US District Court Utah: Deutsches Datenschutzrecht blockiert nicht die US-Beweiserhebung (E-Discovery)

BDSG §4c; HaagerBewÜK
Urteil vom 21.1.2010 – Case No. 2:08cv569, 2010 U.S. Dist. LEXIS 4566 – ACCESSDATA CORPORATION v. ALSTE TECHNOLOGIES GmbH

Leitsätze der Redaktion

1. Das deutsche BDSG, insb. § 4c BDSG, steht nach Abwägung einer Datenübermittlung aus Deutschland in die USA im Zivilprozess nicht grundsätzlich entgegen.

2. Das Haager Abkommen über die Rechtshilfe in Zivilsachen und Erhebung von Beweis im Ausland v. 18.3.1970 (HaagerBewÜK) und das dort vorgesehene Prozedere eines Ersuchens auf Beweisaufnahme über eine Zentrale Behörde in Deutschland ist nicht anwendbar. Vielmehr erfolgt die Beweiserhebung durch die Parteien i.R.d. sog. „E-Discovery" im vorliegenden Fall nach den Regeln des US-Zivilprozessrechts.

Sachverhalt

Die in Utah ansässige Kl. und die in Deutschland ansässige Bekl. streiten über die Auslegung eines Software-Vertriebsvertrags (Reseller Agreement) und darauf basierenden Provisionen vor dem Bundesgericht (in Zivilsachen) in Utah. Die Kl. hat die Beweisermittlung zwischen den Parteien (Discovery) eingeleitet und verlangt von der Bekl. zahlreiche in Deutschland elektronisch gespeicherte Dokumente (im Wesentlichen E-Mails). Die Bekl. weigert sich, der Aufforderung der Kl. nachzukommen und verteidigt sich u.a. mit der pauschalen Behauptung, dass die Vorlage von personenbezogenen Daten ihres Kunden gegen das BDSG und „die deutsche Verfassung" verstoße. Außerdem müsse die Kl. ihr Gesuch im Wege der internationalen Rechtshilfe in Zivilsachen nach dem HaagerBewÜK der in Deutschland ansässigen Bekl. zustellen und dort durchsetzen lassen, was un-

streitig nicht geschehen ist. Die Kl. beantragte deshalb einen Gerichtsbeschluss (*Motion to Compel*), um die Durchsetzung der Vorlage der Dokumente durch die Bekl. zu erzwingen.

Aus den Gründen
...„(1) German Data Protection Act and Hague Convention

While *ALSTE* asserts that providing personal information about its customers and their employee "would be a huge breach of fundamental privacy laws in Germany", *ALSTE* has failed to demonstrate the verity of this assertion. *ALSTE* has not cited to the particular provisions of the German Data Protection Act ("GDPA") and/or German Constitution that would prohibit disclosure of personal third-party information. Based on the court's brief review of the GDPA, it appears that it does not necessarily bar discovery of personal information. In particular, Part I, Section 4c of the GDPA, entitled "Derogation", provides that the transfer of personal information to countries that do not have the same level of data protection "shall be lawful, if . . . the data subject has given his/her consent [or] . . . the transfer is necessary or legally required . . . for the establishment, exercise or defense of legal claims". The GDPA further states that "[t]he body to which the data are transferred shall be informed that the transferred data may be processed or used only for the purpose for which they are being transferred". *ALSTE* has not demonstrated that it has been unable to obtain consent from its customers or that it has even attempted to seek consent. *ALSTE* has also failed to address this particular provision of the GDPA or explain why it would not apply in the instant case.

Furthermore, even assuming that the GDPA prohibited disclosure of personal third-party information, the *United States Supreme Court* has addressed this issue. See Societe Nationale Industrielle Aerospatiale v. United States District Court, 482 U.S. 522, 544, 107 S. Ct. 2542, 96 L. Ed. 2d 461 (1987). In that case, the *Supreme Court* held that "[i]t is well settled that such [blocking] statutes do not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that statute". Id. at 544 n.29. The *Supreme Court* also cited to the American Law Institute Restatement, which summarizes the interplay between blocking statues and discovery orders generally: "[W]hen a state has jurisdiction to prescribe and its courts have jurisdiction to adjudicate, adjudication should (subject to generally applicable rules of evidence) take place on the basis of the best information available . . . . [Blocking] statutes that frustrate this goal need not be given the same deference by courts of the United States as substantive rules of law at variance with the law of the United States."

Id. (quoting Restatement of Foreign Relations Law of the United States (Revised) § 437, Reporter's Note 5 (1986)). *ALSTE* further argues that AccessData should be required to comply with the rules set forth in the Hague Convention for Taking Evidence Abroad with respect to private information regarding *ALSTE's* customers. The court disagrees. As the *Supreme Court* also held in *Societe Nationale*, "we cannot accept petitioners' invitation to announce a new rule of law that would require first resort to [Hague] Convention procedures whenever discovery is sought from a foreign litigant". Id. Parties might properly be required to resort to Hague Convention procedures "in suits involving foreign states, either as parties or as sovereigns with a coordinate interest in the litigation", or if "the additional cost of transportation of documents or witnesses to or from foreign locations . . . increase[s] the danger that discovery [is] sought for [an] improper purpose". Id. At 546. But neither circumstance is present in this breach of contract action where the costs of transmitting information and electronic documents ought to be relatively minimal.

Therefore, *ALSTE* has failed to demonstrate that the GDPA applies or that the Hague Convention procedures are required in this matter. Accordingly, based on the foregoing, this court concludes that the GDPA and Hague Convention procedures are not applicable to the discovery in this case." ...

Anmerkung

RA Dr. Axel Spies, Bingham McCutchen, Washington DC/
RA Dr. Christian Schröder, Hengeler Mueller, Düsseldorf

Amerikakritiker werden jetzt nach der Lektüre ausrufen: Wenn sich ein US-Richter im tiefen Utah mit den Feinheiten des deutschen BDSG auseinandersetzen muss, kann nichts Vernünftiges herauskommen. Im vorliegenden Fall – das müssen auch diese Kritiker einräumen – ist dem Bundesrichter *Warner* jedenfalls positiv anzurechnen, dass er sich überhaupt mit deutschem Datenschutzrecht auseinandergesetzt hat, wo doch noch nicht einmal die englische Übersetzung des deutschen Worts „Datenschutz" mit „Data Protection" in den USA deckungsgleich ist. „Data Protection" bedeutet in den USA die physische Sicherung der Daten oder des Datenträgers – „Privacy" und Datenschutz sind auch nicht begrifflich identisch. Manche Richter schießen da eher aus der Hüfte und stellen sich auf den Standpunkt, dass immer die lex fori gilt (oder wie kürzlich ein US-Fernsehrichter so treffend feststellte: „This is my court and these are my rules – only for me to break."). Solche Richter für die Feinheiten des deutschen Datenschutzes zu begeistern, ist eine Herkulesaufgabe.

Der vorliegende Sachverhalt ist recht banal. Er kommt so oder so ähnlich immer wieder vor und verdeutlicht gut, dass auch in den USA vertiefte Kenntnisse des europäischen Datenschutzrechts sinnvoll sein können, möchte man Strafen oder Herausgabeverlangen vermeiden: Eine deutsches Unternehmen (*ALSTE*) wurde in den USA zivilrechtlich verklagt und sollte zahlreiche elektronische Dokumente i.R.d. in den USA in Zivilverfahren üblichen Beweiserhebung durch die Parteien (Discovery) an die Kl. herausgeben. Die Bekl. weigerte sich mit dem pauschalen Verweis darauf, dass das deutsche Datenschutzrecht die Übertragung von personenbezogenen Daten an den Gegner in den USA nicht zulasse.

Nun kann man sich lange darüber streiten, ob und wann §§ 4c, 28 ff. BDSG i.V.m. Art. 25 und 26 der EU Datenschutz-RL 95/46/EG eine Übermittlung zu Zwecken der Discovery zulassen (vgl. hierzu ausf. *Spies/Schröder*, MMR 2008, 275 ff. sowie die Stellungnahme der *Artikel 29-Arbeitsgruppe* der europäischen Datenschutzbehörden, Working Paper WP 158 v. 11.2.2009). Wenig überzeugend ist jedoch der Hinweis von Richter *Warner*, dass *ALSTE* hätte dartun müssen, dass sie keine Einwilligung für die Übermittlung der Daten hatte bzw. hätte einholen können. So weist die *Artikel 29-Gruppe* zutreffend darauf hin, dass eine informierte und freiwillig erteilte Einwilligung bei Pre-Trial Discovery Verfahren regelmäßig nicht nachgewiesen werden kann (s. S. 8 ff. des WP 158). Des Weiteren zitierte Richter *Warner* auch die weiteren Alternativen des § 4c Abs. 1 Nr. 4 BDSG, wonach eine Übermittlung von personenbezogenen Daten auch in die USA zulässig sein kann, wenn die Übermittlung für die Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich ist. Wenngleich die erste Alternative nicht eingreift, da das öffentliche Interesse (zumindest nicht ausschließlich) von einer fremden, außereuropäischen Jurisdiktion vorgegeben werden kann, hätte *ALSTE* in der Tat zur zweiten Alternative vortragen müssen. Diese Alternative greift regelmäßig ein und kann daher eine Datenübermittlung insb. dann rechtfertigen, wenn Maßnahmen zur Gewährleistung des Verhältnismäßigkeitsgebots getroffen sind (vgl. *Spies/Schröder*, MMR 2008, 275, 279 ff.; S. 9 ff. des WP 158). Gegen eine Übermittlung könnte jedoch z.B. das Fernmeldegeheimnis sprechen,

welches bei E-Mails deutscher Arbeitgeber eingreift, wenn die private Nutzung von E-Mails erlaubt ist. *ALSTE* hatte offenbar aber nicht einmal versucht, durch eine überzeugende Darlegung der deutschen Rechtsgrundlagen das US-Gericht davon zu überzeugen, warum ihrer Einschätzung nach die verlangte Übermittlung von E-Mails gegen das deutsche Recht verstößt. Insofern urteilte Richter *Warner* folgerichtig, dass *ALSTE* ihn nicht davon überzeugt habe, dass das deutsche Recht der Übermittlung entgegensteht.

Aus deutscher Sicht gefährlich erscheinen jedoch die weiteren Ausführungen von Richter *Warner*. Dort beruft er sich ohne abschließende Klärung der Frage, ob deutsches Recht nun der Herausgabe der Daten grds. entgegensteht oder nicht, auf eine bekannte Leitentscheidung des *US Supreme Court*: Société Nationale Industrielle Aerospatiale v. United States District Court, 482 U.S. 522, 544, von 1987 (man könnte sagen, aus der IT-rechtlichen Steinzeit). Hiernach treten ausländische Gesetze, die tatsächlich einem Herausgabeverlangen entgegenstehen (blokking statute) regelmäßig ggü. dem US-amerikanischen Recht auf Herausgabe zurück: „[W]hen a state has jurisdiction to prescribe and its courts have jurisdiction to adjudicate, adjudication should (subject to generally applicable rules of evidence) take place on the basis of the best information available . . . . [Blokking] statutes that frustrate this goal need not be given the same deference by courts of the United States as substantive rules of law at variance with the law of the United States." Ferner zitiert er die gleiche Entscheidung, wonach auch das HaagerBewÜK nach Abwägung der maßgeblichen Umstände ggü. den Regeln für das Bundesprozessrecht (FCPR) zurücktritt. Richter *Warner* übersieht dabei aber, dass die US-Rechtsprechung keineswegs zu einer pauschalen Bevorzugung des US-Rechts kommt, sondern eine Abwägung der widerstreitenden Interessen fordert (s. Société Nationale Industrielle Aérospatiale v United States District Court, 482 U.S. 522, 544 n.28 (1987); Volkswagen AG v Valdez [No.95-0514, November 16, 1995, Texas Supreme Court] and In re: Bayco, Litigation MDL no. 1431 (Mfd/JGL), March 21, 2003).

Was tun? Die Bekl. ist in einer juristischen Zwickmühle. Legt sie die elektronischen Dokumente nicht der Kl. vor, bekommt sie empfindliche Sanktionen des US-Gerichts wegen Beweisvereitelung (Spoiliation) usw. zu spüren – schlimmstenfalls Beugehaft. Verbringt sie – ohne sorgfältige Prüfung der Zulässigkeit und ggf. Beantragung von Schutzmaßnahmen für die übermittelten Daten – personenbezogene Daten aus Deutschland in die USA, riskiert sie Sanktionen u.a. nach dem BDSG wegen unerlaubter Datenübermittlung ins Ausland. Die deutschen Datenschützer dürften wenig erfreut sein, dass Richter *Warner* das BDSG – für den Fall, dass es tatsächlich einer Übermittlung der Daten in die USA entgegensteht – als „Blocking Statute" bewertet. Dann wäre das BDSG von den US-Gerichten nämlich grds. nicht zu beachten. Umgekehrt empfinden viele US-Juristen den Vorwurf der EU geradezu ehrenrührig, dass die USA aus EU-Sicht ein Land mit „inadäquatem Datenschutz" sind. Wie dem auch sei, Urteile wie dieses sind beileibe kein Einzelfall und dürften den Druck auf die Prozessparteien erhöhen, sich zu vergleichen. Im vorliegenden Fall hatten die Parteien noch einmal Glück – es ging offensichtlich um eine relativ beschränkte Anzahl von Dokumenten (E-Mails) bei einem für US-Verhältnisse beinahe lächerlichen Streitwert von rd. US-$100.000. In größeren Verfahren müssen i.R.d. Discovery die Prozessparteien einander tausende, manchmal sogar Millionen von elektronisch gespeicherten oder physisch vorhandenen Dokumenten zur Sichtung und Auswertung vorlegen – ohne dass zwangsläufig ein Richter am Dokumentenaustausch beteiligt ist. Das zeigt, welche Dimension das Problem hat. Z. Zt. wird das Thema „E-Discovery", welches ja nicht nur im Zivilprozess, sondern auch bei weltweiten Ermittlungen von US-Behörden eine Rolle spielt, auf der politischen Ebene beraten. Die in den USA ansässige „Denkfabrik" Sedona Conference (www.thesedonaconference.org), Arbeitsgruppe 6, bemüht sich redlich, aber bislang ohne tiefgreifendes Ergebnis, zusammen mit der *Artikel 29-Gruppe* einen Mittelweg zu finden und den US-Juristen das europäische Datenschutzrecht und Prozessrecht näher darzulegen. In Deutschland gibt es u.a. einen XING-Blog zum Thema „E-Discovery", unter: www.xing.com/ediscovery, in dem Vertreter der Fachwelt Neuigkeiten zu dem Themenkomplex austauschen. Solange keine Klärung durch die Gerichte oder die politischen Kräfte herbeigeführt wird, wandelt der Rechtsanwender in einem juristischen Minenfeld.