BEITRÄGE

AXEL SPIES / CHRISTIAN SCHRÖDER

Auswirkungen der elektronischen Beweiserhebung (eDiscovery) in den USA auf deutsche Unternehmen

In den USA sammeln Kläger und Beklagte in Zivilverfahren notwendige Beweismittel in großem Umfang ohne Einwirkung des Richters im Wege der „Discovery". Sind die Dokumente elektronisch vorhanden (E-Mails, PDF-Dateien, Tabellenkalkulationen, elektronische Anrufbeantworter, elektronisch gespeicherte Fotos), existieren weitgehende Löschungsverbote, Speicher- und Vorlagepflichten nach den kürzlich ergänzten Regeln 26 und 34 der US-Federal Rules of Civil Procedures – teilweise bevor es überhaupt zu einem gerichtlichen Verfahren kommt. Diese Electronic Discovery (abgekürzt: eDiscovery) führt nicht nur zu Konflikten zwischen den Parteien eines Zivilverfahrens, sondern häufig auch innerhalb von Unternehmen, z.B. wenn die Tochtergesellschaft bei einer Datenübermittlung in die USA aus Gründen des Datenschutzes nicht „mitziehen" will. Besondere Brisanz erhält das Thema durch das seit 1.1.2008 geltende deutsche Gesetz zur Vorratsdatenspeicherung, da nunmehr sehr umfangreiche Daten über den Telefonverkehr und bald auch den E-Mail-Verkehr von den TK-Unternehmen und Internet Service Providern (ISP) gespeichert werden müssen. Auch wenn diese Daten laut Gesetz nur für die Verfolgung schwerer Straftaten zur Verfügung stehen sollen, dürfte sich der Druck auf die diese Daten speichernden Unternehmen in Europa verstärken, diese nunmehr vorhandenen Informationen (Anrufer, Zeit, Sender, Empfänger) auch in Verfahren vor US-Gerichten und Behörden einzuführen. Der Beitrag versucht, die US-Rechtslage auf ihre Vereinbarkeit mit deutschem Datenschutzrecht zu prüfen und Lösungsansätze aufzuzeigen.

I. Das US-Recht

In zunehmendem Maße werden in den USA ansässige Unternehmen bei einem drohenden oder schon anhängigen Rechtstreit oder einem behördlichen Verfahren aufgefordert oder verpflichtet, elektronisch gespeicherte Dokumente in großem Umfang vorzulegen, selbst wenn sich die Informationen bei Tochtergesellschaften oder verbundenen Unternehmen im Ausland befinden. All diese Unternehmen müssen sich mit den aus europäischer Sicht sehr weitgehenden US-Vorschriften für die eDiscovery auseinandersetzen.[1] Die Sammlung, Vorhaltung und Übermittlung dieser Unterlagen bindet enorme Unternehmensressourcen.

Während die deutschen Behörden auf diese Entwicklung eher abwartend reagieren, hat die in internationalen Angelegenheiten sehr aktive französische Datenschutzbehörde *Commission Nationale de l'Informatique et des Libertés* (*CNIL*) bereits Alarm geschlagen und in einer Erklärung v. 15.1.2008 eine umfassende Untersuchung der Auswirkungen der eDiscovery auf französische Unternehmen und französisches Datenschutzrecht angekündigt.[2] Sanktionen hat die *CNIL* gegen Unternehmen, die der eDiscovery aus den USA nachkommen, noch nicht verhängt. Es ist auch nicht ersichtlich, dass international tätige Unternehmen oder natürliche Personen ihre sensiblen Datenbanken bereits nach Frankreich verlegen, um sie vor Zugriff aus den USA zu schützen. Detaillierte Untersuchungen der Grenzen der eDiscovery oder Urteile aus deutscher Warte stehen noch aus. Die *Art. 29-Arbeitsgruppe der Datenschutzbehörden in der EU* hat sich laut einer Pressemitteilung des Themas bereits angenommen, aber derzeit noch keine Stellungnahme veröffentlicht.[3] Im Folgenden werden die US-rechtlichen Anforderungen der eDiscovery dargestellt und erläutert sowie anschließend auf ihre Vereinbarkeit mit deutschem Datenschutzrecht geprüft.

1. Aufbewahrungspflichten für einen drohenden oder absehbaren Rechtsstreit

Ist für ein Unternehmen absehbar, dass es zu einem Rechtsstreit kommt, besteht für das Unternehmen nach US-Recht die Pflicht zu einem „Litigation Hold" (Löschungsverbot von potenziellem Prozessmaterial) für physisch oder elektronisch vorhandene Dokumente, die sich in seiner Kontrolle befinden. Sinn dieses Löschungverbots ist es, dass das Unternehmen, wenn es tatsächlich zum Prozess kommt, der anderen Partei oder Behörde die für die Rechtsverfolgung nötigen Dokumente vorlegen kann. Diese Pflicht besteht: (1) für alle Informationen, die nach vernünftiger Würdigung aller Umstände zu einer Aufdeckung von zulässigen Beweismitteln führen könnten und (2) für Informationen, die mit vernünftiger Wahrscheinlichkeit das Unternehmen i.R.d. der anschließenden Discovery der anderen Partei vorlegen muss.[4] Die Schwelle für die Relevanz dieser Dokumente ist niedrig. Für in Euro-

1) Die Lit. zur eDiscovery in den USA wächst nahezu täglich. Das Thema „international eDiscovery" wird allerdings meist nur kursorisch behandelt – von einigen Ausnahmen abgesehen – z.B.: *Bennet*, Practising Law Institute Litigation and Administrative Practice Course Handbook Series Litigation PLI Order No. 11596 October–December, 2007; *Bender*, BNA World Data Protection Report 01/08, S. 19. Die letzte größere, weiterhin lesenswerte deutsche Monografie zur US-Discovery stammt von *Juncker*, Discovery im deutsch-amerikanischen Rechtsverkehr, 1988.

2) *CNIL*-Mitt. v. 15.1.2007: „Les entreprises inquiètes du développement des règles leur imposant la communication de données personnelles aux Etats-Unis": abrufbar unter: http://www.cnil.fr/index.php?id=2379&news[uid]=512&cHash=0b7756c4aa.

3) PM der *Art. 29-Arbeitsgruppe* v. 20.4.2007 und 18./19.2.2008, abrufbar unter: http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_20_04_07_en.pdf und http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_18_19_02_08_en.pdf.

4) Vgl. *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003) – „Zubulake IV".

■ Dr. Axel Spies, C.E.P. Paris, ist Rechtsanwalt bei Bingham McCutchen in Washington DC. Dr. Christian Schröder ist Notarassessor in Asbach.

pa agierende US-Unternehmen oder europäische Unternehmen mit Niederlassungen oder Tochtergesellschaften in den USA bedeutet das, dass sie große Mengen von Informationen, einschließlich personenbezogener Daten, speichern müssen – gleich ob sich die Informationen in den USA oder anderswo befinden. Die meisten Unternehmen sind darauf nicht vorbereitet. Bewahrt die Gesellschaft die Informationen nicht auf, gilt dies in den USA als „Spoliation"[5] (Beweisvereitelung), die zu erheblichen prozessualen Sanktionen und Geldstrafen führen kann.[6] Überdies kann der US-Richter eine sog. Adverse Interference Order erlassen: die Jury in dem Gerichtsverfahren wird instruiert anzunehmen, dass das vernichtete Dokument gegen die Partei spricht, die es vernichtet hat. Vorsätzliche Spoliation kann in den USA überdies strafrechtliche Folgen haben. Während bereits einige international agierende Unternehmen mit Sitz in den USA interne weltweit geltende Richtlinien zur Umsetzung des „Litigation Hold" haben, stellen viele deutsche Unternehmen teilweise mehr oder weniger konzeptlos alle aus den USA eingeforderten Informationen ohne vorherige Prüfung zur Verfügung oder reagieren einfach gar nicht. Neben dieser Vorhaltepflicht für Prozesse gibt es weitere Vorlagepflichten nach US-Recht, die nachfolgend beschrieben werden.

2. Informationsaustausch im Rahmen der Discovery

Das amerikanische Zivilprozessrecht sieht die Möglichkeit einer „Pre-Trial Discovery" vor. Hierbei handelt es sich um ein Verfahren, im Rahmen dessen die Parteien nicht nur schriftliche Beweisfragen stellen und Zeugen vernehmen, sondern auch Dokumente und Informationen, die sich nicht in ihrem Besitz befinden, aber für die Rechtsverfolgung von Bedeutung sein könnten, von der gegnerischen Partei herausverlangen können. Schon sehr früh fordern in einem Rechtsstreit in den USA Kläger und Beklagte von den gegnerischen Seiten die Vorlegung von zahlreichen Dokumenten an, manchmal viele tausend Seiten (Discovery Requests). Einer richterlichen Anordnung bedarf es in der Regel nicht. Die Einzelheiten ergeben sich für die Bundesgerichte aus Regel 34(a) Federal Rules of Civil Procedures – FRCP.[7] Gem. Regel 34 FRCP umfasst der Begriff „Dokumente" auch die elektronisch gespeicherten Informationen. Dabei ist es unerheblich, ob die Informationen streitentscheidend sind – eine bloße Relevanz reicht aus (Regel 26(b) (1) FRCP).[8] In größeren Verfahren werden viele tausend Dokumente gesichtet und meist elektronisch, z.B. durch die Einschaltung von Subunternehmern, über das Internet oder Intranet den Anwälten passwortgeschützt zugänglich gemacht. Nur in wenigen Fällen, z.B. wenn die elektronische Kommunikation unter das Anwaltsprivileg fällt, besteht keine Vorlegungspflicht. Die Regeln für die US-Zivilprozesse regen an, dass beide Parteien Verabredungen über die technische Umsetzung – das Wie und Wann – der Discovery treffen. Die Richter greifen allenfalls korrigierend ein, z.B. wenn die Anforderung der Dokumente zum mit der Klage zu erzielenden Ergebnis in keinem Verhältnis steht.[9] Viele US-Bundesstaaten haben die FRCP ganz oder weitgehend übernommen. Kommt eine Partei der Vorlegungspflicht nicht nach, drohen empfindliche Geldstrafen und andere Sanktionen.

Der Vollständigkeit halber zu erwähnen ist, dass ähnlich weitgehende Übermittlungspflichten gegen im Ausland ansässige natürliche oder juristische Personen auch bei strafrechtlichen oder anderen behördlichen Ermittlungen von US-Behörden bestehen können, z.B. bei der Ermittlung von Wettbewerbsverstößen durch das *US-Department of Justice* oder Ermittlungen der *US-Securities and Exchanges Commission* nach dem Sarbanes Oxley Act[10] oder dem Foreign Corrupt Practices Act, Letzterer verbietet z.B. Zahlungen an ausländische Amtsträger zum Zwecke der Bestechung.[11]

II. Datenschutzrecht: Auswirkungen auf die eDiscovery

1. Unterschiedlicher Ansatz der verschiedenen Rechtsordnungen und bisherige Praxis bei Konflikten mit europäischem Datenschutzrecht

Die Praxis zeigt, dass die deutschen Unternehmen – sei es aus Angst vor Sanktionen des US-Richters, sei es auf Grund unreflektierter Ausführungen einer Anweisung der US-Zentrale, sei es aus Sorglosigkeit oder aus Unkenntnis des deutschen Rechts – den Herausgabeverlangen häufig vollumfänglich nachkommen. Folglich ist es völlig illusorisch (und würde auch in den USA auf wenig Verständnis stoßen), den Datenfluss für eDiscovery-Zwecke aus Deutschland in die USA ganz unterbinden zu wollen. Dann wäre das BDSG aus US-Sicht ein „Blocking Statute" – ein unfreundlicher Akt, den das US-Gericht versuchen würde zu umgehen. Fest steht allerdings auch, dass deutsches Recht durchaus auf in Deutschland gesammelte oder gespeicherte personenbezogene Daten anwendbar und daher einzuhalten ist. Dem Rechtsanwender stellt sich damit die undankbare Aufgabe, die unterschiedlichen Ansätze auf einen Nenner zu bringen. Von Deutschland aus betrachtet zeigt sich sehr bald, dass der Datenschutz in den USA grundsätzlich anders strukturiert ist als in der EU, weshalb in den USA nicht viel Verständnis zu erwarten ist. Schon der Begriff „Datenschutz" passt nicht, weil damit in den USA in erster Linie die physische Sicherheit der Daten gemeint ist. „Privacy" und Datenschutz sind nicht identisch: Die US-Rechtsprechung tut sich sehr schwer, aus dem

---

5) Black's Law Dictionary (2004): „Spoliation: [...] The intentional destruction, mutilation, alteration, or concealment of evidence, usu. a document. If proved, spoliation may be used to establish that the evidence was unfavorable to the party responsible. ... ".

6) Beispiel für ein Unterliegen: *In re NTL, Inc. Sec. Litig.*, 2007 WL 241344 (S.D.N.Y. Jan. 30, 2007): „The court found that NTL Europe's „utter failure" to preserve relevant documents and ESI was „at least grossly negligent," and granted the Gordon plaintiffs' motion for an adverse inference instruction, the precise wording of which would be determined by the District Judge".

7) „A party may serve on any other party a request [...]: 1) to produce and permit the requesting party or its representative to inspect, copy, test, or sample the following items in the responding party's possession, custody, or control: any designated documents or electronically stored information – including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations – stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form ...".

8) „Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any non-privileged matter that is relevant to any party's claim or defense – including the existence, description, nature, custody, condition, and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter. For good cause, the court may order discovery of any matter relevant to the subject matter involved in the action. Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence".

9) S. im Einzelnen Rule 26 (b) (2) FRCP.

10) Gem. 18 U.S.C. §§ 1512, 1519 Sarbanes Oxley Act begeht derjenige eine Straftat, der Dokumente mit der Absicht ändert oder zerstört, um Ermittlungen von US-Behörden zu verhindern. Die Vorschriften setzen nicht voraus, dass sich die Dokumente in den USA befinden.

11) Kommt das Unternehmen der Aufforderung nicht nach, machen sich ihre Geschäftsführer und Manager u.U. einer „Obstruction of Justice" schuldig, die u.a. zu einem faktischen Einreiseverbot in die USA und anderen Sanktionen mittels Rechtshilfe über die Grenze führen können. Festnahmen von Managern bei der US-Einreise hat es schon gegeben.

durch die US-Verfassung garantierten Recht auf Privatsphäre (privacy) zur Abwehr von staatlichen Eingriffen auch Ansprüche gegenüber Privaten herzuleiten.[12] Es gibt in den USA kein übergreifendes Datenschutzgesetz wie das deutsche BDSG.[13] Stattdessen gibt es eine ganze Reihe von sektorspezifischen (und sehr detaillierten) Regeln für verschiedene Industriebereiche, z.B. für Kundendaten in der TK-Industrie (CNPI) oder für Gesundheitsdaten. Ferner unterscheiden sich die spezifischen Datenschutzgesetze erheblich zwischen den einzelnen US-Bundesstaaten; Landesdatenschutzbeauftragte, die Datenschutzfragen koordinieren könnten, gibt es nicht. Große Firmen wie *Google* mit allein 16 Büros in den USA müssen diese Bundesgesetze und evtl. einzelstaatlichen Regeln befolgen.

Bei den US-Gerichten hat es sich bislang nur wenig herumgesprochen, dass überhaupt europäisches Datenschutzrecht möglicherweise der Übersendung von manchmal tausenden von Dokumenten mit personenbezogenen Daten in die USA entgegensteht. Und selbst wenn ein Konflikt mit europäischem Datenschutzrecht offenbar wird, half dies den europäischen Unternehmen bislang nur wenig. Zwar könnten US-Gerichte nach den in den USA viel beachteten, aber rechtlich nicht bindenden „Restatement of Foreign Law Relations" von der Vorlage von Dokumenten aus dem Ausland absehen. Die Gerichte müssen das aber nicht, vor allem, wenn die Partei nicht erst alle Hebel in Bewegung gesetzt hat, an die Daten im Ausland zu kommen.[14] Auch hat das *Bundesgericht des Northern District of California* vor einigen Monaten im Verfahren *Jones v. Deutsche Bank* entschieden, dass die Vorschriften des Haager Beweisübereinkommens, welches die Beweiserhebung für internationale Sachverhalte regelt und daher ggf. auch das beklagte Unternehmen schützen konnte, nicht für das Gericht bindend seien und es für die Beklagte als „international entity with worldwide operations" zumutbar und durchführbar sei, im Ausland befindliche Dokumente in den USA vorzulegen. Die Souveränität anderer Nationen sei durch die Vorlagepflicht nicht ernsthaft beeinträchtigt.[15] Das *Bezirksgericht des Southern District of New York* entschied in einem anderen Fall, dass ein leitender Manager des beklagten Unternehmens „Kontrolle" über die außerhalb der USA befindlichen Dokumente der Gesellschaft habe und er deshalb diese Dokumente vorlegen müsse.[16] Noch im Mai 2007 hat ein US-Bezirksgericht entschieden, dass die mögliche Unvereinbarkeit einer Übermittlung von personenbezogenen Daten nach niederländischem Recht der Rechtmäßigkeit eines Discovery-Herausgabeverlangens nicht grundsätzlich entgegensteht, sondern dass im Urteil näher aufgezählte US-Interessen mit denjenigen des Staates, aus denen die Daten kommen, gegeneinander abgewogen werden müssen.[17] Eine solche Abwägung setzt aber zunächst voraus, dass das Unternehmen überhaupt mit hinreichender Gewissheit einen behaupteten Verstoß gegen das europäische Datenschutzrecht darlegen kann. Und das ist, wie sich im folgenden Abschnitt zeigen wird, kein Spaziergang. In dem genannten Fall hat der US-Richter diese Diskussion „geschickt" umgangen, indem er feststellte, die Beklagten seien an dem Rechtskonflikt selbst schuld, weil sie sich für ihren Server den Standort der Niederlande bewusst so ausgesucht hätten – womöglich um in den Genuss der Übermittlungsrestriktionen für personenbezogene Daten zu gelangen. Indes entschied der *Supreme Court von Texas* im Fall *Volkswagen AG v. Valdez*[18] (1995) nach Abwägung der Interessen, dass *VW* ein internes Telefonverzeichnis der deutschen *VW AG* nicht im Wege der Discovery in die USA herausgeben muss. Inwieweit der deutsche Datenschutz bei dieser Abwägung eine Rolle gespielt hat, ist allerdings nicht klar aus der Entscheidung ablesbar.

Hinzu tritt schließlich noch folgender Umstand: Zwar sind auf völkerrechtlicher Ebene die USA und Deutschland beide Vertragsparteien des Haager Beweisübereinkommens; deutsche Unternehmen müssten daher eigentlich gegen Herausgabeverlangen geschützt sein, da Deutschland nach dem im Übereinkommen abgegebenen Vorbehalt keine Rechtshilfeersuchen auf Grund von Pre-Trial Discovery aus den USA bedient.[19] Die Praxis sieht aber anders aus, weil dieser Begriff nirgends im Abkommen hinreichend definiert ist. Die US-Richter lassen – sollten die deutschen Behörden das Ersuchen wirklich einmal blockieren – durchaus die Beweiserhebung aus den USA unter Umgehung des Übereinkommens direkt bei der Partei im Ausland zu.[20] Der Schutz des Haager Übereinkommens ist daher in der Praxis schwach.

2. Konfliktfelder

Die durch die eDiscovery entstehenden potenziellen Konfliktfelder zwischen beiden Rechtsordnungen sind zahlreich, z.B.:

- fehlende Zustimmung von Arbeitnehmern vor Sichtung und ggf. vor Übersendung ihrer personenbezogenen Daten,
- unverhältnismäßiger Umfang der Datensammlung in deutschen Unternehmen durch Einscannen von Dokumenten oder Überspielen ganzer Datensammlungen auf Festplatten,
- Übermitteln von personenbezogenen Daten in die USA unter Umgehung der Vorgaben des BDSG für die Übermittlung von personenbezogenen Daten ins Ausland,
- fehlende Einsichtnahmemöglichkeit für Personen, deren personenbezogene Daten übermittelt wurden.

Dieser Konflikt wird auch nicht dadurch vermieden, dass in jedem Fall der eDiscovery über die Grenze hinweg nach Deutschland ein deutscher Richter eingeschaltet werden muss. Das BDSG sieht das in seinen auf internatio-

12) Vgl. umfassende Untersuchung in *Schröder*, Die Haftung für Verstöße gegen Privacy Policies und Codes of Conduct nach US-amerikanischem und deutschem Recht, Frankfurter Studien zum Datenschutz, 2007, S. 21 ff.; *Spies/Stutz*, DuD 2006, 373; www.datenschutz-nord.de/presse/veroeffentlichungen/spies_stutz.pdf.

13) Vgl. *Schröder* (o. Fußn. 12), S. 21 ff.

14) S. Restatement (Third) of Foreign Relations Law Section 422(2)(a): „If disclosure of information located outside the United States is prohibited by a law, regulation, or order of a court or other authority of the state in which the information or prospective witness is located, or of the state of which a prospective witness is a national: (a) a court or agency in the United States may require the person to whom the order is directed to make a good faith effort to secure permission from the foreign authorities to make the information available;
(b) a court or agency should not ordinarily impose sanctions of contempt, dismissal, or default on a party that has failed to comply with the order for production, except in cases of deliberate concealment or removal of information or a failure to make a good faith effort in accordance with paragraph (a)."

15) *Jones v. Deutsche Bank AG*, No. C 04 5357 JW (*RS*), 2006 U.S. Dist. Lexis 14631, at 11–13 (N.D. Ca. Mar. 10, 2006) (Magistrate Judge Memo).

16) *In re Flag Telecom Holdings, Ltd.*, 236 F.R.D. 177, 182 (S.D.N.Y. 2006) unter Berufung auf die „Aerospatiale"-Entscheidung des *US Supreme Court: Societé Nationale Industrielle Aerospatiale* v. *U.S. Dist. Court for S. D. of Iowa*, 482 U.S. 522 (1987).

17) *Columbia Pictures Indus. v. Bunnell*, 2007 U.S. Dist. LEXIS 46364 (C.D. Cal. June 19, 2007) unter Verweis auf: *Société Nationale Industrielle Aerospatiale v. United States District Court*, 544 n. 29 (1987); Spies, MMR 3/2008, S. XVIII.

18) *Volkswagen AG v. Valdez*, 909 SW 2nd 900 (Texas 1995).

19) S. dazu näher *Spies*, MMR 7/2007, S. V.

20) S.o. die in Fußn. 16 u. 17 zit. US-Entscheidungen.

nalen Datentransfers gemünzten §§ 4b und 4c BDSG, auf die noch näher einzugehen sein wird, nicht vor.

III. Die Vereinbarkeit der eDiscovery Rules mit deutschem Datenschutzrecht

Unternehmen, deren personenbezogene Daten dem deutschen Datenschutzrecht unterliegen, müssen nicht nur die Vorgaben des US-Rechts beachten, sondern zugleich die sich aus der eDiscovery ergebenden Anforderungen in mehrfacher Hinsicht auf Vereinbarkeit mit dem deutschen Datenschutz- und Arbeitsrecht prüfen. Bei fehlender Einhaltung dieser deutschen Vorgaben drohen Schadensersatzansprüche, Bußgelder und ggf. sogar Geld- oder Freiheitsstrafen. Dabei ist aus der in diesem Artikel näher untersuchten datenschutzrechtlichen Perspektive zwischen vier jeweils für sich betrachtet erlaubnispflichtigen Tatbeständen zu unterscheiden, die nunmehr nachstehend unter 1.–4. näher beleuchtet werden sollen:

1. Zulässigkeit der Speicherung von Daten nach Wegfall des ursprünglichen Speichergrundes

Unternehmen, die grundsätzlich von Discovery-Verfahren in den USA betroffen sein könnten, haben schon bei der Frage der Aufbewahrung von E-Mails oder sonstigen möglicherweise in einem Discovery-Verfahren herauszugebenden Dokumenten die Vereinbarkeit mit deutschem Datenschutzrecht zu prüfen, da das US-amerikanische Recht das deutsche Datenschutzrecht nicht überlagert oder verdrängt.[21] Gem. § 1 Abs. 5 BDSG findet deutsches Datenschutzrecht auf sämtliche Datenverarbeitungen von im Inland belegenen verantwortlichen Stellen Anwendung – einschließlich der Auslandsübermittlung der Daten.

Abgesehen von einer in der Praxis nur theoretisch einholbaren Einwilligung sämtlicher Betroffenen sind folglich die Schranken des BDSG zu beachten. Nach dem BDSG aber ist eine unbegrenzte Speicherung von personenbezogenen Daten ohne konkreten und rechtlich anerkannten Zweck unzulässig, vgl. §§ 4 Abs. 1, 28 BDSG. Folglich sind auch weiterhin sämtliche Daten zu löschen bzw. zu vernichten, sollte der für ihre Erhebung eingreifende Zweck entfallen und sonstige rechtlich anerkannte Zwecke nicht eingreifen.

Ein solcher anderer Rechtsgrund für das Verlängern der Speicherung könnte sich aber aus § 28 Abs. 1 Nr. 2 BDSG ergeben. So könnte das aus den eDiscovery-Regeln folgende Gebot, bestimmte Daten aufzubewahren (Litigation Freeze), ein berechtigtes Interesse der verantwortlichen Stelle gem. § 28 Abs. 1 Nr. 2 BDSG begründen und hiernach eine Speicherung dieser Daten erlauben. Immerhin drohen den betroffenen Unternehmen durch die eDiscovery-Regeln in den USA – wie vorstehend beschrieben – erhebliche Sanktionen.

Damit die verlängerte Speicherung gem. § 28 Abs. 1 Nr. 2 BDSG zulässig ist, müsste die Speicherung von Daten zu berechtigten Zwecken der für die Verarbeitung dieser Daten verantwortlichen Stelle erforderlich sein und es dürften keine überwiegenden schutzwürdigen Interessen der Betroffenen erkennbar sein. Grundsätzlich stellt die Verteidigung von Rechtsansprüchen vor Gericht ein berechtigtes Interesse i.S.d. § 28 Abs. 1 Nr. 2 BDSG dar, Daten für diese Zwecke zu verarbeiten und zu übermitteln.[22] Dies gilt jedoch immer unter der Voraussetzung, dass im Einzelfall keine überwiegenden Interessen der Betroffenen gegen die verlängerte Speicherung bzw. Verarbeitung sprechen. Als Minus zur weiterhin im Unternehmen allgemein zugänglichen Speicherung dieser Daten könnte daher auch an eine Sperrung der Daten i.S.d. § 3 Abs. 4 Nr. 4 BDSG gedacht werden, um den Zugriff auf diese Daten allein für den Zweck der möglichen Rechtsverteidigung einzuschränken und so die Interessenabwägung zu Gunsten der Zulässigkeit der Speicherung zu stärken.

Aus der grundsätzlichen Anwendbarkeit des § 28 Abs. 1 Nr. 2 BDSG ergeben sich für die Zulässigkeit der Speicherung von personenbezogenen Daten i.R.d. eDiscovery folgende Ergebnisse:

- Die lediglich hypothetische Möglichkeit, gewisse Daten in einem möglichen Prozess in den USA nutzen zu können oder sogar übermitteln zu müssen, dürfte als hinreichender Zweck i.S.d. § 28 Abs. 1 Nr. 2 BDSG nicht zur Rechtfertigung der verlängerten Speicherung genügen. Denn die Speicherung dieser Daten ist nicht i.S.d. § 28 Abs. 1 Nr. 2 BDSG erforderlich, da nicht einmal das US-amerikanische Recht die Speicherung von Daten ohne Anlass, d.h. ohne Absehbarkeit eines Rechtsstreits, zwingend vorgibt. Eine Sammlung von Daten auf „Vorrat" ohne drohendes Verfahren ist mit dem deutschen und europäischen Datenschutzrecht nicht vereinbar.
- Selbst wenn ein Rechtsstreit absehbar ist, fordert das US-amerikanische Recht nicht die Aufbewahrung sämtlicher Daten, sondern nur solcher, die nach vernünftiger Würdigung sämtlicher Umstände zu einer Discovery von zulässigen Beweismitteln führen könnten, bzw. solcher, bei denen mit vernünftiger Wahrscheinlichkeit abzusehen ist, dass diese in einer anschließenden Discovery der Gegenseite vorzulegen sind. Nur bzgl. der Speicherung solcher Daten kann folglich überhaupt ein berechtigtes Interesse bestehen, dieselben nach Wegfall des eigentlichen Speicherungszwecks weiterhin aufzubewahren. Da die Daten nur für einen absehbaren Zeitraum, nämlich währenddessen ein Rechtsstreit absehbar ist, gespeichert werden müssen, dürfte regelmäßig auch kein entgegenstehendes Interesse der Betroffenen überwiegen und die Speicherung somit zulässig sein.

2. Zulässigkeit der Sichtung und Durchsuchung von Daten

Auch die spätere z.B. auf Anfrage der eigenen Anwälte oder auf Anfrage der Gegenseite erfolgende Sichtung und Durchsuchung der Daten am Sitz der verantwortlichen Stelle (also dem deutschen Unternehmen vor Ort) ist für sich gem. §§ 4 Abs. 1, 28 BDSG erlaubnispflichtig, da sie zumindest eine Nutzung gem. § 3 Abs. 5 BDSG darstellt. Üblicherweise bedient man sich in der Praxis häufig eines deutschen Anwalts vor Ort, der die Daten beim deutschen Unternehmen sichtet und auf ihre Prozessrelevanz in Abstimmung mit dem Datenschutzbeauftragen des Unternehmens überprüft. Greift man auch bzgl. dieser Nutzung auf die Ermächtigungsgrundlage des § 28 Abs. 1 Nr. 2 BDSG zurück, muss eine solche Sichtung und Vorsortierung durch einen Experten vor Ort ebenfalls zur Verteidigung berechtigter Interessen des Unternehmens erforderlich sein. Für die Erforderlichkeit und damit die Zulässigkeit dieser Vorsortierung spricht, dass hierdurch die An-

21) Stellungnahme (Opinion 1/2006) der *Art. 29-Arbeitsgruppe* zur Zulässigkeit von Whistleblowing Hotlines v. 1.2.2006, WP 117, S. 8, abrufbar unter: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2006_en.htm.

22) Vgl. §§ 28 Abs. 1 Nr. 2, Abs. 6 Nr. 3 BDSG; *Simitis*, in: Simitis, BDSG, § 4c Rdnr. 21.

zahl der später ggf. in die USA übermittelten Daten auf das nach US-Recht erforderliche Minimum reduziert wird. Zumeist werden die Daten auch mit automatischen Filterprogrammen durchsucht. Dadurch wird gewährleistet, dass nachfolgend nur noch diejenigen Dokumente tatsächlich eingesehen werden müssen, die auf Grund der gewählten Stichwörter mit einiger Wahrscheinlichkeit Bezug zum Rechtsstreit haben.

3. Zulässigkeit der Übermittlung der Daten an die eigenen Anwälte der verantwortlichen Stelle in den USA

Sofern die eigenen US-Anwälte der verantwortlichen Stelle im Falle eines Rechtsstreits oder Pre-Trial Discovery-Verfahrens die nach dem Filtern gewonnenen Dokumente einsehen wollen, wird auch die Übermittlung der Daten an diese ggf. gem. § 28 Abs. 1 Nr. 2 BDSG zu rechtfertigen sein, da die eigenen Anwälte die Daten einsehen müssen, um eine effektive Rechtsverteidigung der verantwortlichen Stelle zu gewährleisten.[23] Allerdings stellt sich bei Anwälten mit Niederlassung in den USA das Problem, dass die EU die USA als Staat mit „nicht adäquatem Datenschutzniveau" i.S.d. § 4b Abs. 2 BDSG (Art. 25 Abs. 3 i.V.m. Abs. 6 EU-Datenschutz-RL) eingestuft hat. Insofern müssen Daten vor einer Übermittlung in die USA grundsätzlich durch gesonderte Maßnahmen geschützt werden, vgl. §§ 4b, 4c BDSG.

Üblicherweise wird hierfür zwischen der Daten exportierenden und Daten importierenden Stelle ein Vertrag auf Basis der von der *EU-Kommission* erlassenen Standardvertragsklauseln geschlossen.[24] In den USA bietet sich Unternehmen darüber hinaus grundsätzlich auch der Beitritt zum US/EU-Safe-Harbor-Programm an, das die EU mit den USA ausgehandelt hat und das vom *US-Department of Commerce* verwaltet wird.[25] Manche Industriebereiche sind jedoch von diesem Programm ausgenommen, z.B. die von der *Federal Communications Commission* (*FCC*) beaufsichtigte TK-Branche und weite Teile des Finanzsektors.

Möglicherweise hilft aber § 4c Abs. 1 Nr. 4 BDSG weiter, wonach eine Übermittlung von personenbezogenen Daten in ein Drittland mit keinem adäquaten Datenschutzniveau zulässig ist, wenn sie zur Ausübung oder Verteidigung von „Rechtsansprüchen vor Gericht" erforderlich ist. Diese Ausnahme betrifft nicht nur die Übermittlung an das Gericht selbst, sondern auch an sämtliche am gerichtlichen Verfahren beteiligten Personen, solange die Übermittlung auf den Verfahrenszweck beschränkt ist.[26] Insofern dürfte die Einsichtnahme in die betroffenen Dateien durch die eigenen Anwälte in den USA wegen ihrer Erforderlichkeit zur Verteidigung der Rechtsansprüche der verantwortlichen Stelle gem. §§ 4c Abs. 1 Nr. 4, 28 Abs. 1 Nr. 2 BDSG zulässig sein. Bedienen sich die Anwälte jedoch Dritter, um die Dokumente zu speichern, dürfte der sichere Weg sein, dass diese Dritten die EU-Standardvertragsklauseln unterzeichnen oder sich entsprechend dem o.g. Safe Harbor-Programm vom *US-Department of Commerce* registrieren lassen, um so gem. § 4c Abs. 2 BDSG i.V.m. Art. 25 Abs. 6 Datenschutz-RL ein ausreichendes Schutzniveau für den Transfer von personenbezogenen Daten in die USA zu gewährleisten.

4. Zulässigkeit der Übermittlung der Daten an die Prozessgegner und das Gericht

Die Zulässigkeit der Weiterleitung der nach deutschem zivilprozessualem Verständnis u.U. sehr umfassenden Dokumentenbestände an die Gegner in einem US-Prozess könnte sich ebenfalls grundsätzlich aus § 28 Abs. 1 Nr. 2 i.V.m. § 4c Abs. 1 Nr. 4 BDSG ergeben. Immerhin dient auch diese Übermittlung der Daten unmittelbar der Verteidigung von Rechtsansprüchen vor einem ausländischen Gericht. Bei Nichtbefolgung der US-eDiscovery-Vorgaben drohen sogar die zuvor beschriebenen Sanktionen durch den US-Richter.

a) Mangelnde Zweckbindung

Problematisch könnte jedoch die Vorgabe in § 4c Abs. 1 Satz 2 BDSG sein, wonach die Stelle, an die die Daten übermittelt werden, darauf hinzuweisen ist, dass die übermittelten Daten nur zu dem Zweck verarbeitet oder genutzt werden dürfen, zu dessen Erfüllung sie übermittelt werden. Diese Pflicht zum Hinweis auf die Zweckbindung könnte aber ins Leere laufen, wenn schon vor der Datenübermittlung an die Dritten, d.h. den Gegner oder das Gericht, klar ist, dass diese Stellen sich nicht an die Zweckbindung halten werden, da sie dies entweder nach US-amerikanischem Recht nicht müssen oder sogar rechtlich gar nicht dürfen. So handelt es sich z.B. bei in US-Verfahren eingebrachte Dokumente grundsätzlich um Dokumente, die der Öffentlichkeit auf Antrag zugänglich gemacht werden müssen, sofern nicht Geschäftsgeheimnisse oder andere höherrangige Interessen berührt sind, worüber das Gericht entscheidet.[27] Sollte folglich die Zweckbindung der Übermittlung nicht gewährleistet sein, könnte vieles dafür sprechen, dass dann die Interessen der Betroffenen überwiegen und eine Übermittlung gem. § 28 Abs. 1 Nr. 2 BDSG wie aber auch § 4c Abs. 2 BDSG unzulässig ist.

b) Vorrang der deutschen Rechtsordnung

Hinzu kommt die Überlegung, dass zwar aus Sicht des betroffenen Unternehmens wegen des Zwangs des US-Rechts die Übermittlung dieser Daten erforderlich ist, dass bei einem solch für andere Rechtsordnungen offenen Rechtsverständnis der §§ 4c Abs. 1 Nr. 4, 28 Abs. 1 Nr. 2 BDSG allerdings ein effektiver Schutz der personenbezogenen Daten höchst gefährdet erscheint. Immerhin würde dann jeder durch fremde Rechtsordnungen auf deutsche Unternehmen ausgeübte Zwang automatisch zur Freigabe von ansonsten nach europäischem/deutschem Recht streng geschützten Daten von natürlichen Personen führen. Auch die *Art. 29-Gruppe* der Datenschutzbeauftragten in der EU sah in ihrer Stellungnahme zu den Whistleblowing-Hotlines nach dem US-Sarbanes Oxely Act die Gefahr, dass ausländisches Recht das europäische Datenschutzrecht aushöhle, würde das europäische Datenschutzrecht jede zwingende ausländische Vorgabe zur Übermittlung von personenbezogenen Daten anerkennen.[28]

---

23) *Simitis* stützt die Zulässigkeit der Übermittlung von Daten an eigene Anwälte sogar auf das Mandatsverhältnis und damit auf § 28 Abs. 1 Nr. 1 BDSG, *Simitis* (o. Fußn. 22), § 28 Rdnr. 87.

24) Entscheidungen der *Kommission* (2002/16/EG) v. 27.12.2001; 2001/497/EG v. 15.6.2001 und (2004/915/EG) v. 27.12., alle abrufbar unter: http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_de.htm.

25) Kommission 2000/520/EG v. 26.7.2000 – ABl. EG Nr. L 215/7 v. 25.8.2000, abrufbar unter: http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_de.htm. Viele US-Unternehmen unterwerfen sich den Safe Harbor-Principles sehr ungern, u.a. deswegen, weil sie dadurch unter die Aufsicht der US-Behörden für die ordnungsgemäße Umsetzung des Datenschutzes fallen. Außerdem scheuen sie den Aufwand eines jährlichen Audits.

26) Vgl. *Simitis* (o.Fußn. 22), § 4c Rdnr. 21.

27) *Junker* (o. Fußn. 1), S. 140 unter Verweis auf *American Tel. & Tel. Co. V. Grady*, 594 (7th Cir. 1979).

28) Stellungnahme der *Art. 29-Gruppe* zur Zulässigkeit von Whistleblowing-Hotlines v. 1.2.2006, WP 117, S. 8.

c) Die widerstreitenden Interessen

Will man ein solches Ergebnis vermeiden, muss die Zulässigkeit der Übermittlung von personenbezogenen Daten ins außereuropäische Ausland zur Rechtsverteidigung auf nach autonom europäischem Rechtsverständnis vertretbare Umstände eingegrenzt werden und zudem alles getan werden, um den an das US-Gericht bzw. die gegnerische Partei gelangten Daten größtmöglichen Schutz zuteil werden zu lassen. Insofern wäre hiernach nur diejenige Übermittlung von personenbezogenen Daten „erforderlich" und damit zulässig, die nach autonomer Wertung des europäischen Datenschutzrechts noch hinnehmbar ist. Kriterien für diese Abwägung sind, soweit ersichtlich, noch nicht von den Datenschutzaufsichtsbehörden formuliert worden. Lediglich in einer Pressemitteilung der *Art. 29-Gruppe* wurde bekannt gegeben, dass diese sich mit dem Thema befasst.[29]

I.R.d. gebotenen Einzelfallabwägung dürfte zum einen das grundsätzlich gem. §§ 4c Abs. 1 Nr. 4 wie 28 Abs. 6 BDSG anerkannte Interesse an einer effektiven Rechtsverteidigung zu berücksichtigen sein. Für die Zulässigkeit einer Übermittlung sprächen auch die deutschen internationalzivilprozessrechtlichen Wertungen, wonach Beweiserhebungsbeschlüsse, denen deutsche Unternehmen in internationalen Verfahren unterliegen, abgesehen von Missbrauchsfällen grundsätzlich anzuerkennen sind.[30] Das *BVerfG* hielt in dem vorstehend zitierten Beschluss fest, dass der deutsche Bürger, der sich im internationalen Rechtsverkehr bewegt, nicht grundsätzlich vor der Verantwortlichkeit gegenüber ausländischen Rechtsordnungen zu schützen sei.[31] Andererseits ist aber zu berücksichtigen, dass Deutschland z.B. im Haager Beweisübereinkommen ausdrücklich einen Vorbehalt gegen die Durchsetzung US-amerikanischer Pre-Trial Discovery-Herausgabeverlangen erhoben hat.[32] Auch kann man die der Entscheidung des *BVerfG* vermutlich zu Grunde liegende Wertung, wonach derjenige, der sich selbst in den Anwendungsbereich der fremden Rechtsordnung gebracht hat, weniger schützenswert ist, nicht ohne weiteres auf die Zulässigkeit der Herausgabe personenbezogener Daten Dritter übertragen. Denn im Unterschied zu einem deutschen Unternehmen, welches wegen bestimmter Anknüpfungspunkte, z.B. wirtschaftlicher Tätigkeit auf dem Gebiet der USA, sich selbst in den Anwendungsbereich des US-Rechts gebracht hat, gilt dies nicht für Dritte (z.B. Mitarbeiter dieses Unternehmens, Empfänger und Sender von E-Mails von und zu dem Unternehmen), deren personenbezogene Daten nun in die USA übermittelt werden sollen. Diese Dritten haben u.U. zu der ihre Daten herausverlangenden Rechtsordnung überhaupt keinen Bezug und sind daher unvermindert schützenswert.

IV. Fazit: Möglicher Interessenausgleich

Jede verantwortliche Stelle und die betreffenden Parteien selbst müssen folglich versuchen, möglichst großen Einklang zwischen beiden in Konflikt zueinander stehenden Rechtsordnungen herzustellen. Dies wird zum einen eine strenge Begrenzung des zu übermittelnden Datenmaterials auf Dokumente mit Bezug zum Rechtsstreit erfordern. Der entscheidende Ort für eine solche Diskussion der Parteien über eine Begrenzung der zugänglich zu machenden Dokumente ist in einem frühen Stadium des Prozesses die sog. Discovery Conference der Parteien nach Regel 26(f) FCPR[33] oder der Pre-Trial Conference gem. Rule 16 FCPR.[34] Gerade der Discovery Conference kommt hierbei eine zentrale Bedeutung zu. Beide Parteien sollten sich spätestens zu diesem Zeitpunkt ernsthaft Gedanken gemacht haben, wo sich die verlangten Daten und elektronischen Unterlagen befinden. Das erfordert natürlich von beiden Parteien, dass sie von einem Ansatz des „alles oder nichts" abrücken und die Rechtspflichten auf beiden Seiten des Atlantiks zumindest zur Kenntnis nehmen. Sie sollten auch wissen, welche der Unterlagen sich bereits in den USA befinden.

Überdies sollte nach vorheriger anwaltlicher Sichtung auf die Übermittlung nicht unmittelbar prozessrelevanter sensitiver Daten verzichtet werden, z.B. durch Schwärzen von Textpassagen oder Namen. Schließlich sollte versucht werden, vom US-Gericht eine Sperrung der Daten gegen eine Einsichtnahme durch Dritte zu erlangen. So könnte der US-Prozessvertreter eine solche Sperrung über sog. „Protective Orders" oder ein „Filing under Seal" (vertrauliche Einreichung von Unterlagen bei Gericht) erreichen.[35] Denkbar ist auch eine Prozessvereinbarung, wonach nur die Anwälte der Gegenseite, nicht aber die Parteien selbst die Unterlagen sichten. All diese Versuche dürften ggf. auch aus US-prozessualer Sicht dazu führen, dass ein Bemühen der verantwortlichen Stelle in Deutschland anerkannt wird, möglichst umfassend Daten herauszugeben und mit dem US-Gericht zu kooperieren. Dies wiederum kann dazu führen, dass das US-Gericht selbst bei Verweigerung der Übermittlung von bestimmten Daten von dem Erlass von Sanktionen absieht, wenn dieses Thema z.B. i.R.d. Discovery Conference eingehend mit der Gegenseite diskutiert wurde.[36]

Das beschriebene Prüfungs- und Abwägungsgebot befreit jedoch die betroffenen Unternehmen nicht von der großen Unsicherheit, entweder gegen das US-Recht oder gegen das deutsche Datenschutzrecht zu verstoßen. Deshalb sind die deutschen und europäischen Regierungsstellen, wie die *Art. 29-Arbeitsgruppe* in Brüssel, auf den Plan gerufen, um die Probleme zu erörtern und praktische Lösungen zu finden, die beide Seiten des Atlantiks akzeptieren können, ohne dass eine Seite der anderen mit dem Zaunpfahl möglicher Sanktionen winkt. Die *Art. 29-Arbeitsgruppe* der Datenschutzbehörden und das *US-Department of Commerce* wären hierfür ein geeignetes Forum. Dies könnte das Thema auf europäischer Ebene unter Einbeziehung der US-Regierung einer Lösung zuführen. Gespräche auf dieser Ebene sind anscheinend für dieses Jahr vorgesehen. Eine schnelle Klärung wäre sehr zu begrüßen.

---

29) PM der *Art. 29-Gruppe* v. 20.4.2007, http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_20_04_07_en.pdf.

30) Vgl. *BVerfG*, E. v. 24.1.2007 – 2 BvR 1133/04, abrufbar unter: http://www.bverfg.de/entscheidungen/rk20070124_2bvr113304.html.

31) *BVerfG* (o. Fußn. 30).

32) *Spies*, MMR 7/2007, S. V und VI.

33) „At any time after commencement of an action the court may direct the attorneys for the parties to appear before it for a conference on the subject of discovery ...".

34) S. insb. Abs. 2 i.V.m. Abs. 3 (B) (iii) von Rule 16: „The judge must issue the scheduling order as soon as practicable, but in any event within the earlier of 120 days after any defendant has been served with the complaint or 90 days after any defendant has appeared. . . The scheduling order may . . . provide for disclosure or discovery of electronically stored information." In Frage kommt z. B. eine Berufung auf Datenschutzregeln gem. Rule 26 (2) (B) FRCP:„ A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost."

35) *Junker* (o. Fußn. 1), S. 138, 141 zu FCPR Rule 26(c).

36) *Junker* (o. Fußn. 1), S. 397 f.

Beide Seiten haben schon bei der gemeinsamen Entwicklung des Systems der EU/US-Safe Harbor Principles und bei der Lösung des Streits um die Whistleblowing Hotlines[37] eng zusammengearbeitet. Das würde gewährleisten, dass eine EU-weite Lösung der Probleme gefunden wird, die die US-Richter eher überzeugt als ein Flickenteppich einzelstaatlicher Lösungen. Die Ergebnisses und Vorschläge der *Arbeitsgruppe 6* (International Electronic Information Management, Disclosure and Discovery) des in den USA sehr angesehenen Instituts „Sedona Conference"[38] sollten in die Diskussionen auf Regierungsebene mit einfließen. Möglicherweise können auch die von den US-Gerichten bei der Abwägung des Erlasses von Sanktionen entwickelten Kriterien in Europa weiterhelfen. So wurden z.B. in der Entscheidung *Columbia Pictures v. Brunnel* für die Abwägung zwischen US-Recht und deutschem Datenschutzrecht folgende Kriterien berücksichtigt:

- Wie wichtig sind die verlangten Dokumente für den anhängigen Rechtsstreit?
- Wie spezifisch hat die ersuchende Partei die verlangten Dokumente eingegrenzt?
- Gibt es Alternativen für die Partei, an diese Informationen zu kommen, ohne auf die sich in Deutschland befindlichen elektronischen Dokumente zuzugreifen?
- Inwieweit sind wichtige Staatsinteressen bei Nichtübermittlung der Informationen berührt?
- Wie aufwändig ist es für die ersuchte Partei, die verlangten Dokumente zu beschaffen?
- Hat die ersuchte Partei den Interessenkonflikt zwischen den Rechtsordnungen selbst herbeigeführt oder ist sie sonstwie dafür verantwortlich?[39]

Da das deutsche Datenschutzrecht dem Schutz des allgemeinen Persönlichkeitsrechts des Betroffenen dient, dürften die Kriterien wie „Bedeutung des Staatsinteresses" oder „Verursachung des Interessenkonflikts" jedoch eher von geringerer Bedeutung sein.

Auch aus diesem Abwägungskatalog wird allerdings deutlich, dass eine Klärung der deutschen bzw. europäischen Rechtslage dringend geboten ist. Denn je eher den Unternehmen klare und anwendbare Vorgaben für die Prüfung der Zulässigkeit der Datenübermittlung zur Verfügung stehen, desto eher werden die Unternehmen in die Lage versetzt, bei unterstellter Unzulässigkeit der Übermittlung diesen Rechtsstandpunkt ggf. auch erfolgversprechend im US-Verfahren geltend zu machen.[40] Sofern die Rechtslage für die Datenübermittlung aber selbst in Deutschland noch unklar ist, werden bloße Zweifel an der Vereinbarkeit der Übermittlung mit deutschem Datenschutzrecht US-Gerichte kaum überzeugen.

---

37) *Knoepfel*, Whistleblowing und Sarbanes-Oxley - kein extraterritorialer Arbeitnehmerschutz?, RIW 2007, 493-495.

38) http://www.sedonaconference.org/wgs. Die Aufgabe dieser international besetzten Arbeitsgruppe ist: „[t]o serve as a global forum and think tank for sharing information, developing best practices, and advising and educating on matters of national and international law and policy regarding the disclosure/discovery, management, and protection of electronically stored information."

39) *Columbia Pictures v. Brunnel* (o. Fußn.17) *48 (S. 14). Der Kriterienkatalog geht anscheinend zurück auf *Richmark v. Timber Falling Consultant*, 959 F.2d 1468 (1475) – 9th Cir. 1992.

40) S. zur Verteidigung über das sog. „Privilege": *Junker* (o. Fußn. 1), S. 124 ff.