

Dr. Ivo Geis

eDiscovery und Datenschutz

Hamburg, September 2008

<http://www.ivo-geis.de/>
geis@ivo-geis.de

Einleitung

Das US-amerikanische Recht ist das Leitrecht im Internet. Es zeigen sich immer wieder Konstellationen, in denen sich das US-Recht durchsetzt. Eine solche Konstellation besteht, wenn eine deutsche Muttergesellschaft für eine in den USA ansässige Tochtergesellschaft die E-Mail-Kommunikation speichert. Droht dem Tochterunternehmen in den USA ein Prozess, so muss die deutsche Muttergesellschaft der Tochtergesellschaft in den USA entsprechend den US-eDiscovery-Rules die E-Mail-Dokumente übermitteln, die für den Prozess relevant sein können (1.0). Dies kann zu Konflikten mit dem deutschen Datenschutzrecht führen (2.0). Die Löschungspflichten dieses Rechts sind streng und kennen kein Aufbewahrungsrecht aus prozessrechtlichen Gründen. Die Lösung dieses Rechtsrisikos oder zumindest seine Minimierung kann mit Binding Corporate Rules, Unternehmensregeln, gesucht werden (3.0), für deren Formulierung ein Vorschlag gemacht wird (4.0).

1.0 eDiscovery Rules

Unter dem Stichwort „eDiscovery“ wird die Beweisführung mit elektronischen Dokumenten im zivilrechtlichen Verfahren vor US-Gerichten diskutiert. Im US-amerikanischen Zivilprozessrecht ist das Vorhalten von Dokumenten besonders kritisch. Ist für ein Unternehmen absehbar, dass es zu einem Rechtsstreit kommt, besteht für das Unternehmen die Pflicht zu einem „Litigation Hold“, einem Lösungsverbot von potentiell Prozessmaterial, das sich in seiner Kontrolle befindet. Damit soll gesichert werden, dass das Unternehmen, wenn es zu einem Prozess kommt, der anderen Partei die für die Rechtsverfolgung nötigen Dokumente vorlegen kann. Dies gilt schon für das Vorverfahren, in dem Parteien Dokumente, die sich nicht in ihrem Besitz befinden, aber für die Rechtsverfolgung von Bedeutung sein können, von der gegnerischen Partei herausverlangen können (Pre-Trial-Discovery). Bewahrt die Gesellschaft die Informationen nicht auf, gilt dies als Beweisvereitelung (Spoliation), die zu prozessualen Sanktionen und Geldstrafen führen kann. So kann der Richter eine „Adverse Interference Order“ erlassen, mit der die Jury angewiesen wird, dass das vernichtete Dokument gegen die Partei spricht, die es vernichtet hat. Diese Regeln, die auch elektronische Dokumente umfassen, sind durch die Flut der

E-Mail-Kommunikation zu einem aktuell diskutierten Thema geworden.¹ Der Beweiswert der E-Mail-Kommunikation wird durch die Rules of Evidence und die Rules of Civil Procedure bestimmt. Nach den Rules of Evidence for United States Courts and Magistrates (Rule 1001 Definitions) gilt das "Recording" als zulässiges Beweismittel. Als Recording ist definiert: set down by typewriting on electronic recording². Nach den Federal Rules of Civil Procedure (Rule 34 Producing Documents, Electronically Stored Information) werden keine näheren Anforderungen gestellt, wie elektronisch gespeicherte Dokumente für das Gericht zu produzieren sind. Dies soll in nutzbarer Form (reasonably usable form) erfolgen.

2.0 Datenschutzrechtliche Aspekte

Das nach dem US-Zivilprozessrecht notwendige Speichern großer Mengen von Informationen mit Daten, die sich auf bestimmte Personen beziehen, ist ein datenschutzrechtliches Problem. Dieses Problem ist im US-Recht weniger ausgeprägt als im deutschen Recht. In den USA gibt es kein allgemeines Datenschutzgesetz wie das deutsche Bundesdatenschutzgesetz (BDSG), sondern sektorspezifische Gesetze. Als übergeordnetes datenschutzrechtliches Prinzip gilt das Right to Privacy, das aus den ersten vier Zusätzen zur US-Verfassung abgeleitet wird. Dieses Recht richtet sich nach der Rechtsprechung nur gegen staatliche Institutionen und nicht gegen Unternehmen. Vor diesem Hintergrund wird nach dem in den USA bestehenden Rechtsverständnis kein Konflikt zwischen der zivilprozessrechtlichen Pflicht zum Speichern von Datenmengen und dem Datenschutzrecht gesehen. Anders verhält sich das deutsche Datenschutzrecht, das auf deutsche Unternehmen, die wie die Nord/LB, in Deutschland für ihre US-amerikanische Niederlassung Dokumente mit personenbezogenen Daten speichern, anzuwenden ist. Probleme zwischen den Anforderungen des BDSG mit den Anforderungen der eDiscovery Rules entstehen, wenn elektronische Dokumente nach Wegfall der handelsrechtlichen/steuerrechtlichen Aufbewahrungspflicht für Zwecke der eDiscovery weiter gespeichert werden, wenn elektronische Dokumente auf ihre Prozessrelevanz durchsucht werden, wenn elektronische Dokumente in die USA an die eigenen Anwälte, an die Beweisgegner und an das Gericht übermittelt werden. In allen Fällen kommt als gesetzliche Grundlage § 28 Abs. 1 Nr. 2 BDSG in Frage. Hiernach ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten für eigenen Geschäftszwecke zulässig, „soweit es

¹ *Spies/Schröder*, MMR 2008, 275 ff., 275 f. und *Junker*, Electronic Discovery gegen deutsche Unternehmen, zum Verstoß der eDiscovery gegen das Haager Beweisübereinkommen (S. 25-50) und gegen allgemeine Regeln des Völkerrechts (S. 51-68).

² Siehe *Skupsky*, Legal Requirements, S. 66 f.

zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt“. In allen vier Fällen ist nicht eindeutig zu klären, dass die Interessen des Unternehmens, den Anforderungen der eDiscovery zu entsprechen, die schutzwürdigen Interessen des Betroffenen überwiegen. Dieser Zustand der Rechtsunsicherheit erhöht sich wegen der Übermittlung in die USA als ein Land, in dem aus europäischer Sicht nicht ein angemessenes Datenschutzniveau besteht. Da die Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erfolgt, könnte sie nach § 4c Abs. 1 Satz 1 Nr. 4 BDSG zulässig sein. Hierfür muss die Übermittlung „erforderlich“ sein. Dieser unbestimmte Begriff der Erforderlichkeit verursacht Rechtsunsicherheit. Nach dem Zweck des Datenschutzrechts muss der Begriff restriktiv ausgelegt werden und dürfen deshalb möglichst wenige Dokumente übermittelt werden. Hierfür wird ein US-amerikanisches Gericht kein Verständnis haben und auf der umfangreichen Dokumentation entsprechend den eDiscovery-Rules bestehen. Der Konflikt des deutschen Unternehmens zwischen deutschem Datenschutzrecht und eDiscovery-Rules ist damit unausweichlich.³ Ein Lösungsmöglichkeit für diesen Konflikt besteht in Binding Corporate Rules (BCR), die die Speicherung der Dokumente entsprechend den eDiscovery-Rules unter Berücksichtigung des deutschen Datenschutzrechts definieren.

3.0 Binding Corporate Rules zur Litigation Hold und zum Datenschutz

Binding Corporate Rules (BCR) gelten EU-rechtlich als die angebrachte Lösung, dass multinationale Unternehmen für die Übermittlung personenbezogener Daten außerhalb der Europäischen Union einen datenschutzrechtlichen Standard sichern⁴ Solche Regeln schaffen ein System, an das sich die Nutzer der Dokumente halten können und das für die Betroffenen den Umgang mit ihren Daten transparent macht. BCR zur Litigation und zum Datenschutz sind noch nicht publiziert. Sie sollten aus Richtlinien zur Umsetzung des Litigation Hold und zum möglichst datenschutzkonformen Umgang mit personenbezogenen Daten während der rechtlichen Auseinandersetzung in den USA bestehen. Ausgangspunkt einer BCR ist die zivilprozessrechtliche Notwendigkeit der „Litigation Hold“. Um diese Anforderung umzusetzen sollte ein Lösungsverbot für alle physisch oder elektronisch vorhandenen Dokumente bestimmt werden, die als Prozessmaterial in Frage kommen, wenn es absehbar

³ *Spies/Schröder*, MMR 2008, 275 ff., 276-280 und *Junker*, Electronic Discovery gegen deutsche Unternehmen, S. 73-80.

⁴ Working Paper 155 der Article 29 Data Protection Working Party.

ist, dass es zu einem Rechtsstreit kommt. Der datenschutzkonforme Umgang mit den Dokumenten kann durch verschiedene Methoden gesichert werden. Grundlegend ist, dass nur prozessrelevante und nicht wahllos alle Informationen, die aus den USA eingefordert werden, übermittelt werden. Nach Beginn des Prozesses bieten sich weitere Möglichkeiten zur Einschränkung des Prozessmaterials: In der Pre-Trial Conference (Rule 16 FCPR) und der Discovery Conference (Rule 26 (f) FCPR) können die Parteien in einem frühen Stadium des Prozesses über eine Begrenzung der zugänglich zu machenden Dokumente diskutieren. Der US-Prozessvertreter könnte versuchen, eine Sperrung der Daten gegen Einsichtnahme durch Dritte über sog. „Protective Orders“ oder ein „Filing under Seal“ (vertrauliche Einreichung von Unterlagen bei Gericht) zu erreichen. Möglich ist auch eine Prozessvereinbarung, wonach nur die Anwälte der Gegenseite, nicht aber die Parteien selbst die Unterlagen sichten. Diese Regeln können dazu führen, dass das US-Gericht die Bemühungen des europäischen Unternehmens anerkennt, möglichst umfassend Daten herauszugeben und von dem Erlass von Sanktionen absieht, wenn die Übermittlung bestimmter Daten verweigert wird.⁵

4.0 Ein Vorschlag für Binding Corporate Rules

Die Lösung des Konflikts kann in einer Vereinbarung gesucht werden, in der sich das in den USA ansässige Unternehmen gegenüber dem in Deutschland ansässigen Unternehmen verpflichtet, die ihr wegen eines Rechtsstreits in den USA von der in Deutschland ansässigen Muttergesellschaft übermittelte E-Mail-Kommunikation mit personenbezogenen Mitarbeiter- und Kundendaten nach den Anforderungen des deutschen Datenschutzrechts speichert und verarbeitet und darauf hinwirkt,

- dass in der Pre-Trial Conference und der Discovery Conference die dem Prozessgegner und dem Gericht zugänglich zu machenden Dokumente begrenzt werden,
- dass über eine Sperrung der Daten gegen Einsichtnahme durch Dritte oder eine vertrauliche Einreichung von Unterlagen bei Gericht verhandelt wird,
- dass eine Prozessvereinbarung erreicht wird, wonach nur die Anwälte der Gegenseite, nicht aber die Parteien selbst, die Unterlagen sichten.

Diese Datenschutzvereinbarung zwischen Mutter- und Tochtergesellschaft sollte durch eine Betriebsvereinbarung zwischen dem Vorstand der in Deutschland ansässigen

⁵ *Spies/Schröder*, MMR 2008, 275 ff., 280 f.

Muttergesellschaft und deren Betriebsrat ergänzt werden, worin die Geschäftsleitung versichert, dass die an die Gesellschaft in den USA übertragenen personenbezogenen Daten der Mitarbeiter entsprechend der Binding Corporate Rules und damit nach dem Standard des Datenschutzrechts geschützt werden.

Literatur

Article 29 Data Protection Working Party

Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules adapted on 24 June 2008.

Junker

Electronic Discovery gegen deutsche Unternehmen – Rechtliche Grenzen und Abwehrstrategien, Frankfurt/Main 2008.

Skupsky, Legal Requirements for Microfilm, Computer and Optical Disk Records, Denver 1996.

Spies/Schröder

Auswirkungen der elektronischen Beweiserhebung (eDiscovery) in den USA auf deutsche Unternehmen, Multi Media und Recht (MMR) , 2008, S. 275 ff.