E-Discovery

Lösungswege aus dem Spannungsfeld des Datenschutzes

Von Katharina A. Weimer, LL.M.

Der Begriff „E-Discovery" bewegt derzeit viele deutsche Unternehmen. Dahinter stecken bestimmte Pflichten zur Offenlegung von Informationen insbesondere nach US-amerikanischem Prozessrecht. Dies ist für deutsche Unternehmen besonders dann relevant, wenn sie selbst Prozesspartei in den USA sind, entweder als Kläger oder als Beklagte. In der Praxis kommt häufig auch der Fall vor, dass eine Mutter- oder Tochtergesellschaft eines deutschen Unternehmens in den USA verklagt wird oder selbst klagt und das deutsche Unternehmen Informationen besitzt, die für den Ausgang des Rechtsstreits relevant sind.

In allen diesen Fällen sind die Prozessparteien dazu verpflichtet, alle Informationen, die für den Rechtsstreit relevant sind, der gegnerischen Partei auf entsprechende Anfrage hin zur Verfügung zu stellen, auch und gerade, wenn sie der offenlegenden Partei zum Nachteil gereichen. Die Weigerung einer Partei, alle Informationen zur Verfügung zu stellen, kann nach dem einschlägigen US-Recht als Verhinderung eines „Fair Trial" ausgelegt und entsprechend sanktioniert werden. Solche Sanktionen reichen von der Unterstellung, dass die von der gegnerischen Partei vorgebrachten Behauptungen wahr sind, bis zum Unterliegen im Prozess aufgrund der Sanktionen.

Beide Parteien eines Gerichtsprozesses sind schon im Vorfeld des Verfahrens dazu verpflichtet, alle Informationen in ihrer Kontrolle, die möglicherweise für das Verfahren von Relevanz sind, gegenüber dem Gericht und der gegnerischen Partei offenzulegen. Diese Informationen sind bereits ab dem Zeitpunkt aufzubewahren, zu dem der Prozess begonnen hat oder die Parteien vernünftigerweise mit einem Rechtsstreit rechnen mussten. Aufgrund des Fortschritts der elektronischen Datenverarbeitung bedingt dies, dass mittlerweile eine kaum zu bewältigende Menge an Informationen zu speichern, zu sichten und ggf. zu übermitteln ist.

Unternehmen befinden sich nun in dem Spannungsfeld, dass viele der verlangten Informationen personenbezogene Daten enthalten, die nach den europäischen und deutschen Datenschutzbestimmungen geschützt sind und nicht ohne weiteres verarbeitet und übermittelt werden dürfen. Dies gilt speziell für berufliche E-Mail-Adressen und Inhalte von Geschäftskorrespondenz, Details zu bestimmten Projekten, sofern darin die beteiligten Personen genannt werden oder anderweitig bestimmbar sind, und ähnliche geschäftliche Informationen, die einer bestimmten (oder bestimmbaren) Person zuordenbar sind.

Die Übermittlung an einen Empfänger in den USA bedarf nach geltendem Datenschutzrecht zum einen einer Legitimierung jedes einzelnen Verarbeitungsschritts (also der Erhebung, der Speicherung, der Übermittlung in die USA und der dortigen Verarbeitung durch das Gericht bzw. die gegnerische Partei und deren Anwälte) und zum anderen eines angemessenen Schutzniveaus beim Empfänger.

Der Beitrag gibt einen kurzen Abriss der rechtlichen Grundlagen der E-Discovery sowie Empfehlungen für das Vorgehen im Unternehmen.

Legitimation der Verarbeitungsschritte

Die einzelnen Verarbeitungsschritte im Rahmen eines E-Discovery Verfahrens sind üblicherweise die Datenerhebung (1. Schritt) von den jeweils relevanten Betroffenen (oder „Custodians") und das Einspielen dieser Daten in eine getrennte Review-

Datenbank (2. Schritt). Hier können die Informationen noch vor Ort in Deutschland daraufhin überprüft werden, ob eine Übermittlung rechtlich überhaupt möglich ist, was bei besonderen Arten personenbezogener Daten in den meisten Fällen ausgeschlossen sein dürfte und bei privaten Informationen, die entsprechend gekennzeichnet sind (wie z.B. E-Mails in einem als „privat" gekennzeichneten Unterordner), auch zu bezweifeln ist. Bereits zu diesem Zeitpunkt sollte eine erste Prüfung der Relevanz für das anhängige Verfahren durchgeführt werden (3. Schritt). Erst im Anschluss daran werden die als „übermittelbar" eingestuften Informationen an das Gericht bzw. den Prozessgegner übermittelt (4. Schritt). In manchen Fällen findet zusätzlich eine Übermittlung an die mit dem Prozess betrauten Anwälte in den USA statt, die die Dokumente nochmals durchsehen und kategorisieren, so dass ein weiterer Verarbeitungsschritt anfällt. Die weitergehende Verarbeitung durch den Gegner bzw. das Gericht liegt meist nicht mehr im Einflussbereich des deutschen Unternehmens.

Keinesfalls ist eine solche Verarbeitungskette durch den Zweck des Arbeitsvertrags (§ 32 Bundesdatenschutzgesetz – BDSG) gedeckt. Auch würde die Vielzahl von Informationen anderer Betroffener wie Lieferanten, Kunden, Geschäftspartner, Dienstleister etc. nicht darunter gefasst werden können.

Die Berechtigung für das E-Discovery-Verfahren ist daher an anderer Stelle zu suchen. Sofern das deutsche Unternehmen selbst in den USA verklagt ist, ergäbe sich eine Legitimation aus § 28 Abs. 1 Nr. 2 BDSG, da das deutsche Unternehmen jedenfalls ein berechtigtes Interesse an der eigenen Verteidigung hat. Abhängig von der Ausgestaltung des Prozesses überwiegt dieses Interesse des Unternehmens die schutzwürdigen Interessen des Betroffenen, so dass die nach § 28 Abs. 1 Nr. 2 BDSG durchzuführende Abwägung zugunsten des Unternehmens ausfällt. Allerdings ist das Augenmerk darauf zu legen, dass die einzelne Datenverarbeitung tatsächlich notwendig ist für den verfolgten Zweck (die Verteidigung bzw. Durchsetzung eigener Ansprüche) und nicht lediglich vorteilhaft. Dies dürfte jedoch im Hinblick auf zwingendes Prozessrecht, das es zu befolgen gilt, bei tatsächlich relevanten Informationen unproblematisch sein.

Für den Fall, dass eine amerikanische Tochtergesellschaft eines deutschen Unternehmens in einen Prozess involviert ist, dürfte die Abwägung ähnlich ausfallen – die deutsche Muttergesellschaft hat üblicherweise ein ausgeprägtes Interesse daran, dass die Tochtergesellschaft sich adäquat verteidigen bzw. ihre Ansprüche durchsetzen kann. Diese Wertung kann (muss aber nicht) anders ausfallen, wenn die amerikanische Muttergesellschaft einer deutschen Tochter in den USA verklagt wird und nun umfangreiche Informationen der deutschen Tochter verlangt. Hier ist im Einzelfall zu entscheiden, inwiefern Informationen übermittelt werden dürfen und wie weit das berechtigte Interesse der deutschen Tochter am Ausgang des Rechtsstreits der amerikanischen Muttergesellschaft tatsächlich geht.

Angemessenes Datenschutzniveau beim Empfänger

Gemäß § 4b Abs. 2 BDSG hat die Übermittlung an Empfänger mit Sitz außerhalb des Europäischen Wirtschaftsraums zu unterbleiben, wenn ein angemessenes Datenschutzniveau nicht gewährleistet ist. Abgesehen von einigen Ländern, für welche die Europäische Kommission pauschal ein angemessenes Datenschutzniveau festgestellt hat – es handelt sich dabei um Andorra, Argentinien, Australien, Kanada, die Schweiz, die Faröer Inseln, Guernsey, Jersey, die Isle of Man sowie Israel –, fehlt es fast allen übrigen Ländern an entsprechenden Gesetzen, die für dort sitzende Empfänger ein angemessenes Datenschutzniveau gewährleisten. Die USA sind diesbezüglich keine Ausnahme. Daher ist das erforderliche Datenschutzniveau anderweitig herzustellen

Üblicherweise gibt es dazu drei Wege, die allerdings alle im Fall der E-Discovery nicht greifen:

- Der in den USA sitzende Empfänger kann sich nach dem Safe-Harbor-Programm selbst zertifizieren (mehr Informationen unter http://export.gov/safeharbor/). Auch wenn einige Anwaltskanzleien sich dem unterworfen haben, erscheint es als sehr unwahrscheinlich, dass sich die gegnerische Partei und US-Gerichte diesen Regeln unterwerfen können (im Fall des Gerichts) und dies auch tun werden.
- Die beteiligten Parteien könnten die von der Europäischen Kommission genehmigten Standardvertragsklauseln abschließen (mehr Informationen hierzu unter http://ec.europa.eu/justice/policies/privacy/modelcontracts/index_en.htm). Nach einer Entscheidung der Kommission stellen diese Klauseln einen Weg dar, ein angemessenes Datenschutzniveau beim Empfänger herzustellen. Allerdings dürfte es schwierig sein, die gegnerischen Anwälte und insbesondere das US-Gericht davon zu überzeugen, sich diesen Klauseln freiwillig zu unterwerfen.
- Die sogenannten „Binding Corporate Rules" gelten nur innerhalb von Konzernstrukturen und sind daher in dieser Situation kein probates Mittel zur Herstellung eines angemessenen Datenschutzniveaus.

Alternativ zu diesen Lösungswegen bleiben nur einige wenige Fälle, bei denen ein angemessenes Datenschutzniveau ausnahmsweise nicht notwendig ist. Eine davon ist die Einwilligung des Betroffenen, die jedoch in den meisten Fällen allein schon aufgrund der Anzahl an möglichen Betroffenen nicht praktikabel ist.

Allein zielführend erscheint die Ausnahme des § 4c Abs. 1 Nr. 4 BDSG, wonach das Datenschutzniveau dann nicht mehr ausschlaggebend ist, wenn die Datenübermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich ist. Problematisch dürfte diese Ausnahmeregelung als Grundlage für die Übermittlung allerdings in den Fällen sein, in denen nicht die verantwortliche Stelle selbst in den USA Partei eines Verfahrens ist, sondern ein Mutter- oder Tochterunternehmen, denn dann werden keine eigenen Positionen geltend gemacht oder verteidigt. Dies muss im Einzelfall überprüft werden.

Zusammenfassung und Empfehlungen

Die Datenübermittlung an die gegnerische Prozesspartei und das US-Gericht im Rahmen eines E-Discovery-Verfahrens erscheint unter dem Gesichtspunkt der Verteidigung gegen oder der Geltendmachung von Ansprüchen unter den obigen Voraussetzungen als legitim. Dies ist jedoch im Einzelfall zu überprüfen, und jedes Unternehmen sollte sich bereits im Vorhinein mit den Problemfeldern befassen. Dabei sollten im Idealfall die folgenden Schritte vorgenommen bzw. überprüft werden:

- Jedes Unternehmen sollte sich im Vorfeld Gedanken über die Handhabung solcher Streitfälle machen und entsprechende Prozesse mit Richtlinien implementieren. Sinnvollerweise wird bei Vorhandensein eines Betriebsrats eine Betriebsvereinbarung abgeschlossen, die zumindest den Umgang mit Arbeitnehmerdaten im Rahmen einer E-Discovery abdecken kann.
- Bei Bekanntwerden eines „möglichen" Streitfalls sollte bereits die interne Prüfung des Sachverhalts und der datenschutzrechtlichen Relevanz beginnen. Der (Konzern-)Betriebsrat sowie der Datenschutzbeauftragte sollten involviert werden.
- Ein „Litigation Hold" muss ausgesprochen und die betroffenen Mitarbeiter müssen entsprechend angewiesen werden.
- Die Daten werden eingesammelt und in einer gesonderten Datenbank gespeichert. Hier werden sie zunächst auf besondere Arten personenbezo-

gener Daten und Irrelevanz überprüft. Dies sollte noch in Deutschland geschehen. Nicht relevante Informationen sollten zumindest gesperrt werden.

- Erst anschließend sollte eine Übermittlung der Daten an die eigenen Anwälte in den USA bzw. an die gegnerische Partei und das Gericht erfolgen. Ggf. müssen prozessuale Sicherheitsvorkehrungen zum Schutz der Daten wie „Protective Orders" und Ähnliches in Erwägung gezogen werden.
- Nach Durchführung des Verfahrens wird der Litigation Hold aufgehoben, und die Daten sind zu löschen.

Es ist ratsam, alle Stufen dieses Vorgehens zu dokumentieren und bei Zweifeln die Datenschutzaufsicht zu involvieren. So gewappnet, haben deutsche Unternehmen die Möglichkeit, den Anforderungen des deutschen Datenschutzrechts gerecht zu werden, ohne hierdurch ein Unterliegen im Prozess in den USA zu provozieren.

Rechtsanwältin
Katharina A. Weimer ,
LL.M., Reed Smith LLP,
München

kweimer@reedsmith.com