Technische Universität München
Boltzmannstrasse 3
85748 Garching b. München
Software Engineering for Business Information Systems (sebis)
Im Rahmen des Proseminars „Unternehmensübergreifende IT-Transformationen“ SS 201
Referentin: Ertida Muka
ertida_muka90@yahoo.de

Electronic Discovery

Abstract: Jedes Jahr wird von Unternehmen eine Menge elektronischer Daten aus einer Vielzahl von internen und externen Quellen gesammelt, verarbeitet und für Entscheidungen herangezogen. Unternehmen die geschäftstätig in den USA sind, müssen spätestens bei einer gerichtlichen Auseinandersetzung elektronische Informationen gemäß Electronic Discovery-Rules bereitstellen, für den Fall, dass diese als Beweismittel in Betracht kommen würden [Schmid 2008]. Diese Arbeit stellt die Vorgehensweise dieses Prozesses dar, und geht dabei auf wichtige Herausforderungen, Problemen und Lösungen ein. Ein wichtiger Punkt dabei ist die „Unternehmensübergreifende IT-Transformation“, wodurch IT-Systeme verwandelt werden, um als Ergebnis eine schützende Form gegenüber e-Discovery zu erhalten.

1 Ausgangsbasis

Das Electronic-Discovery (e-Discovery) -Verfahren wurde von dem US Supreme Court im Jahr 2006 in Kraft gesetzt, als neue Änderungen bei den Federal Rules of Civil Procedure (FRCP) aufgestellt wurden [K&L Gates]. Die FRCP-Änderungen gelten für alle öffentlichen oder privaten US-Unternehmen und definieren deren Rechte und Pflichten in Bezug auf e-Discovery. Laut dieser Regeln sollte ein Unternehmen in der Lage sein, innerhalb eines bestimmten Zeitrahmens, elektronisch gespeicherte Informationen, die als Nachweis in einem gerichtlichen Verfahren dienen, zu produzieren. Da große Mengen von Dokumenten in einem Unternehmen als potenzielle Beweismittel in zukünftige Streitigkeiten gesehen werden können, wird e-Discovery auch wie ein wichtiger Prozess des Risikomanagements betrachtet.
E-Discovery kann nicht nur zu Konflikten zwischen den Parteien eines Zivilverfahrens führen, sondern häufig auch innerhalb von Unternehmen, da laut e-Discovery Regelungen müssen auch die Informationen einer Tochtergesellschaft oder verbundenen Unternehmen, die sich im Ausland befindet, übermittelt werden [MMR 2008]. Die Praxis zeigt, daß deutsche Unternehmen den Herausgabeverlangen häufig vollumfänglich nachkommen [Spies 2008], obwohl keine unmittelbare „Pflicht deutscher Unternehmen zur Mitwirkung“ existiert [K&R 2008]. Dies geschieht aus verschiedenen Gründen, wie z.B. aus Angst vor Sanktionen, Sorglosigkeit, Unkenntnis des deutschen Rechtes oder wegen unreflektierter Ausführung einer Anweisung der US-Zentrale [Tsolkas 2008].

2 e-Discovery in der amerikanischen Zivilprozessordnung

Die amerikanische Zivilprozessordnung ist in drei Teile aufgeteilt: Discovery & Disclosure (Pre-Trial), Trials und Judgment. E-Discovery kann als ein Teilprozess der Voruntersuchung betrachtet werden, dessen Konsequenzen in den weiteren Phasen entstehen.

Abbildung 1. Ablauf in der amerikanischen Zivilprozessordnung [Schmid 2008]

2.1 Vorverfahren: Discovery & Disclosure

In der ersten Phase der „Pre-Trial Discovery Regeln“ im US-amerikanischen Zivilrecht, kann der Kläger, die Rechtsanwälte, die Insolvenzverwalter, die Revisoren, die Steuerfahnder und Behörden durch einen Schriftsatz an das Gericht eine Klage gegen ein Unternehmen erheben und damit jede Information abfragen, die für den Klageanspruch von Bedeutung sein könnte [Geis 2008]. Dieser Anstoß ermöglicht dem Gericht dem Beklagten ein Preservation Letter oder Discovery Order (eine schriftliche Anforderung) zu senden, wodurch er aufgefordert wird, bestimmte Beweismittel ordnungsgemäß der e-Discovery Regelungen zu sichern. Gleichzeitig wird auch ein Litigation Hold ausgegeben, was im Kern eine Pflicht zu Löschungsverbot prozessrelevanter Informationen und zur Datensicherung für Prozesszwecke ist. Diese Pflicht besteht:
a)für alle Informationen die nach vernünftiger Beurteilung aller Umstände zu einer Aufdeckung von zulässigen Beweismittel führen könnten und
b)für Informationen, die mit große Wahrscheinlichkeit das Unternehmen i.d.R. der anschließenden Discovery der anderen Partei vorlegen muss [MMR 2008].
Zu diesem Zeitpunkt muss der Beklagte alle Informationen sammeln die er „in possession, custody or control“ hat [SS 2010]. De Facto bedeutet dies, dass die amerikanische Prozesspartei alles was in ihrer Macht steht, tun muss, um die erforderliche Informationen und Dokumente von anderen Konzernunternehmen zu beschaffen.

2.2 Hauptverfahren: Trials & Judgment

Normalerweise ist es für eine Partei ein strategischer Vorteil, alle potenziell relevanten Dokumente so lange wie möglich aufzubewahren. Wo potenziell relevante Dokumente zerstört oder nicht bewahrt werden, gilt dies als eine Beweisvereitelung „Spoliation“ das zu sehr schwerwiegende Folgen führen könnte. So hat der Richter das Recht, ein „Adverse interference order“ zu erlassen, womit die Jury eingewiesen wird, dass die manipulierten Dokumente gegen der Partei sprechen, die sie vernichtet hat [Geis 2008], dazu kann dem Kläger die Zahlung der Kosten der gegnerischen Parteien erfordern, oder in extremen Fällen kann eine Klage abgewiesen werden. Zuletzt kann die Jury die beklagte Partei, bei einer nicht korrekten Beweisführung der elektronischen Dokumente, mit Sanktionen zivilrechtlich ahnden.

3 Datenschutzrechte in USA und Deutschland im Vergleich

Da e-Discovery die Untersuchung und Bereitstellung auch von personenbezogenen Daten festlegt, müssen die Unterschiede zwischen der amerikanischen und deutschen Rechtslage hinsichtlich des Umganges dieser Daten, verdeutlicht werden. Im nachfolgendem Teil werden die Unterschiede erläutert, dabei die entstehende Probleme analysiert und Lösungsvorschlage gemacht.

3.1 Unterschiede

Aus deutscher Sicht, ist deutlich erkennbar, dass der Datenschutz in USA grundsätzlich anders strukturiert ist als in Deutschland. Es gibt in den USA kein übergreifendes Datenschutzgesetzt wie das deutsche Bundesdatenschutzgesetz (BDSG). Stattdessen gibt es eine Reihe von Sektor-spezifischen Regeln für verschiedene Industriebereiche, jedoch keine umfassende Regelung für den Umgang mit persönlichen Daten. Außerdem unterscheiden sich die Datenschutzgesetzte auch zwischen den einzelnen US-Bundesstaaten.

Amerikanische Sicht	**Deutsche Sicht**
Kein übergreifendes Datenschutzrecht	Bundesdatenschutzgesetz (BDSG)
-Zugriff auf private Daten	-Recht auf informationelle Selbstbestimmung
-Kein Recht für Daten die aus dem Ausland kommen	-Übermittlung von Daten an Drittstaaten (nicht europäische Länder) zulässig falls ein “angemessener Schutzniveau“ gewährleistet wird
-Keine rechtliche Vorgabe über die Aufbewarungsdauer personenbezogener Daten	-Rechtliche Vorgabe von Aufbewahrungsfristen und Aufbewahrungspflichten

Abbildung 2. Datenschutzrechtliche Unterschiede zwischen Deutschland und USA

In Deutschland hat man laut BDSG das Recht auf Informationelle Selbstbestimmung, z.B., wenn ein Unternehmen einem Mitarbeiter einen Laptop-PC zur Verfügung stellt mit dem er arbeiten soll, so sind die gespeicherte Daten als persönlich anzusehen. Das Unternehmen braucht die individuelle Erlaubnis des Mitarbeiters, bevor jemand auf die Informationen zugreifen kann. Für US-Verfahren gilt allerdings der Grundsatz, dass Dokumente auf Antrag der Öffentlichkeit zugänglich zu machen sind [MMR 2008]. Die Übermittlung von Informationen, aus Deutschland in Drittstaaten (nicht europäische Länder) erfolgt gem. § 4 b Abs. 2 S. 2 BDSG, ist nur dann zulässig, falls ein „angemessener Schutzniveau“ im Vergleich zu den europäischen Datenschutzrechten gewährleistet wird. Da es in den USA kein Recht für Daten die aus dem Ausland kommen, gehören die USA zu den Staaten mit einen niedrigen Datenschutzniveau. Nach dem BDSG ist eine unbegrenzte Speicherung von Daten ohne einen rechtlich anerkannten Zweck unzulässig. Infolgedessen sollte der Zweck für die Erhebung entfallen, können die Daten gelöscht oder vernichtet werden. Das heißt, dass in Deutschland

rechtliche Vorgaben zu Aufbewahrungspflichten und Fristen gibt, im Gegensatz dazu gibt es in den USA keinerlei rechtliche Vorgaben über die Aufbewahrungsdauer gesammelter personenbezogener Daten.

3.2 Übermittlung der personenbezogene Daten in die USA

Die europäische Datenschutz-Richtlinie [95/46/EC] verbietet grundsätzlich, personenbezogene Daten aus EU-Mitgliedländer in Staaten zu übertragen die über keinem EG-Recht „vergleichbares" Recht verfügen. Laut Entscheidung der EU-Kommission bieten die USA kein angemessenes Schutzniveau das heißt die USA gehören zu den Staaten wo die Übertragung der elektronischen Informationen nicht möglich wäre. Dies bedeutet erhebliche Herausforderungen für Unternehmen, die eine Präsenz in USA haben. Unternehmen, die US-Tochterunternehmen, Zweigniederlassungen, Agenturen, Verleiher und die direkte Kunden in USA haben (z. B. über das Internet) werden alle von dieser Regelung betroffen. Es bedeutet, dass zum Beispiel eine Tochtergesellschaft nicht auf seine US-Muttergesellschaft Kundendaten oder HR-Daten wie Leistung- und Gesundheits- Daten und Gehaltsinformationen im Fall einer gerichtlichen Auseinandersetzung übertragen werden darf. Aber das Verbot der Weitergabe personenbezogener Daten außerhalb European Economic Area (EEA) ist nicht absolut.

Zwei Lösungen bieten sich an falls Unternehmen, personenbezogene Daten aus der EU in die USA übertragen wollen oder müssen.

a)Binding Corporate Rules

Die EU hat die Möglichkeit geschafft, dass Unternehmen in großen multinationalen Konzernen ihre eigenen internen verbindliche unternehmensweit geltende Richtlinien bekannt als Binding Corporate Rules (BCR) anwenden können [DGJ 2010]. Die Idee dahinter ist, dass eine Gruppe ihre eigenen Regeln, Richtlinien und Verfahren entwickelt für die Gewährleistung des Datenschutzes. Diese Regeln werden erst bei der Datenschutzbehörde des EU-Landes geprüft, zu dem die Muttergesellschaft oder der operative Hauptsitz der Gruppe gehört, und dann die Zustimmung für die Regelung von allen anderen EU-Datenschutzbehörden bekommt.
Im Jahr 2005 genehmigte die EU-Kommission eine aktualisierte Modell Checkliste, die die erforderlichen Inhalte für die Genehmigung von BCR von einer Datenschutzbehörde darstellte (ARTICLE 29 Data Protection Working Party). Im Dezember 2005 wurde General Electric als erstes Unternehmen von der britischen Datenschutzbeauftragten genehmigt worden, um Informationen außerhalb des Europäischen Wirtschaftsraums mit verbindlichen unternehmensinternen Vorschriften zu übertragen. General Electric ist nun in der Lage, persönliche Daten wie Mitarbeiter-Daten innerhalb der multinationalen Unternehmen zu behandeln.

b)Safe Harbor

Safe Harbor-Regelungen wurden durch das US-Department of Commerce in Absprache mit der europäischen Kommission entwickelt, für die europäische Unternehmen, die eine Präsenz in den USA haben. Es ist eine besondere Datenschutz-Vereinbarung, die es europäischen Unternehmen ermöglicht, personenbezogene Daten in die USA genehmigungsfrei zu übermitteln und überlassen. Die Entscheidung von US-Organisationen in den Safe Harbor

einzulaufen ist vollkommen freiwillig. Die US-Unternehmen, die Teil dieser Vereinbarung sind, haben Vorteile in einen Zivilprozess, zum Beispiel laut Artikel 37-- „Safe Harbor-Provision“: darf ein Gericht, außer bei außergewöhnlichen Umständen, keine Sanktionen erlassen gegenüber der Partei die elektronische Informationen wegen einer „Routinen“ Löschung eines Informationssystems gelöscht hat. Bei Unternehmen die nicht daran beteiligt sind, würde dieser Fall gemäß e-Discovery Regelungen als „Spoliation“ gelten und vermutlich mit Sanktionen bestrafft werden.

4 Durchsuchen der elektronischen Dokumente

Heutzutage benutzen Unternehmen moderne Applikationslandschaften, die aus mehreren durch Schnittstellen verbundenen betrieblichen Applikationen bestehen [Matthes 2009]. Diese Anwendungssoftware werden von Mitarbeitern benutzt, die ein bestimmten Zugang und Zugriff auf bestimmte Business Objekte des Systems haben, das heißt, dass ein Mitarbeiter durch seine Kompetenzen, auf die Informationen zugreifen kann die nur seine Rolle entsprechen [Buckl 2009]. Im Falle einer e-Discovery aufgrund Federal Rules of Civil Procedure, erhält der Anwalt in einen Zivilprozess Zugriff auf elektronisch gespeicherte Informationen, abrufbar durch den Einsatz betrieblicher Anwendungssysteme. Er hat das legale Recht die Rolle jener Mitarbeiter, die mit dem entsprechenden Business Objekt zu tun hatten das vom Gericht untersucht wird, zu übernehmen. Aufgrund der Vernetzung der betrieblichen Anwendungen, entsteht ein transitiver Zugriff auf Informationen über mehrere Business Objekte die überhaupt keine Bedeutung zu dem Prozess haben [Buckl 2009]. So entsteht die Möglichkeit dass der Anwalt durch diesen Zugriff andere Probleme findet und damit weitere Klagen erstellen kann. Die Abbildung 3 stellt diesen Zugriff dar

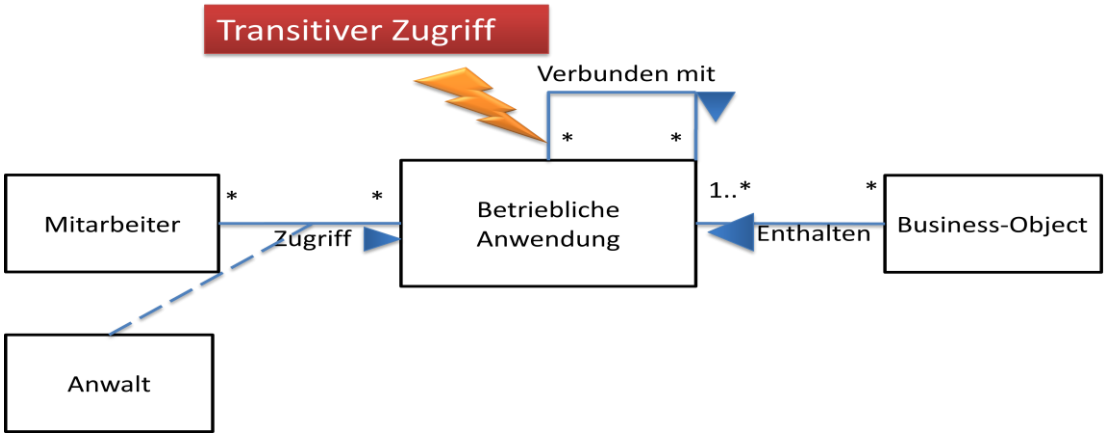

Abbildung 3 [Buckl 2009]

4.1 Vorschlag: IT-Transformation

In diesen Fall ermöglicht eine IT-Transformation die konkreten Zusammenhänge zwischen Rolle(Mitarbeiter), Business Objekte und Business Anwendungen festzulegen und den durch Schnittstellen ermöglichten Zugriff auf Business Objekte von Mitarbeiter zu löschen. So könnte man die transitiven Zugriffe beseitigen und dabei ein geschütztes Rollen-basiertes System erhalten. Das heißt bei möglichen gerichtlichen Auseinandersetzungen, ein Zugang

bezüglich auf die Rollen der Mitarbeiter stattfindet. Die Suche durch dieses System würde nur Informationen die mit dem entsprechenden Business Objekt verbunden sind. Um das zu erreichen brauchen wir eine Methode wie man eine unternehmensweite Zugriffskontrolle auf relevante Business Objekte bilden kann, sowie in Abbildung 4

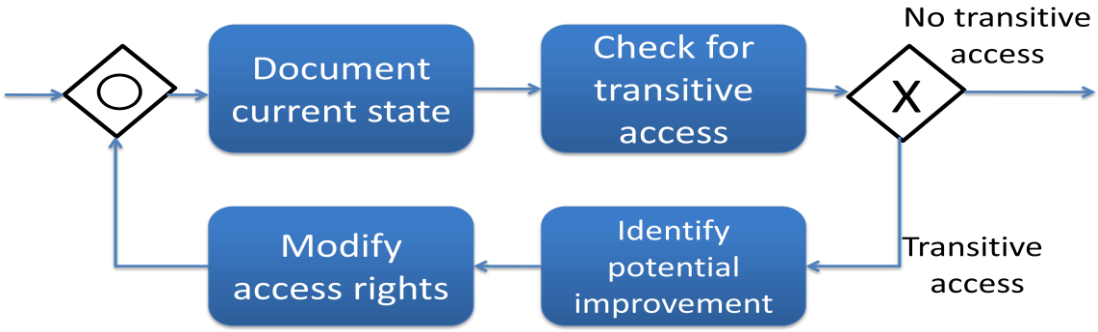

Abbildung 4 [Buckl 2009]

Diese Methode besteht aus 4 Schritten die sich zyklisch wiederholen können falls ein transitiver Zugriff vorhanden ist. Im ersten Schritt „**Document current state**“, werden Informationen gesammelt, wie die aktuellen Beziehungen zwischen Rollen, Business Objekte und betriebliche Anwendungen stehen, und dann tabellarisch dargestellt. Der kritische Punkt in dieser Phase ist die Beziehung zwischen den Applications, was zu der zweiten Phase „**Check for transitive access**“ führt in dem Experten die durch Schnittstellen der betrieblichen Anwendung transitive Zugriffe der Rollen auf Business Objekte finden. Die nächste Phase „**Identify potential for improvement**“ ist eine Analyse der gesammelten Informationen. Daraus folgen potenzielle Verbesserungen die im letzten Schritt „**Modify access permissions**“ durch Methoden verwirklicht werden können. Der neue Zustand wird dokumentiert und der Vorgang beginnt von vorne, und läuft weiter bis keine transitiven Zugriffe mehr vorhanden sind. [Buckl 2009]

5 Ausblick [Foltyn 2009]

Die rasante Zunahme des Volumens von elektronisch gespeicherten Informationen (ESI) hat die Situation von Rechtsstreitigkeiten dramatisch verändert und eine Paradigmenwechsel in der e-Discovery und Computer Forensics verursacht. Aber nicht nur Volumen von Daten ist ein Problem für e-Discovery, heutzutage ist ein neues Problem aufgetaucht: Cloud Computing.
"Cloud computing means that data may always be in transit, never anywhere, always somewhere” (Teppler). Aus dieser Aussage folgen Fragen wie: Wie können Unternehmen erkennen "wer, wann und wo" in der cloud arbeitet? Wie können Organisationen auf aufbewahrte Dokumenten zugreifen? Ist „Storage Manager“ sich bewusst, dass manche Informationen unter dem e-Discovery Prozess befinden? Die Antworten zu diesen Fragen sind immer noch offen [Foltyn 2009].
Mit der IT Entwicklung steigt der Aufwand die e-Discovery-Regelungen zu verfolgen, trotzdem werden gleichzeitig auch Software entwickelt, die diesen Aufwand erleichtern. So wird e-Discovery immer ein aktuelles Thema bleiben, besonders für Unternehmen, die sich außerhalb der USA befinden, aber in den USA Geschäfte abwickeln.

Literaturverzeichnis

[DGJ 2010] Directorate-General Justice. Overview BCR 2010. http://ec.europa.eu/justice/policies/privacy/binding_rules/index_en.htm

[Foltyn 2009] Foltyn M. Cloud Computing Poses E-Discovery, Legal Risks 2009. http://ediscoveryconsulting.blogspot.com/2008/09/cloud-computing-is-coming-to-ediscovery.html

[Geis 2008] Ivo Geis. eDiscovery und Datenschutz. Website, 2008. http://www.ivogeis. de/veroeffentlichungen/eDiscovery und Datenschutz.pdf

[K&L Gates] K&L Gates. United States Supreme Court Approves Electronic Discovery Amendments to FRCP 2006. http://www.ediscoverylaw.com/2006/04/articles/federal-rules-amendments/united-states-supreme-court-approves-electronic-discovery-amendments-to-frcp/

[K&R 2008] Michael R. Saskia K. e-Discovery in Deutschland, K&R Kommunikation & Recht (10/2008), 2008.

[Buckl 2009] Buckl, S. u.a. A Method for Constructing Enterprise-wide Access Views on Business Objects. 2009

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

[Schmid 2008] Claus S. Richard L. White Paper Electronic Discovery, Die Compliance des innerbetrieblichen Informationsmanagements bringt hohen unternehmerischen Nutzen 2008

[Spies 2008] Spies A. Christian S. Auswirkungen der elektronischen Beweiserhebung (eDiscovery) in den USA auf deutsche Unternehmen. Redaktion MultiMedia und Recht 2008

[SS 2010] Seyfarth Shaw. Possession, Custody or Control in the Electronic Age 2010. http://www.seyfarth.com/index.cfm/fuseaction/publications.publications_detail/object_id/074db5be-17c4-44c2-a476-1089a9d918d8/eDiscoveryIssuesPossessionCustodyorControlintheElectronicAge.cfm

[Tsolkas 2008] Peter T. Gabriel R. Litigation in the Age of the Terabyte: The 2006 eDiscovery Amendments to the U.S. Rules of Civil Procedure, DAJV-Newsletter (1/2007), 2007