwischen öffentlichen Verwaltungen zählen, obwohl Vorsicht geboten ist, damit diese Bestimmung nicht zu weit ausgelegt wird. Dabei reicht ein einfaches öffentliches Interesse nicht aus, sondern es muß sich um ein *wichtiges* öffentliches Interesse handeln. Aus Punkt 58 geht hervor, daß die Datenübermittlung zwischen Steuer- oder Zollverwaltungen oder zwischen Diensten, die für Angelegenheiten der sozialen Sicherheit zuständig sind, generell abgedeckt ist. Auch Übermittlungen zwischen den Kontrollstellen im Finanzdienstleistungssektor können unter diese Ausnahmeregelung fallen. Die zweite Komponente betrifft Übermittlungen, die im Rahmen internationaler Rechtsstreitigkeiten oder Gerichtsverfahren vorgenommen werden, und speziell Übermittlungen, die für die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche vor Gericht erforderlich sind.

Die fünfte Ausnahme bezieht sich auf Übermittlungen im Interesse der Wahrung lebenswichtiger Interessen der betroffenen Person. Ein einleuchtendes Beispiel wäre hier die dringende Übermittlung von medizinischen Unterlagen in ein Drittland, in dem ein zuvor in der EU behandelter Tourist in einen Unfall verwickelt ist oder sich eine gefährliche Erkrankung zugezogen hat. Allerdings wird in Punkt 31 der Richtlinie das „lebenswichtige Interesse“ recht eng als „für das Leben der betroffenen Person wesentliches Interesse“ ausgelegt. Ein Interesse aus finanziellen, eigentumsbezogenen oder familiären Gründen wäre im Normalfall ausgeschlossen.

Die sechste und letzte Ausnahme betrifft die Übermittlung aus einem Register, das gemäß den Rechts- oder Verwaltungsvorschriften zur Information der Öffentlichkeit bestimmt ist, soweit die gesetzlichen Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind. Hinter dieser Ausnahme steht die Absicht, daß in Fällen, in denen ein Register in einem Mitgliedstaat zur Einsichtnahme durch die Öffentlichkeit oder Personen, die ein berechtigtes Interesse nachweisen können, offensteht, die Tatsache, daß die zur Einsichtnahme berechtigte Person in einem Drittland ansässig ist und der Vorgang der Einsichtnahme ohne Datenübermittlung unmöglich ist, die Übermittlung der Informationen nicht verhindert. Entsprechend Punkt 58 ist die Übermittlung der Gesamtheit oder ganzer Kategorien der im Register enthaltenen Daten nicht gestattet. Aufgrund dieser Einschränkungen darf diese Ausnahmebestimmung nicht als allgemeine Ausnahme für die Übermittlung der Daten aus öffentlichen Registern angesehen werden. So kann beispielsweise kein Zweifel darüber bestehen, daß die massenhafte Übermittlung von Daten aus öffentlichen Registern für kommerzielle Zwecke oder die Erfassung ganzer Bestände öffentlich zugänglicher Daten zum Zwecke der Erarbeitung von Profilen bestimmter Personen von den Ausnahmebestimmungen nicht abgedeckt sind.

KAPITEL 6: VERFAHRENSFRAGEN

In Artikel 25 ist ein auf dem Einzelfall beruhendes Konzept vorgesehen, bei dem die Beurteilung der Angemessenheit sich auf die einzelne Datenübermittlung oder eine Kategorie von Datenübermittlungen bezieht. Dennoch ist natürlich klar, daß angesichts der enormen Anzahl der täglich aus der Gemeinschaft übermittelten personenbezogenen Daten und der zahllosen Akteure, die an den Übermittlungen beteiligt sind, kein Mitgliedstaat imstande ist, jeden einzelnen Fall im Detail zu prüfen, welches System er für die Umsetzung von Artikel 25 auch wählt.[19] Dies heißt natürlich nicht, daß überhaupt keine Fälle einer gründlichen Kontrolle unterzogen werden, sondern daß Mechanismen zu entwickeln sind, mit denen der Entscheidungsprozeß für eine große Anzahl von Fällen gestrafft wird, so daß die Entscheidung oder zumindest eine vorläufige Entscheidung ohne unnötige Verzögerung oder übermäßigen Aufwand getroffen werden kann.

Eine solche Rationalisierung ist unabhängig davon notwendig, wer die Entscheidung trifft - der für die Verarbeitung Verantwortliche, die Kontrollstelle oder eine sonstige vom Mitgliedstaat festgelegte Stelle.

(i) Anwendung von Artikel 25 Absatz 6 der Richtlinie

Ein Beitrag zu einem rationelleren Verfahren bestünde, wie in der in der Richtlinie vorgesehen, in der Feststellung, daß bestimmte Drittländer ein angemessenes Schutzniveau gewährleisten. Derartige Feststellungen dienten „nur der Orientierung“ und würde daher Fälle unberührt lassen, in denen es zu besonderen Schwierigkeiten kommt. Doch zumindest würde das Problem praktisch angegangen.

Mit einer solchen Feststellung würde insbesondere für die Wirtschaftsteilnehmer ein Grad von Sicherheit hinsichtlich der Länder geboten, bei denen allgemein von der Gewährleistung eines „angemessenen“ Schutzniveaus ausgegangen werden kann. Zudem würde für Drittländer, die sich noch im Prozeß der Entwicklung und Verbesserung der eigenen Schutzsysteme befinden, ein klarer und öffentlicher Anreiz gegeben. Würden obendrein mehrere solcher Feststellungen auf Gemeinschaftsebene getroffen, so wäre dies ein Beitrag zur Festlegung eines einheitlichen Ansatzes in dieser Frage, und es würde verhindert, daß von den Mitgliedstaaten bzw. den Datenschutzstellen unterschiedliche und womöglich einander widersprechende „weiße Listen“ erstellt werden.

Dieser Ansatz birgt natürlich auch Schwierigkeiten. An erster Stelle ist dabei der Aspekt zu nennen, daß viele Drittländer über keinen für alle Wirtschaftszweige einheitlich geltenden Schutz verfügen. So gibt es in vielen Staaten Datenschutzbestimmungen für den öffentlichen Sektor, jedoch nicht für die Privatwirtschaft. In einigen Ländern, beispielsweise in den USA, bestehen besondere Gesetze für bestimmte Bereiche (Meldung von Kreditaufnahmen, Unterlagen über die Ausleihe von Videos im Fall der USA), für andere hingegen nicht. Zusätzliche Schwierigkeiten existieren in Ländern mit Föderalstruktur wie den USA, Kanada und Australien, wo sich die Bestimmungen vielfach

[19] Von den Mitgliedstaaten können zur Erfüllung der Pflichten gemäß Artikel 25 unterschiedliche Verwaltungsverfahren festgelegt werden. Dazu gehört die direkte Verpflichtung des für die Verarbeitung Verantwortlichen ebenso wie die Einrichtung von Systemen zur vorherigen Genehmigung oder zur Ex-Post-Prüfung der Fakten durch die Kontrollstelle.

von Bundesstaat zu Bundesstaat unterscheiden. Wie die Bilanz zeigt, ist es derzeit nicht wahrscheinlich, daß bei vielen Drittländern generell von der Gewährleistung eines angemessenen Schutzniveaus ausgegangen werden kann. Dabei wäre die Aktion dem Anliegen, den für die Verarbeitung Verantwortlichen größere Sicherheit zu bieten, um so weniger dienlich, je kleiner die Anzahl der Länder, für die sich eine positive Feststellung treffen ließe. Weiterhin besteht die Gefahr, daß einige Drittländer die Versagung der Feststellung, daß sie ein angemessenes Schutzniveau bieten, als politische Provokation oder zumindest als politisch diskriminierend ansehen, da die Versagung der Feststellung ebenso durch das Versäumnis, die Bedingungen in dem Land überhaupt zu prüfen, wie im Ergebnis der Beurteilung des Datenschutzsystems zustande gekommen sein kann.

Nach sorgfältiger Abwägung dieser unterschiedlichen Argumente ist die Arbeitsgruppe dessen ungeachtet der Ansicht, daß es nützlich wäre, Arbeiten auf den Weg zu bringen, um die Lage zu erfassen und Feststellungen entsprechend Artikel 25 Absatz 6 zu treffen. Dabei würde es sich um einen kontinuierlichen Prozeß handeln, der nicht in einer endgültigen Liste mündet, sondern in einer Liste, die in Abhängigkeit von den Entwicklungen ständig ergänzt und überarbeitet würde. Die positive Feststellung sollte dabei grundsätzlich nicht auf Länder mit horizontalen Datenschutzgesetzen beschränkt sein, sondern auch einzelne Sektoren innerhalb eines Landes umfassen, in denen das Datenschutzniveau angemessen ist, obwohl dies in anderen Sektoren desselben Landes nicht der Fall ist.

Es sei darauf verwiesen, daß der nach Artikel 29 eingesetzten Datenschutzgruppe im Zusammenhang mit Entscheidungen zu einer bestimmten Datenübermittlung oder bei der Feststellung der „Angemessenheit“ gemäß Artikel 25 Absatz 6 keine spezielle Rolle zufällt, da in beiden Fällen das in Artikel 31 genannte Ausschußverfahren zur Anwendung kommt. Eine der speziellen Aufgaben der Datenschutzgruppe nach Artikel 29 besteht jedoch darin, gegenüber der Kommission zum Schutzniveau in der Gemeinschaft und in Drittländern Stellung zu nehmen (siehe Artikel 30 Absatz 1 Buchstabe b)). Somit gehören zum Zuständigkeitsbereich der Gruppe nach Artikel 29 durchaus auch die Beurteilung der Lage in bestimmten Drittländern und die Erarbeitung einer vorläufigen Position zum jeweiligen Schutzniveau. Um nicht wirkungslos zu bleiben, sind positive Feststellungen entsprechend Artikel 25 Absatz 6 möglichst breit bekanntzumachen. Wird andererseits festgestellt, daß ein Land nicht über ein angemessenes Schutzniveau verfügt, so bedeutet dies nicht unbedingt, daß es auf eine „schwarze Liste“ gesetzt werden müßte. Gegenüber der Öffentlichkeit müßte erklärt werden, daß es gegenwärtig nicht möglich ist, für das betreffende Land eine allgemeine Orientierung zu geben.

(ii) Risikoanalyse konkreter Übermittlungen

Obwohl die Anwendung von Artikel 25 Absatz 6, wie sie hier beschrieben wurde, im Entscheidungsprozeß bezüglich einer großen Anzahl von Datenübermittlungen eine wertvolle Hilfe ist, wird es häufig vorkommen, daß für das betreffende Land (ganz oder partiell) eine positive Feststellung nicht möglich ist. Die Art und Weise, in der die Mitgliedstaaten mit diesen Fällen umgehen, hängt davon ab, wie Artikel 25 von ihnen in einzelstaatliches Recht (siehe Fußnote auf der vorherigen Seite) umgesetzt wurde. Ist der Kontrollstelle eine konkrete Handlungsweise vorgegeben, d. h. Datenübermittlungen noch vor der eigentlichen Übermittlung zu genehmigen oder Prüfungen *ex post facto* im Nachgang vorzunehmen, dürfte es schon allein von der Menge der Übermittlungen her notwendig sein, für die Kontrollstelle ein System der Aufgabenschwerpunkte festzulegen. Ein solches System könnte aus einem vereinbarten Bündel bestimmter Kriterien bestehen, anhand derer eine Übermittlung oder Kategorie von Datenübermittlungen aufgrund der Tatsache, daß sie für die Privatsphäre des einzelnen eine besondere Gefahr darstellen, als prioritär eingestuft werden könnte.

Selbstverständlich würde sich damit nichts an der Verpflichtung jedes einzelnen Mitgliedstaats ändern, dafür zu sorgen, daß nur solche Übermittlungen zulässig sind, bei denen der Drittstaat ein angemessenes Schutzniveau gewährleistet. Es bestünde also eine Orientierung in der Frage, welche Fälle der Datenübermittlung als „vorrangige Fälle" für eine Prüfung oder sogar eine Untersuchung anzusehen sind. Damit würden auch die zur Verfügung stehenden Mittel in Richtung jener Übermittlungen gelenkt, die in puncto Schutz der betroffenen Personen besonderen Anlaß zur Besorgnis geben.

Die Arbeitsgruppe ist der Ansicht, daß bei den folgenden Kategorien von Datenübermittlungen für den Schutz der Privatsphäre ein besonderes Risiko besteht und sie daher spezieller Aufmerksamkeit bedürfen:

- Übermittlungen, bei denen auch sensible Kategorien von Datenübermittlungen entsprechend der Definition von Artikel 8 der Richtlinie weitergegeben werden;
- Übermittlungen, mit denen die Gefahr finanzieller Schädigung verbunden ist (z. B. Kreditkartenzahlung über das Internet);
- Übermittlungen, mit denen eine Gefahr für die persönliche Sicherheit verbunden ist;
- Übermittlungen zum Zwecke einer Entscheidung von erheblicher Bedeutung für die betreffende Person (z. B. Entscheidung über die Einstellung oder Beförderung, über eine Darlehensgewährung usw.);
- Übermittlungen, mit denen der Betreffende ernsthaft in eine peinliche Lage gebracht werden kann oder sein Ruf beschädigt wird;
- Übermittlungen mit dem Ergebnis bestimmter Aktionen, die in bedeutendem Maße ein Eindringen in das Privatleben darstellen, z. B. unerwünschte Telefonanrufe;
- Wiederholte Übermittlungen großer Datenbestände (wie über Fernmeldenetze, das Internet u.ä. verarbeitete Transaktionsdaten);
- Übermittlungen, bei denen unter Verwendung neuer Technologien Daten gesammelt werden und dies auf besonders verborgene oder heimliche Art geschieht (z. B. Internet-Cookies).

(i) Standardvertragsklauseln

Wie bereits in Kapitel 4 ausführlich dargestellt ist in der Richtlinie die Möglichkeit vorgesehen, daß in den Fällen, in denen das Schutzniveau nicht angemessen ist, der für die Verarbeitung Verantwortliche durch Vertragsabschluß angemessene Sicherheitsmaßnahmen herbeiführen kann. Nach Artikel 26 Absatz 2 der Richtlinie können die Mitgliedstaaten Übermittlungen auf der Grundlage von Vertragsklauseln genehmigen, wobei die Kommission anschließend von dieser Entscheidung in Kenntnis gesetzt werden muß. Bestehen gegen die Genehmigung Einwände, so kann die Kommission die Entscheidung entsprechend dem in Artikel 31 bestimmten Ausschußverfahren aufheben oder bestätigen. Doch kann die Kommission nicht nur hinsichtlich der Genehmigungen durch die Mitgliedstaaten tätig werden, sondern darf nach Artikel 26 Absatz 4 der Richtlinie auch darüber befinden, ob bestimmte Standardvertragsklauseln ausreichende Garantien bieten, wobei sie auch hier nach dem Ausschußverfahren von Artikel 31 vorgehen muß. Diese Feststellungen sind dann für die Mitgliedstaaten bindend.

Angesichts der nicht zu übersehenden Kompliziertheit vertraglicher Lösungen und der damit verbundenen Schwierigkeiten besteht zweifellos das Erfordernis, den für die Verarbeitung Verantwortlichen, die auf diese Weise mit Verträgen zu arbeiten beabsichtigen, eine abgestimmte Orientierung an die Hand zu geben. Auf der Ebene der Mitgliedstaaten tragen wahrscheinlich die zuständigen staatlichen Stellen ein Großteil der Verantwortung für diese Orientierung, insbesondere im Zusammenhang mit Genehmigungen entsprechend Artikel 26 Absatz 2. Die Behörden der Mitgliedstaaten und die Kommission sollten zusammenarbeiten und ihre Ansichten zu den ihnen vorgelegten Vertragsklauseln austauschen. Für vorgeschlagene Standardvertragsklauseln, die den Behörden der Mitgliedstaaten oder direkt der Kommission vorgelegt werden, sollte ein Verfahren entwickelt werden, mit dem gewährleistet wird, daß diese Klauseln im Interesse der Verhinderung des Entstehens voneinander abweichender einzelstaatlicher Praktiken auch von der Arbeitsgruppe geprüft werden. Bei Entscheidungen gemäß Artikel 26 Absatz 4 könnte sich die Kommission damit auf den Rat der entsprechenden Sachverständigen stützen.

ANHANG 1

ARTIKEL 25 UND 26 DER RICHTLINIE UND IHRE PRAKTISCHE AUSWIRKUNG AUF DIE ÜBERMITTLUNG PERSONENBEZOGENER DATEN IN DRITTLÄNDER

Einführung

Im Hauptteil dieser Arbeitsunterlage wird ein allgemeiner Ansatz für die Problematik der Datenübermittlung in Drittländer dargelegt und dabei auf folgendes eingegangen:

- Einschätzung des angemessenen Schutzniveaus im Sinne von Artikel 25 der Datenschutzrichtlinie
- Einschätzung alternativer Möglichkeiten zur Herbeiführung angemessener Garantien mittels vertraglicher Lösungen, wie sie in Artikel 26 Absatz 2 vorgesehen sind;
- Einschätzung der Ausnahmen vom Erfordernis des angemessenen Schutzniveaus entsprechend Artikel 26 Absatz 1.

Die Darlegung der Probleme wäre jedoch unvollständig ohne eine Beschreibung der Art und Weise, wie sich der allgemeine Ansatz dann tatsächlich auf die Übermittlung personenbezogener Daten auswirkt. In diesem Anhang werden daher einige realistische (wenn auch fiktive) Fallbeispiele für die Übermittlung von Daten so geprüft, wie dies aller Wahrscheinlichkeit mit dem Inkrafttreten der einzelstaatlichen Gesetze zur Umsetzung der Richtlinie geschehen soll.

Es werden drei Fälle vorgestellt, bei denen im ersten Schritt jeweils zu bewerten ist, ob das Schutzniveau im Bestimmungsland aufgrund der geltenden Gesetze oder der bestehenden freiwilligen Selbstkontrolle im Privatsektor als angemessen gelten kann. Ist dies nicht der Fall, so besteht der zweite Schritt darin, unter den in Artikel 26 Absatz 1 (Ausnahmen) und 2 (vertragliche Lösung) angebotenen Möglichkeiten eine Lösung für das Problem zu ermitteln. Der dritte Schritt, die Verhinderung der Übermittlung, darf nur dann getan werden, wenn keine der Lösungen geeignet ist.

FALL (1) : Datenübermittlung zur Feststellung der Kreditwürdigkeit

Ein Bürger der Gemeinschaft möchte in Land A außerhalb der EG ein Ferienhaus kaufen und stellt bei einem Kreditinstitut in jenem Land einen Kreditantrag. Vom Kreditinstitut wird daraufhin eine Auskunftei mit einer entsprechenden Recherche beauftragt. Der Auskunftei liegt zu der betreffenden Person keine Akte vor, doch läßt sie sich alle Angaben über die bisherige Kreditaufnahme dieser Person von ihrer „Schwesterauskunftei" im Vereinigten Königreich übermitteln. Bei Land A handelt es sich um ein fortgeschrittenes Industrieland mit seit langem bestehenden und stabilen demokratischen Institutionen. Das Justizsystem ist voll ausgebaut und arbeitet effektiv. Es handelt sich um einen föderal verfaßten Staat.

ERSTER SCHRITT: EINSCHÄTZUNG DER ANGEMESSENHEIT DES SCHUTZNIVEAUS

Die geltenden Vorschriften

Der für die Verarbeitung Verantwortliche unterliegt einem Bundesgesetz, das Vorschriften zu personenbezogenen Informationen zum Zwecke der Einschätzung von Kreditvergaberisiken enthält. Der für die Verarbeitung Verantwortliche behauptet zudem, eigene, öffentlich bekanntgemachte Datenschutznormen zu befolgen. Es ist keines der Gesetze der Teilstaaten anwendbar, und ein branchenweiter Selbstkontrollkodex besteht nicht.

Bewertung des Inhalts der anwendbaren Vorschriften

Zunächst sei vermerkt, daß die Mitteilung der im Vereinigten Königreich ansässigen Auskunftei wie jede andere Mitteilung an einen für die Verarbeitung Verantwortlichen im Vereinigten Königreich oder einem anderen Mitgliedstaat den normalen Anforderungen des Rechts des Vereinigten Königreichs unterworfen wäre, mit denen alle Artikel der Richtlinie mit Ausnahme der Artikel 25 und 26 umgesetzt werden. Dies ist deshalb so wichtig, weil sich dadurch die Prüfung der Rechtmäßigkeit der Mitteilung selbst erübrigt. Im Mittelpunkt der Aufmerksamkeit steht daher der Schutz der in das Land A übermittelten Daten.

Bei der Bewertung des Inhalts der Vorschriften sollte logischerweise mit der Bundesgesetzgebung begonnen werden. Werden hier Lücken festgestellt, so sind zunächst die „weniger strengen" Datenschutznormen des Unternehmens zu betrachten, um herauszufinden, ob die Lücken damit ausgefüllt werden. Danach wird eine Aufstellung zu den als notwendig erachteten inhaltlichen Punkten erarbeitet, und es wird beurteilt, ob die erforderlichen inhaltlichen Punkte im Gesetz oder in den Datenschutznormen des Unternehmens enthalten sind.

Der Grundsatz der Beschränkung der Zweckbestimmung kann in diesem Zusammenhang nur die Anforderung betreffen, daß die Sekundärnutzung und -offenlegung der übermittelten Daten mit der Zweckbestimmung, für die die Übermittlung erfolgte, nicht unvereinbar sein dürfen. Die Aufnahme der Daten in eine auf dem freien Markt zu verkaufende oder zu vermietende Versandliste dürfte ebenso als unvereinbar eingestuft

werden wie die Offenlegung der Daten gegenüber potentiellen Arbeitgebern oder an der Solvenz der betroffenen Person interessierten Geschäftspartnern. Offenlegung der Daten gegenüber Kreditgebern (Banken, Kreditkartenunternehmen) könnte hingegen als vereinbar angesehen werden.
Im hier geschilderten Fall ist im Bundesgesetz tatsächlich eine begrenzte Anzahl von Zweckbestimmungen festgelegt, bei denen die personenbezogenen Kreditinformationen legal offengelegt werden können. Zu den Zweckbestimmungen gehören „Beschäftigung" und „rechtmäßige geschäftliche Erfordernisse im Zusammenhang mit einer geschäftlichen Transaktion, an der die betroffene Person beteiligt ist." Im letztgenannten Fall umfaßt dies bestimmte Nutzungen der Daten für Marketingzwecke, die auch das Marketing von Waren oder anderen Leistungen als Kredite durch Dritte einschließen.
Daraus ergibt sich, daß die Zweckbestimmung durch das Bundesgesetz nicht ausreichend begrenzt wird und das Schutzniveau in diesem Punkt nicht ausreicht. Auch die zum Schutz der Privatsphäre vom Unternehmen für sich festgelegten Datenschutznormen tragen nicht zur Verbesserung der Lage bei.

Nach dem Grundsatz der Transparenz müßten der betroffenen Person die Identität der Auskunftei in Land A und mögliche neue Zweckbestimmungen, für die die Daten verarbeitet werden sollen, mitgeteilt werden. Die Art und Weise, in der dies geschieht, sollte der Vorgehensweise in Artikel 11 der Richtlinie vergleichbar sein.
Im vorliegenden Fall kennt das Bundesgesetz keine speziellen Transparenzvorschriften, die unmittelbar die Auskunftei betreffen würden. Allerdings muß der Kreditgeber in Land A die betroffene Person davon in Kenntnis setzen, daß er sich zwecks Kreditinformationen an eine Auskunftei wenden wird, deren Namen und Anschrift er jedoch nicht zu nennen braucht.
Für die betroffene Person ist also rechtlich nicht garantiert, daß sie darüber informiert wird, daß ihre Daten durch die betreffende Auskunftei verarbeitet werden. Da die Auskunftei mit der betroffenen Person nicht in direktem Kontakt steht, erschiene die Pflicht der Auskunftei zur Kontaktaufnahme mit der betroffenen Person mit dem speziellen Ziel ihrer Unterrichtung als „unverhältnismäßiger Aufwand" im Sinne von Artikel 11 der Richtlinie. Das Schutzniveau in bezug auf Transparenz ist also offensichtlich ausreichend.

Der Grundsatz der Datenqualität und -verhältnismäßigkeit umfaßt mehrere unterschiedliche Elemente. Im Bundesgesetz ist keine Einschränkung für die Sammlung und Verarbeitung unnötiger Daten vorgesehen. Zur Dauer der Datenspeicherung bestehen Vorschriften, mit denen die Verbreitung veralteter Informationen (mehr als zehn Jahre zurückliegende Urteile in Konkursverfahren) verhindert wird, was praktisch zur Löschung dieser Informationen führt. Zwar besteht rechtlich keine Auflage zur Führung korrekter Daten, doch stellt eine betroffene Person, die auf Antrag Zugang zu der sie betreffenden Kreditauskunft bekommen hat, einen Teil der Informationen in Frage, so sind als nichtzutreffend nachweisbare Daten zu löschen.
Erneut scheint das Schutzniveau nicht in vollem Umfang angemessen, und auch die Datenschutznormen des Unternehmens gehen über die Regelungen im Bundesgesetz nicht hinaus.

Der Grundsatz der Sicherheit spiegelt sich im Bundesgesetz in dem Erfordernis wider, geeignete Maßnahmen gegen die unrechtmäßige Datenoffenlegung zu ergreifen. Aus den Datenschutznormen des Unternehmens geht hervor, daß zur Verhinderung des unberechtigten Zugriffs auf die Kreditinformationen und ihrer Manipulation ein strenges

Kontrollsystem besteht. Hierzu werden sowohl technische Mittel (Paßwörter usw.) eingesetzt als auch die Mitarbeiter entsprechend unterwiesen, wobei eine Verletzung dieser Pflicht zu disziplinarischen Maßnahmen führen kann. Damit wäre ein angemessenes Sicherheitsniveau gewährleistet.

Das Recht auf Zugriff und Berichtigung ist bundesrechtlich geregelt und mit dem Recht, wie es diesbezüglich in der Richtlinie besteht, vergleichbar. Wurde einer betroffenen Person der Kredit verwehrt, so ist die Einsichtnahme in die Auskunft kostenlos. Es besteht kein Recht auf Widerspruch, doch kann ein Betroffener Beschwerde bei der zuständigen Bundesbehörde einreichen oder Klage vor Gericht (siehe unten) erheben, wenn seine nach dem Bundesgesetz bestehenden Rechte verletzt wurden.

Sensible Daten zum Gesundheitszustand der betroffenen Person sind Teil der übermittelten Daten. Im Bundesgesetz sind strengere Vorschriften für die Verarbeitung von Informationen im Zusammenhang mit strafrechtlichen Verurteilungen sowie zu Geschlecht, Rasse, ethnischer Herkunft, Alter und Familienstand enthalten, nicht jedoch zu Informationen über den Gesundheitszustand. In den Datenschutznormen der Auskunftei ist jedoch festgelegt, daß bei Kreditauskünften keine Gesundheitsdaten weitergegeben werden, sondern nur bei Überprüfungen im Zusammenhang mit einer beabsichtigten Einstellung oder dem Abschluß einer Versicherung. In diesen beiden Fällen wird die Verwendung dieser Daten durch die betroffene Person auf den dazu erforderlichen Vordrucken genehmigt.
Hier bestünde also für die in diesem Beispiel vorkommenden Gesundheitsdaten ein in der Sache verstärkter Schutz, auch wenn dieser Schutz vom Gesetz nicht vorgesehen ist.

Die Verwendung der Daten für Zwecke des Direktmarketing durch die Auskunftei (und die Offenlegung der Daten gegenüber anderen zu diesem Zweck) ist in diesem Zusammenhang ein wichtiger Punkt. Einer solchen Verwendung steht rechtlich nichts wirklich im Wege, und es gibt kein rechtliches Erfordernis, aus dem heraus dies verwehrt werden kann. Damit ist das Schutzniveau in diesem Punkt eindeutig unangemessen, da insbesondere in diesem Fall die Daten nicht nur durch die Auskunftei (zum Versand von Mailings an Kreditinstitute) verwendet werden, sondern auch gegenüber Dritten für das Vermarkten sowohl von finanztechnischen Produkten als auch branchenfremden Produkten wie Rasenmähern und Urlaubsangeboten offengelegt werden.

Wie es scheint, kann angesichts der Zweckbestimmung der Übermittlung eine automatisierte Entscheidung darüber getroffen werden, ob der betroffenen Person ein Kredit gewährt werden soll. Für die betroffene Person müssen daher zusätzliche Garantien bestehen. Im Bundesgesetz gibt es Bestimmungen, mit denen die betroffene Person in der Auskunft enthaltene Informationen anfechten und der Auskunft erforderlichenfalls Erklärungen beifügen kann, aber es sind keine Regelungen vorgesehen, nach denen eine auf falschen oder unvollständigen Informationen beruhende Entscheidung angefochten, überprüft und, sollten sich die Einwände als berechtigt erweisen, geändert werden kann. Mit diesem Mechanismus können an einer Auskunft zwar Änderungen vorgenommen werden, um Probleme in der Zukunft zu vermeiden, doch wird das Problem einer bereits getroffenen Kreditentscheidung damit nicht unbedingt angesprochen. Dieser rückwirkende Rechtsschutz ist nicht ausreichend, da nicht vorhanden.

Beschränkungen der Weiterübermittlung der Daten an ein weiteres Drittland oder an Organisationen in anderen, den Vorschriften im Bundesgesetz nicht unterstellten Sektoren

in Land A. Weder im Bundesgesetz noch in den Datenschutznormen des Unternehmens ist derartiges vorgesehen.

Anwendungsbereich des Bundesgesetzes und der Datenschutznormen des Unternehmens
In einem weiteren Kontrollgang ist sicherzustellen, daß sowohl das Bundesgesetz als auch die Datenschutznormen des Unternehmens für die Daten aller betroffenen Personen und nicht nur für die Daten der Staatsangehörigen oder Bürger des Landes A gelten. Im vorliegenden Fall besteht eine solche Beschränkung des Anwendungsbereichs nicht.

Bewertung der Wirksamkeit des Schutzes

Das betreffende Bundesgesetz ist geltendes Recht, und nach seinen Bestimmungen ist auch eine öffentliche Stelle mit bestimmten externen Überwachungsbefugnissen eingerichtet worden. Zur Durchsetzung ihrer Rechte können die betroffenen Personen den Rechtsweg einschlagen. Allerdings ist die öffentliche Stelle nicht eindeutig dazu verpflichtet, sämtlichen Beschwerden von betroffenen Personen nachzugehen, und einigen Kommentatoren zufolge hat sie sich bei der Durchsetzung des Rechts auch nicht immer durch besondere Aktivität ausgezeichnet. Klagen vor Gericht zur Wiedergutmachung sind für die betroffenen Personen kostspielig und häufig auch zeitaufwendig - dies besonders dann, wenn die betroffene Person in einem anderen Land wohnt als in dem, wo das Gerichtsverfahren stattfindet.

Die Datenschutznormen des Unternehmens enthalten keinen eigenständigen Mechanismus, mit dem Betroffene ihre Rechte durchsetzen können, doch sind disziplinarische Strafen für Mitarbeiter vorgesehen, die die Grundsätze verletzen. Mehrere Beschäftigte sind bereits wegen entsprechender Vergehen disziplinarisch zur Verantwortung gezogen worden.

Die Kombination von gesetzlichen Regelungen und unternehmensinternen Datenschutznormen muß anhand der für die verfahrensrechtlichen Mechanismen festgelegten „Ziele“ bewertet werden. Im vorliegenden Fall könnten folgende Schlüsselfragen geprüft werden:

Allgemein hohes Einhaltungsniveau

Für das Unternehmen besteht der Hauptanreiz zur Einhaltung der eigenen Datenschutznormen in der Gefahr eines negativen Echos in der Presse, sollte festgestellt werden, daß es sich nicht an die eigenen Vorgaben hält. Zudem werden den Mitarbeitern des Unternehmens für den Fall der Verletzung der Sicherheitsvorschriften disziplinarische Maßnahmen angedroht.
Indes reichen diese Mechanismen allein wahrscheinlich nicht aus, um die Einhaltung der Datenschutznormen in der Praxis zu gewährleisten.
Diese Schlußfolgerung würde anders ausfallen, wenn:
(1) die Datenschutznormen des Unternehmens ihren Ausdruck in einem branchenweiten, vom Fachverband erarbeiten Verhaltenskodex gefunden hätten, nach dessen Bestimmungen ein Unternehmen, das gegen den Kodex verstößt, sofort aus dem Fachverband ausgeschlossen würde oder
(2) es nach einem allgemeinen Rechtsgrundsatz möglich wäre, von einer staatlichen Stelle gegen Unternehmen, die die eigenen veröffentlichen Datenschutznormen verletzen, wegen „unlauterer und betrügerischer“ Geschäftspraktiken strafrechtlich vorzugehen.

Was das Bundesgesetz angeht, so wird die Einhaltung dadurch gefördert, daß vom Betroffenen im Falle der Nichteinhaltung Klage erhoben werden kann. Die Aussicht, vor Gericht auf der Anklagebank zu sitzen, dürfte auf den für die Verarbeitung Verantwortlichen einen gewissen abschreckenden Effekt ausüben. Allerdings ist die Wahrscheinlichkeit einer direkten externen Prüfung der Datenverarbeitungsverfahren sehr gering, da die staatliche Stelle erst reagiert, wenn sie beispielsweise durch den Beschwerdeführer oder die Presse darauf aufmerksam gemacht wird.

Unterstützung und Hilfe für einzelne betroffene Personen
Es ist eindeutig so, daß eine staatliche Stelle vorhanden ist, bei der betroffene Personen Beschwerde gegen die für sie erstellten Kreditauskünfte einlegen können. Die Kosten der Untersuchungen im Zusammenhang mit der Beschwerde braucht die betroffene Person nicht zu tragen.

Angemessene Entschädigung
Zwar hat im Falle der Verletzung der recht enggefaßten Regelungen im Bundesgesetz die betroffene Person die Möglichkeit, eine Wiedergutmachung auf dem Gerichtswege durchsetzen, doch ist dies ein relativ kostspieliges Unterfangen, und häufig fehlt es hierbei an Unterstützung durch die staatliche Stelle. Das Gericht kann den für die Verarbeitung Verantwortlichen zur Leistung von Schadenersatz verurteilen (sofern es der Meinung ist, daß eine Schädigung erfolgte) und ihn anweisen, die Datenverarbeitungsverfahren und den Inhalt der betreffenden Kreditkartei zu ändern. Für die Verletzung der lediglich in den internen Datenschutznormen festgelegten Datenschutzgrundsätze ist eine solche Entschädigung nicht möglich.

Der Urteilsspruch

1) Etliche der Datenschutzgrundsätze, die im Diskussionspapier als „Kerngrundsätze“ herausgearbeitet wurden, finden sich in der einen oder anderen Form im für die Kreditkartei geltenden Bundesgesetz, während andere in den Datenschutznormen des Unternehmens verankert sind. Doch auch wenn beide zusammen betrachtet werden, kann nicht behauptet werden, daß sämtliche „Kerngrundsätze“ vorkommen. Selbst bei denen, die vorhanden sind (z. B. der Grundsatz der Beschränkung der Zweckbestimmung), sind einige nur in relativ abgeschwächter Form anzutreffen.
2) Hier ergibt sich als allgemeineres Problem die Frage, ob die Datenschutznormen des Unternehmens überhaupt als ausreichend wirksamer Mechanismus in Betracht gezogen werden können. Werden die Datenschutznormen nicht dadurch untermauert und durchsetzbarer gemacht, daß dem Fachverband oder einer staatlichen Stelle die Befugnis zur externen Kontrolle übertragen wird, so sind die Bestimmungen dieser Normen größtenteils nicht durchsetzbar und brauchen daher nicht berücksichtigt zu werden.
3) Auch wenn die zur Durchsetzung des Bundesrechts eingerichtete öffentliche Stelle nicht ganz mit denselben Befugnissen ausgestattet ist wie die typische Datenschutzbehörde in Europa, so bietet sich durch das Gesetz eine gewisse Rechtssicherheit, was insbesondere auf das gut funktionierende Rechtssystem und die „Prozeßkultur“ in Land A zurückzuführen ist. Das Gesetz enthält klar formulierte Vorschriften zum möglicherweise wichtigsten aller Datenschutzgrundsätze, dem Recht auf Zugriff und Berichtigung, und es grenzt die Zweckbestimmung der Datenverarbeitung in gewissem Maße ein.

Schlußfolgerung

Das Schutzniveau ist unangemessen, da das Gesetz zu wenige der „Kerngrundsätze“ beinhaltet, und die unternehmensinternen Datenschutznormen sind für sich allein genommen kein wirksames Mittel zur Gewährleistung von Schutz. Der Urteilsspruch könnte auf Angemessenheit lauten, wenn das Gesetz in Richtung solcher Grundsätze wie Transparenz und Schutz von Daten zum Gesundheitszustand ausgebaut oder die unternehmensinternen Datenschutznormen mit Hilfe einer der vorgeschlagenen Methoden wirksamer gestaltet werden (d. h. Einhaltung als Voraussetzung für die Mitgliedschaft im Fachverband oder Bevollmächtigung einer staatlichen Stelle zur strafrechtlichen Verfolgung des Unternehmens wegen irreführender und betrügerischer Geschäftspraktiken im Falle der Verletzung der eigenen Datenschutznormen).

ZWEITER SCHRITT: LÖSUNGSSUCHE

Von den in Artikel 26 Absatz 1 genannten möglichen Ausnahmen kommt nur der die Einwilligung der betroffenen Person betreffende Buchstabe a) in Frage. Die in Buchstabe b) geregelte Ausnahme im Interesse der Erfüllung eines Vertrags ist nicht anwendbar, da zwischen der übermittelnden Partei, der im Vereinigten Königreich ansässigen Auskunftei, und der betroffenen Person kein Vertragsverhältnis besteht. Auch kann schwerlich darauf verwiesen werden, daß die Übermittlung zur Erfüllung eines Vertrags „im Interesse der betroffenen Person“ erforderlich sei, wie dies für die Ausnahme in Buchstabe c) geregelt ist.

Mit der Einwilligung durch die betroffene Person würde für das Problem jedoch eine relativ unkomplizierte Lösung gefunden. Die Einwilligung könnte entweder direkt durch die im Vereinigten Königreich ansässige Auskunftei oder in ihrem Auftrag durch das Kreditinstitut in Land A erlangt werden, das hierzu die betroffene Person auf dem Kreditantragsformular um Einwilligung ersuchen könnte. Unabhängig vom gewählten Verfahren sollte die betroffene Person von den konkreten Gefahren in Kenntnis gesetzt werden, die mit der Übermittlung der Daten in ein Land ohne angemessenes Schutzniveau verbunden sind.

Solange Übermittlungen dieser Art noch relativ selten sind, besteht die zweckmäßigste Methode wahrscheinlich darin, die Einwilligung jeweils einzeln einzuholen. Kommt es jedoch zu einem systematischeren weltweiten Datenaustausch mit Auskunfteien, so können andere Vorkehrungen, wie vertragliche Lösungen oder ein internationaler Verhaltenskodex, getroffen werden.

FALL (2) : Übermittlung sensibler Daten in der Luftfahrt

Ein portugiesischer Bürger bucht in einem Lissabonner Reisebüro einen Flug an Bord einer Maschine einer in Land B ansässigen Luftfahrtgesellschaft. Dabei wird u. a. erfaßt, daß der Bürger behindert ist und einen Rollstuhl benutzt. Die Daten werden in ein internationales Computerreservierungssystem eingegeben und von dort durch die Fluggesellschaft in ihre Passagierdatenbank in Land B heruntergeladen, in der sie auf unbegrenzte Zeit gespeichert werden. Von der Fluggesellschaft werden die Daten abgesehen von internen Planungszwecken dazu verwendet, die Dienstleistung für den Passagier bei künftigen Flügen mit dieser Fluggesellschaft zu verbessern.[20]

ERSTER SCHRITT: EINSCHÄTZUNG DER ANGEMESSENHEIT DES SCHUTZNIVEAUS

Die geltenden Vorschriften

In bezug auf die Daten in der Datenbank der Fluggesellschaft in Land B bestehen keine Datenschutzbestimmungen, obwohl es für Daten in Computerreservierungssystemen einen internationalen Verhaltenskodex gibt.

Bewertung des Inhalts der anwendbaren Vorschriften

Es sind keine Vorschriften anwendbar.

Bewertung der Wirksamkeit des Schutzes

Nicht zutreffend

Der Urteilsspruch

Das Schutzniveau in Land B ist insbesondere angesichts der Sensibilität der Daten nicht angemessen.

ZWEITER SCHRITT: LÖSUNGSSUCHE

Die Übermittlung der Daten an das Computerreservierungssystem und ihre Verwendung durch die Fluggesellschaft zum Zwecke der Erbringung der entsprechenden Dienstleistung für den behinderten Passagier im Zusammenhang mit dem betreffenden Flug stellt eine Übermittlung dar, die für die Erfüllung des Vertrags zwischen dem Passagier und der Fluggesellschaft (Artikel 26 Absatz 1 Buchstabe b)) erforderlich ist. Für den weiteren Verbleib der Daten (einschließlich sensibler Daten zum Gesundheitszustand der betroffenen Person) in der Datenbank der Fluggesellschaft ist dies jedoch kein Grund. Folglich muß die Übermittlung der Daten an die Fluggesellschaft von einer anderen Ausnahmeregelung abgedeckt sein.

---

[20] Dieser Fall weist gewissen Ähnlichkeiten mit einem tatsächlich geschehenen Fall auf, der schwedischem Recht unterliegt und in den amerikanische Fluggesellschaften und die Lufthansa verwickelt sind. Gegenwärtig läuft das Berufungsverfahren.

Wie in Fall (1) wäre die Einwilligung der betroffenen Person die beste Lösung. Sie könnte vom Reisebüro in Lissabon im Namen der Fluggesellschaft eingeholt werden. Dabei sollten der betroffenen Person die mit der Speicherung der Daten in Land B verbundenen Risiken ebenso mitgeteilt werden wie die Tatsache, daß die Übermittlung und die Speicherung der Daten in der Datenbank der Fluggesellschaft aus Gründen, die mit dem gebuchten Flug in Verbindung stehen, nicht erforderlich sind.

FALL (3): Übermittlung von Daten für Marketinglisten

Ein Unternehmen in den Niederlanden ist auf die Erstellung von Versandlisten spezialisiert. Unter Verwendung der Vielzahl unterschiedlicher Quellen, die es in den Niederlanden für öffentliche Informationen gibt, sowie von Kundenverzeichnissen von anderen niederländischen Unternehmen entstehen Listen, in denen Personen aufgeführt sind, die einem bestimmten sozio-ökonomischen Profil entsprechen. Verkauft werden diese Listen an die Kunden dieser Firma nicht nur in den Niederlanden und der EU, sondern auch in zahlreichen Drittländern. Die Empfängerunternehmen nutzen die Listen (in denen die Postanschrift, die Telefonnummer und häufig auch die E-Mail-Adresse angegeben sind), um mit den in den Listen aufgeführten Personen in Kontakt zu treten und ihnen die unterschiedlichsten Erzeugnisse und Dienstleistungen zu verkaufen. Sehr viele der auf den Listen genannten Personen haben bei der niederländischen Datenschutzbehörde Beschwerde gegen die Marketingangebote eingelegt.

Die geltenden Vorschriften

Einige der Unternehmen, die die Versandlisten der niederländischen Firma kaufen, sind in Ländern ansässig, in denen allgemeine gesetzliche Datenschutzvorschriften gelten, die das Recht der betroffenen Personen beinhalten, die Entgegennahme von Marketingangeboten zu verwehren. Andere befinden sich in Ländern ohne derartige gesetzliche Regelungen, sind jedoch Mitglied von Selbstkontrollvereinigungen, von denen Datenschutzkodizes erarbeitet worden sind. Weitere Firmen unterliegen überhaupt keinen Datenschutzvorschriften.

Bewertung des Inhalts der anwendbaren Vorschriften

In diesem Fall müßten zahllose Gesetze und Kodizes bewertet werden. Bleibt die in den Niederlanden ansässige Firma ihrem Grundsatz treu, ihre Listen an Unternehmen in jedem beliebigen Land der Welt zu verkaufen bzw. zu vermieten, so kommt es zwangsläufig zu Situationen, in denen das Schutzniveau nicht angemessen ist.

ZWEITER SCHRITT: LÖSUNGSSUCHE

Im vorliegenden Beispiel wäre es für die niederländische Firma kaum möglich, die Einwilligung jeder einzelnen Person zur Aufnahme in die Versandlisten zu erlangen, da die stammen die Daten aus öffentlichen Quellen stammen und ohne direkten Kontakt mit der betroffenen Person erfaßt wurden. Es ist daher nicht wahrscheinlich, daß hier eine der Ausnahme von Artikel 26 Absatz 1 greift.

Der niederländischen Firma stehen zwei Möglichkeiten offen, die sie alternativ oder im Verbund nutzen kann. Zum einen könnte sie den Handel mit den Versandlisten auf Unternehmen in Ländern begrenzen, in denen aufgrund von gesetzlichen Regelungen bzw. entsprechenden Instrumenten der freiwilligen Selbstkontrolle eindeutig feststeht, daß ein angemessenes Schutzniveau gewährleistet ist. Bei der Entscheidung könnte sich die Firma an möglicherweise bestehenden „weißen Listen“ orientieren.

Als zweite Möglichkeit könnten von allen Kunden (oder zumindest von den Kunden in Ländern mit „unangemessenem“ Schutzniveau) vertragliche Verpflichtungen hinsichtlich der übermittelten Daten gefordert werden. Bei den vertraglichen Regelungen sollten die in Kapitel 4 des Haupttextes gegebenen Hinweise befolgt werden. Insbesondere sollte dabei gesichert werden, daß die niederländische Firma gemäß niederländischem Recht für alle Verletzungen der Datenschutzgrundsätze seitens der Empfängerunternehmen der übermittelten Versandlisten haftbar bleibt.

Mit einer solchen vertraglichen Lösung würde bei ordnungsgemäßer Umsetzung ein Beitrag zur Überwindung des Handelshemmnisses geleistet, das das Fehlen eines angemessenen Schutzniveaus in bestimmten Drittländern darstellt.

Geschehen zu Brüssel am 24. Juli 1998

Für die Arbeitsgruppe

Der Vorsitzende

P. J. HUSTINX