

Dr. Ivo Geis/Carolin Klas

Der Beweiswert elektronischer Dokumente im Austausch mit den USA

Ein besonderer Aspekt des deutschen Datenschutzrechts

Die heutige Informations- und Wissensgesellschaft und ihre Zukunft sind ohne einen ständigen weltweiten Datenaustausch nicht mehr denkbar. Die Informations- und Kommunikationstechnik wird immer stärker und in vielfältiger Form zu einem festen Bestandteil unseres Alltags und des Geschäftslebens. Dem Schutz der Daten kommt in diesem gewandelten Umfeld ein immer größerer Stellenwert zu, was die gesellschaftliche Diskussion der letzten Monate über die Datenpannen bei deutschen Unternehmen eindrucksvoll belegt. Dabei geht es zum einen um die technische Sicherheit der Daten. Dies ist Sache von unternehmensinternen Sicherheitskonzepten, so dass beispielsweise ein Datenzugriff von Außen durch eine Firewall ausgeschlossen ist. Der Schutz der personenbezogenen Daten ist der andere Aspekt. Sie werden in Deutschland durch das Bundesdatenschutzgesetz geschützt. Allerdings lässt sich Datenschutz in einer Welt grenzenloser Datenflüsse nicht mehr als nationale „Inselpolitik“ betreiben. Insgesamt bestehen weltweit erhebliche Unterschiede im Datenschutzniveau fort und für viele nationale Rechtsordnungen ist Datenschutz noch immer ein Fremdwort.

Gleichwohl weist die internationale elektronische Kommunikation über den Raum des deutschen Rechts hinaus. So ist beispielsweise der Beweiswert elektroni-

scher Dokumente im Austausch mit den USA wegen der E-Mail-Kommunikation zwischen deutschen und amerikanischen Geschäftspartnerschaften ein aktuelles Thema. Unter dem Stichwort „eDiscovery“ wird die Beweisführung mit elektronischen Dokumenten im zivilrechtlichen Verfahren vor US-Gerichten diskutiert. Droht dem deutschen Geschäftspartner in den USA ein Prozess, so muss dieser Dokumente in die USA übermitteln, die für den Prozess relevant sein können. Dies kann zu Konflikten mit dem deutschen Datenschutzrecht führen. Die Lösung dieses Rechtsrisikos oder zumindest seine Minimierung kann mit Binding Corporate Rules, Unternehmensregeln, gesucht werden.

Das US-Beweisrecht: eDiscovery Rules

Der Beweiswert elektronischer Dokumente 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 recording¹. 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 nutz-

barer Form (reasonably usable form) erfolgen. Ist für ein Unternehmen absehbar, dass es zu einem Rechtsstreit kommt, so darf ein Unternehmen entsprechend der Pflicht „Litigation Hold“ potenzielles Prozessmaterial nicht löschen. Damit soll gesichert werden, dass das Unternehmen 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 beklagte Prozesspartei die Informationen nicht auf, gilt dies als Beweisvereitelung (Spoliation), die zu prozessualen Sanktionen und Geldstrafen führen kann. So kann das Gericht eine „Adverse Interference Order“ erlassen, mit der die Jury belehrt 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 und die mit ihr verbundenen elektronischen Dokumente zu einem aktuell diskutierten Thema geworden.² Sie verpflichten die deutsche Prozesspartei in einen Rechtsstreit vor einem US-Gericht zum Übermitteln elektronischer Dokumente in die USA. Dies bringt die deutsche Prozesspartei in eine datenschutzrechtlich problematische Situation.

¹ Siehe Skupsky, Legal Requirements, S. 66 f.

² 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).

Der Konflikt mit dem deutschen Datenschutzrecht

Probleme mit den Anforderungen des Bundesdatenschutzgesetzes (BDSG) entstehen, 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. Die Abwägung dieser Vorschrift zwischen den berechtigten Interessen des Unternehmens als verantwortlicher Stelle und dem schutzwürdigen Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung der Daten wird regelmäßig nicht eindeutig zu klären sein. Selbst wenn das Unternehmen die Daten nach § 28 BDSG weitergeben darf, so muss wegen der Übermittlung in die USA als einem Land, in dem aus europäischer Sicht ein angemessenes Datenschutzniveau nicht besteht, die Übermittlung nach § 4c BDSG zulässig sein.³ 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. Nach dem Zweck des Datenschutzrechts muss der Begriff „erforderlich“ restriktiv ausgelegt werden und dürfen deshalb möglichst wenige Dokumente übermittelt werden.⁴ Es wird allgemein angenommen, dass ein US-amerikanisches Gericht für diese Anforderung des deutschen Datenschutzrechts kein Verständnis haben wird und auf der umfangreichen Dokumentation entsprechend den eDiscovery Rules bestehen wird. Dies liegt nahe, da für Rechtstreitigkeiten in den USA

das US-Recht gilt und in diesem Recht nicht ein dem BDSG vergleichbares allgemeines Datenschutzgesetz besteht.⁵ Der Konflikt zwischen deutschem Datenschutzrecht und eDiscovery Rules ist damit für das deutsche Unternehmen unausweichlich.⁶ Eine Lösungsmöglichkeit für diesen Konflikt wird in Binding Corporate Rules (BCR) gesehen, die die Speicherung der Dokumente entsprechend den eDiscovery Rules unter Berücksichtigung des deutschen Datenschutzrechts definieren.⁷

Ein Lösungsvorschlag: Binding Corporate Rules

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 sichern.⁸ 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. Ausgangspunkt einer BCR ist die zivilprozessrechtliche Notwendigkeit der „Litigation Hold“. Um diese Anforderung umzusetzen, wird ein Lösungsverbot für alle physisch oder elektronisch vorhandenen Dokumente bestimmt werden, die als Prozessmaterial in Frage kommen, wenn es absehbar ist, dass es zu einem Rechtsstreit kommt. Der datenschutzkonforme Umgang mit den Dokumenten kann durch verschiedene Methoden gesichert werden. Grundsätzlich 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 der deutschen Prozesspartei 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. In Frage kommt 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 der deutschen Prozesspartei anerkennt, möglichst umfassend Daten herauszugeben und von dem Erlass von Sanktionen absieht, wenn die Übermittlung bestimmter Daten verweigert wird.⁹

Eine unsichere Rechtslage

Im Falle eines Rechtsstreits in den USA muss die deutsche Prozesspartei archivierte elektronische Dokumente, die prozessrelevant sind, in die USA übermitteln. Das deutsche Datenschutzrecht liefert hierfür keine sichere Rechtsgrundlage. Unternehmensinterne Vereinbarungen (Binding Corporate Rules) gelten als eine Möglichkeit, dieses Rechtsrisiko zu minimieren und sollten von international tätigen Unternehmen abgeschlossen werden, um einer Bestrafung zu entgehen.

Dr. Ivo Geis arbeitet als Rechtsanwalt in Hamburg, Carolin Klas als Referentin bei der AWW.

³ Zur vorrangigen Prüfung des § 28 BDSG gegenüber § 4c BDSG siehe Simitis/Simitis, Bundesdatenschutzgesetz, § 4c Rdnr. 6.

⁴ Zur restriktiven Interpretation des § 4c Abs. Nr. 4 BDSG siehe Simitis/Simitis, Bundesdatenschutzgesetz, § 4c Rdnr. 20-21.

⁵ Siehe zu dem Datenschutzrecht der USA Roßnagel/Burkert, Handbuch Datenschutzrecht, Internationale Grundlagen, Rdnr. 78-84.

⁶ Spies/Schröder, MMR 2008, 275 ff., 276-280 und Junker, Electronic Discovery gegen deutsche Unternehmen, S. 73-80.

⁷ So Spies/Schröder, MMR 2008, 275, 280.

⁸ Working Paper 155 der Article 29 Data Protection Working Party.

⁹ Spies/Schröder, MMR 2008, 275 ff., 280 f.