ARTIKEL-29- DATENSCHUTZGRUPPE

00339/09/DE
WP 158

Arbeitsunterlage 1/2009 über Offenlegungspflichten im Rahmen der vorprozessualen Beweiserhebung bei grenzübergreifenden zivilrechtlichen Verfahren (pre-trial discovery)

Angenommen am 11. Februar 2009

Zusammenfassung

Dieses Arbeitspapier soll den Personen, die nach EU-Recht für die Datenverarbeitung verantwortlich sind, als Leitfaden bei der Bearbeitung von Ersuchen um Übermittlung personenbezogener Daten ins Ausland zwecks Verwendung in einem Zivilprozess dienen. Anlass für die Ausarbeitung dieses Dokuments war die Feststellung der Arbeitsgruppe, dass die Richtlinie 95/46/EG in den Mitgliedstaaten unterschiedlich angewandt wird, was zum Teil auf die Vielfalt der zivilrechtlichen Verfahren in der EU zurückzuführen ist.

Im ersten Abschnitt dieses Papiers legt die Arbeitsgruppe kurz die unterschiedlichen Positionen zu Rechtsstreitigkeiten und insbesondere zu Offenlegungspflichten im Rahmen der vorprozessualen Beweiserhebung (pre-trial discovery) in den angloamerikanischen (u. a. USA und Vereinigtes Königreich) und kontinentaleuropäischen Rechtssystemen dar.

Im Anschluss daran werden Leitlinien für die in der EU für die Datenverarbeitung Verantwortlichen aufgestellt, die die prozessualen Anforderungen eines bei einem ausländischen Gericht anhängigen Rechtsstreits mit den Datenschutzverpflichtungen aufgrund der Richtlinie 95/46/EG in Einklang zu bringen suchen.

Einleitung

Die Frage der grenzübergreifenden Offenlegung, insbesondere in Bezug auf in Europa gespeicherte Daten, die beispielsweise für ein Gerichtsverfahren in den Vereinigten Staaten angefordert werden, hat in letzter Zeit an Bedeutung gewonnen. Oft stehen Unternehmen mit einer Niederlassung oder Tochtergesellschaft in den Vereinigten Staaten unter erheblichem Druck, weil sie für Rechtsstreitigkeiten und Ermittlungen der Strafverfolgungsbehörden in den USA Unterlagen und Material (einschließlich elektronisch gespeicherter Daten) vorlegen müssen. Dabei umfasst das angeforderte Material häufig personenbezogene Daten von Arbeitnehmern oder Dritten, einschließlich Auftraggebern oder Kunden.

Zwischen der Offenlegungspflicht aufgrund des US-amerikanischen Prozess- oder Verwaltungsrechts und der Anwendung datenschutzrechtlicher Bestimmungen der EU besteht ein Spannungsverhältnis. Gleiches gilt für die geografische und territoriale Grundlage des Datenschutzsystems der EU im Verhältnis zum multinationalen Charakter der Wirtschaftstätigkeit, demzufolge ein Unternehmen überall in der Welt Tochtergesellschaften oder Niederlassungen haben kann. Von besonderer Bedeutung ist dies für die europäischen Tochtergesellschaften multinationaler Unternehmen, die dem Dilemma der kollidierenden Anforderungen amerikanischer Gerichtsverfahren und der europäischen Vorschriften für den Datenschutz und den Schutz der Privatsphäre, die für die Übermittlung personenbezogener Informationen gelten, ausgesetzt sind.

Die Arbeitsgruppe räumt ein, dass die an einem Rechtsstreit beteiligten Parteien ein legitimes Interesse am Zugang zu den erforderlichen Informationen haben, um Ansprüche geltend zu machen oder sich zu verteidigen; dies muss aber in einem ausgewogenen Verhältnis zu den Rechten der Person stehen, um deren Daten es geht.

Bei den in diesem Arbeitspapier vorgeschlagenen Leitlinien ist zu bedenken, dass sich die Frage der Offenlegungspflichten im Pre-trial-Discovery-Verfahren nicht mit einer Stellungnahme der Arbeitsgruppe beantworten lässt, sondern nur zwischenstaatlich - etwa durch die Einführung weiterer globaler Vereinbarungen im Sinne des Haager Übereinkommens – geregelt werden kann.

1. Konzept der pre-trial discovery

Verschiedene Aspekte des amerikanischen Prozessrechts und seiner Verfahren können sich auf im Besitz europäischer Unternehmen befindliche Daten auswirken. Besonders verbreitet sind:

- Präventives Vorhalten von Unterlagen in Erwartung eines Gerichtsverfahrens in den USA oder als Reaktion auf ein diesbezügliches Ersuchen, so genanntes „freezing“
- Vorprozessuale Beweisanträge in zivilrechtlichen Verfahren in den USA, die Offenlegungspflichten begründen
- Vorlage von Dokumenten bei straf- oder verwaltungsrechtlichen Ermittlungen in den USA
- Straftaten im Zusammenhang mit der Vernichtung von Daten in den USA.

In diesem Dokument werden nur die beiden ersten Aspekte behandelt, da diese Auswirkungen auf den Prozessverlauf und die Frage der Übermittlung personenbezogener Daten an einen Drittstaat haben. Die vorprozessuale Beweisbeschaffung kann nicht nur die Offenlegung von Daten im Rahmen von Gerichtsverfahren umfassen, sondern auch die Vorratsspeicherung von Daten mit Blick auf ein etwaiges künftiges Verfahren.

Mit dem vorprozessualen Beweisbeschaffungsverfahren soll sichergestellt werden, dass die Parteien in einem Rechtsstreit Zugang zu den Informationen haben, die für ihren Fall aufgrund der Vorschriften und Verfahren des Gerichts, bei dem der Prozess anhängig ist, erforderlich und relevant sind. In den Common-Law-Staaten sind die Offenlegungsanforderungen nicht beschränkt auf beispielsweise personenbezogene Daten oder elektronische Dokumente. Die angeforderten Informationen können sensible personenbezogene Daten wie Gesundheitsdaten oder private E-Mails (deren Bereitstellung den Verpflichtungen aus dem Fernmeldegeheimnis oder anderen Geheimhaltungsvorschriften zuwiderlaufen kann) und Daten Dritter, z. B. von Angestellten oder Kunden, einschließen.

Im Zivilprozessrecht des Vereinigten Königreichs wird der Begriff „document“ verwendet; er schließt neben aus Computersystemen und anderen elektronischen Geräten leicht zugänglichen Dokumenten elektronische Dokumente, darunter E-Mail und andere elektronische Kommunikation, textverarbeitete Dokumente und Datenbanken, ein. Er umfasst auch auf Servern gespeicherte Dokumente und Datensicherungssysteme sowie „gelöschte“ elektronische Dokumente. Er erstreckt sich ferner auf Metadaten, d. h. alle gespeicherten und zugehörigen zusätzlichen Informationen zu elektronischen Dokumenten.

Der verstärkte Einsatz elektronischer Aufzeichnungen, wo früher nur mit Druckexemplaren gearbeitet worden wäre, hat dazu geführt, dass mehr Informationen als je zuvor verfügbar sind. Aufgrund der einfachen Abrufung, Übermittlung oder sonstigen Handhabung elektronischer Aufzeichnungen produziert das vorprozessuale Beweisbeschaffungsverfahren oft eine Fülle an Informationen, von denen die Parteien bestimmen müssen, welche Teile für den entsprechenden Einzelfall relevant sind. Die elektronisch gespeicherten Informationen haben ein weitaus größeres Volumen als Aufzeichnungen auf Papierträger, so dass heute aufgrund der

Speicherkapazität der verschiedenen Memory-Produkte mehr Informationen zur Verfügung gestellt und offen gelegt werden können[1]..

Unterschiede zwischen dem angloamerikanischen und dem kontinentaleuropäischen Recht

Als Erstes fällt auf, dass nicht nur beim Prozessrecht allgemein, sondern insbesondere bei der Beweiserhebung Unterschiede zwischen dem angloamerikanischen und dem kontinentaleuropäischen Recht bestehen. Die Beweisbeschaffung ist in den beiden Rechtssystemen höchst unterschiedlich geregelt. Die Möglichkeit, im Laufe des Rechtsstreits Informationen zu erhalten, ja die Pflicht, diese schon vor dem Prozess bereitzustellen, ist in den angloamerikanischen Rechtsordnungen Bestandteil des Verfahrens. Der extensive Informationsaustausch vor der eigentlichen Gerichtsverhandlung gilt als die effizienteste Methode zur Klärung strittiger Fragen. Insbesondere gilt dies für die Vereinigten Staaten, in denen die vorprozessuale Beweiserhebung sehr viel weiter geht als in den anderen Common-Law-Staaten.

Common Law – Vereinigte Staaten

Sobald ein Rechtsstreit begonnen hat, müssen Unternehmen in den USA den Verpflichtungen nachkommen, die ihnen das amerikanische Prozessrecht nicht nur nach dem Bundesrecht, sondern auch nach den Zivilprozessordnungen der einzelnen Bundesstaaten auferlegt, nach denen die Parteien dazu angehalten werden, vor dem Prozess Informationen auszutauschen[2]. Dies betrifft nicht nur die Offenlegung relevanter Informationen, sondern auch die Offenlegung von Informationen, die an sich vielleicht nicht unmittelbar relevant sind, aber zur Offenlegung relevanter Informationen führen könnten (die so genannten „smoking-gun“). Dies steht im Widerspruch zu vielen europäischen Rechtsordnungen, in denen solche „Fischzüge“ („fishing expeditions“) untersagt sind.

Nach Rule 26f der Zivilprozessordnung der USA müssen sich die Parteien treffen und beraten („meet and confer“), um den Parteien in einem frühen Stadium des Prozesses die Diskussion und Einigung über die mit der Offenlegung zusammenhängenden Fragen zu ermöglichen. Ein Ziel dieses Treffens ist die Sicherung der Beweismittel, einschließlich der für den Rechtsstreit erforderlichen Daten und Unterlagen.

US-Gerichte können auch von sich aus oder auf Antrag einer Partei mittels einer Schutzverfügung (Protective Order) den Umfang zu weit reichender vorprozessualer Beweisanträge einschränken, da sie aufgrund der Vorschriften befugt sind, die Häufigkeit oder

---

1 Gemäß den Zahlen des Advisory Committee on Civil Rules in den USA existieren 92 % aller neuen Informationen heute in digitaler Form, von denen ca. 70 % nie ausgedruckt werden. Infolgedessen hat sich das Verfahren der Pre-trial-Discovery fast vollständig zur E-Discovery entwickelt. Die USA haben jetzt Schritte zur Regelung dieses neuen Bereichs unternommen.

2 So sehen die Federal Rules of Civil Procedure (Zivilprozessordnung) beispielsweise unter Rule 34 (b) vor, dass jede Partei jede andere Partei auffordern kann, alle bezeichneten Dokumente oder elektronisch gespeicherten Informationen vorzulegen – einschließlich Schriften, Zeichnungen, Grafiken, Karten, Fotographien, Tonaufnahmen, Bilder und andere in einem Medium gespeicherte Daten oder Datensammlungen, von dem die Informationen abgerufen werden können … die sich im Besitz, im Gewahrsam oder unter der Kontrolle der Partei befinden, an die die Aufforderung gerichtet ist, und der Antrag stellenden Partei oder einer in ihrem Namen handelnden Person zu erlauben, Einsicht in diese Dokumente und Informationen zu nehmen, sie zu kopieren, zu testen oder von ihnen Stichproben zu nehmen.

das Ausmaß der Verwendung solcher Anträge aus verschiedenen Gründen zu begrenzen; unter anderem wegen der Möglichkeit, die Information aus einer geeigneteren Quelle zu erhalten, oder wenn die Belastung oder die Ausgaben in Bezug auf die vorgeschlagene Offenlegung den zu erwartenden Nutzen übertreffen. Mittels dieser Schutzverfügung können die Gerichte ferner eine Person oder Partei vor Belästigungen, Unannehmlichkeiten, Schikane, unzumutbaren Belastungen oder Ausgaben schützen, indem sie z. B. anordnen, dass eine Offenlegung oder Aufdeckung nur unter bestimmten Voraussetzungen erfolgen kann, wobei auch die Methode oder der Sachverhalt zu berücksichtigen ist.
Ein US-Richter wird somit einem Beweisantrag stattgeben, solange dieser in vertretbarer Art und Weise auf die Erlangung zulässiger Beweismittel abzielt und keine unmöglichen Forderungen enthält.

Vereinigtes Königreich
Ähnlich, aber weniger umfassend ist die Regelung in Rule 31 der Zivilprozessordnung des Vereinigten Königreichs, wonach eine Partei Unterlagen offen legen muss, auf die sie sich zu stützen gedenkt, sowie alle weiteren Unterlagen, die für sie nachteilig sind, eine andere Partei belasten oder unterstützen oder die durch einschlägige Anweisungen des Gerichts offen zu legen sind. Im Gegensatz zu den USA bestehen im Vereinigten Königreich (wie auch in Kanada) Datenschutzverpflichtungen.

Länder mit kontinentaleuropäischem Rechtssystem
Im Gegensatz zu dem auf völlige Transparenz abstellenden Discovery-Verfahren in den USA und anderen Common-Law-Staaten verfahren die meisten kontinentaleuropäischen Systeme restriktiver und kennen oft kein formelles Offenlegungsverfahren im Rahmen der Beweiserhebung. Viele kontinentaleuropäische Rechtsordnungen beschränken die Offenlegung von Beweismitteln auf für den Prozess erforderliche Beweise und untersagen eine weitergehende Offenlegung. Es ist Sache der Streitpartei, zur Unterstützung ihrer Sache Beweismittel vorzulegen. Benötigt die gegnerische Partei diese Informationen, so ist es an ihr, sich Kenntnis darüber zu verschaffen und die Informationen genau zu benennen. In Frankreich und Spanien ist die Offenlegung einzig und allein auf die Dokumente beschränkt, die vor Gericht zulässig sind. Die Offenlegung der Dokumente wird von dem Richter überwacht, der über die Relevanz und die Zulässigkeit des von den Parteien vorgeschlagenen Beweismittels entscheidet.

In Deutschland sind die Streitparteien nicht verpflichtet, der anderen Partei Dokumente offen zu legen. Sie müssen nur die Dokumente vorlegen, die ihr Vorbringen unterstützen. Dabei muss es sich um authentische und beglaubigte Originale handeln. Die Partei, die die Vorlage eines Dokuments begehrt, muss bei Gericht eine entsprechende Anordnung erwirken. Dazu ist eine genaue Beschreibung des Dokuments erforderlich, die den Sachverhalt, für den das Dokument als Beweismittel dienen soll, und die Rechtfertigung für die Vorlage des Dokuments umfasst. Befindet sich das Dokument im Besitz eines Dritten, so benötigt die Partei, die sich um das Dokument bemüht, die Genehmigung dieser Person. Wird die Genehmigung verweigert, so muss der Antragsteller gegen den Besitzer der Dokumente ein Verfahren anstrengen.

Die Unterschiede zwischen der Herangehensweise des angloamerikanischen und des kontinentaleuropäischen Rechts bei der Offenlegung von Informationen, einschließlich personenbezogener Daten, werden – vom Datenschutz abgesehen – an der Dichotomie zwischen der „Überzeugung von der Wahrheit“ und dem Postulat „die Wahrheit und nichts als die Wahrheit“ deutlich.

Präventive Rechtsvorschriften

Einige Länder, im Wesentlichen Länder mit kontinentaleuropäischem Recht, aber auch einige Common-Law-Staaten, haben Gesetze (*blocking statutes*) erlassen, um die grenzüberschreitende Offenlegung von Informationen zwecks Vorlage bei ausländischen Gerichten zu beschränken. Wenig Einheitlichkeit lässt sich bezüglich ihrer Einführung, ihres Anwendungsbereichs und ihrer Wirkung feststellen. Einige, wie zum Beispiel Frankreich, verbieten die Offenlegung bestimmter Kategorien von Dokumenten oder Informationen als Beweismittel für gerichtliche oder administrative Verfahren im Ausland. Eine Partei, die Informationen offen legt, kann sich des Verstoßes gegen die Gesetze des Landes schuldig machen, in dem sich die Informationen befinden, und das kann zu zivil- oder sogar strafrechtlichen Sanktionen führen[3].

Die amerikanischen Gerichte haben bisher solche Bestimmungen nicht als Grund akzeptiert, die Offenlegung von Daten für Rechtsstreitigkeiten in den USA zu verweigern. Gemäß der dritten Anpassung (Third restatement) des Gesetzes Nr. 442 über die Außenbeziehungen der Vereinigten Staaten (Foreign Relations Law) kann ein Gericht eine unter seine Gerichtsbarkeit fallende Person anweisen, Beweismittel vorzulegen, auch wenn sich die Informationen nicht in den Vereinigten Staaten befinden[4] Wie von einem Teil der Rechtsprechung befürwortet[5], sollte eine Abwägung erfolgen mit dem Ziel, dass das Gericht über den Antrag einer Partei auf Vorlage von im Ausland befindlichen Informationen nur nach Berücksichtigung folgender Aspekte entscheiden sollte:

(1) Bedeutung der angeforderten Informationen für den Rechtsstreit;

(2) Detailliertheit der angeforderten Informationen;

(3) ob die Informationen aus den Vereinigten Staaten stammen;

(4) Verfügbarkeit alternativer Mittel zur Informationssicherung;

(5) inwieweit ein Zurückweisen den Interessen der Vereinigten Staaten bzw. ein Stattgeben den Interessen eines souveränen ausländischen Staates schaden würde.

---

[3] Ein Beispiel dafür ist das französische Strafgesetz Nr. 80-538, das Folgendes vorsieht:
Vorbehaltlich geltender internationaler Verträge oder Abkommen, Rechts- und Verwaltungsvorschriften ist es jeder Person untersagt, schriftlich, mündlich oder in anderer Form als Beweismittel im Hinblick auf gerichtliche oder administrative Verfahren im Ausland oder im Rahmen derartiger Verfahren Dokumente oder Informationen wirtschaftlicher, kommerzieller, industrieller oder finanzieller Art anzufordern, zu beantragen oder zu übermitteln. 2008 bestätigte der französische Oberste Gerichtshof wegen Verletzung dieser Vorschriften die strafrechtliche Verurteilung eines französischen Anwalts, der einem Ersuchen amerikanischer Gerichte in der Rechtssache Strauss gegen Crédit Lyonnais, S.A., 2000 U.S. Dist. Lexis 38378 (E.D.N.Y. 25. Mai 2007) nachgekommen war. Dem Anwalt wurde eine Geldstrafe von 10 000 EUR (ca. 15 000 USD) auferlegt.

[4] Dazu ist anzumerken, dass vom Standpunkt des amerikanischen Richters aus – unabhängig vom „materiellen" Aufbewahrungsort der Daten - das amerikanische Recht anwendbar ist und keine Notwendigkeit besteht, internationale Übereinkommen wie das Haager Übereinkommen anzuwenden, wenn das Unternehmen amerikanischem Recht unterliegt und sich die Informationen in seinem Besitz, unter seiner Kontrolle oder in seinem Gewahrsam befinden oder wenn es vom Hoheitsgebiet der USA aus (über einen Computer) auf diese Informationen zugreifen darf.

[5] Société Nationale Industrielle Aérospatiale gegen United States District Court, 482 U.S. 522, 544 n.28 (1987), Volkswagen AG gegen Valdez [Nr.95-0514, 16. November 1995, Texas Supreme Court] und In re: Baycol Litigation MDL nr. 1431 (Mfd/JGL), 21. März 2003. Für eine weitergehende Analyse der amerikanischen Rechtsprechung siehe Sedona Conference Framework for Analysis of Cross Border Discovery Conflicts (Fußnote 6).

Die jüngste Veröffentlichung der Sedona-Konferenz über Konflikte bei der grenzüberschreitenden Beweisbeschaffung enthält eine detaillierte Analyse der Rechtsprechung in den USA sowie eine Betrachtung der Faktoren, die für den Umfang grenzübergreifender Offenlegungspflichten maßgebend sind[6]. Danach sind Notwendigkeit, Kosten und Belastung der Offenlegung mit den Interessen der betreffenden ausländischen Rechtsordnung am Schutz der Privatsphäre und des Gemeinwohls ihrer Bürger abzuwägen. Im Sedona Conference Framework wird auch festgestellt, dass die französische Entscheidung im Crédit-Lyonnais-Fall bei den US-Gerichten dazu geführt hat, ausländische Präventivgesetze mit anderen Augen zu sehen[7].

Das Haager Beweisübereinkommen

Informationsverlangen können auch über das Haager Übereinkommen über die Beweisaufnahme im Ausland in Zivil- oder Handelssachen erfolgen. Es bietet ein Standardverfahren für Rechtshilfeersuchen, d. h. für Anträge eines Gerichts an die benannte Zentrale Behörde eines anderen Staates auf Unterstützung bei der Erlangung relevanter Informationen, die sich in ihrem Staat befinden. Allerdings sind nicht alle EU-Mitgliedstaaten Vertragsstaaten des Haager Übereinkommens.

Eine weitere Komplikation besteht aufgrund von Artikel 23 des Übereinkommens, demzufolge „[j]eder Vertragsstaat bei der Unterzeichnung, bei der Ratifikation oder beim Beitritt erklären [kann], dass er Rechtshilfeersuchen nicht erledigt, die ein Verfahren zum Gegenstand haben, das in den Ländern des „Common Law“ unter der Bezeichnung „pre-trial discovery of documents“ bekannt ist“. Viele Vertragsstaaten, darunter Frankreich, Deutschland, Spanien und die Niederlande, haben einen entsprechenden Vorbehalt nach Artikel 23 eingelegt und erklärt, dass eine Offenlegung von Informationen, ungeachtet ihrer Relevanz, nicht genehmigt würde, wenn die Informationen für ein Gerichtsverfahren im Ausland bestimmt sind. In Frankreich kann der zuständige Richter solche Rechtshilfeersuchen erledigen, wenn die angeforderten Dokumente/Informationen in den Rechtshilfeersuchen genau bezeichnet sind und mit dem betreffenden Rechtsstreit unmittelbar und konkret zusammenhängen.

Gemäß dem Haager Übereinkommen fallen unter das Verfahren der „pre-trial discovery“ Beweisanträge, die nach der Klageerhebung, aber vor der Hauptverhandlung gestellt werden. Im Vereinigten Königreich wird diese Regel weiter ausgelegt. Danach kann ein Antrag gestellt werden, wenn die Beweismittel für Zivilverfahren erlangt werden sollen, die vor dem ersuchenden Gericht anhängig sind oder deren Einleitung vor diesem Gericht geplant ist[8]. Dies würde somit im Vereinigten Königreich eine großzügigere Bereitstellung von Informationen ermöglichen als in anderen Mitgliedstaaten.

Laut einer Entscheidung des Obersten Gerichtshofs der Vereinigten Staaten stellt das durch das Haager Beweisübereinkommen vorgesehene Verfahren ein fakultatives, aber kein bindendes Mittel zur Erlangung von Beweismitteln im Ausland für Streitparteien vor US-Gerichten dar[9].

---

6 The Sedona Conference Framework for analysis of cross border discovery conflicts – A practical guide to navigating the competing currents of international data privacy and discovery – 23. April 2008 (Public Comment Version), A Project of the Sedona Conference Working Group 6 on International Electronic Information Management, Discovery and Disclosure.

7 Sedona Framework, S. 31.

8 Evidence (Proceedings in Other Jurisdictions) Act 1975.

9 Société Nationale Industrielle Aérospatiale gegen United States District Court, 482 U.S. 522, 544 Nr. 28 (1987).

Seitdem sind die amerikanischen Gerichte weitgehend diesem Ansatz gefolgt, gelegentlich haben sie aber auch Streitparteien aufgefordert, auf das Haager Beweisübereinkommen zurückzugreifen[10].

Sonstige Probleme
Eine der Hauptschwierigkeiten bei grenzübergreifenden Rechtsstreitigkeiten liegt in der Kontrolle der Verwendung von personenbezogenen Daten, die bereits aus anderen Gründen – z. B. aufgrund von BCR- oder Safe-Harbour-Regeln - ordnungsgemäß in die USA übermittelt worden sind. Diese Frage wird hier nicht behandelt, aber die Arbeitsgruppe räumt ein, dass dies der Offenlegung von Daten Vorschub leisten kann.

2. Stellungnahme

Die Arbeitsgruppe hält es für notwendig, die Erfordernisse des US-amerikanischen Prozessrechts mit den Datenschutzbestimmungen der EU in Einklang zu bringen. Sie räumt ein, dass die Richtlinie Übermittlungen für Verfahrenszwecke nicht ausschließt und weltweit tätige Unternehmen im Ausland oft kollidierenden Anforderungen ausgesetzt sind, so dass diese sich genötigt fühlen, die für den Rechtsstreit im Ausland angeforderten Informationen zu übermitteln. Bestimmte Datenschutzerfordernisse müssen jedoch erfüllt sein, wenn für die Datenverarbeitung Verantwortliche personenbezogene Daten im Hinblick auf einen Rechtsstreit übermitteln wollen. Um die Datenschutzauflagen mit den Erfordernissen des ausländischen Rechtsstreits in Einklang zu bringen, schlägt die Arbeitsgruppe für die in der EU für die Datenverarbeitung Verantwortlichen die nachstehenden Leitlinien vor.

Leitlinien
Ein Rechtsstreit umfasst verschiedene Phasen. Die Verwendung personenbezogener Daten gilt in jeder dieser Phasen als Verarbeitung. Für die Legitimierung der Verarbeitung personenbezogener Daten in jeder einzelnen Phase ist eine entsprechende Voraussetzung zu erfüllen. Diese verschiedenen Phasen umfassen:

- Aufbewahrung
- Offenlegung
- Weiterleitung
- Sekundäre Nutzung.

Verschiedene Aspekte sind im Zusammenhang mit der Aufbewahrung zu betrachten, da gemäß der Richtlinie personenbezogene Daten während der für die Zwecke erforderlichen Dauer aufzubewahren sind, für die die Daten gesammelt wurden oder für die sie weiter verarbeitet werden. Es ist nicht wahrscheinlich, dass die betroffenen Personen darüber unterrichtet wurden, dass ihre personenbezogenen Daten in ihrem eigenen Land oder im Ausland Gegenstand eines Rechtsstreits sein könnten. Auch wegen der unterschiedlichen Fristen, die in den einzelnen Ländern gelten, um Ansprüche geltend zu machen, lässt sich eine bestimmte Aufbewahrungsdauer für Daten nicht vorsehen.

Verantwortliche in der Europäischen Union besitzen keine Rechtsgrundlage dafür, personenbezogene Daten aufs Geratewohl unbefristet aufzubewahren, weil es möglicherweise in den Vereinigten Staaten zu einem Rechtsstreit kommen könnte. Nach den US-

[10] Siehe die Sammlung von post-Aérospatiale-Fällen, die sich auf das Haager Beweisübereinkommen berufen, zusammengestellt für die amerikanische Anwaltskammer von McNamara/Hendrix/Charepoo (Juni 1987 bis Juli 2003).

Zivilprozessregeln müssen lediglich *vorhandene* Informationen offen gelegt werden. Verfolgt der Verantwortliche eine klare Dokumentenverwaltungspolitik, die auf der Grundlage gesetzlicher Anforderungen kurze Aufbewahrungszeiten vorsieht, so verstößt er nicht gegen US-Recht. Anzumerken ist, dass in jüngster Zeit auch in den Vereinigten Staaten dahin tendiert wird, eine restriktive Aufbewahrung zu verfolgen, um die Wahrscheinlichkeit von Offenlegungsanträgen zu reduzieren.

Wenn jedoch die personenbezogenen Daten rechtserheblich sind und in einem konkreten oder unmittelbar bevorstehenden Verfahren verwendet werden sollen, sollten sie bis zum Verfahrensabschluss und bis zum Ende der Berufungsfrist aufbewahrt werden. Die Vernichtung von Beweismitteln kann einschneidende verfahrensrechtliche und andere Sanktionen nach sich ziehen.

Es kann sich als notwendig erweisen, Informationen, einschließlich personenbezogener Daten, präventiv oder für ein Gerichtsverfahren („litigation hold“) aufzubewahren. De facto bedeutet dies, dass das Unternehmen Dokumente, die für bereits anhängige oder noch zu erwartende Klagen relevant sein können, vorübergehend aus seinem Dokumentenverwaltungssystem, das die Aufbewahrung oder Vernichtung von Dokumenten regelt, herausnimmt.

Ein weiteres Problem kann sich ergeben, wenn die Informationen für einen zusätzlichen anhängigen Rechtsstreit erforderlich sind oder wenn ein künftiger Rechtsstreit vorhersehbar ist. Die Möglichkeit, dass eine Sache vor ein US-Gericht gebracht werden könnte, reicht allein ohne eine fundierte Begründung für die Offenlegung nicht aus.

In den Vereinigten Staaten wird zwar die Speicherung personenbezogener Daten für einen Rechtsstreit nicht als Verarbeitung angesehen, nach der Richtlinie 95/46/EG stellt aber jede Aufbewahrung, Konservierung oder Archivierung von Daten für derartige Zwecke eine Verarbeitung dar. Die Aufbewahrung von Daten für einen künftigen Rechtsstreit ist lediglich gemäß Artikel 7 Buchstaben c oder f der Richtlinie 95/46/EG möglich.

Rechtmäßigkeit der Verarbeitung für gerichtliche Verfahren

Ein rechtmäßiges Pre-trial-Discovery-Verfahren setzt eine zulässige Verarbeitung personenbezogener Daten im Einklang mit Artikel 7 der Datenschutzrichtlinie voraus. Außerdem müssen für Übermittlungen an ein ausländisches Gericht die Erfordernisse gemäß Artikel 26 erfüllt sein.

Die Verarbeitung kann aus drei Gründen rechtmäßig sein: die betroffene Person hat ihre Einwilligung erteilt, die Erfüllung der vorprozessualen Offenlegungspflichten ist für die Erfüllung einer rechtlichen Verpflichtung gemäß Artikel 7 Buchstabe c oder gemäß Artikel 7 Buchstabe f zur Verwirklichung eines berechtigten Interesses erforderlich, das von dem für die Verarbeitung Verantwortlichen oder Dritten wahrgenommen wird, denen die Daten übermittelt werden. Aus den nachstehend dargelegten Gründen ist die Arbeitsgruppe der Ansicht, dass in den meisten Fällen nicht damit zu rechnen ist, dass die Einwilligung einen triftigen Grund für eine solche Verarbeitung darstellt.

Einwilligung
Nach Artikel 7 ist zwar die Einwilligung eine Voraussetzung für die Verarbeitung, die Arbeitsgruppe vertritt aber die Auffassung, dass es in den meisten Fällen nicht wahrscheinlich ist, dass sie eine gute Grundlage für eine Verarbeitung darstellt. In Artikel 2 Buchstabe h ist die Einwilligung der betroffenen Person definiert als „jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden." Seit dem Aérospatiale-Fall ist das Hauptargument der US-Rechtsprechung, dass ein Unternehmen, wenn es sich für eine Geschäftstätigkeit in den Vereinigten Staaten oder mit Einbeziehung amerikanischer Partner entschieden hat, die US-Zivilprozessregeln zu beachten hat. Sehr oft haben allerdings betroffene Personen wie Kunden und Mitarbeiter dieses Unternehmens diese Wahl nicht oder waren nicht an der Entscheidung beteiligt, in den oder in Verbindung mit den Vereinigten Staaten Geschäfte zu tätigen.

Deshalb sollten für die Übermittlung ins Ausland Verantwortliche in der Europäischen Union in der Lage sein, die Einwilligung der betroffenen Person in jedem einzelnen Fall eindeutig nachweisen zu können. Außerdem kann von ihnen der Nachweis verlangt werden, dass die betroffene Person ordnungsgemäß informiert war. Handelt es sich bei den angeforderten personenbezogenen Daten um Daten eines Dritten, beispielsweise eines Kunden, so ist derzeit unwahrscheinlich, dass der für die Verarbeitung Verantwortliche den Beweis erbringen könnte, dass die betroffene Person gebührend informiert war und von der Verarbeitung in Kenntnis gesetzt wurde.

Gleichzeitig beinhaltet eine gültige Einwilligung, dass die betroffene Person ihre Einwilligung tatsächlich verweigern konnte, ohne Sanktionen zu erleiden, oder sie später zurückziehen konnte, falls sie ihre Meinung geändert hat. Dies kann vor allem im Fall der Einwilligung von Arbeitnehmern von Belang sein. Die Artikel-29-Datenschutzarbeitsgruppe führt dazu in ihrem Papier zur Auslegung von Artikel 26 Absatz 1 aus: „Das Erfordernis der Einwilligung kann also als vermeintlich gute Lösung erscheinen, die auf den ersten Blick einfach, in der Praxis jedoch komplex und schwerfällig ist"[11].

Die Arbeitsgruppe räumt ein, dass es Situationen geben kann, in denen der Betroffene Kenntnis von dem Rechtsstreit hat oder sogar daran beteiligt ist und somit seine Einwilligung als korrekte Grundlage für die Verarbeitung anzusehen ist.

Erforderlich für die Erfüllung einer rechtlichen Verpflichtung
Eine durch ein ausländisches Rechtssystem oder ausländische Vorschriften auferlegte Verpflichtung kann nicht als rechtliche Verpflichtung eingestuft werden, die eine Datenverarbeitung in der EU legitimieren würde. In einzelnen Mitgliedstaaten kann es jedoch eine rechtliche Vorschrift geben, einer Anordnung eines ausländischen Gerichts Folge zu leisten, mit der um Offenlegung ersucht wird.

In den Mitgliedstaaten, in denen keine derartige Verpflichtung besteht (z. B. wegen eines Vorbehalts aufgrund von Artikel 23 des Haager Beweisübereinkommens), kann Artikel 7 Buchstabe f dem für die Datenverarbeitung Verantwortlichen, der um Offenlegung im Rahmen des Discovery-Verfahrens ersucht wird, eine Handlungsgrundlage bieten.

[11] Siehe Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995 (WP 114), S. 11.

Erforderlich zur Verwirklichung eines berechtigten Interesses
Die Erfüllung der Erfordernisse eines Gerichtsverfahrens kann für die Zwecke eines berechtigten Interesses von dem für die Verarbeitung Verantwortlichen oder Dritten für notwendig gehalten werden, denen die Daten gemäß Artikel 7 Buchstabe f übermittelt werden. Diese Grundlage ist nur akzeptabel, „sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person überwiegen".

Es käme zweifellos den Interessen der Justiz entgegen, wenn die Handlungsfähigkeit einer Organisation hinsichtlich der Förderung oder Verteidigung eines rechtmäßigen Anspruchs nicht unnötig eingeschränkt würde. Das Pre-trial-Discovery-Verfahren zielt darauf ab, für den Rechtsstreit potenziell relevante Informationen zu sichern und bereitzustellen. Jede Partei soll den Zugang zu solchen Informationen erhalten, die zur Unterstützung ihrer Forderung oder Verteidigung benötigt werden. Auf diese Weise soll für Fairness im Verfahren und ein gerechtes Ergebnis gesorgt werden.

Diese Ziele müssen allerdings gegen die Rechte und Freiheiten der betroffenen Person abgewogen werden, die - wie z. B. Mitarbeiter und Kunden - nicht unmittelbar am Rechtsstreit beteiligt ist und die nur deshalb einbezogen wird, weil ihre personenbezogenen Daten im Besitz einer Streitpartei sind und für die behandelten Fragen für erheblich erachtet werden.

Bei dieser Interessenabwägung sollten Aspekte der Verhältnismäßigkeit, die Relevanz der personenbezogenen Daten für den Rechtsstreit und die Konsequenzen für die betroffene Person berücksichtigt werden. Ferner müssen angemessene Garantien festgelegt werden und insbesondere müssen die Widerspruchsrechte der betroffenen Person nach Artikel 14 der Richtlinie anerkannt werden, wenn die Verarbeitung sich auf Artikel 7 Buchstabe f stützt und in Ermangelung anderslautender einzelstaatlicher Rechtsvorschriften zwingende legitime Gründe in Bezug auf die besondere Situation der betroffenen Person vorliegen.

Als ersten Schritt sollten die für die Verarbeitung Verantwortlichen die Offenlegung nach Möglichkeit auf anonymisierte oder zumindest pseudonymisierte Daten beschränken. Nach dem Herausfiltern irrelevanter Daten – möglicherweise durch eine vertrauenswürdige dritte Partei in der Europäischen Union – würden in einem zweiten Schritt personenbezogene Daten in einem sehr viel begrenzteren Umfang offen gelegt werden.

Sensible personenbezogene Daten und andere besondere Kategorien
Wenn es sich bei den betreffenden Informationen um sensible personenbezogene Daten handelt, muss gemäß Artikel 8 der Richtlinie eine Grundlage für die Verarbeitung gefunden werden. Ein angemessener Grund wäre die ausdrückliche Einwilligung der betroffenen Person nach Artikel 8 Buchstabe a oder die Notwendigkeit der Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche nach Artikel 8 Buchstabe e. In den einzelnen Mitgliedstaaten kann es spezifische Erfordernisse hinsichtlich der Verarbeitung und Übermittlung personenbezogener Daten nach Übersee geben, die der für die Verarbeitung Verantwortliche erfüllen muss.

Datenschutz ist nicht die einzige Frage, die sich im Zusammenhang mit der Verwendung personenbezogener Daten eines Individuums stellt. Geht es beispielsweise bei den angeforderten personenbezogenen Daten um Gesundheitsdaten, so können sie der ärztlichen Schweigepflicht unterliegen. Weitere Geheimhaltungserfordernisse oder Verpflichtungen zur Vertraulichkeit können aufgrund des Beichtgeheimnisses oder der anwaltlichen Schweigepflicht bestehen. Darüber hinaus kann ein Rechtsschutz für bestimmte

Informationsarten gelten, z. B. in Gestalt der Datenschutzrichtlinie für die elektronische Kommunikation. In einem solchen Fall ist es möglicherweise nicht fair oder rechtmäßig, diese personenbezogenen Daten in einer Weise zu verarbeiten, die mit den übrigen Verpflichtungen nicht vereinbar ist. Nicht zuletzt können Verstöße gegen das Fernmeldegeheimnis in einer Reihe von Mitgliedstaaten zu strafrechtlichen Sanktionen führen.

Verhältnismäßigkeit
Nach Artikel 6 der Richtlinie müssen personenbezogene Daten nach Treu und Glauben und auf rechtmäßige Weise verarbeitet sowie für festgelegte eindeutige und rechtmäßige Zwecke erhoben werden und dürfen nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise verwendet werden. Personenbezogene Daten müssen dem Zweck entsprechen, für den sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sein und dürfen nicht darüber hinausgehen.

Bei der Offenlegung in Verbindung mit der vorprozessualen Beweiserhebung besteht ein Dilemma zwischen dem Bedürfnis der Parteien, alle Informationen zu erhalten, bevor ihre Rechtserheblichkeit in der Streitsache feststeht, und den Rechten der Betroffenen, deren personenbezogene Daten Teil der für das Verfahren angeforderten Informationen sind.

Aus den amerikanischen Zivilprozessregeln und den Grundsätzen der Sedona-Konferenz ergibt sich eindeutig, dass sowohl das US-Recht als auch die Rechtssysteme in der EU dem Verhältnismäßigkeitsprinzip und dem Ausgleich der verschiedenen Interessen Bedeutung beimessen.

Die für die Verarbeitung Verantwortlichen, die an einem Rechtsstreit beteiligt sind, sind verpflichtet, geeignete Vorkehrungen zu treffen (im Hinblick auf die Sensibilität der betreffenden Daten sowie auf alternative Informationsquellen), um die Offenlegung personenbezogener Daten auf die Daten zu beschränken, die für die zur Verhandlung anstehenden Fragen objektiv erheblich sind. Dieses „Filtern“ erfolgt in mehreren Phasen: zunächst wird festgestellt, welche Informationen für den Rechtsstreit relevant sind, dann wird geprüft, inwieweit diese Informationen personenbezogene Daten enthalten. Sind personenbezogene Daten betroffen, muss der für die Verarbeitung Verantwortliche abwägen, ob es erforderlich ist, dass die personenbezogenen Daten vollständig verarbeitet werden, oder ob sie beispielsweise in einer stärker anonymisierten oder überarbeiteten Form vorgelegt werden können. Wenn die Identität der betroffenen Person für den Streitgegenstand nicht relevant ist, besteht keine Notwendigkeit, eine solche Information in erster Instanz bereitzustellen. Diese kann allerdings in einer späteren Phase vom Gericht angefordert werden, was zu einer weiteren „Filterung“ führen kann. In den meisten Fällen wird es ausreichen, die personenbezogenen Daten pseudonymisiert, d. h. mit anderen Identifikatoren als dem Namen der betroffenen Person, zu übermitteln.

Wenn personenbezogene Daten benötigt werden, sollte die „Filterung“ in dem Land vorgenommen werden, in dem sich die personenbezogenen Daten befinden, und zwar bevor die für den Rechtsstreit relevanten Daten in einen Drittstaat übermittelt werden.

Die Arbeitsgruppe räumt ein, dass es wegen der strengen Fristen, die aufgrund der amerikanischen Zivilprozessregeln für die Offenlegung der angeforderten Informationen gelten, schwierig werden kann, eine geeignete Person zu bestimmen, die beurteilen kann, welche Informationen für den Rechtsstreit relevant sind. Es liegt auf der Hand, dass es sich um eine Person handeln muss, die mit dem ausländischen Streitverfahren hinreichend vertraut ist.

Hierzu muss möglicherweise auf die Dienste eines vertrauenswürdigen Dritten in einem Mitgliedstaat zurückgegriffen werden, der in dem Rechtsstreit keine Rolle spielt, aber über ein ausreichendes Maß an Unabhängigkeit und Vertrauenswürdigkeit verfügt, um korrekt bestimmen zu können, welche personenbezogenen Daten relevant sind.

Die Arbeitsgruppe fordert die Streitparteien auf, die Datenschutzbeauftragten so früh wie möglich in das Pre-trial-Discovery-Verfahren (einschließlich der Datensicherung für Prozesszwecke) einzubeziehen. Sie möchte ferner die für die Verarbeitung Verantwortlichen in der EU ermutigen, an die amerikanischen Gerichte heranzutreten, um die ihnen obliegenden Datenschutzverpflichtungen zu erläutern, und die US-Gerichte um Schutzmaßnahmen zu ersuchen, um die Datenschutzauflagen in der EU und den Mitgliedstaaten zu erfüllen. Wie der Oberste Gerichtshof im Aérospatiale-Fall hervorhob, sollten amerikanische Gerichte bei vorprozessualen Verfahren besondere Sorgfalt darauf verwenden, ausländische Streitparteien vor der Gefahr zu schützen, dass sie durch eine unnötige oder unverhältnismäßig aufwändige Offenlegung benachteiligt werden[12].

Transparenz
In den Artikeln 10 und 11 der Richtlinie geht es um die Informationen, die die betroffene Person erhalten sollte.

Im Kontext des Discovery-Verfahrens bedeutet dies, dass die betroffene Person vorab davon in Kenntnis gesetzt wird, dass generell die Möglichkeit besteht, dass ihre personenbezogenen Daten für einen Rechtstreit verarbeitet werden könnten. Werden die personenbezogenen Daten dann tatsächlich für einen Rechtsstreit verarbeitet, sind die Identität aller Empfänger, die Zweckbestimmung der Verarbeitung, die Kategorien der betreffenden Daten und die diesbezüglichen Rechte mitzuteilen.

Nach Artikel 11 sind betroffene Personen darüber zu unterrichten, wenn personenbezogene Daten nicht unmittelbar bei ihnen, sondern bei Dritten erhoben werden. Dies kommt wahrscheinlich häufig vor, wenn personenbezogene Daten sich im Besitz einer der Streitparteien oder einer Tochtergesellschaft oder eines Mitglieds einer solchen Streitpartei befinden.

In diesen Fällen sollten die betroffenen Personen vom für die Verarbeitung Verantwortlichen informiert werden, sobald dies vernünftigerweise nach Verarbeitung der Daten möglich ist. Gemäß Artikel 14 besitzt die betroffene Person ferner ein Widerspruchsrecht gegen die Verarbeitung ihrer Daten, wenn sich die Legitimität der Verarbeitung auf Artikel 7 Buchstabe f stützt und der Widerspruch aus überwiegenden, schutzwürdigen, aus der besonderen Situation der Person ergebenden Gründen erfolgt.

In der Stellungnahme der Artikel-29-Datenschutzgruppe zu internen Verfahren zur Meldung mutmaßlicher Missstände[13] ist allerdings eine Ausnahme von dieser Regel vorgesehen, wenn das erhebliche Risiko besteht, dass eine solche Mitteilung die Fähigkeit der Streitpartei zur wirksamen Untersuchung der Sache oder zur Sammlung der erforderlichen Beweismittel gefährden würde. In einem solchen Fall kann die Unterrichtung der betroffenen Person so

[12] 482 U.S. 522, 546 (Nr.15, 16a).

[13] Stellungnahme 1/2006 zur Anwendung der EU-Datenschutzvorschriften auf interne Verfahren zur Meldung mutmaßlicher Missstände in den Bereichen Rechnungslegung, interne Rechnungslegungskontrollen, Fragen der Wirtschaftsprüfung, Bekämpfung von Korruption, Banken- und Finanzkriminalität (WP 117 00195/06/DE).

lange aufgeschoben werden, wie dieses Risiko besteht; das soll dazu dienen, die Vernichtung oder Veränderung von Beweismitteln durch diese Person zu verhindern und somit Beweismittel zu sichern. Diese Ausnahme muss restriktiv und fallbezogen angewandt werden.

Rechte auf Auskunft, Berichtigung und Löschung von Daten
Nach Artikel 12 der Richtlinie hat jede betroffene Person das Recht auf Zugang zu den sie betreffenden Daten, um ihre Richtigkeit zu überprüfen und sie zu berichtigen, falls sie unrichtig, unvollständig oder überholt sind. Der in der EU für die Verarbeitung Verantwortliche hat sicherzustellen, dass die Rechte des Einzelnen auf Auskunft sowie auf Berichtigung unrichtiger, unvollständiger oder überholter personenbezogenen Daten vor der Übermittlung gewahrt werden.

Die Arbeitsgruppe schlägt vor, dass diese Verpflichtungen der Partei auferlegt werden, die die Informationen erhält. Dies könnte über eine gerichtliche Verfügung (Protective Order) erreicht werden. Das hätte den Vorteil, dass einer betroffenen Person die Überprüfung der personenbezogenen Daten ermöglicht würde und sie sich selbst davon überzeugen könnte, dass die Datenübermittlung nicht unverhältnismäßig ist.

Einschränkungen dieser Rechte sind nur aufgrund von Artikel 13 und nur im Einzelfall möglich, wenn beispielsweise die Rechte und Freiheiten anderer Personen geschützt werden müssen. Die Arbeitsgruppe stellt klar, dass die Rechte der betroffenen Person während des Gerichtsverfahrens weiter gelten und es keinen allgemeinen Verzicht auf Auskunfts- oder Änderungsrechte gibt.

Es ist allerdings darauf hinzuweisen, dass sich aus diesen Rechten ein Konflikt mit den prozessualen Anforderungen ergeben könnte, zu einem bestimmten Zeitpunkt fixierte Daten aufzubewahren, da Datenänderungen (wenn auch nur für Berichtigungszwecke) eine Änderung der Beweismittel in der Streitsache bewirken würden.

Datensicherheit
Gemäß Artikel 17 der Richtlinie führt der für die Verarbeitung Verantwortliche alle geeigneten technischen und organisatorischen Maßnahmen durch, die für den Schutz gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust und die unberechtigte Weitergabe oder den unberechtigten Zugang erforderlich sind. Diese Maßnahmen müssen in einem angemessenen Verhältnis zu der Untersuchung der entsprechend den Sicherheitsvorschriften der einzelnen Mitgliedstaaten angesprochenen Fragen stehen. Diese Auflagen sollen nicht nur für den für die Verarbeitung Verantwortlichen gelten, sondern auch für Anwaltskanzleien, die mit der Streitsache befasst sind, sowie für Personen, die ihnen zuarbeiten, und alle anderen Experten, die an der Sammlung oder Überprüfung der Informationen beteiligt sind. Gleiches gilt für die Gerichte, da ein Großteil der relevanten personenbezogenen Daten, die für den Ausgang des Verfahrens erheblich sind, bei ihnen aufbewahrt werden.

Externe Dienstleister
Werden externe Dienstleister beispielsweise als sachverständige Zeugen im Streitverfahren eingesetzt, so bleibt der für die Verarbeitung Verantwortliche für die entsprechenden Verarbeitungen zuständig, da diese Dienstleister im Sinne der Richtlinie als Verarbeiter tätig sind.

Die externen Dienstleister müssen ebenfalls die Grundsätze der Richtlinie beachten. Sie haben sicherzustellen, dass die Informationen gemäß den Grundsätzen der Richtlinie gesammelt und verarbeitet werden und dass sie lediglich für die spezifische Zweckbestimmung verarbeitet werden, für die sie erhoben wurden. Sie müssen sich insbesondere an die strikten Vertraulichkeitsbestimmungen halten und dürfen die verarbeiteten Informationen nur an bestimmte Personen weitergeben. Sie haben ferner die Aufbewahrungsfristen einzuhalten, die für den für die Verarbeitung Verantwortlichen gelten. Der für die Verarbeitung Verantwortliche muss auch regelmäßig überprüfen, ob die externen Dienstleister die Bestimmungen der Richtlinie einhalten.

Übermittlungen in Drittländer

Wenn personenbezogene Daten in Drittländer übermittelt werden, finden die Artikel 25 und 26 der Richtlinie Anwendung.

Gewährleistet das Drittland, in das die Daten übermittelt werden sollen, kein angemessenes Schutzniveau im Sinne von Artikel 25, so können die Daten unter folgenden Voraussetzungen übermittelt werden:

(1) Der Empfänger der personenbezogenen Daten ist ein Unternehmen mit Sitz in den USA, das die Grundsätze des „sicheren Hafens“ (Safe Harbour Scheme) angenommen hat.
(2) Der Empfänger hat mit dem EU-Unternehmen, das die Daten übermittelt, einen Übermittlungsvertrag geschlossen, in dem das EU-Unternehmen ausreichende Garantien bietet, beispielsweise auf der Grundlage der Standardvertragsklauseln der Europäischen Kommission in ihren Entscheidungen vom 15. Juni 2001 oder vom 27. Dezember 2004.
(3) Der Empfänger hat verbindliche unternehmensinterne Datenschutzregelungen (BCR) eingeführt, die von den zuständigen Datenschutzstellen genehmigt wurden.

Handelt es sich bei der Übermittlung personenbezogener Daten für einen Rechtsstreit voraussichtlich um eine einzige Übermittlung aller relevanten Informationen, wäre ein möglicher Verarbeitungsgrund nach Artikel 26 Absatz 1 Buchstabe d der Richtlinie gegeben, wenn die Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich oder gesetzlich vorgeschrieben ist. Im Falle der Übermittlung einer signifikanten Datenmenge sollte die Anwendung der BCR oder der Grundsätze des „sicheren Hafens“ in Betracht gezogen werden. Die Arbeitsgruppe bekräftigt jedoch ihre frühere Stellungnahme, dass Artikel 26 Absatz 1 Buchstabe d nicht zur Rechtfertigung der Übermittlung der Datensätze aller Angestellten der Muttergesellschaft für den Fall herangezogen werden kann, dass eines Tages ein Gerichtsverfahren in den USA angestrengt werden könnte[14].

Die Arbeitsgruppe erkennt an, dass ein Rechtshilfeersuchen auf der Grundlage des Haager Übereinkommens eine formelle Grundlage für die Übermittlung personenbezogener Daten darstellt, doch haben nicht alle Mitgliedstaaten das Haager Übereinkommen unterzeichnet und die, die es unterzeichnet haben, haben unter Umständen einen Vorbehalt erklärt.

[14] WP 114, S. 15.

Möglicherweise bestehen Bedenken aufgrund der möglichen Dauer eines solchen Rechtshilfeverfahrens, doch kennen sich die Gerichte, beispielsweise in den Vereinigten Staaten, mit der Anwendung des Haager Übereinkommens aus und können entsprechende Fristen im Streitverfahren berücksichtigen. Wo die Anwendung des Haager Übereinkommens möglich ist, fordert die Arbeitsgruppe, die Übermittlung von Informationen für prozessuale Zwecke zuerst auf der Grundlage des Übereinkommens in Erwägung zu ziehen.

Fazit

Dieses Arbeitspapier stellt eine erste Betrachtung der Übermittlung personenbezogener Daten zur Verwendung in grenzübergreifenden zivilrechtlichen Verfahren dar. Es ist als Einladung an alle Beteiligten, ausländische Gerichte und sonstige Akteure gedacht, sich an einer öffentlichen Konsultation zu beteiligen und in einen Dialog mit der Arbeitsgruppe einzutreten.

Brüssel, den 11.2.2009

Für die Datenschutzgruppe
Der Vorsitzende
Alex TÜRK