EUROPÄISCHE KOMMISSION
GENERALDIREKTION XV
Binnenmarkt und Finanzdienstleistungen
Freier Verkehr von Informationen; Gesellschaftsrecht und finanzielle Informationen
Freier Verkehr von Informationen und damit zusammenhängende internationale Aspekte

DG XV D/5005/98 endg.
WP9

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

Arbeitsunterlage: Erste Überlegungen zur Verwendung vertraglicher Bestimmungen im Rahmen der Übermittlungen personenbezogener Daten an Drittländer

Von der Arbeitsgruppe am 22. April 1998 angenommen

Die Verwendung vertraglicher Bestimmungen im Rahmen von Übermittlungen personenbezogener Daten an Drittländer

1. Einführung

In der von der Datenschutzgruppe am 26. Juni 1997 angenommenen Diskussionsgrundlage mit dem Titel "Erste Leitlinien für die Übermittlung personenbezogener Daten in Drittländer - mögliche Ansätze für eine Bewertung der Angemessenheit" hat die Arbeitsgruppe versprochen, in ihrer künftigen Arbeit zu prüfen, unter welchen Voraussetzungen vertragliche *ad hoc*-Lösungen ein geeignetes Mittel für den Schutz von Personen sein können, wenn personenbezogene Daten in ein Drittland übermittelt werden, in dem das Schutzniveau nicht generell angemessen ist. Dieses Dokument ist als Grundlage für eine solche Prüfung gedacht.

Nach Artikel 25 Absatz 1 der Datenschutzrichtlinie (95/46/EG) gilt der Grundsatz, daß die Übermittlung personenbezogener Daten lediglich erfolgen soll, wenn dieses Drittland ein angemessenes Schutzniveau gewährleistet. Artikel 26 Absatz 1 enthält bestimmte Ausnahmen von dieser Regel. Diese Ausnahmen werden in diesem Papier nicht geprüft. Hier soll die zusätzliche 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". Artikel 26 Absatz 4 befugt ferner die Kommission, wenn sie nach dem Verfahren des Artikels 31 tätig wird, 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 über die Frage verantwortlich.[1] 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. Verträge sind auch weiterhin als ein Mittel der Behandlung von Datenschutzproblemen eingesetzt worden, die sich aus der Ausfuhr personenbezogener

[1] "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

Daten aus bestimmten EU-Mitgliedstaaten ergeben. Seit den späten 80er Jahren sind sie in Frankreich häufig verwendet worden. In Deutschland fand das jüngste Beispiel des "BahnCard"-Falls, an dem die Citibank beteiligt war, große Beachtung.[2]

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 und zu regeln, wenn mehr als eine Stelle an der betreffenden Datenverarbeitung beteiligt ist. Nach der Richtlinie hat eine Einheit, der "für die Verarbeitung Verantwortliche" die Hauptverantwortung für die Erfüllung der substantiellen Grundsätze des Datenschutzes zu übernehmen. Die zweite Einheit, der "Auftragsverarbeiter", ist lediglich für die Datensicherheit zuständig. Von einem "für die Verarbeitung Verantwortlichen" wird gesprochen, wenn eine Person die Beschlußfassungsbefugnis über die Zweckbestimmung und die Mittel der Datenverarbeitung besitzt, während der "Auftragsverarbeiter" lediglich die Stelle ist, die den Datenverarbeitungsdienst materiell erbringt. Die Beziehung zwischen den beiden wird durch Artikel 7 Absatz 3 der Richtlinie geregelt, der 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 jede die für den für die Verarbeitung Verantwortlichen tätige Person, einschließlich des Auftragsverarbeiters selbst, personenbezogene Daten nur auf Weisung des für die Verarbeitung Verantwortlichen verarbeiten darf (außer bei entsprechenden gesetzlichen Verpflichtungen).

Bei der Übermittlung personenbezogener Daten in Drittländer wird normalerweise auch mehr als eine Partei betroffen sein. Hier ist die betreffende Beziehung eine Beziehung zwischen der die Daten übermittelnden (dem "Übermittler") und der Stelle, die die Daten im Drittland erhält (dem "Empfänger"). Dabei sollte ein Zweck des Vertrags darin bestehen, festzulegen, wie die Zuständigkeit für die Einhaltung des

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

Datenschutzes auf die beiden Seiten verteilt wird. Der Vertrag hat aber noch viel mehr zu leisten: er muß zusätzliche Sicherheiten für die betroffene Person bieten, die dadurch erforderlich werden, daß für den Empfänger im Drittland kein durchsetzbares Regelwerk von Datenschutzbestimmungen zur Verfügung steht, 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 übermittelt werden (und somit außerhalb des durch die Richtlinie und natürlich durch das allgemeine Regelwerk des Gemeinschaftsrechts vorgesehenen Schutzes[3]) in ein Drittland übermittelt werden, in dem kein angemessenes allgemeines Schutzniveau vorhanden ist. Eine Vertragsbestimmung, die diese Funktion erfüllen soll, muß einen befriedigenden Ausgleich für das Fehlen eines allgemeinen angemessenen Schutzniveaus bieten, indem sie die wesentlichen Elemente des Schutzes enthält, die in einer bestimmten besonderen Situation fehlen.

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 bereits ausführlich in der Unterlage "Erste Leitlinien für die Übermittlung personenbezogener Daten in Drittländer - mögliche Ansätze für eine Bewertung der Angemessenheit" eingegangen wurde.[4] In diesem Dokument wird ein Ansatz dargelegt, der sich auf eine Reihe von Grundsätzen des Datenschutzes und drei weitere Erfordernisse stützt: eine gute Befolgungsrate der Bestimmungen muß vorliegen, Unterstützung und Hilfe für einzelne betroffene Personen bei der Wahrnehmung ihrer Rechte muß zur Verfügung stehen, und es muß eine angemessene Entschädigung für die geschädigte Partei geben, wenn die Bestimmungen nicht eingehalten werden.

(i) *Die wesentliche Datenschutzbestimmungen*

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

1) **Der Grundsatz der Beschränkung der Zweckbestimmung -** Daten sind für einen spezifischen Zweck zu verarbeiten und dementsprechend nur insofern zu verwenden

---

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

[4] "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.

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 (u.a. Staatssicherheit, Ermittlung von Straftaten).[5]

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

3) **Der Grundsatz der Transparenz** - natürliche Personen müssen Informationen über die Zweckbestimmung der Verarbeitung und die Identität des im Drittland für die Verarbeitung Verantwortlichen sowie andere Informationen erhalten, sofern dies aus Billigkeitsgründen erforderlich ist. Ausnahmen sind lediglich im Einklang mit den Artikeln 13 oder 11 Absatz 2 der Richtlinie möglich, der Organisationen, die Daten nicht direkt von der betroffenen Person erfaßt haben, die Möglichkeit bietet, von dem Erfordernis der Unterrichtung der betroffenen Person befreit zu werden, wenn diese Information unverhältnismäßigen Aufwand erfordert oder unmöglich ist.

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) **Die Rechts 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 der sie betreffenden Daten einlegen können. Die einzigen Ausnahmen von diesen Rechten müssen mit Artikel 13 der Richtlinie im Einklang stehen.

6) Beschränkungen der Weiterübermittlung an Nichtvertragspartner - 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.

Darüber hinaus sind in einigen Situationen weitere Grundsätze anzuwenden:

1) **sensible Daten** - sind ‘sensible’ Kategorien von Daten betroffen (in Artikel 8 aufgelistet), so müssen zusätzliche Sicherheiten eingeführt werden, wie das Erfordernis, daß die betroffene Person ausdrücklich in die Verarbeitung einwilligt.

---

[5] Anzumerken ist, daß statistische Zwecke und Zwecke der wissenschaftlichen Forschung im allgemeinen unter der Voraussetzung als vereinbar angesehen werden, daß geeignete Sicherheiten bestehen.

2) D**irektmarketing -** 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 verwehren.

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 natürlichen Person zu schützen.

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 Situationen - wenn beispielsweise der Schutz in einem Drittland durch ein allgemeines Datenschutzgesetz vorgesehen ist, das der Richtlinie ähnelt - sind wahrscheinlich andere Mechanismen vorhanden, die klären, in welcher Art und Weise die Datenschutzvorschriften in der Praxis Anwendung finden (Verhaltenskodexe, Notifizierung, beratende Funktion der Aufsichtsbehörde). In einer vertraglichen Situation ist dies nicht der Fall. Details sind deshalb von imperativer Bedeutung, wenn die Übermittlung auf der Grundlage eines Vertrags erfolgt.

(ii) Den substantiven Vorschriften Geltung verschaffen

Das Dokument "Erste Leitlinien…" legt für die Beurteilung der Effizienz eines Datenschutzsystems drei Kriterien dar. Diese Kriterien sind die Fähigkeit des Systems:
1) eine **gute Befolgungsrate** der Vorschriften zu gewährleisten. (Kein System kann eine 100%-ige Einhaltung garantieren, einige sind aber besser als andere). Ein gutes System 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 Durchsetzung sehr stark bewußt sind. Die Existenz wirksamer, abschreckender Sanktionen ist wichtig, um die Einhaltung der Bestimmungen sicher zu stellen; ebenso wichtig sind natürlich Systeme der direkten Überprüfung durch Behörden, Buchprüfer oder unabhängige Datenschutzbeauftragte.

2) **Unterstützung und Hilfe für einzelne betroffene Personen** bei der Wahrnehmung ihrer Rechte bereitzustellen. Jeder Einzelne muß seine Rechte rasch und wirksam, ohne überhöhte Kosten durchsetzen können. Dafür muß es eine Art Struktur oder Mechanismus geben, die eine unabhängige Prüfung der Beschwerden ermöglichen.

3) **eine angemessene Entschädigung** für die geschädigte Partei vorzusehen, wenn die Bestimmungen nicht eingehalten werden. Für dieses Schlüsselelement muß es ein System unabhängiger Schlichtung geben, das die Zahlung einer Entschädigung und gegebenenfalls die Auferlegung von Sanktionen ermöglicht.
Dieselben Kriterien müssen bei der Beurteilung der Effizienz einer vertraglichen Lösung gelten. Dies ist natürlich eine große, allerdings nicht unmögliche 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 bieten.

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

Bereitstellung einer Entschädigung für eine betroffene Person

Einer betroffenen Person über einen Vertrag zwischen dem "Übermittler" der Daten und dem "Empfänger" Rechtshilfe bereitzustellen (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. Voraussichtlich wird das anwendbare Recht im allgemeinen 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.
Allgemeine Regel ist allerdings, daß die Rechtssicherheit für die betroffene Person 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. Führt man sich vor Augen, daß es um Fälle unangemessenen allgemeinen Schutzes geht, so wäre die Lösung vorzuziehen, daß der Vertrag die Art und Weise festlegt, in der der Empfänger die Basisprinzipien des Datenschutzes anzuwenden hat, und zwar so detailliert, daß der Empfänger der Übermittlung tatsächlich keine autonome Beschlußfassungsbefugnis im Hinblick auf die übermittelten Daten oder die Art und Weise besitzt, in der diese anschließend verarbeitet werden. Der Empfänger hat nur nach Anweisung des Übermittlers zu handeln; wenn die Daten möglicherweise materiell aus der Europäischen Union übermittelt worden sind, bleibt die Beschlußfassungskontrolle über die Daten 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 unter diesen Voraussetzungen das Recht des betreffenden Mitgliedstaats weiter für die in dem Drittland erfolgte Verarbeitung[6] und 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.[7]
Diese Art der Übereinkunft ist der nicht unähnlich, die in der interterritorialen Vereinbarung ausgeführt wurde, mit der der zuvor erwähnte Citibank-BahnCard-Fall gelöst wurde. Hier enthielt die vertragliche Vereinbarung die Anordnungen für die Datenverarbeitungen im Detail, insbesondere im Hinblick auf die Datensicherheit, und schloß alle anderen Nutzungen der Daten durch den Empfänger der Übermittlung aus. Das deutsche Recht fand auf die in dem Drittland erfolgte Datenverarbeitung Anwendung und stellte damit Rechtsmittel für die betroffenen Personen sicher.[8]

---

6 Aufgrund von Artikel 4 Absatz 1 Buchstabe a der Richtlinie 95/46/EG.

7 Vgl. Artikel 23 der Richtlinie 95/46/EG.

8 Weil dieser Fall sich auf der Grundlage eines Gesetzes ergab, das vor der Richtlinie galt, fand die Rechtsvorschrift selbst nicht automatisch Anwendung auf alle Verarbeitungen Anwendung, die durch einen in Deutschland niedergelassenen, für die Verarbeitung

Natürlich wird es Fälle geben, in denen diese Art der Lösung nicht möglich ist. Der Empfänger der Übermittlung erbringt vielleicht nicht nur einen reinen Datenverarbeitungsdienst für den Verantwortlichen mit Sitz in der Europäischen Union. Der Empfänger kann beispielsweise die Daten für eine Nutzung für seinen eigenen Gewinn oder für seine eigenen Zwecke gemietet oder erworben haben. Unter diesen Umständen benötigt der Empfänger einen gewissen Handlungsspielraum, um die Daten nach seinem Belieben zu verarbeiten, und wird eigentlich zu einem Verantwortlichen der Daten in seinem eigenen Recht.

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 Rechtshilfe bereitzustellen. Wie oben erwähnt wurde, erlauben einige Rechtssysteme Dritten, Vertragsrechte geltend zu machen, und dies könnte genutzt werden, um Rechte einer betroffenen Person über einen offenen, veröffentlichten Vertrag zwischen Übermittler und Empfänger zu begründen. Die Position der betroffenen Personen würde weiter gestärkt, wenn die Parteien sich als Teil des Vertrages selbst zu einer Art zwingender Schlichtung für den Fall verpflichten, daß eine betroffene Person die Vertragserfüllung in Frage stellt. Einige sektorspezifische, selbstregulierende Kodexe enthalten derartige Schlichtungsmechanismen, und die Verwendung von Verträgen in Verbindung mit derartigen Kodexen könnte nutzbringend in Erwägung gezogen werden.

Eine andere Möglichkeit besteht darin, daß der Übermittler, vielleicht zum Zeitpunkt des ersten Erhaltens der Daten von der betroffenen Person, mit der betroffenen Person eine eigene vertragliche Vereinbarung schließt, die festlegt, daß er (der Übermittler) für jeden Schaden oder Notfall haftbar bleibt, der dadurch entsteht, daß der Empfänger einer Datenübermittlung das vereinbarte Paket der Grundprinzipien des Datenschutzes nicht einhält. So werden der betroffenen Person für die Delikte des Empfängers Rechtsmittel gegenüber dem Übermittler garantiert. Es ist dann Sache des Übermittlers, mögliche Entschädigungen, zu deren Zahlung an die betroffene Person er genötigt war, anschließend über Maßnahmen wegen Vertragsbruchs gegen den Empfänger zurückzufordern.

Eine derartige Drei-Wege-Lösung ist vielleicht machbarer, als dies scheinen mag. Der Vertrag mit der betroffenen Person könnte Teil der Standardbedingungen werden, mit denen beispielsweise eine Bank oder ein Reisebüro ihren Kunden Dienstleistungen bereitstellen. Sie hat den Vorteil der Transparenz: Die betroffene Person wird über ihre Rechte voll informiert.

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

Unterstützung und Hilfe für betroffene Personen

Verantwortlichen kontrolliert wurden. Die Rechtshilfe für die betroffene Person wurde durch die Möglichkeit des deutschen Vertragsrechts geschaffen, Rechte Dritter zu begründen.

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 Einzelproblems, 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.[9] Deshalb muß für ein angemessenes Schutzniveau eine Art von institutionellem Mechanismus vorhanden sein, der eine unabhängige Untersuchung von Beschwerden ermöglicht.

Die Überwachungs- und Untersuchungsfunktion einer Kontrollbehörde eines Mitgliedstaats beschränkt sich auf die Datenverarbeitung, die im Hoheitsgebiet des Mitgliedstaats erfolgt.[10] Werden Daten in einen anderen Mitgliedstaat übermittelt, so gewährleistet ein System der gegenseitigen Unterstützung der Kontrollbehörden, 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 Ausgleichmechanismus im Rahmen einer Datenübermittlung auf der Grundlage eines Vertrags geplant werden kann.

Eine Möglichkeit wäre es, lediglich eine vertragliche Klausel zu fordern, die der Kontrollbehörde 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 Kontrollbehörde ernannten Vertreter vorgenommen werden (beispielsweise eine spezialisierte Buchprüferfirma). Bei diesem Ansatz besteht allerdings das Problem, daß die Kontrollbehörde nicht generell[11] Vertragspartei ist und somit in einigen Rechtssystemen den Vertrag nicht geltend machen kann, um Zugriff zu erhalten. Eine andere Möglichkeit wäre eine gesetzliche Verpflichtung des Empfängers im Drittland unmittelbar gegenüber der entsprechenden Kontrollbehörde des EU-Mitgliedstaats, mit der der Empfänger der Daten einwilligt, der Kontrollbehörde oder einem benannten Vertreter im Fall einer vermuteten Nichterfüllung der Grundsätze des Datenschutzes den Zugriff zu erlauben. Diese Verpflichtung könnte auch die Forderung umfassen, daß die an der Datenübermittlung Beteiligten die Kontrollbehörde 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 Kontrollbehörde eines EU-Mitgliedstaats machbar ist, die Zuständigkeit für eine Untersuchung und Überprüfung der Datenverarbeitung zu übernehmen, die in einem Drittland erfolgt.

---

9 Auch wenn einer betroffenen Person Rechte durch einen Vertrag garantiert werden, wird sie oft nicht in der Lage sein, zu beurteilen, ob ein Vertragsbruch vorliegt und wenn, durch wen. Dafür ist ein Untersuchungsverfahren außerhalb der formellen zivilrechtlichen Verfahren erforderlich.

10 Vgl. Artikel 28 Absatz 1 der Richtlinie 95/46/EG.

11 Die französische Delegation könnte sich Situationen vorstellen, in denen die Kontrollbehörde Vertragspartner ist.

Eine gute Befolgungsrate gewährleisten

Auch wenn keine Beschwerde oder kein Problem einer betroffenen Person vorliegt, ist das Vertrauen nötig, daß die Vertragsparteien den Vertrag tatsächlich erfüllen. Das Problem bei der vertraglichen Lösung ist die Schwierigkeit, Sanktionen für die Nichterfüllung festzulegen, die stark genug sind, um die abschreckende Wirkung zu haben, die für das Herstellen dieses Vertrauens erforderlich ist. Auch in Fällen, in denen eine tatsächliche Kontrolle über die Daten weiterhin von innerhalb der Gemeinschaft ausgeübt wird, wird der Empfänger der Übermittlung möglicherweise keiner direkten Strafe unterworfen, wenn er Daten in Zuwiderhandlung gegen den Vertrag verarbeitet. Die Haftung bliebe 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.

So ist es wahrscheinlich, daß eine vertragliche Lösung in den meisten Fällen durch zumindest die Möglichkeit einer Art externer Überprüfung der Verarbeitungstätigkeiten des Empfängers ergänzt werden muß, wie bspw. ein Audit durch ein zuständiges Gremium oder ein spezialisiertes Rechnungsprüfungsunternehmen.

5. Das Problem des vorrangigen Rechts

Eine besondere Schwierigkeit bei dem vertraglichen Ansatz ist die Möglichkeit, daß die allgemeinen Rechtsvorschriften des Drittlands möglicherweise das Erfordernis für den Empfänger einer Datenübermittlung enthalten, unter bestimmten Umständen personenbezogene Daten für den Staat offenzulegen (Polizei, Gerichte oder Steuerbehörden) und daß derartige gesetzliche Erfordernisse ein Vorrecht gegenüber jedem Vertrag haben können, dem der Verarbeiter unterworfen ist.[12] Für Verarbeiter in der Gemeinschaft ist diese Möglichkeit in Artikel 16 der Richtlinie angesprochen, demzufolge Auftragsverarbeiter 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 die 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 für den 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

[12] Das Ausmaß der staatliche Befugnis zur Forderung der Offenlegung von Informationen ist auch eine Frage bei der allgemeineren Beurteilung der Angemessenheit des Schutzes in einem Drittland.

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

Die vorausgehende Analyse hat deutlich gemacht, daß jede vertragliche Lösung detailliert und gebührend an die betreffende Datenübermittlung angepaßt sein muß. Diese notwendige Präzision im Hinblick auf die genauen Zweckbestimmungen und die Voraussetzungen, unter denen die übermittelten Daten verarbeitet werden, schließt die Möglichkeit der Entwicklung eines Mustervertrags nicht aus, bringt aber die Notwendigkeit für jeden auf diesen Mustervertrag aufbauenden Vertrag mit sich, in einer Art und Weise ergänzt zu werden, die den besonderen Umständen des Einzelfalls entspricht.

Die Analyse hat auch 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 kein Kontrollgremium vorgesehen ist. Diese beiden Erwägungen bedeuten, daß es Situationen geben wird, in denen eine vertragliche Lösung eine geeignete Lösung darstellen kann, und andere, in denen ein Vertrag unmöglich die notwendigen "angemessenen Sicherheiten" garantieren kann.

Die notwendige detaillierte Anpassung eines Vertrags an die Besonderheiten der betreffenden Übermittlung impliziert, daß ein Vertrag besonders für Situationen geeignet ist, in denen ähnliche, repetitive Datenübermittlungen vorgenommen werden. Die Schwierigkeiten im Hinblick auf die Überwachung bedeuten, daß eine vertragliche Lösung effizienter sein kann, wenn es sich bei den Vertragsparteien um bedeutende Wirtschaftsteilnehmer handelt, die bereits öffentlicher Prüfung und Regelung unterworfen sind[13]. Große internationale, - wie die für Kreditkartengeschäfte und Flugbuchungen verwendeten - Netze weisen diese beiden Merkmale auf und bieten somit eine Lage, in der Verträge sehr zweckmäßig sein können. Unter diesen Umständen könnten sie auch durch multilaterale Vereinbarungen ergänzt werden, die eine größere Rechtssicherheit schaffen.

Auch wenn die an der Übermittlung Beteiligten einer selben Unternehmensgruppe angehören oder angeschlossen sind, besteht wahrscheinlich eine weitaus größere Möglichkeit, eine Nichterfüllung des Vertrags zu untersuchen, aufgrund der engen Bindungen zwischen dem Empfänger im Drittland und der Stelle mit Sitz in der Gemeinschaft. Unternehmensinterne Übermittlungen sind deshalb ein weiterer Bereich, in dem es ein deutliches Potential für die Entwicklung effizienter vertraglicher Lösungen gibt.

Wichtigste Schlußfolgerungen und Empfehlungen

[13] Im Citybank "Bahncard"-Fall arbeitete der Berliner Datenschutzbeauftragte mit den amerikanischen Bankaufsichtsbehörden zusammen.

- Verträge werden in der Gemeinschaft als Mittel zur Spezifizierung der Aufteilung der Zuständigkeit für die Erfüllung des Datenschutzes zwischen dem für die Verarbeitung Verantwortlichen und einem Auftragsverarbeiter verwendet. Wird ein Vertrag bei Datenflüssen in Drittländer verwendet, so muß er viel mehr leisten: er muß zusätzliche Sicherheiten für die betroffene Person bereitstellen, die erforderlich werden, weil der Empfänger im Drittland keinem durchsetzbaren Paket von Datenschutzvorschriften unterworfen ist, die ein angemessenes Schutzniveau sicherstellen.
- Die Grundlage für die Beurteilung der Angemessenheit der Sicherheiten aufgrund einer vertraglichen Lösung ist dieselbe wie die Grundlage für die Beurteilung der Angemessenheit des allgemeinen Schutzniveaus in einem Drittland. Eine vertragliche Lösung muß alle grundlegenden Grundsätze des Datenschutzes umfassen und die Mittel bereitstellen, mit denen die Grundsätze durchgesetzt werden können.
- Der Vertrag sollte die Zweckbestimmungen, die Mittel und Bedingungen detailliert darlegen, unter denen die übermittelten Daten zu verarbeiten sind, und die Art und Weise, in der die grundlegenden Prinzipien des Datenschutzes anzuwenden sind. Größere Rechtssicherheit wird durch Verträge gewährleistet, die die Möglichkeit des Datenempfängers einschränken, die Daten autonom in seinem eigenen Namen zu verarbeiten. Der Vertrag sollte deshalb soweit möglich als ein Mittel verwendet werden, mit dem die die Daten übermittelnde Stelle die Beschlußfassungskontrolle über die in dem Drittland erfolgte Verarbeitung behält.
- Besitzt der Empfänger Autonomie im Hinblick auf die Verarbeitung der übermittelten Daten, so ist die Situation nicht unkompliziert, und ein einfacher Vertrag zwischen den an der Übermittlung Beteiligten ist vielleicht nicht immer eine ausreichende Grundlage für die Wahrnehmung der Rechte durch einzelne betroffene Personen. Möglicherweise 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 sein, es sei denn, es ist möglich, derartige beteiligte Dritte vertraglich auf die Einhaltung derselben Datenschutzgrundsätze zu verpflichten.
- Das Vertrauen, daß die Grundsätze des Datenschutzes nach Übermittlung der Daten eingehalten werden, wird gestärkt, wenn die Erfüllung des Datenschutzes durch den Empfänger der Übermittlung einer externen Überprüfung durch beispielsweise 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. Die Kontrollbehörden des EU-Mitgliedstaats werden praktische Probleme bei der Durchführung einer solchen Prüfung haben.
- Vertragliche Lösungen sind wahrscheinlich am besten geeignet für große internationale Netze (Kredtikarten, Flugbuchungen), die durch große Mengen repititiver Datenübermittlungen gleicher Art und eine relativ kleine Anzahl bedeutender Wirtschaftsteilnehmer in Industriezweigen charakterisiert sind, die

bereits signifikanter öffentlicher Prüfung und Regelung unterworfen sind. Unternehmensinterne Datenübermittlungen zwischen verschiedenen Zweigen derselben Unternehmensgruppe sind ein weiterer Bereich, in dem es ein beträchtliches Potential für die Verwendung von Verträgen gibt.

- Länder, in denen die Befugnisse der staatlichen Behörden im Hinblick auf den Zugang zur Information 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.

Geschehen zu Brüssel, 28. April 1998
Für die Arbeitsgruppe
Der Vorsitzende
P.J.HUSTINX