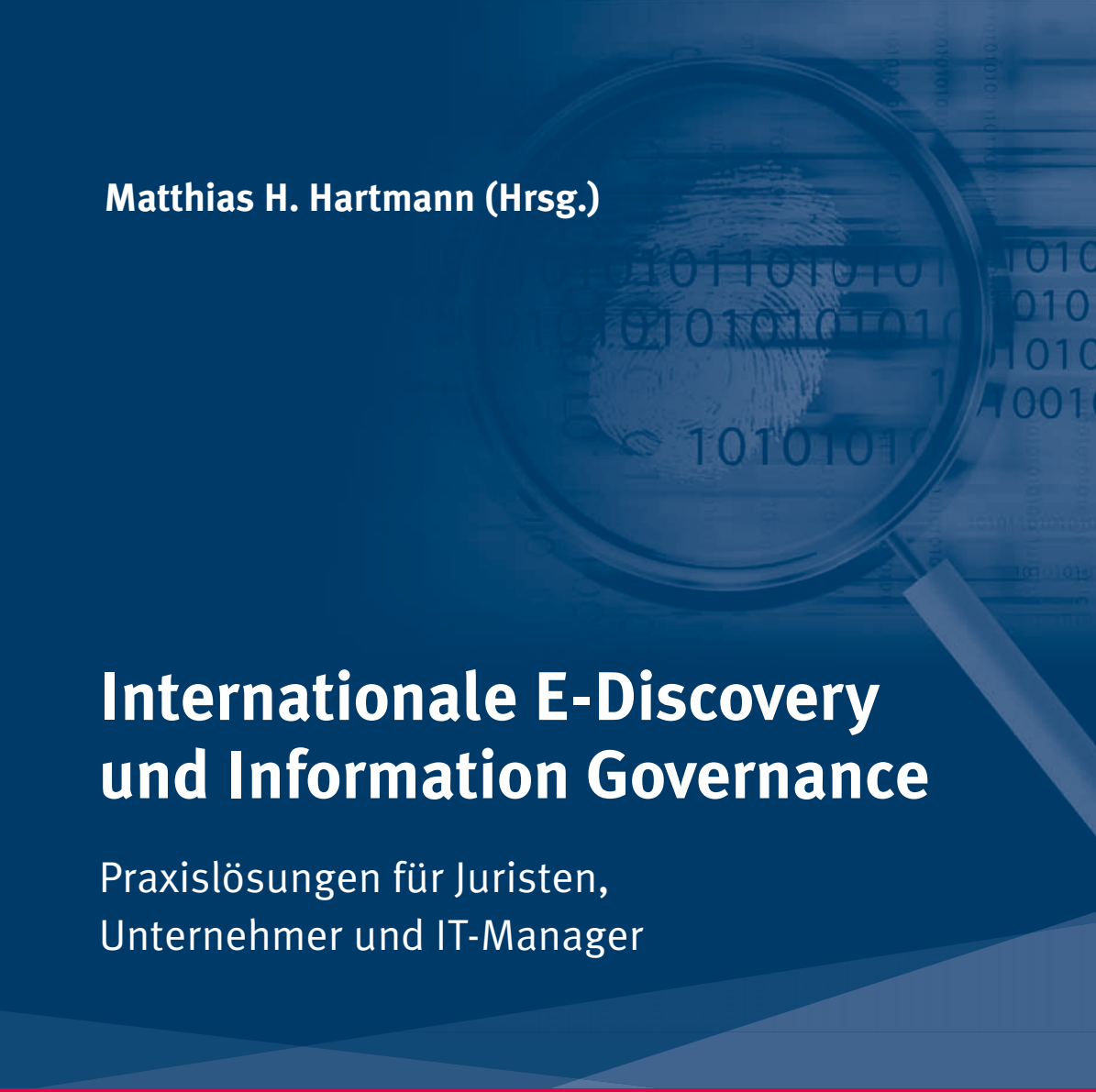
Matthias H. Hartmann (Hrsg.)



Internationale E-Discovery und Information Governance

Praxislösungen für Juristen, Unternehmer und IT-Manager

ESV
ERICH SCHMIDT VERLAG

Internationale E-Discovery und Information Governance

Praxislösungen für Juristen, Unternehmer und IT-Manager

Herausgegeben von
Prof. Dr. Matthias H. Hartmann

Mit Beiträgen von

Meribeth Banaschik
Richard G. Braman
Elmar Brunsch
M. James Daley
Amor Esteban
Thomas Hampp-Bahnmüller
Prof. Dr. Matthias H. Hartmann
Wolfgang Jung
Sandra Kiemes
Dr. Philip Laue
Stephan T. Meyer
Nigel Murray
Deidre Paknad
Jörg Pauseback
David Rosenthal
Dr.-Ing. Claus Schmid
Jürgen Venhofen
Dr. Stephan Wilske
Kenneth Withers
Christian Zeunert

ERICH SCHMIDT VERLAG

Weitere Informationen zu diesem Titel finden Sie im Internet unter
ESV.info/978 3 503 13075 7

Gedrucktes Werk: ISBN 978 3 503 13074 0
eBook: 978 3 503 13075 7

Vorwort

Die Idee zu diesem Buch entstand in einem Beratungsprojekt während einer zweijährigen Beurlaubung des Herausgebers von der Hochschule für Technik und Wirtschaft, Berlin. Praktischer Anlass war ein konkretes E-Discovery-Projekt. Wissenschaftliches Forschungsinteresse war gegeben, als es darum ging, ein komplexes Thema aufzuarbeiten. Komplex ist E-Discovery aus drei Gründen:

E-Discovery erfordert erstens in hohem Maße interdisziplinäres Denken von Jurisprudenz, Betriebswirtschaft und Informationstechnologie. Klassischerweise verstehen die drei Disziplinen die jeweilige Fachsprache der anderen Disziplin nur wenig. Und wie schon Wittgenstein formulierte: „Die Grenzen meiner Sprache sind die Grenzen meiner Welt."

E-Discovery erfordert zweitens ein Verständnis für die Eigenheiten nationaler Rechtskulturen. Es gibt bereits eine Reihe von englischsprachigen Büchern zu E-Discovery in den USA. Die deutsche und auch europäische Sicht auf E-Discovery ist jedoch aufgrund des unterschiedlichen Datenschutzrechtes und des unterschiedlichen Prozessrechtes weitgehend eine andere.

E-Discovery erfordert drittens Kenntnis der Konsequenzen des Informationszeitalters auf Menschen und Unternehmen. Es geht um digitale Spuren, Daten in Wolken (Cloud Computing), virtuelle Realitäten usf. Wie kann Informationsherrschaft sichergestellt werden? Wie kann das Entstehen, Administrieren und (finale) Löschen von Daten gesteuert werden (Information Governance)?

E-Discovery ist nicht nur komplex, sondern in seinen Wirkungen fallweise auch paradox. Pointiert formuliert, kann sich ein Unternehmer im Negativfall aussuchen, ob er nach amerikanischem oder deutschem/europäischem Recht verurteilt wird. Verurteilt wird er auf jeden Fall. Das Buch möchte Hilfestellung sein, einen schiffbaren Weg zwischen Scylla und Charybdis zu finden.

Zu diesem Zweck hat der Herausgeber Experten mit internationaler Erfahrung gebeten, ihr Wissen zu E-Discovery zu dokumentieren. Entstanden ist ein interdisziplinäres Werk, das einen Einblick in Ziel, Erfolgsfaktoren und Ablauf einer E-Discovery aus mehreren fachlichen Perspektiven geben soll. Entsprechend ist der Aufbau des Buches:

Einführung:	Notwendigkeit einer interdisziplinären Perspektive
Kapitel I:	Juristische Perspektive
Kapitel II:	Datenschutz-Perspektive
Kapitel III:	Betriebswirtschaftliche und technologische Perspektive
Kapitel IV:	The Sedona Conference® – eine Institution in den USA

Allen Autoren sei an dieser Stelle noch einmal ausdrücklich für ihre Beiträge und ihr Engagement gedankt. Einige Beiträge wurden im Original in Englisch geschrieben und im Anschluss ins Deutsche übersetzt. Für die Inhalte aller Beiträge

sowie für etwaige Übersetzungsfehler wird jegliche Haftung ausgeschlossen. Das Buch ist kein Rechtsratgeber.

Die Takticum Consulting GmbH hat finanziell und mit Know-how zum Buchprojekt beigetragen.

Meiner Frau Klára darf ich herzlich für die Unterstützung bei der Kommunikation mit den Autoren sowie bei der Durchsicht und Übersetzung von Texten danken.

An der Übersetzung vom Englischen ins Deutsche haben sich mit viel Mühe auch Frau Dr. Martina Ludewig und Frau Kristina von Wrede beteiligt. Frau Juliane Wessel hat bei der Durchsicht der Texte assistiert.

Ganz besonders sei Frau Victoria Telcharov gedankt, die unermüdlich die Formatierung, die vielen Korrekturläufe und die redaktionelle Zusammenarbeit mit dem Verlag verantwortet hat.

Last but not least sei dem Erich Schmidt Verlag – namentlich Frau Claudia Splittgerber und Frau Anja Ludwig – für die kompetente Beratung und das Lektorat gedankt.

Berlin, im Januar 2011 Prof. Dr. Matthias H. Hartmann

Inhaltsübersicht

Vorwort V

Abkürzungsverzeichnis IX

Einführung

Matthias H. Hartmann
Systematische E-Discovery und Information Governance 1

Kapitel I: E-Discovery im internationalen Rechtsstreit

David Rosenthal/Christian Zeunert
E-Discovery und Datenschutz: Herausforderungen und Lösungsansätze für multinationale Unternehmen 23

Nigel Murray
E-Discovery-Strategien für international agierende Unternehmen 73

Meribeth Banaschik
Leitfaden für Unternehmensjuristen zur Reaktion auf Anforderungen der U.S.-Discovery aus der amerikanischen Perspektive..... 81

Stephan Wilske
E-Discovery im kontinentaleuropäischen Rechtsraum: Discovery-Verfahren in der Schiedsgerichtsbarkeit 93

Kapitel II: E-Discovery und deutscher Datenschutz

Philip Laue
E-Discovery und Prüfschema zum internationalen Datentransfer..... 109

Stephan Meyer
Deutsches Datenschutzrecht und Betriebsratsbeteiligung bei E-Discovery in den USA..... 123

Elmar Brunsch
Safe in Germany. E-Discovery-Datenschutz im IT-Outsourcing 151

Kapitel III: E-Discovery und Information Governance

Claus Schmid

E-Discovery
im Kontext IT-Management und Enterprise Data Management 173

Deidre Paknad/Wolfgang Jung/Thomas Hampp-Bahnmüller

Information Governance als Erfolgsfaktor für Electronic Discovery 205

Matthias H. Hartmann/Jürgen Venhofen

Strategisches Innovations- und Technologie-Management
für E-Discovery 231

Sandra Kiemes/Jörg Pauseback

Prozess der E-Discovery in der technischen Umsetzung 247

Kapitel IV: The Sedona Conference®

The Sedona Conference®

Historie „The Sedona Conference®“ 271

The Sedona Conference®

Ergebnisse von „The Sedona Conference®“ Working Group
„International Electronic Information Management,
Discovery and Disclosure“ (WG6) 283

Autorenverzeichnis..... 307

Stichwortverzeichnis 315

DAVID ROSENTHAL · CHRISTIAN ZEUNERT

E-Discovery und Datenschutz: Herausforderungen und Lösungsansätze für multinationale Unternehmen

1. Einleitung 24

2. Ausgangslage für multinationale Konzerne 27
2.1 Überblick 27
2.2 Rechtliche Herausforderungen 28
2.2.1 Konflikte unterschiedlicher Rechtskulturen 28
2.2.2 Die fünf rechtlichen Herausforderungen des Datenschutzes 32
2.3 Organisatorische Herausforderungen 43
2.3.1 Fallspezifische und konzernweite Interessen 43
2.3.2 Die vier organisatorischen Herausforderungen der internationalen E-Discovery 44

3. Lösungsansätze für multinationale Konzerne 51
3.1 Vorbemerkungen 51
3.2 Den eigenen Fall kennen 54
3.2.1 Besondere organisatorische Aspekte multinationaler Konzerne 55
3.2.2 Besondere IT-Aspekte multinationaler Konzerne 55
3.2.3 Analyse einer grenzüberschreitenden E-Discovery im multinationalen Konzern 56
3.3 Pragmatische Kompromisse akzeptieren 59
3.3.1 Vorbemerkungen 59
3.3.2 Standardprozedur zur Durchführung einer E-Discovery in Europa. 60
3.4 Dokumentation & Reglementierung des grenzüberschreitenden Datentransfers 66
3.4.1 Vorbemerkung 66
3.4.2 Grenzüberschreitende Bekanntgabe 66
3.4.3 Schutz der Daten nach ihrer Offenlegung 69

1. Einleitung

Über die Herausforderung, vor die eine E-Discovery einen multinationalen Konzern stellt, lässt sich viel schreiben. Für den Datenschutz gilt das gleiche. Beides sind Konzepte, die jeweils aus einer bestimmten Rechtskultur entstammen, und beides sind Konzepte, die insbesondere multinationale Konzerne nicht ignorieren können, weil sie ihnen naturgemäß ausgesetzt sind. Die besondere Schwierigkeit, die sich diesen Unternehmen stellt, liegt darin, dass die beiden Konzepte E-Discovery und Datenschutz einander scheinbar widersprechende Anforderungen aufstellen: Das Verfahren der Pre-trial Discovery nach US-amerikanischem Vorbild verlangt schonungslose Offenlegung aller im weitesten Sinne für den Fall relevanten Unterlagen eines Unternehmens noch vor dem eigentlichen Prozess, der Datenschutz nach europäischem Vorbild schränkt eine solche massiv ein und lässt sich in jeder Hinsicht vom Gebot der Datensparsamkeit – ganz besonders bei der Bekanntgabe an Dritte – leiten.

Doch multinational tätige Unternehmen, von denen in der Praxis die Umsetzung dieser Konzepte verlangt wird, müssen diese Widersprüche trotzdem lösen. Denn sie befinden sich unverrückbar zwischen den Fronten der beiden Rechtskulturen, wenn sie einerseits in Rechtsstreitigkeiten in den USA (und anderen Ländern mit vergleichbarem Rechtssystem) verwickelt werden, andererseits aber aufgrund der von ihnen bearbeiteten Unterlagen und Information zahlreichen Datenschutzgesetzen in Europa und anderswo unterliegen. Diese Unternehmen wollen in aller Regel das tun, was jedes vernünftig geführte Unternehmen tun will: Allen Anforderungen, welche das jeweils anwendbare Recht aufstellt, so gut wie möglich gerecht werden.

In vielen Fällen ist dieses Streben nach allseitiger *legal compliance* zwar aufwändig, aber letztlich ohne Normkollision möglich. Im hier relevanten Bereich scheint das anders: Denn wo E-Discovery und Datenschutz aufeinandertreffen, geraten viele multinationalen Unternehmen unweigerlich in einen Zielkonflikt, der einem Unternehmen auf den ersten Blick nur die Wahl lässt, zwischen dem schlechteren Übel zu wählen – die massive Einschränkung oder gar Verweigerung einer E-Discovery oder die Missachtung des Datenschutzes. So erschien es jedenfalls, als im Rahmen einer Anpassung des US-Prozessrechts (d.h. den *US Federal Rules of Civil Procedure*) im Jahre 2006 klargestellt wurde, in welcher Form auch elektronische Daten (*electronically stored information*, ESI) der Discovery unterliegen, was rückblickend betrachtet die Schleusen hinsichtlich dem Sammeln und Offenlegen von in Unternehmen bearbeiteten Daten weiter öffnete und den Grundstein für die heutige Form der E-Discovery legte[40].

Nachdem die Anwälte, Gerichte und Unternehmen realisiert hatten, wie weit eine E-Discovery nach den Regeln des US-Zivilprozesses letztlich gehen kann,

---

[40] Vgl. zur unternehmerischen Perspektive auf E-Discovery den Beitrag von Hartmann in diesem Herausgeberband.

aber auch wie wertvoll die dabei gewonnenen Informationen wie etwa interne E-Mails zur Streitsache sein können, waren die Reaktionen in der alten und neuen Welt entsprechend extrem.

Kam es in den USA zum Prozess, begannen die Anwälte in ihren *discovery requests*[41] jede erdenkliche Kategorie von Dokumenten und Daten einzuverlangen, auch wenn sie so breit formuliert waren, dass von Anfang an klar war, dass auch zahlreiche für den Fall irrelevante Unterlagen erfasst würden oder zumindest erhebliche Zweifel an der Relevanz bestand. Dies wiederum führte dazu, dass die Anwälte ihren eigenen Klienten schon im Vorfeld eines Prozesses dringend anrieten, sämtliche Dokumente oder Daten, die auch nur im entferntesten für einen Fall relevant sein könnten, sicher aufzubewahren um sich später in keinem Fall einem Risiko von Sanktionen wegen der Vernichtung von Beweismitteln auszusetzen, die je nach Gerichtsbezirk in den USA auch dem blühen, der nicht bösgläubig handelt[42]. Ebenso rieten die Anwälte ihren Klienten, im Zweifel lieber mehr offenzulegen als zu wenig.

Währenddessen hoben die Datenschützer und Datenschutzspezialisten quer durch Europa warnend den Finger und wiesen darauf hin, dass letztlich gegen das Gesetz verstößt, wer Personendaten einfach so in die USA sende und dort offenlege – ganz besonders, wenn es sich um letztlich irrelevante Daten handle. Dass eine E-Discovery in großem Umfang nicht nur Personendaten, sondern letztlich auch irrelevante Personendaten zu Tage fördert und ihre unbeschränkte Offenlegung sich schwerlich mit dem Gebot der Verhältnismäßigkeit einer jeden Bearbeitung von Personendaten nicht vereinen ließ, war für sie offenkundig.

Die Fronten waren rasch ausgemacht. Unterstützung erfuhren die jeweiligen Lager von Richtern in den USA, welche ungeachtet des europäischen Datenschutzrechts die Offenlegung von Unterlagen anordneten, und von europäischen Datenschutzgremien wie etwa die Artikel-29-Datenschutzgruppe[43], welche bereits in einem Arbeitspapier[44] derart weitreichende Forderungen aufstellte, dass sich eine E-Discovery auf vernünftige Weise nicht durchführen lassen würde, würden sie

---

41 Gemeint sind die Listen jener Dokumentenkategorien (einschließlich ESI), mit welchen jede Partei von der anderen im Vorfeld eines Verfahrens die Herausgabe von Unterlagen und Information im Rahmen einer Pre-trial Discovery verlangt, d.h. der freiwilligen Offenlegung vor dem Prozess.

42 Als eine der schwersten Sanktionen gilt die „adverse inference“ im Prozess: Die Jury wird angewiesen anzunehmen, dass die nicht offengelegten bzw. verlorenen Unterlagen für die Partei, welche sie nicht offengelegt bzw. nicht aufbewahrt hat, schädlich sind, also das belegen, was die Gegenseite behauptete. Als einer bekannteren Fälle, in welchem es zu dieser Sanktion kam, gilt etwa The Pension Committee of the University of Montreal Pension Plan, et al. V. Banc of America Securities, LLC, wo verschiedene der Kläger es unterlassen hatten, bei Klageeinleitung für die Erhaltung von möglicherweise relevanten Unterlagen zu sorgen.

43 Ein gemäß Art. 29 der EU-Datenschutz-Richtlinie 95/46/EG eingesetztes unabhängiges europäisches Beratungsgremium in Datenschutzfragen.

44 Arbeitsunterlage 1/2009 über Offenlegungspflichten im Rahmen vorprozessualen Beweiserhebungen bei grenzübergreifenden zivilrechtlichen Verfahren (Pre-trial Discovery) vom 11. Februar 2009, WP 158 (zit. "WP158").

wirklich alle befolgt. Zwar sieht sowohl das europäische Datenschutzrecht wie auch das US-amerikanische Zivilprozessrecht die Möglichkeit von Interessenabwägungen und somit die Möglichkeit entsprechender Einschränkungen der eigenen Grundsätze vor. Die Interessen der anderen Seite erachten sie aber jeweils als untergeordnet, oder sie wollten sich damit schlichtweg nicht auseinandersetzen.

Bis vor kurzem war diese Ignoranz und Konfrontation statt Dialog auf beiden Seiten an der Tagesordnung. Wer sich als betroffenes Unternehmen dem Konflikt nicht entziehen konnte, musste nicht nur versuchen, alle Beteiligten zu einem realisierbaren Kompromiss zu bewegen. Vor allem musste Aufklärungsarbeit betrieben werden, damit die Beteiligten überhaupt realisierten, warum letztlich nur ein Kompromiss zum Ziel führen kann. Dies wurde in den letzten Jahren denn auch getan – getrieben vor allem durch multinationale Konzerne, die beiden Rechtskulturen ausgesetzt waren. Kam es zum Prozess in den USA, wurden nicht mehr nur Anwälte aus den USA beigezogen, sondern auch solche in Europa. In den Unternehmen wurden Verantwortliche für E-Discovery aufgebaut und die Unternehmen begannen sich untereinander auszutauschen.

Inzwischen sind erste Früchte dieser Anstrengungen zu erkennen: Immer mehr Richter, Anwälte und Behörden in den USA wissen inzwischen um die zahlreichen Beschränkungen, die der Datenschutz Unternehmen in Europa auferlegt und multinationale Unternehmen diese Bestimmungen nicht einfach ignorieren können. Datenschützer wiederum haben erkannt, dass ein Unternehmen, dass auf dem US-Markt tätig sein will, sich letztlich den Gepflogenheiten des US-Rechtssystems nicht entziehen kann (wie dies umgekehrt in Europa auch für US-Unternehmen gilt) und gewisse Abstriche im Datenschutz zwar unumgänglich (so etwa bezüglich der Lösch- und Berichtigungsrechte betroffener Personen), letztlich aber auch durchaus in vertretbarer Weise möglich sind, sodass der Datenschutz seines Kerngehalts nicht beraubt wird[45].

Der vorliegende Beitrag widmet sich diesen Zielkonflikten und ihrer Lösung aus der Sicht multinationaler Konzerne. Er legt zunächst die rechtlichen und organisatorischen Herausforderungen solcher über die Landesgrenzen hinweg tätigen und präsenten Unternehmen in diesem Bereich dar und widmet sich dann der Frage, mit welchen rechtlichen und organisatorischen Lösungsansätzen heute in der Praxis im Bereich der Discovery und insbesondere der E-Discovery operiert wird, um gangbare Kompromisse mit vertretbaren Risiken zu erreichen.

---

[45] Comment of The Sedona Conference Working Group 6 to Article 29 Data Protection Working Party Working Document 1/2009 („WP 158“), October 2009.

2. Ausgangslage für multinationale Konzerne

2.1 Überblick

Die Herausforderungen, welche grenzüberschreitende Discovery im Bereich des Datenschutzes bieten, sind zum einen rechtlicher Natur und zum anderen organisatorischer Art.

Im *rechtlichen Bereich* (Kapitel 2.2 nachfolgend) stehen neben den bereits erwähnten Konflikten der unterschiedlichen Philosophien der US-amerikanischen und kontinentaleuropäischen Rechtskultur fünf Herausforderungen im Vordergrund: Es ist dies der enorm breite sachliche und örtliche Geltungsbereich des Datenschutzes, die Gebote der Zweckbindung, Transparenz und Verhältnismäßigkeit, die Sicherstellung der Rechte der betroffenen Personen und die besonderen Regeln, die für eine grenzüberschreitende Bekanntgabe von Personendaten in die USA und andere Länder ohne – aus europäischer Sicht – angemessen Datenschutz gelten.

Im *organisatorischen Bereich* (Kapitel 2.3 nachfolgend) geht es neben der fallspezifischen und Konzernübergreifenden Interessen im Kern um vier Herausforderungen: Das frühzeitige Involvieren von E-Discovery-Experten mit einer unternehmensweiten Sicht- und Denkweise, das Schaffen von Verständnis und Kooperationsbereitschaft bei den am Streitfall beteiligen Personen, dem Umgang mit durch die Anforderungen des europäischen Datenschutzrechts hervorgerufenen zusätzlichen Zeitbedarfs sowie der praktischen Umsetzung dieser Anforderungen im konkreten Fall in Anbetracht des Umstands, dass viele Hilfsmittel hierfür noch nicht ausgerüstet sind.

Diese Herausforderungen gelten vor allem im rechtlichen Bereich nicht nur im Falle einer E-Discovery, sondern für das Verfahren der Discovery ganz generell, also auch für die Offenlegung von nicht-elektronischen Unterlagen. In Anbetracht der in den meisten Unternehmen heute elektronisch gespeicherten Datenmengen und der in Anbetracht der Tatsache, dass viele gedruckte Unterlagen auch in elektronischer Form vorliegen und sich auf diese Weise einfacher verarbeiten lassen als auf Papier, ist es vor allem die E-Discovery, die in der Praxis Fragen aufwirft. Sie produziert erfahrungsgemäß nicht nur wesentlich mehr Material, sondern zum Beispiel auch wesentlich mehr irrelevantes Material oder Material, bei welchem die betroffenen Personen womöglich nicht mit einer Offenlegung gerechnet haben, was wiederum aus Optik des Datenschutzes von Bedeutung ist.

Aus: Hartmann (Hrsg.), Internationale E-Discovery und Information Governance.

2.2 Rechtliche Herausforderungen

2.2.1 Konflikte unterschiedlicher Rechtskulturen

Die besonderen rechtlichen Herausforderungen eines Discovery-Verfahrens nach angloamerikanischen Vorbild bestehen für ein multinational tätiges Unternehmen – wie eingangs erwähnt – vor allem darin, dass es sich einerseits mit sich entgegenstehenden rechtlichen Konzepten konfrontiert sieht, andererseits diesem Konflikt der Rechtssysteme aber aus operativen und geschäftlichen Gründen nicht ausweichen kann. Es bleibt ihm somit wie beschrieben nur die Möglichkeit, einen in seinen etwaigen Konsequenzen geschäftlich tragbaren Kompromiss zu finden.

Diese rechtlichen Konflikte haben ihre Ursache in den unterschiedlichen Traditionen im angloamerikanischen und kontinentaleuropäischen Recht[46]: So gehen im US-Prozessrecht alle beteiligten Parteien selbstverständlich davon aus, dass zunächst jeder alle möglicherweise relevanten Daten in seinem Bereich sicherstellt bzw. zusammenträgt, den eigenen US Anwälten zur Sichtung auf den Tisch legt und im breiten Umfang letztlich allen Beteiligten am Prozess, also auch der Gegenpartei, zur Beweisführung zur Verfügung stellt. Dies geschieht typischerweise noch vor dem eigentlichen Prozessbeginn (Pre-trial Discovery). Zu dieser Offenlegung kann eine Partei zwar gezwungen werden, doch so weit kommt es normalerweise nicht. Streit entsteht beispielsweise über Umfang, Zeitplan und Art der Offenlegung bzw. den bereits erwähnten *discovery requests* jeder Partei[47], über die sich die Parteien nach den Regeln des US-Zivilprozesses vorgängig direkt verständigen sollen (*meet and confer*)[48]. Eine Folge dieser Tradition der Offenlegung aller im weitesten Sinne relevanten Dokumente (notabene auch der schädlichen) hat beispielsweise dazu geführt, dass viele Unternehmen die (vorprozessuale) Aufbewahrung von Dokumenten[49] inzwischen zeitlich auf ein Minimum begrenzen – mitunter auf wenige Monate und nur selten länger als anderthalb Jahre. Ähnlich verhält es sich auch in anderen Common-Law-Staaten.

Ganz anders die Tradition im kontinentaleuropäischen Recht: Statt dem Grundsatz der völligen Transparenz wird es hier jeder Partei selbst überlassen, die für ihren Standpunkt nötigen Beweismittel einzubringen. Parteien sind nicht wie etwa in den USA verpflichtet, auch schädliche Dokumente offenzulegen. Zur Offenlegung von Unterlagen kann eine Gegenseite oder Drittpartei – wenn überhaupt – oft nur in beschränktem Umfange und unter strengen Voraussetzungen gezwungen werden. Dementsprechend bewahren Unternehmen im kontinentaleuropäischen

---

46 Vgl. zur Unterschiedlichkeit der Rechtsordnungen in den USA und Europa den Beitrag von BANASCHIK in diesem Herausgeberband.

47 Vgl. Fn. 41.

48 US Federal Rules of Civil Procedure, Rule 26f.

49 Gemeint ist die Aufbewahrung von Unterlagen im üblichen Geschäftsgange (also das klassische records management), also noch bevor sich ein Prozess anbahnt und somit nach dem US-Zivilprozessrecht keine besonderen Aufbewahrungspflichten bestehen.

Rechtskreis ihre Unterlagen meist wesentlich länger auf, als dies Unternehmen im angelsächsischen Bereich tun. Oft sind sie zur langjährigen Aufbewahrung ihrer geschäftlichen Unterlagen – E-Mails inklusive – sogar gesetzlich verpflichtet. Aufbewahrungsfristen von fünf oder zehn Jahren sind nicht ungewöhnlich und werden häufig auch überschritten, weil die Unternehmen sich aus einer längeren Aufbewahrung im Streitfalle Vorteile erhoffen: Sie wissen, dass das Risiko, der Gegenpartei Einblick in solche Unterlagen gewähren zu müssen, jedenfalls vor kontinentaleuropäischen Gerichten gering ist.

Schon allein diese Unterschiede in der angelsächsischen und kontinentaleuropäischen Rechtskultur stellen multinational präsente Unternehmen vor rechtliche Herausforderungen, wenn sie sich über die Landes- und Kontinentalgrenzen hinweg technisch und organisatorisch integrieren möchten: Wie lange werden in einem Konzern beispielsweise E-Mails aufbewahrt? Die Antwort muss je nach Region oder sogar je nach Land unterschiedlich ausfallen, auch wenn immer mehr Konzerne aus Kostenüberlegungen dazu übergehen, die die Aufbewahrung elektronischer Dokumente technisch zentral zu organisieren.

Doch während sich mit hohem Aufwand durch organisatorische und technische Mittel landesspezifische Aufbewahrungsvorschriften auch landesspezifisch erfüllen lassen, sind die geschäftlichen Aktivitäten eines international tätigen Konzerns regelmäßig grenzüberschreitend. Weil ein Teil dieser Aktivitäten früher oder später zwangsläufig zu Rechtsstreitigkeiten führt, ist es für den multinational tätigen Konzern letztlich unvermeidbar, zwischen die erwähnten Fronten der beiden unterschiedlichen Rechtskulturen zu geraten.

Solche Fälle nehmen mit der zunehmenden konzerninternen Vernetzung und Arbeitsteilung zu. Immer häufiger werden Geschäfte nicht nur von einem Standort aus betreut, sondern über verschiedene Rechtsordnungen hinweg. Der Zwang zur Effizienz führt überdies zur Zentralisierung bestimmter Konzernfunktionen und damit zwangsläufig zu Strukturen, die im Streitfalle zur Konsequenz haben, dass sich die für einen solchen Streit möglicherweise relevanten Informationen nicht nur geographisch über den Globus verteilen, sondern auch von unterschiedlichsten Konzerngesellschaften und beauftragten Drittfirmen verwaltet werden.

Ist beispielsweise die US-Tochter eines europäischen Konzerns Beklagte in einen US-Zivilprozess, kann die Pre-trial Discovery in jenem Verfahren ohne weiteres auch von der Konzernzentrale in Europa aufbewahrte Unterlagen erfassen. Für die Zwecke der Offenlegungspflicht nach US-Prozessrecht genügt es vereinfacht ausgedrückt, wenn die fraglichen Unterlagen den Prozessparteien zugänglich sind. Die US-Tochter kann also auch zur Offenlegung von Unterlagen der Konzernmutter gezwungen werden, wenn diese ihr solche über das konzerninterne Computernetz im Fernzugriff zur Verfügung stellt. Ist die Muttergesellschaft wie oft selbst Beklagte, werden sämtliche Unterlagen von ihr auch direkt einverlangt, noch bevor es zur Klärung der Frage kommt, ob die Muttergesellschaft in Europa überhaupt zu Recht (mit)eingeklagt worden ist.

Aus: Hartmann (Hrsg.), Internationale E-Discovery und Information Governance.

Ein US-Gericht kann von einer unter seine Gerichtsbarkeit fallenden Person die Offenlegung von allen in ihrem Besitz, unter ihrer Kontrolle oder in ihrem Gewahrsam befindlichen Unterlagen unabhängig davon verlangen, wo sich diese physisch befinden[50]. In solchen Fällen ist es gemäß US-Recht selbst bei Unterlagen auf fremdem Territorium nicht erforderlich, zur Beweisbeschaffung entsprechende internationale Übereinkommen wie etwa das Haager Übereinkommen über die Beweisaufnahme im Ausland in Zivil- oder Handelssachen anzuwenden. Der Richter kann bei vorhergehender Verweigerung einer Prozesspartei somit die Herausgabe der betreffenden Partei mit entsprechenden Sanktionsdrohungen direkt anordnen (*subpoena*), wenngleich eine Anordnung der Herausgabe von im Ausland befindlichen Unterlagen an sich erst nach einer Abwägung der Umstände zugelassen werden sollte[51].

Das kontinentaleuropäische Recht hält diesen Tendenzen des US-Rechts durchaus entgegen, und macht es damit dem multinational tätigen Unternehmen nicht unbedingt einfacher. So kennen verschiedene Staaten wie etwa die Schweiz und Frankreich Gesetzesbestimmungen zum Schutz ihrer Souveränität, welche die private Beschaffung von Beweismitteln auf ihrem Territorium unter Umgehung der internationalen Rechtshilfe in bestimmten Fällen unter Strafe stellen[52]. Diese oft als *blocking statutes* bezeichneten Bestimmungen verbieten zum Teil sogar die Herausgabe eigener Unterlagen in eigenen ausländischen Verfahren. Wurde diese Herausgabe entsprechender Unterlagen vom ausländischen Richter seinerseits unter Androhung von Strafe im Unterlassungsfalle angeordnet, so wird sich das Unternehmen in den betroffenen Ländern letztlich zwischen Pest und Cholera entscheiden müssen – falls es nicht rechtzeitig Vorkehren getroffen hat, um einer solchen Zwickmühle zu entgehen.

Das ist im Alltag eines multinationalen Konzerns freilich in den meisten Fällen möglich. In der Schweiz gehen zum Beispiel selbst strenge Lehrmeinungen davon, dass die fragliche Bestimmung – Art. 271 des schweizerischen Strafgesetzbuches (StGB) – die Herausgabe eigener Unterlagen im eigenen Verfahren erst dann untersagt, wenn die Herausgabe solcher Unterlagen unter Zwang erfolgt, d.h. auf eine entsprechende Anordnung unter Strafe[53]; die Offenlegung eigener Unterlagen im Rahmen einer Pre-trial Discovery ist in der Schweizer also nicht strafbar im Sinne der genannten Bestimmung. Wenn ein Unternehmen allerdings darauf spekulierte,

---

50 Restatement (Third) of Foreign Relations Law of the United States, Nr. 442.

51 Vgl. 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]; In re: Baycol Products Litigation MDL no. 1431, March 21, 2003.

52 So z.B. Art. 271 des schweizerischen Strafgesetzbuches und das französische Strafgesetz Nr. 80-538.

53 Davon zu unterscheiden sind prozessleitende Anordnungen wie etwa scheduling orders, welche lediglich den Fahrplan eines Prozesses und damit auch den Zeitpunkt der Offenlegungen der Parteien regelt, diese aber freiwillig im Rahmen dieser Verfügung nicht (wie im Falle einer subpoena) erzwungen werden sollen; vgl. zum Ganzen Rosenthal, Handkommentar zum Datenschutzgesetz, Zürich 2008, Art. 271 StGB, N 19 ff.

zunächst selbst von der Gegenpartei vernünftigerweise verlangte Unterlagen nicht zu liefern in der Hoffnung, einer Offenlegung schädlicher Dokumente zu entgehen, dreht es sich unter Umständen den eigenen Strick: Wird ihm später vom Richter unter Strafe angeordnet, die Unterlagen offenzulegen, darf es dies nicht mehr außerhalb des Rechtshilfeweges tun, selbst wenn es dann dazu bereit wäre, weil ihm sonst schlimmeres Ungemach droht. Dieses Szenario zeigt, dass Unternehmen somit gut beraten sind, sich bereits frühzeitig über die möglichen Implikationen einer Nichtkooperation ein Bild zu verschaffen, und zwar nicht nur nach US-amerikanischem Recht. Der eine oder andere Verantwortliche wird aus Opportunitätsgründen auch die Sanktionsdrohungen gegeneinander abwägen: In der Schweiz wird er zum Beispiel zum Schluss kommen, dass eine Verletzung des Datenschutzes im Rahmen einer Pre-trial Discovery normalerweise (falls überhaupt) wesentlich weniger schwerwiegende Sanktionen mit sich bringt als im Falle einer erzwungenen Offenlegung die Verletzung von Art. 271 StGB[54].

Befindet sich ein Unternehmen erst einmal in einer solchen Zwickmühle, kann die internationale Rechtshilfe hier nur teilweise befriedigende Lösungen bieten, selbst wenn der US-Richter bereit ist, sie durchzuführen: So nehmen zum Beispiel nicht alle Staaten in Europa am bereits erwähnten Haager Übereinkommen über die Beweisaufnahme im Ausland teil und etliche Vertragsstaaten[55] haben Vorbehalte bezüglich der Offenlegung von Unterlagen für ein Pre-trial Discovery angebracht.

Immerhin bieten andere Vertragsstaaten des Haager Übereinkommens jedenfalls dann, wenn alle Beteiligten einverstanden sind, weitreichende Möglichkeiten zur Beweisbeschaffung auf dem Rechtshilfeweg und unter Ausschaltung der Datenschutzgesetzgebung[56]. Allerdings sind auch hier aus US-amerikanischer Sicht Kompromisse erforderlich, so etwa was die Zeitdauer zur Durchführung einer Beweiserhebung betrifft[57] oder den Umfang und die Anforderung zur vorgängigen Spezifizierung der Beweiserhebung, die mitunter über jene hinausgehen kann, welche im US-Recht erforderlich ist.

---

54 Art. 271 des schweizerischen Strafgesetzbuches, welcher ein Strafmaß von drei Jahren Freiheitsstrafe oder Geldstrafe für die verantwortlichen Einzelpersonen vorsieht.

55 So etwa Deutschland, Spanien, Frankreich und die Niederlande.

56 So etwa im Schweizer Recht, wo im Rahmen der Rechtshilfe unter Einsatz eines „commissioners“ sogar Kreuzverhöre möglich sind. Im Bereich der internationalen Rechtshilfe findet in der Schweiz auch das Datenschutzgesetz keine Anwendung (Art. 2 Abs. 2 Bst. c DSG).

57 Welche im Einzelfall erfahrungsgemäß wesentlich von der Kooperation der Parteien und der Vorbereitung und Qualität entsprechender Anfragen abhängt.

Auch vertragliche oder gesetzliche Geheimhaltungspflichten, wenn sie die Offenlegung im Prozess mit Dritten oder den Export untersagen[58], können multinationale Unternehmen in eine Zwickmühle versetzen, vor allem, wenn diese Geheimhaltungspflichten strafrechtlich abgesichert sind, was mitunter sogar mit spezifischem Fokus zur Verhinderung der Preisgabe von Geschäftsgeheimnissen ins Ausland geschieht[59]. Hier kann eine Offenlegung im US-Prozess, jedenfalls dann, wenn keine weiteren Schutzvorkehren[60] getroffen worden sind, zur Strafbarkeit der verantwortlichen Personen des betreffenden Unternehmens führen, selbst wenn dieses von einem US-Gericht gezwungen wurde, die fraglichen Unterlagen preiszugeben.

Der im Alltag multinationaler Unternehmen häufigste Konflikt zwischen den Offenlegungspflichten im angloamerikanischen Zivilprozess und dem kontinentaleuropäischen Recht betrifft allerdings den Datenschutz, wie nachfolgend erläutert wird. Dieser existiert in der heutigen Form zwar schon seit vielen Jahren, doch hat seine Wichtigkeit in der öffentlichen Wahrnehmung und der *legal compliance* der Unternehmen ebenso zugenommen wie die Sanktionierung von Datenschutz-Verletzungen in den verschiedenen Staaten in den letzten Jahren deutlich verschärft worden ist[61].

2.2.2 Die fünf rechtlichen Herausforderungen des Datenschutzes

Der Datenschutz stellt multinationale Unternehmen im Bereich des Discovery vor besondere Herausforderungen rechtlicher Natur. Aus der Optik multinational tätiger Unternehmen lassen sich diese Herausforderungen in fünf Punkten zusammenfassen:

---

58 Beispiele sind hier einerseits Berufsgeheimnisse (so untersagt z.B. das schweizerische Bankgeheimnis grundsätzlich die Preisgabe von Bankkundendaten ins Ausland, weil dort das Bankgeheimnis nicht mehr gewährleistet werden kann; ein weiteres Beispiel ist das deutsche Fernmeldegeheimnis, das auch auf E-Mails der eigenen Arbeitnehmer auf dem eigenen Server Anwendung finden kann) und andererseits vertragliche Geheimhaltungspflichten, die so formuliert sind, dass sie keinen Vorbehalt für Zivilprozesse vorsehen und die Preisgabe selbst dann nicht erlauben, wenn die Prozessbeteiligten ihrerseits zur Geheimhaltung verpflichtet sind. Ob eine solche Klausel vorliegt, muss erfahrungsgemäß häufig durch Auslegung ermittelt werden, da bei der Formulierung solcher Regelungen normalerweise nicht an den Fall einer Offenlegung im Prozess (und erst Recht nicht an den Prozess im Ausland) gedacht wird.

59 So z.B. Art. 273 des schweizerischen Strafgesetzbuches oder Art. 124 des österreichischen Strafgesetzbuches.

60 Wie etwa Schwärzungen oder Schutzverfügungen (protective orders).

61 Im Vereinigten Königreich kann der U.K. Information Commissioner inzwischen Bußgelder von bis zu GBP 500'000 verhängen, in Spanien können Bußgelder bis zu EUR 600'000 betragen. In Frankreich wurde die Maximalsummer schon vor einigen Jahren auf EUR 150'000 erhöht und in Deutschland sind Bußgelder bis EUR 300'000 möglich, in gewissen Fällen sogar Freiheitsstrafen.

Erste Herausforderung: Geltungsbereich

Die erste Herausforderung im Spannungsfeld zwischen Discovery und Datenschutzes ist der breite Anwendungsbereich der Datenschutzgesetzgebung, und zwar sowohl in sachlicher als auch in örtlicher Hinsicht.

Extensiv ist zunächst der *örtliche* Geltungsbereich vieler Datenschutzgesetze: Berührt ein E-Discovery-Projekt Europa auch nur teilweise, so muss regelmäßig mit der Anwendung der nationalen Datenschutzgesetze all in jener europäischen Länder gerechnet werden, in denen Daten für eine E-Discovery gesammelt oder weiterverarbeitet werden. In der EU zum Beispiel finden die nationalen Datenschutzgesetze normalerweise dann Anwendung, wenn entweder die für die Datenbearbeitung verantwortliche Stelle (was im Falle einer E-Discovery typischerweise der Arbeitgeber sein wird, bei dessen Mitarbeitern und von dessen Servern die Daten zusammengetragen werden) sich im betreffenden Land befindet oder – falls die verantwortliche Stelle nicht in der EU ist – die Datenbearbeitung in der EU erfolgt (was zum Beispiel dann der Fall ist, wenn E-Discovery-Daten aus Nicht-EU-Jurisdiktionen auf Servern in der EU vor der Weiterverarbeitung zusammengezogen werden).

Schon für ein Unternehmen, welches nur in einer Rechtsordnung tätig ist, kann die Einhaltung der Bestimmungen des Datenschutzes einen erheblichen Aufwand mit sich bringen. Multinationale Unternehmen hingegen sind mit dem Problem konfrontiert, letztlich die Datenschutzgesetze aller Länder kennen und befolgen zu müssen, in denen im Rahmen einer E-Discovery Daten gesammelt werden müssen oder in denen die Daten weiter verarbeitet werden und möglicherweise auch jener Länder, aus denen betroffene Personen stammen, wo das nationale Recht eine extensivere Geltung beansprucht als in Europa normalerweise üblich[62].

Das Schweizer Datenschutzrecht ist so ein Beispiel: Es kann zur Anwendung gelangen, wenn nur schon die betroffene Person sich normalerweise in der Schweiz aufhält, selbst wenn die Daten ausschließlich im Ausland gesammelt und weiterverarbeitet werden[63]. Muss also im Rahmen einer Datensammlung davon ausgegangen werden, dass sich darin Personendaten auch aus der Schweiz befinden oder Personendaten, die Personen aus der Schweiz betreffen, immer auch Schweizer Datenschutzrecht zur Anwendung kommt, selbst wenn die Daten für die Zwecke einer E-Discovery ausschließlich außerhalb der Schweiz gesammelt und bearbeitet wurden bzw. werden sollen. Da das Schweizer Datenschutzrecht – wie nachstehend gezeigt – auch juristische Personen schützt, findet es in multinationalen Konzernen mit relevanten Berührungspunkten in der Schweiz somit im Ergebnis meistens irgendwie Anwendung. Aus Sicht der *legal compliance* im Konzern wiederum bedeutet dies, dass ein Unternehmen entweder in der Lage sein muss, seine Datenbe-

---

62 Vgl. zur Zulässigkeit der Datenübermittlung und einem Prüfschema zum internationalen Datentransfer den Beitrag von Laue in diesem Herausgeberband.

63 Art. 139 des schweizerischen Gesetzes über das Internationale Privatrecht; vgl. Rosenthal, Fn. 53, Art. 139 IPRG, N 2.

stände nach anwendbarem Recht zu klassifizieren, oder aber den strengsten Schutzstandard der möglicherweise (wenn auch nur auf einen Teil der Datensammlung) anwendbaren Datenschutzbestimmungen anzuwenden. In der Praxis wird aufgrund fehlender Datenklassifizierung und aus Gründen der Praktikabilität meist letztere Variante gewählt.

Zu beachten ist ferner, dass die nationalen Datenschutzgesetze auch auf Importdaten angewandt werden wollen, also nicht nur auf im Inland generierte Daten. Trägt beispielsweise eine Konzernmutter in der Schweiz für einen US-Prozess Personendaten in ganz Europa (oder auch aus den USA) zusammen und sendet sie diese dann aus der Schweiz weiter an die Anwälte in den USA, müssen die materiellen nationalen Datenschutzgesetze jeweils bezüglich der in den einzelnen Ländern gesammelten Daten beachtet werden, für alle Daten aber immer auch das Schweizer Datenschutzgesetz, da es auf sämtliche Daten Anwendung findet, welche die Konzernmutter in der Schweiz bearbeitet. Das gilt auch dann, wenn die Daten ursprünglich nicht aus der Schweiz stammen und somit lediglich für die Zwecke der E-Discovery in die Schweiz gelangten. Das materielle Schweizer Datenschutzrecht bleibt auch dann anwendbar, wenn die Daten längst in die USA übermittelt worden sind. Zwar lässt es sich womöglich vor Ort nicht gerichtlich durchsetzen, doch Schadenersatzansprüchen wegen Datenschutzverletzungen in den USA können gegen die Konzernmutter und die weiteren Mitwirkenden (also zum Beispiel die Anwälte in den USA) unter Umständen auch in der Schweiz erhoben werden, auch wenn die Daten dort nur einen "Zwischenhalt" einlegten. In der Praxis zeigt sich umgekehrt freilich auch, dass es durchaus von Vorteil sein kann, wenn Datenströme über bestimmte Rechtsordnungen gelenkt werden, wenn dort wie etwa im genannten Beispiel der Schweiz die formalen Voraussetzungen für den Datenexport weniger streng sind als in den meisten Ländern der EU, denn bezüglich der Frage des Exports der Personendaten aus der Schweiz kommt, wenn die Daten erst einmal in der Schweiz sind, grundsätzlich nur noch das Schweizer Datenschutzrecht zur Anwendung (vgl. dazu Kapitel 3.4.2 unten).

Auch in *sachlicher* Hinsicht finden die Datenschutzgesetze europäischer Konzeption Anwendung an breiter Front. Sie knüpfen dabei regelmäßig an den Begriff der "Personendaten" an. Hierbei handelt es sich um alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen[64]. Hierbei gibt es Rechtsordnungen, die den Begriff weiter einschränken[65]. Allerdings gibt es ebenso solche, die ihn ausdehnen, indem sie Personendaten juristischer und nicht nur natürlicher Personen erfassen[66]. Dies kann multinationale Unternehmen in besonderem Masse treffen,

---

64 Art. 2 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (zit. "EU Datenschutz-Richtlinie").

65 Ein Beispiel ist Kanada, dessen Personal Information Protection and Electronic Documents Act festhält, dass Informationen über den Namen, den Titel, die Geschäftsadresse und die Telefonnummer des Arbeitnehmers einer Organisation nicht als Personendaten gelten.

66 So z.B. in der Schweiz, Italien, Österreich, Luxemburg, Dänemark.

etwa wenn eine zentralisierte Bearbeitung von Daten – wie dargelegt – dazu führt, dass auf ein- und dieselben Daten die Datenschutzgesetze verschiedener Rechtsordnungen anwendbar werden können und ein Konzern vor der Wahl steht, entweder das strengste anwendbare Recht zu befolgen (hier: auch Daten juristischer Personen zu schützen) oder aber die Verletzung von bestimmten nationalen Datenschutzgesetzen riskieren (indem der konzerninterne Datenschutz auf Daten natürlicher Personen fokussiert wird). Erfahrungsgemäß wählen viele multinational tätige Konzerne letztere Variante und überlassen es ihren Ländergesellschaften, allenfalls weitergehende Vorkehrungen zu treffen.

Der Anwendungsbereich des Datenschutzes ist freilich so oder so breit, denn Personendaten kommen überall vor: Zwar erfolgt die Diskussion um den Datenschutz im Bereich des E-Discovery vornehmlich mit Blick auf die E-Mails von Arbeitnehmern der betroffenen Unternehmen. Doch der Datenschutz geht wesentlich weiter und schützt auch die Daten jeder anderen Person, die identifiziert wird oder allenfalls mit Hilfe weiterer Informationen identifizierbar ist. Er ist also ebenso zu beachten, wenn in den E-Mails, Textdokumenten oder Datenbanken eines Unternehmens auch andere Personen wie etwa Kunden, Geschäftspartner oder auch Konkurrenten genannt werden (bzw. deren Organe und sonstigen Mitarbeiter, soweit eine Rechtsordnung nur die Daten natürlicher Personen schützt und die betreffenden Daten der Arbeitnehmern nicht vom Schutz ausnimmt), auch wenn deren Schutzbedarf letztlich geringer sein mag.

Dies führt im Zusammenhang mit E-Discovery-Vorhaben in der Praxis immer wieder zu Missverständnissen und falschen Vorstellungen dies- und jenseits des Atlantiks:

- Zum einen wird der Begriff der Personendaten (personal data) im US-Rechtsraum oft enger perzipiert, als er in Wirklichkeit ist (der in den USA inzwischen teilweise geläufige Begriff der personally identifiable information ist nicht einheitlich definiert, meint aber mitunter dasselbe wie Personendaten[67]). So ist es nicht ungewöhnlich, dass ein US-Gericht auf Verlangen eine Schutzverfügung zwecks Geheimhaltung von Informationen einer Pre-trial Discovery erlässt, in welcher sämtlichen Personendaten derselbe Schutz wie Geschäftsgeheimnissen bzw. anderen vertraulichen Daten zukommt. Dass dies im Ergebnis dazu führt, dass sämtliche offengelegten E-Mails, Unterlagen und Daten geheim gehalten werden müssen, wird oft erst später realisiert. Es wird in einer Pre-trial Discovery jedenfalls kaum Dokumente geben, die nicht Personendaten im Sinne des europäischen Datenschutzrechts darstellen – es sei denn, sie wurden aufwändig anonymisiert worden, was regelmäßig nur mit besonders heiklen Daten und nur sehr gezielt geschieht. Eine häufige Quelle für Fehlvorstellungen sind auch Ver-

[67] Vgl. aber etwa NIST, US Department of Commerce, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), Special Publication 800-122, S. 2-1 (http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf).

wechslungen der beiden Begriffe personal data und private data: Während ersteres normalerweise Personendaten im vorgenannten Sinne meint und somit auch solche Daten erfasst, die zwar personenbezogen, aber trotz allem geschäftlicher Natur sind, umfasst letzterer Begriff die rein privaten Personendaten, also personenbezogene Daten, die nicht geschäftlicher Natur sind.

- Zum anderen denken Datenschützer in Europa und US-Prozessjuristen in ihrem Bereich oftmals in unterschiedlichen Kategorien: Ersterer will die Umgang mit bestimmten Informationen an sich regeln, wo und wie auch immer diese zum Ausdruck kommen, während letzterer die Verkörperung der Information im Fokus hat, also das Dokument oder den Datensatz, welches eine bestimmte Information enthält. Diese Unterscheidung zwischen Inhalt und Träger bzw. Form kann durchaus von Relevanz sein, etwa wenn Vereinbarungen oder Verfügungen zur Sicherstellung des Datenschutzes getroffen werden. Der Schutz nur der Dokumente genügt nicht; auch das gesprochene Wort oder und der Transfer einer Informationen in ein anderes, ggf. nicht erfasstes Dokument wie etwa eine Rechtschrift oder Urteilsdokument muss erfasst sein.

Zweite Herausforderung: Zweckbindung und Transparenz

Die zweite Herausforderung des Datenschutzes in E-Discovery-Unterfangen ist der Grundsatz der Zweckbindung und Transparenz. Diese besagen vereinfacht ausgedrückt, dass die betroffenen Personen vorab informiert sein müssen, für welche Zwecke ihre Daten erhoben und bearbeitet werden sollen[68]. Eine nachträgliche Umnutzung von Personendaten verletzt diese Grundsätze und ist nur mit einer entsprechenden Rechtfertigung zulässig[69].

Im Kontext eines Discovery-Verfahrens bedeutet dies, dass allen betroffenen Personen – und dies sind nicht nur die eigenen Arbeitnehmer – bei der Beschaffung ihrer Daten durch das Unternehmen in genereller Weise klar sein muss, wozu ihre Daten verwendet werden können, nämlich für die Zwecke eines Zivilprozesses in den USA, sollte das betreffende Unternehmen oder ein verbundenes Unternehmen in einen solchen verwickelt werden. Während eine ausdrückliche Information im Falle der eigenen Mitarbeiter sich noch auf die eine oder andere Weise mit vertretbarem Aufwand bewerkstelligen lässt (z.B. durch eine generelle Information im Rahmen interner Richtlinien und eine konkrete Informationen im jeweiligen Einzelfall vor der Sicherstellung der Daten), ist dies bei allen anderen betroffenen Personen (z.B. den in den E-Mails genannten Mitarbeitern von Kunden, Geschäftspartnern und anderen externen Stellen) in aller Regel nicht mehr in vernünftiger Weise möglich. Hierbei wird in der Praxis auf die ausdrückliche Information unter

---

68 Art. 6 und 10 der EU-Datenschutz-Richtlinie; Art. 4 Abs. 3 und 4 des schweizerischen Datenschutzgesetzes.

69 Art. 7, 11 und 13 der EU-Datenschutz-Richtlinie; Art. 12 Abs. 1 und 2 sowie Art. 13 des schweizerischen Datenschutzgesetzes.

anderem mit dem Argument verzichtet, dass heute jeder, der mit einem Unternehmen verkehrt, generell damit rechnen muss, dass dieses Unternehmen auch im Ausland in Rechtsstreitigkeiten verwickelt werden kann und es dabei auch zur Offenlegung von Unterlagen eben dieses Unternehmens kommen kann. Das Unternehmen wird in solchen Fällen letztlich nur dafür sorgen müssen, dass es zu keiner Zweckentfremdung der offengelegten Personendaten kommt, sie also von der Gegenpartei, dem Gericht und den anderen beteiligten Personen einzig für die Zwecke des Verfahrens eingesetzt wird und namentlich nicht veröffentlicht werden darf.

Mag dies im Falle der in aller Regel überblickbaren Verhältnisses eines national tätigen Unternehmens noch ohne Weiteres funktionieren, so stellt die Einhaltung des Grundsatzes der Zweckbindung und Transparenz in einem multinationalen Konzern eine größere Herausforderung dar: Denn die Daten einer betroffenen Person werden mitunter nicht mehr nur für die Zwecke des Unternehmens verwendet, mit welchem die betreffende Person in direktem Kontakt steht und das die Person kennt. Sie können über konzerninterne Vernetzungen und Aufgabenteilungen oder auch bloße Zufälligkeiten ohne Weiteres auch Eingang in Rechtsstreitigkeiten anderer Konzerngesellschaften und damit auch in anderen Rechtsordnungen finden. Ist beispielsweise der Mitarbeiter der deutschen Tochtergesellschaft eines US-Konzerns an einem US-Projekt beteiligt, welches in den USA zu einem Zivilprozess führt, so finden möglicherweise auch Mails dieses Mitarbeiters mit seinen deutschen Kunden Eingang in die Pre-trial Discovery in den USA.

Selbstverständlich lässt sich auch in solchen Fällen mit guten Gründen vertreten, dass Mitarbeiter wie Dritte in der heutigen vernetzten Geschäftswelt mit solchen Datentransfers rechnen müssen – erst recht, wenn sie es mit einer Gesellschaft zu tun haben, die einem multinationalen Konzern angehört. Konzerne werden jedoch noch immer in den meisten Datenschutzgesetzen nicht privilegiert behandelt: Der Transfer von Personendaten unter Konzerngesellschaften gilt gemeinhin als Datentransfer unter Dritten, der eine entsprechende vorgängige Information der betroffenen Personen erfordert, sofern die eine Konzerngesellschaft nicht lediglich im Auftrag der Datenbeschafferin tätig wird, was in den im Bereich der discovery relevanten Konstellationen regelmäßig nicht der Fall sein wird. Hinzu kommt, dass in vielen Rechtsordnungen Daten der eigenen Mitarbeiter einem besonderen Schutz unterstellt wird, der es Unternehmen erschwert, Daten über ihre eigenen Angestellten mit anderen Unternehmen auszutauschen – und sei es nur, damit das eine Konzernunternehmen einem anderen verbundenen Unternehmen mit seinen Daten in dessen Prozess vor Gericht beisteht[70].

[70] Vgl. zum Schutz der Arbeitnehmerrechte und Beteiligung des Betriebsrats den Beitrag von MEYER in diesem Herausgeberband.

Dritte Herausforderung: Verhältnismässigkeit

Die dritte datenschutzrechtliche Herausforderung im Bereich der E-Discovery stellt das datenschutzrechtliche Gebot der Verhältnismäßigkeit jeder Datenbearbeitung dar. Er verlangt zusammengefasst, dass Daten nur soweit bearbeitet werden, als dies für die Erreichung des angestrebten Verwendungszwecks geeignet und erforderlich ist und die Bearbeitung der Personendaten für die betroffenen Personen letztlich zumutbar sind[71]. Im Kontext einer E-Discovery bedeutet dies, dass Daten grundsätzlich nur soweit offenzulegen sind, als dies für den konkreten Fall tatsächlich erforderlich ist.

Europäische Datenschützer, allen voran die bereits erwähnte Artikel-29-Datenschutzgruppe, haben aus diesem Grundsatz der Verhältnismäßigkeit der Datenbearbeitung die Forderung abgeleitet, dass alle im Rahmen einer Pre-trial Discovery in einem US-Prozess offenzulegenden Informationen entsprechend vorgängig gefiltert werden müssen. In ihrem 2009 veröffentlichten Arbeitspapier, welches das Spannungsverhältnis zwischen den Anforderungen des europäischen Datenschutzes und dem US-amerikanischen pre trial-discovery-Verfahren umschrieben wird, haben sie sich auch zur Einhaltung des Grundsatzes des Verhältnismäßigkeit geäußert[72]: Entweder seien demnach alle für den Streitgegenstand irrelevanten Personendaten zu entfernen oder aber die vorhandenen Informationen müssen anonymisiert oder pseudonymisiert, d.h. der Personenbezug für den Empfänger der Daten entfernt werden (z.B. durch Schwärzung oder Ersatz der tatsächlichen Namen durch ein Pseudonym)[73]. Sie begründen dies dadurch, dass wenn in einer Discovery irrelevante Personendaten offengelegt werden, dies *per se* einen Verstoß gegen die Grundsätze des Datenschutzes darstellt, weil bezüglich dieser Daten eine Bearbeitung stattfindet, die für den Streitfall definitionsgemäß nicht erforderlich sind. Ist also die Identität einer betroffenen Person (z.B. des Senders oder Empfängers einer E-Mail) für den konkreten Streitfall nicht relevant, darf er aus Sicht dieser Datenschützer auch nicht offengelegt werden. Die betreffende Filterung muss nach Ansicht der Datenschützer im Ursprungsstaat geschehen (d.h. noch bevor die relevanten in den Drittstaat wie etwa die USA übermittelt werden) und am besten durch einen "vertrauenswürdigen Dritten", der zwar Kenntnisse des Rechtsstreits habe, in ihm aber keine Rolle spielt[74].

Zwar setzt sich auch in europäischen Datenschutzkreisen allmählich die Erkenntnis durch, dass solche Forderungen übertrieben, praxisfremd und für Unternehmen nicht vernünftig realisierbar sind; auch aus dem Datenschutzrecht der EU lassen sich mit etwas gutem Willen weniger strenge Anforderungen ableiten (ein Lösungsansatz, der nach der hier vertretenen Ansicht ohne Weiteres dem Gebot der Verhältnismäßigkeit entspricht ist nachfolgend unter Kapitel 3.3.2 dargestellt). Das

---

71 Art. 6 EU-Datenschutz-Richtlinie; Art. 4 Abs. 2 des schweizerischen Datenschutzgesetzes.

72 WP158, Fn. 44.

73 WP158, Fn. 44, S. 12.

74 WP158, Fn. 44, S. 12 f.

Kernanliegen, die Vermeidung jeder unnötigen Bearbeitung von Personendaten, bleibt jedoch bestehen. Die Herausforderung besteht jedoch nicht in einer mangelnden Akzeptanz dieses Kernanliegens. Es findet sich ganz im Gegenteil auch im US-Zivilprozessrecht wieder. Die Herausforderung besteht in der Praxis letztlich in unterschiedlichen Auffassungen, wie weit eine Offenlegung für den Streitgegenstand Unterlagen tatsächlich erforderlich ist, d.h. was erstens wirklich relevant ist und zweitens von einer Partei vernünftigerweise verlangt werden kann. Die *US Federal Rules of Civil Procedure* kannten den Grundsatz der Verhältnismäßigkeit (*proportionality rule*) schon vor ihrer Anpassung im Jahre 2006, bloß wurde dieser Grundsatz in der Vergangenheit vergleichsweise selten angerufen und erfährt erst in jüngster Zeit – wohl aufgrund überbordender E-Discovery-Forderungen – mehr Aufmerksamkeit. Immerhin kann auch die Offenlegung von Unterlagen, die für den Fall selbst irrelevant sind zum Beispiel dort erforderlich werden, wo sonst der Entscheid über die Relevanz und die Ordnungsmäßigkeit der Abwicklung eines Filterungsprozesses im Rahmen einer E-Discovery sonst nicht hinreichend überprüft werden könnte. Oder aber es stehen für die Filterung aller irrelevanten Unterlagen zum Zeitpunkt der Offenlegung nicht genügend Ressourcen, nicht genügend Informationen oder aber nicht genügend Zeit zur Verfügung.

Schließlich ist auch die Relevanz bzw. Irrelevanz letztlich eine Frage der Definition. Was jedenfalls für die Offenlegung relevant ist, spiegelt sich zunächst in den *discovery requests* der Parteien wieder und ist letztlich das Ergebnis der Verhandlungen der Parteien im Rahmen der *meet-and-confer*-Gespräche oder, wenn diese nicht fruchten, der richterlichen Anordnung. Wie eine Partei es erreicht, aus allen ihr zur Verfügung stehenden Dokumente und Daten möglichst nur jene für die Zwecke der Offenlegung herauszuschälen, die in den vorgängig definierten Kreis der relevanten Dokumente und Daten gehören, ist ihre Sache. Fehler in der Selektion werden hierbei jedoch tendenziell nur zugunsten einer breiteren Offenlegung akzeptiert. Ein Unternehmen muss also grundsätzlich nicht alle E-Mails offenlegen, die bestimmte formale, äußere Kriterien erfüllen (z.B. punkto Zeitraum, Empfänger, Sender, Stichworte). Diese dienen lediglich einer ersten Eingrenzung. Den verbliebenden Rest wird es jedoch typischerweise einem semi-automatischen Filterungsprozess unterziehen und die Treffer, welche gewisse Suchkriterien erfüllen und in einer manuellen Sichtung durch die eigenen Anwälte nicht als klar irrelevant (oder aus anderen Gründen nicht offenlegungspflichtig) erkannt werden, offenlegen. Der richtigen Wahl der Suchbegriffe und Suchstrategie und deren Optimierung (*keyword refinement*) kommt somit eine zentrale Rolle in der Bestimmung des Kreises der offengelegten Informationen zu. Was verbleibt, ist das, was als im weitesten Sinne als relevant bezeichnet werden kann und offengelegt wird.

Freilich wird sich auch dieser Kreis im Laufe der Zeit weiter einschränken, weil es in jedem Verfahren viele Themen gibt, die wegfallen oder an Relevanz verlieren – bis am Schluss wenige Fragen übrig bleiben und das Gericht darüber entscheiden muss, auf welche E-Mails (und sonstigen Beweismittel) es sich diesbezüglich für seinen Entscheid abstützen will, weil es nur diese hierfür letztlich als relevant er-

achtet. Dies wiederum bedeutet nicht, dass alle anderen E-Mails in den früheren Stadien des Prozesses unzulässiger oder unnötigerweise offengelegt wurden. Da die Pre-trial Discovery am Anfang des Prozesses steht und zu einem Zeitpunkt stattfindet, an welchem oft noch nur vage abzuschätzen ist, was genau Prozessthema sein geschweige denn relevant sein wird (anders als im kontinentaleuropäischen Rechtsraum kann eine Klage im angelsächsischen Rechtsraum zum Zeitpunkt der Pre-trial Discovery sehr allgemein gehalten sein), besteht die Herausforderung letztlich darin, eine Datenfilterung zustande zu bringen, die trotz dieser Ungewissheit ein Mindestmaß an Verhältnismäßigkeit garantiert.

Zu beachten ist, dass die datenschutzrechtlich relevante Datenbearbeitung schon vor dem Einreichen einer Klage beginnen kann, verpflichtet doch das US-amerikanische Prozessrecht die Prozessparteien, möglicherweise relevante Informationen im Unternehmen bereits ab dem Zeitpunkt zu bewahren (*preserve*) an welchem ein Prozess vernünftigerweise absehbar ist (*anticipated*). Dementsprechend kann ein dem Rechtsdienst eines Unternehmens telefonisch vorgebrachte Prozessdrohung eines Gegenanwalts genügen, damit das Unternehmen eine *legal hold* veranlassen wird, also eine schriftliche Anweisung erteilt, dass sämtliche für einen solchen Prozess möglicherweise relevanten Informationen nicht mehr löscht bzw. ändert und bereits in diesem Stadium mit entsprechenden Hilfsmitteln dafür sorgt, dass sie für die Zwecke eines etwaigen Prozesses aufbewahrt und verfügbar sind. Eine generelle Pflicht, alle Daten einzusammeln und getrennt aufzubewahren, gibt es nicht. Unterliegen sie jedoch der Gefahr einer Änderung, Löschung oder sonstigem Verlust, müssen diese jedoch schon zum Zeitpunkt des *legal hold* sichergestellt werden (z.B. durch Überführung in ein besonderes System zur Datenkonservierung). Wie eingangs bereits erwähnt, können Nachlässigkeiten in diesem Bereich für die betreffende Partei schwer wiegende Konsequenzen in einem späteren Prozess haben.

All diese Vorgänge sind letztlich datenschutzrechtlich relevant, und zwar deshalb, weil die betroffenen Personendaten damit erstens einem neuen Zweck (der allfälligen Verwendung im Prozess) zugeführt werden und zweitens möglicherweise länger als nach dem normalen Gang der Dinge aufbewahrt werden (d.h. länger als vom Unternehmen normalerweise nötig erachtet). Werden Unterlagen plötzlich für weitere Zwecke aufbewahrt oder geschieht dies länger als sonst üblich, stellen sich unmittelbar Fragen bezüglich der Einhaltung der datenschutzrechtlichen Grundsätze der Zweckbindung, Transparenz und Verhältnismäßigkeit der Datenbearbeitung.

Die Einhaltung dieser Grundsätze ist nicht nur für den multinational tätigen Konzern eine Herausforderung. Sie kann ihn allerdings dann in verschärfter Form treffen, wenn eine Discovery in einem Konzern nicht nur eine sondern zahlreiche Ländergesellschaften betreffen und daher auch Daten in unterschiedlichsten Rechtsordnungen gesammelt und zusammengetragen werden müssen. Nicht nur aus Gründen der Effizienz und Kosten, sondern auch aus Gründen der Einheitlichkeit der Verarbeitung dieser Daten wird es in solchen Fällen meist unrealistisch

sein, eine umfassende Filterung der erhobenen Daten in jedem der betroffenen Staaten separat durchzuführen bevor es zu einer Konsolidierung der Daten kommt (siehe hierzu das Standardprozedere gem. Kapitel 3.3.2 unten).

An dieser Stelle zu erwähnen ist allerdings auch, dass das Prinzip Verhältnismäßigkeit nicht nur Restriktionen für das betroffene Unternehmen mit sich bringt. Es gilt auch umgekehrt: Der Datenschutz verlangt nicht jede erdenkliche Maßnahme, die im Interesse des Datenschutzes der betroffenen Personen liegen könnte. Der Datenschutz verlangt lediglich Vorkehren, die ihrerseits verhältnismäßig sind. Je weniger heikel die betroffenen Daten und Interessen der betroffenen Personen gegen eine Datenbearbeitung sind, desto geringer sind grundsätzlich auch die Anforderungen des Datenschutzes an den Datenbearbeiter, so die Faustregel, die oft vergessen geht.

Vierte Herausforderung: Rechte der betroffenen Personen

Die vierte Herausforderung betrifft die Gewährleistung der Rechte der betroffenen Personen. Diese Rechte bestehen im Recht auf Auskunft über ihre Daten, dem Recht auf Berichtigung und dem Recht auf Löschung ihrer Daten bzw. Widerspruch gegen deren Bearbeitung[75]. Sie gelten grundsätzlich auch bezüglich der im Rahmen einer Discovery offengelegten Personendaten. Auch dies ist eine Herausforderung des Datenschutzes, die keineswegs nur multinationale Konzern trifft. Ihre Schwierigkeit besteht darin, dass das Gericht und die Gegenpartei, gegenüber welcher die betreffenden Personendaten offengelegt wird, in aller Regel nicht bereit sein werden, das Recht einer betroffenen Person auf Auskunft, Berichtigung und Löschung ihrer Daten bzw. Widerspruch anzuerkennen.

Fünfte Herausforderung: Grenzüberschreitende Bekanntgabe

Die fünfte Herausforderung des Datenschutzes im Rahmen einer Discovery stellen die Beschränkungen bei der grenzüberschreitenden Bekanntgabe von Personendaten dar. Sie sind auch innerhalb der EU in jedem Land etwas anders geregelt, auch wenn das Regelungsprinzip in allen Ländern Europas – auch der Schweiz – stets dasselbe ist: Personendaten dürfen (von einigen Ausnahmen) abgesehen nur dann ins Ausland exportiert werden, wenn dort entweder ein angemessener gesetzlicher Datenschutz besteht oder aber ein angemessenes Datenschutzniveau auf andere Weise sichergestellt wird[76].

Im Kontext einer Discovery in einem US-Zivilprozess wird diesen Exportregelungen meist eine besonders hohe Bedeutung beigemessen, auch wenn sie keineswegs übergeordneter Natur sind. Letztlich geht es darum sicherzustellen, dass die

---

[75] Art. 12 und 14 der EU-Datenschutz-Richtlinie; Art. 5, 8, 12 Abs. 2 Bst. b und Art. 15 des schweizerischen Datenschutzgesetzes.

[76] Art. 25 ff. der EU-Datenschutz-Richtlinie, Art. 6 des schweizerischen Datenschutzgesetzes (zit. "DSG").

Daten auch außerhalb Europas und Ländern mit gesetzlichem Datenschutz nur in einem eng gesteckten Rahmen bearbeitet werden können. In Europa ist dieser Rahmen garantiert, weshalb der Datentransfer von für die Zwecke einer E-Discovery erhobenen Daten unter den Staaten der EU und den von ihnen anerkannten sicheren Drittstaaten wie der Schweiz letztlich unproblematisch ist (je nach nationalem Recht kann allerdings auch der Export in ein sicheres Drittland außerhalb der EU bzw. des EWR bestimmten zusätzlichen Anforderungen unterliegen[77], weshalb selbst in diesem Rahmen nicht ganz auf den Blick in das nationale Datenschutzrecht des Exportlandes verzichtet werden sollte).

Besondere Vorkehrungen werden jedoch regelmäßig dann erforderlich, wenn gesammelte Daten in die USA übermittelt werden müssen – und zwar gleichgültig ob den eigenen Anwälten zwecks Sichtung oder später der Gegenpartei zwecks Offenlegung. Da die USA jedenfalls nach herrschender Ansicht nicht über eine Datenschutzgesetzgebung verfügen, die nach europäischen Maßstäben als angemessen bezeichnet werden kann, müssen europäische Unternehmen den Datenschutz entweder auf andere Weise sicherstellen oder aber sich von dieser Anforderung befreien, indem sie eine hinreichende Rechtfertigung hierfür vorweisen können.

Der heute im internationalen Datenverkehr meistpraktizierte Ansatz des Abschluss eines Datenübermittlungsvertrags (*transborder data transfer agreement*) kommt im Prozess allenfalls im Verkehr zwischen einem europäischen Unternehmen und seinen US-Anwälten in Frage, kaum aber mit der Gegenseite oder gar dem Gericht. Das gilt jedenfalls für jene Länder, in welchen faktisch nur die von der Europäischen Kommission verabschiedeten Musterklauseln eingesetzt werden können. In Ländern, in denen das lokale Datenschutzrecht dem Datenexporteur mehr Freiheit in der Gestaltung einer Maßnahme zur Gewährleistung des Datenschutzes im Ausland lässt[78], sind immerhin auch fallspezifische Lösungen für den rechtmäßigen Export wie etwa der Erlass einer gerichtlichen Schutzverfügung (*protective orders*) mit (auch) den Datenschutz sicherstellenden Regelungen möglich.

Das Einholen einer Einwilligung der betroffenen Personen wäre zwar ebenfalls ein Lösungsweg, doch wird dieser in der Praxis in aller Regel daran scheitern, dass nicht alle relevanten Personen vorab kontaktiert werden können; eine nachträgliche Einwilligung wäre unwirksam. Hinzu kommt, dass eine Einwilligung nur gültig ist, wenn sie freiwillig erfolgt, was aber gemäß der herrschenden Rechtsauffassung in manchen europäischen Staaten bei Arbeitnehmern, die nicht zum oberen Kader gehören, normalerweise nicht gewährleistet ist.

Somit bleiben im europäischen Datenschutzrecht grundsätzlich nur zwei weitere Möglichkeiten, wie die Personendaten rechtskonform offengelegt werden kön-

---

77 Dies sind insbesondere Pflichten zur Notifikation oder Bewilligung der Exporte bei den zuständigen Datenschutzbehörden des Export-Landes (so etwa in Österreich, Bulgarien, Zypern, Estland, Finnland, Frankreich, Ungarn, Island, Lettland, Liechtenstein, Litauen, Malta, Portugal, Rumänien und Spanien).

78 So etwa in der Schweiz, wo Art. 6 Abs. 2 Bst. a DSG beliebige Verträge aber auch andere Methoden zur Sicherstellung eines angemessenen Schutzniveaus im Ausland zulässt.

nen, wenn eine flexible Lösung wie dargelegt nicht in Frage kommt: Entweder der US-Empfänger der offenzulegenden Daten hat sich im Rahmen des Safe-Harbor-Privacy-Frameworks[79] bezüglich der betroffenen Daten selbst zertifiziert und damit den entsprechenden Datenschutzgrundsätzen unterworfen, oder aber es wird eine Ausnahmeregelung im europäischen Datenschutzrecht angerufen, welche die Übermittlung von Personendaten dann erlaubt, wenn sie zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist[80]. Allerdings wird diese Ausnahmeregelung unterschiedlich eng ausgelegt; mitunter wird vertreten, sie könne nur in Fällen der internationalen Rechtshilfe angerufen werden, was die Ausnahmeregelung letztlich überflüssig erscheinen lässt.

Die besondere Herausforderung für den multinationalen Konzern besteht vor diesem Hintergrund darin, die unterschiedlichen Regelungen in den verschiedenen europäischen Staaten möglichst zu seinem Vorteil zu nutzen und ungünstige Export-Konstellationen zu vermeiden. Müssen für einen US-Prozess beispielsweise Daten verschiedener Ländergesellschaften in Europa gesammelt werden, mag der direkte Export der Daten jeder Gesellschaft in die USA die naheliegenste Lösung sein, doch ist diese womöglich auch mit dem größten Aufwand verbunden, da die Exportformalitäten in jedem Land mit eigenem Datenschutzrecht anders sein werden. Hier kann sich beispielsweise ein vorgängiges Zusammenführen (*pooling*) von E-Discovery-Daten in einem ausgewählten europäischen Land lohnen, das über vergleichsweise tiefe formale Anforderungen an einen Datenexport in die USA verfügt, aber dennoch selbst als Staat mit angemessener Datenschutzgesetzgebung anerkannt ist und somit der Export in diesen Staat auch ohne besondere Schutzmaßnahmen möglich ist.

2.3 Organisatorische Herausforderungen

2.3.1 Fallspezifische und konzernweite Interessen

Die besonderen organisatorischen Herausforderungen für einen multinationalen Konzern im Rahmen eines Rechtsfalles mit internationaler E-Discovery haben meist in der einen oder anderen Form damit zu tun, dass die mit dem Management des Falls konzernintern beauftragten Personen in erster Linie meist nur fallspezifische, auf das eigene Unternehmen fokussierte Blickwinkel einnehmen und erst viel später, mitunter auch zu spät einen den eigenen, lokalen Betrieb übergreifenden, konzernweiten Blickwinkel einnehmen.

Die Konsequenzen einer solchen Vorgehensweise werden dadurch verschärft, dass internationale Belange den betreffenden Personen oft nicht richtig bewusst sind und der Fall daher gar nicht als internationaler Fall wahrgenommen wird. Doch in einem international tätigen Konzern können auf den ersten Blick landesspezifische Angelegenheiten rasch und tagtäglich in verschiedenster Hinsicht zu

---

79 Vgl. www.export.gov/safeharbor.

80 Art. 26 Ziff. 1 Bst. d EU-Datenschutz-Richtlinie.

einer internationalen Angelegenheit werden. Es liegt auf der Hand, dass dies die Organisation einer solchen Angelegenheit entsprechend kompliziert. Während das Bewusstsein der internationalen Dimension auch von scheinbar lokalen Tätigkeiten in der Zentrale eines multinationalen Konzerns regelmäßig vorhanden sein wird, tritt es in den Landesgesellschaften allzu oft in den Hintergrund.

Eine Schaffung standardisierter, globaler Richtlinien und Prozessen sollte somit für multinationale Konzerne auch im Bereich E-Discovery eine Konzernaufgabe sein und nicht alleinig den Landesgesellschaften in den USA überlassen werden. Dies wird in vielen Konzernen eine Herausforderung sein, wird doch das Thema E-Discovery vielerorts ausschließlich als US-amerikanisches Thema wahrgenommen. Dass es für einen multinationalen Konzern ein globales Thema sein muss, wird erst allmählich realisiert. Die zum Teil exorbitanten Sanktionen in den USA bei Fehlern in der Aufbewahrung von Unterlagen im Hinblick eines sich abzeichnenden Prozesses (*legal hold*) und die Offenlegung im Rahmen einer Pre-trial Discovery mag lange Zeit mit ein Grund dafür gewesen sein, dass die diesbezüglichen Prozesse sich vor allem darauf fokussiert haben, den Anforderungen des US-Prozessrechts zu genügen. Es gibt jedoch immer mehr Fälle, in denen die Nichtbefolgung der betroffenen Rechtsnormen anderer Staaten – namentlich des europäischen Rechts – im Zusammenhang mit der Durchführung einer E-Discovery nicht nur signifikanten Imageschäden, sondern auch Bußgelder (wie etwa im Bereich des Datenschutzes) oder strafrechtliche Konsequenzen für einzelne Verantwortliche nach sich ziehen können (wie etwa bei der Verletzung der erwähnten *blocking statutes*).

2.3.2 Die vier organisatorischen Herausforderungen der internationalen E-Discovery

Die Internationalität der E-Discovery stellt multinationale Unternehmen vor besondere Herausforderungen organisatorischer Natur. Aus dem Blickwinkel international tätiger Unternehmen lassen sich diese Herausforderungen in vier Punkten zusammenfassen:

Erste Herausforderung: Frühzeitiges Involvieren von E-Discovery Experten

Wie kann eine mit einem Rechtsfall in den USA betraute Person frühzeitig erkennen, dass es sich um einen grenzüberschreitenden E-Discovery-Fall handeln könnte und einschätzen, welches die allfällige Konsequenzen für das Unternehmen sind und welche Maßnahmen zu ergreifen sind?

Diese Frage stellt sich letztlich in jedem Rechtsfall, mit dem ein multinationaler Konzern in den USA konfrontiert wird. Für die meisten Personen, die mit dem Management solcher Fälle betraut werden[81], wird sie auf den ersten Blick kaum zu

[81] Die mit dem Rechtsfall betraute Person einer Unternehmung wird im Folgenden "Case Handler" genannt.

beantworten sein. Denn in vielen Konzernen werden solche Fälle erstens jeweils von unterschiedlichen Personen betreut, sodass Erfahrungen oft fehlen. Zweitens ist all diesen Personen vielerorts gemeinsam sein, dass sie weder Spezialisten im Bereich des E-Discovery sind, noch über spezifische Informatikkenntnisse verfügen (geschweige denn Kenntnisse über die im eigenen Konzern eingesetzten Systeme) noch werden sie mit den Datenschutzgesetzen und weiteren relevanten rechtlichen Rahmenbedingungen außerhalb der USA vertraut sein. Ihre Expertise wird typischerweise eine andere sein: Entweder sind es mehr oder weniger Prozesserfahrene *inhouse counsel* mit Kenntnissen des relevanten US-Rechts, oder aber sie werden einen besonderen Bezug zum eigentlichen Thema des Falles aufweisen und deshalb mit dessen Betreuung beauftragt worden sein.

Die praktische Erfahrung zeigt denn auch, dass ein solcher „Case Handler" weder die richtigen Fragen kennt, geschweige denn die rechtlichen, organisatorischen und technischen Anforderungen, die sich im Rahmen einer Sicherstellung und Beschaffung von Beweismitteln außerhalb den USA ergeben, wie zum Beispiel die Rahmenbedingungen des Datenschutzes oder der Inhalt einschlägiger *blocking statutes* und deren Implikationen. Er wird auch nicht über die Zeit und Mittel verfügen, sich diese Anforderungen mit einer gewissen Gründlichkeit zu erarbeiten. Damit als Organisation umzugehen, stellt die erste große Herausforderung dar, denn ungeachtet des fehlenden Bewusstseins oder Wissens des Case Handlers werden diese Rahmenbedingung eingehalten werden müssen.

Der wichtigste Schritt bei jedem drohenden US Rechtsstreits ist es daher, dass der Case Handler bereits im Anfangsstadium intern – oder falls nicht vorhanden extern – einen oder mehrere E-Discovery-Experten hinzuziehen kann. Die Erfahrung zeigt, dass die üblicherweise beigezogenen externen US-Prozessanwälte zur Vertretung im eigentlichen Fall aus Sicht des Unternehmens bzw. Konzerns aus verschiedenen Gründen nicht die idealen Partner hierfür sind:

Zum einen haben viele US-Prozessanwälte – auch wenn sie dies normalerweise nicht zugeben – noch immer wenig praxisrelevante Erfahrungen in der Durchführung von E-Discovery-Vorhaben, geschweige denn Erfahrungen in E-Discovery-Verfahren, die über die Landesgrenzen der USA hinausreichen. Zwar haben immer mehr große US-Anwaltskanzleien inzwischen eigene E-Discovery-Partner oder -Counsel, von denen manche auch weitreichende Erfahrung mit internationalen E-Discovery-Projekten gewonnen haben[82]. Die Praxis zeigt aber, dass diese aber allzu häufig aus Kostengründen nicht standardmäßig hinzugezogen werden oder jedenfalls nicht gleich zu Beginn eines Falls[83].

Zum anderen fehlt externen Anwälten normalerweise die Kenntnis der unternehmensspezifischen Situation in den für eine E-Discovery relevanten Bereichen. Denn gerade in multinationalen Konzernen, die oft eine Vielzahl von externen An-

---

82 So etwa viele der Mitglieder der Sedona Conference Working Group 6.

83 Immerhin gibt es inzwischen erste Unternehmen, welche standardmäßig bei jedem neuen Rechtsfall in den USA einen National E-Discovery Counsel beauftragen.

wälten beschäftigen, fehlt es normalerweise an der Konstanz dieser Beziehungen nicht nur auf Ebene der Kanzleien, sondern auch der betreffenden Personen: Selbst wenn die Kanzlei immer dieselbe ist, wechseln die mit einem Fall betrauten Partner und erst recht die Mitarbeiter (*associates*), obwohl für ein Unternehmen wichtig wäre, dass gerade letztere die unternehmensspezifische Situation am besten kennen, führen sie doch oft die eigentliche Arbeit im Bereich einer Discovery durch.
Verlässlicher, effizienter und letztlich auch kostengünstiger ist die Schaffung einer unternehmensinternen E-Discovery-Organisation[84] oder zumindest einer konstanten Beziehung zu einem bestimmten E-Discovery-Service-Provider oder einer auf E-Discovery spezialisierten Kanzlei oder Beratungsfirma, die nicht nur forensisch, sondern auch unabhängig von einem Fall oder lediglich Fallbegleitend beratend tätig sein können, während andere Kanzleien die eigentliche Vertretung vor Gericht übernehmen. Diese Organisation bzw. Berater müssen auch keineswegs in den USA angesiedelt sein.

Das frühzeitige Involvieren solcher Stellen muss typischerweise schon dann beginnen, wenn mit einem neuen Rechtsfall gerechnet (*anticipated*) werden muss, also von Beginn weg. Denn von dieser ersten Minute an setzt gemäß US-Prozessrecht auch die fallspezifische Aufbewahrungspflicht möglicherweise relevanter Dokumenten und Daten zum Rechtsfall ein und das Unternehmen muss mit den nötigen organisatorischen und technischen Mitteln dafür sorgen, dass keine potenziellen Beweismittel mehr vernichtet werden können.

Letztlich kann dieses Ziel nur durch die Einführung eines standardisierten (und letztlich auch zentral gesteuerten) *legal-hold*-Prozesses erreicht werden, da nur so sichergestellt werden kann, dass in US-Rechtsfällen, die sich naturgemäß immer zunächst mit einem US-Fokus entwickeln, auch der Datenschutz und andere internationale Aspekte nicht vergessen werden. Mit einem solchen standardisierten Prozess kann auch dafür gesorgt werden, dass den Spezialisten genügend Zeit bleibt, um schon vor dem Beginn der eigentlichen Discovery eine standardmäßige E-Discovery-Analyse[85] durchlaufen werden kann und sich falls notwendig die richtigen Weichen stellen lassen.

Nach den *meet-and-confer*-Gesprächen mit der Gegenpartei zur Regelung der Discovery[86] ist diese Chance bereits verpasst, weil die Rahmenbedingungen für die Discovery dann bereits feststehen und erfüllt werden müssen. Leider führen noch immer viele externe US-Anwälte diese Gespräche mit der Gegenseite durch, noch bevor sie mit ihrem Klienten die besonderen rechtlichen und organisatorischen Herausforderungen einer E-Discovery mit internationaler Ausprägung, wie sie in einem multinationalen Konzern üblich sind, erörtert und realistische Rahmenbedingungen definiert haben. Entsprechend werden sie nicht rechtzeitig berücksichtigt. Werden die europäischen Sonderanforderungen dann zu einem Zeitpunkt aufge-

---

84 Dazu nachstehend Abschnitt S. 58ff.

85 Dazu nachstehend Kapitel 3.2.3.

86 US Federal Rules of Civil Procedure, Rule 26f

bracht, an welchem mit der Gegenseite die Regeln zur Durchführung der Pre-trial Discovery schon vereinbart worden sind und der Zeitplan wie üblich eng gesteckt ist, stößt die Forderung nach Einhaltung solcher Anforderungen regelmäßig auf Unverständnis und Ablehnung.
Sind keine Standardprozesse zur Berücksichtigung solcher Anforderungen implementiert und somit zeitgerecht durchführbar, ist die Gefahr groß, dass eine aus Sicht des konkreten Falls aber auch des Unternehmens angemessene Risikoabwägung zum Nachteil der Einhaltung der Anforderungen des Datenschutzes und anderer Nicht-US-amerikanischer Rechtsanforderungen unter den Tisch fällt oder aber das Unternehmen im US-Prozess in die Zwickmühle gerät, die getroffene Vereinbarung zur Pre-trial Discovery nicht einhalten zu können.

Zweite Herausforderung: Verständnis und Kooperationsbereitschaft

Ein Verständnis bezüglich der rechtlichen Anforderungen des Datenschutzes in Europa und ihren praktischen Auswirkungen auf einen Discovery-Prozess ist in den USA aber auch in Europa vielerorts selbst unter Juristen erst im Entstehen. Überall besteht Handlungsbedarf: Innerhalb des eigenen Unternehmens, den eigenen beigezogenen externen Anwälten, jenen der Gegenseite sowie den US-Richtern müssen allfällige Konsequenzen dieser Anforderungen auf die Art und Weise und den Umfang einer Discovery, deren Zeitplan sowie der Notwendigkeit, weitere Vorkehrungen zu treffen, erläutert und um die nötige Kooperationsbereitschaft zur Erfüllung dieser Anforderungen geworben werden.

Die Erfahrung zeigt leider, dass bis auf wenige Ausnahmen ein US-Richter wenig bis kein Verständnis für die europäische Belange der genannten Art haben wird, da auch er unter einem enormen Zeitdruck bei der Abarbeitung der unterschiedlichsten Fälle steht. Schon das Thema E-Discovery für sich ist für den typischen US-Richter eine neue Materie und stellt ihn dementsprechend vor enorme Herausforderungen, wenn von ihm verlangt wird, in diesem Bereich Entscheide zu treffen – Entscheide, die massive Konsequenzen bezüglichen Kosten und Beweisführung im Prozess haben können. Dass hier erheblicher Schulungsbedarf besteht, ist in den USA inzwischen erkannt worden[87] und entsprechende Schulungsangebote werden dort auch schrittweise geschaffen[88]. Der noch immer häufige Nebeneffekt ist freilich, dass ein US-Richter sich zunächst auf seinen „Heimmarkt" konzentrieren wird und nur wenig Interesse und kaum Ressourcen hat, sich auch noch um ausländische Sonderanforderungen an die Durchführung einer E-Discovery zu kümmern.

Umso wichtiger ist es für einen multinational tätigen Konzern, der diesen Sonderanforderungen oft zwangsläufig ausgesetzt ist, eine Lösung seiner diesbezüg-

---

87 Vgl. z.B. das Memo from Honorable Mark R Kravitz, Chair, Advisory Committee on Federal Rules of Civil Procedure to Honorable Lee H. Rosenthal, Chair, Standing Committee on Rules of Practice and Procedure RE: Report of the Civil Rules Advisory Committee (May 17, 2010).

88 So etwa kostenfrei und dennoch hochwertig durch "The Law Institute".

lichen Probleme bereits vorgängig zu finden. In der Praxis bedeutet dies, dass die Anforderungen des europäischen Datenschutzes und die weiteren rechtlichen und anderen Herausforderungen einer internationalen E-Discovery letztlich im Rahmen der *meet-und-confer*-Gespräche[89] adressiert und gelöst werden müssen.

Diese entsprechende Vorgabe aus dem Jahre 2006 haben allerdings noch immer nicht alle US-Anwälte verinnerlicht, wie praktische Erfahrungen leider zeigen. Statt der Probleme der Gegenseite Gehör zu schenken und zu versuchen, beidseitig akzeptable Lösungen zu finden, wird allzu oft aus taktischen Gründen mit überzogenen Forderungen oder sogar einer totalen Verweigerung operiert, was im besten Fall für die Klienten beider Seiten nur unnötige und signifikante Kosten nach sich zieht. Im schlechtesten Fall drohen strategische Prozessnachteile sowie die gerichtliche Anordnung der Offenlegung unter Sanktionsandrohung im Falle einer Verweigerung (*subpoena*). Im Beispiel der Schweiz kann dies aufgrund besonderer rechtlicher Hindernisse (Art. 271 StGB) den Handlungsspielraum eines Unternehmens bezüglich dort befindlicher Dokumente wie bereits erwähnt massiv einschränken und zu schwerwiegenden Nachteilen im Prozess führen[90].

Will ein Unternehmen dem entgegenwirken, steht es somit vor der Herausforderung, seine eigene Situation im Hinblick auf die Durchführung einer E-Discovery im Konzern auch in Bezug auf die technischen, organisatorischen und rechtlichen Gegebenheiten außerhalb der USA schon im Vorfeld erörtert zu haben und somit in der Lage zu sein, im Falle einer sich abzeichnenden E-Discovery die eigene Situation und die zu befolgenden Rahmenbedingungen jederzeit ohne Verzug in dokumentierter Form darlegen zu können und entsprechende Handlungsvorgaben an die externen US-Anwälte und anderen Akteure in einem konkreten Streitfall formulieren zu können.

Dies alles muss bereits vor den *meet-and-confer*-Gesprächen geschehen sein – und letztlich auch bevor es ein konkreter Fall auf dem Tisch liegt. Denn ansonsten bleibt erfahrungsgemäß zu wenig Zeit für eine entsprechend gründliche Aufarbeitung. Dies wiederum bedeutet, dass in einem ersten Schritt das Verständnis für ein solches Vorgehen innerhalb der verantwortlichen Stellen im eigenen Unternehmen geschaffen werden muss, sind doch auch solche Vorbereitungsmaßnahmen regelmäßig mit entsprechenden Kosten verbunden – und zwar Kosten, die meist keinem konkreten Rechtsfall belastet werden können[91].

---

89 US Federal Rules of Civil Procedure, Rule 26f. Sie sieht vor, dass sich die Parteien in einem Rechtsfall über alle allfälligen Hindernisse und Fragen im Zusammenhang mit einer Discovery in kooperativer Weise zu besprechen und wenn möglich zu regeln haben, noch bevor die formale Phase der Discovery beginnt. Ziel ist ein gemeinsam festgelegter Plan, welcher den Umfang, die Abfolge und die Form der Offenlegung von Dokumenten für die Zwecke der Discovery definiert.

90 Dazu vorstehend Kapitel 2.2.1.

91 Vgl. zu einem Reifegradmodell und den entsprechenden Kosten für E-Discovery für ein Unternehmen den Beitrag von Paknad/Jung/Hampp in diesem Herausgeberband.

Zudem sollte die erarbeitete Vorgehensweise mit den zuständigen Personen vorgängig erörtert werden. So betrauen multinationale Konzerne normalerweise nicht irgendwelche Kanzleien mit ihrer Prozessvertretung, sondern streben längerfristige Beziehungen mit ausgewählten, quasi „bevorzugten" Kanzleien an (*outside counsel panel*). In solchen Fällen bietet es sich an, die besonderen Herausforderungen einer E-Discovery im internationalen Umfeld sowie die geplanten Maßnahmen[92] mit dem entsprechenden Hauptansprechpartner der verschiedenen „bevorzugten" Kanzleien in den üblichen, nicht mandatsbezogenen Gesprächen in allgemeiner Weise vorab zu erörtern, eine standardmäßige Vorgehensweise zu vereinbaren und die nötigen Beziehungen zwischen den eigenen Case Handlern und etwaigen E-Discovery-Spezialisten schon unabhängig von einem konkreten Fall aufzubauen. Schon solche Maßnahmen können sich in einem konkreten Fall äußerst positiv auf die Handlungsfähigkeit eines Konzerns und die Kosten einer späteren E-Discovery auswirken.

Dritte Herausforderung: Zeitraubende Zusatzmaßnahmen

Die Maßnahmen, die zur Einhaltung landesspezifischer rechtlicher Vorgaben im Rahmen einer E-Discovery nötig sind, sind unterschiedlich zeitintensiv. Erfahrungsgemäß führen sie aber fast immer zu einer Verzögerung der Offenlegung – nur schon die Abklärung der rechtlichen Rahmenbedingung kann, ist sie nicht vorgängig durchgeführt worden, mehrere Wochen in Anspruch nehmen. Dies ist zur berücksichtigen, wenn ein entsprechender Zeitplan der Offenlegung mit der Gegenseite in den *meet-and-confer*-Gesprächen besprochen und vereinbart werden soll.

In der Praxis als sinnvolle Herangehensweise erwiesen hat sich die Vereinbarung einer „rollenden" Offenlegung der Dokumente (*rolling production*), bei welcher mit dem in aller Regel unproblematischen US-Teil der Discovery begonnen wird. So wird der Beginn der Offenlegung nicht verschleppt. Gleichzeitig gewinnt der Konzern die Zeit, die er für die Beschaffung und Offenlegung der Daten von außerhalb den USA und insbesondere aus Europa benötigt[93].

Vierte Herausforderung: Praktische Umsetzung

Eine sorgfältige Umsetzung der Anforderungen des US-Rechts im Bereich der E-Discovery stellt in der Praxis eine weitere Herausforderung für Unternehmen dar[94]. Es erstaunt daher nicht, dass diese Anforderungen immer wieder mit einem Minenfeld verglichen werden, in welchem jedes Unternehmen pro Fall mindestens einmal in die Falle tappt. Kommt eine internationale Komponente mit – wie dargelegt – etlichen weiteren Anforderungen hinzu, ist die Herausforderung einer sorgfältigen Umsetzung in der Praxis umso grösser.

---

92 Dazu nachstehend Kapitel 3.3.2.

93 Dazu nachstehend Kapitel 3.3.2.

94 Illustrativ legen dies z.B. die verschiedenen Publikationen der Sedona Conference Working Group 1 dar.

Eine der Schwierigkeiten, mit welchen multinationale Konzerne regelmäßig konfrontiert werden, ist der Umstand, dass die in den Fachgremien und von Experten ausgearbeiteten Prozesse[95] und entsprechende Hilfsmittel – sprich: Softwarelösungen – oft nur auf den US-amerikanischen Binnenmarkt zugeschnitten sind. Die europäische Forderung einer „data privacy by design" ist von vielen Herstellern von E-Discovery-Software leider noch nicht beherzigt oder wird erst allmählich in ihre Lösungen aufgenommen.

Dies hat zur Folge, dass multinationale Konzerne die konkrete Umsetzung dieser Anforderungen selbst initiieren und durchführen müssen. Während sich entsprechende Prozeduren auf dem Papier noch einigermaßen einfach umgeschrieben und entsprechend anpassen werden können, ist die konkrete Implementierung eine zeitaufwendige und bisweilen kostspielige Angelegenheit.

So muss beispielsweise bei der Organisation der Zugriffsrechte von Datenbanken und Systemen zur Durchführung von *legal holds* und einer Discovery regelmäßig von den Vorgaben der Herstellern abgewichen und diese entsprechend angepasst werden, das mit der nötigen Zahl an unterschiedliche Rollen und geographischen Standorten der Bearbeiter gearbeitet werden kann und ihr Zugriff wirksam jeweils auf den für den Fall für diese Personen tatsächlich benötigten Teil eingeschränkt werden kann. Dabei ist auch die geographische Herkunft der Daten zu berücksichtigen. Doch genau dafür sind manche der Softwarelösungen noch nicht eingerichtet: Eine Meta-Daten-Kategorie „Länderzugehörigkeit", mit welcher Dokumente entsprechend klassifiziert werden können, ist zum Beispiel bei manchen Produkten konzeptionell nicht vorgesehen: Alle Daten landen gewissermaßen im selben Topf. Fehlt eine solche Klassifizierung, wird das geographische *scoping*, also die Bildung von Untermengen von Dokumenten je nach ihrer geographischen Herkunft nur auf Umwegen möglich. Ohne ein solches *scoping*, muss ein Unternehmen auf sämtliche Daten die strengsten Anforderungen bezüglich Datenschutz anwenden oder aber die Nichteinhaltung solcher Vorgaben in Kauf nehmen statt sie gezielt nur dort umzusetzen, wo dies wirklich nötig ist.

Auch die heute bestehenden ausgefeilten technischen Hilfsmittel zur Filterung und Reduktion von Datenbeständen[96] sind in ihrer Handhabung keineswegs trivial, sollen sie die gewünschten Ergebnisse erzielen. Sie bedürfen entsprechend ausgebildeter und erfahrener Fachkräfte. Die mit einem Fall betrauten Rechtsanwälte verfügen über das hierzu erforderliche methodische und technische Wissen allerdings in den seltensten Fällen. E-Discovery-Service-Provider können zwar oft die neusten Technologien in diesem Bereich vorweisen und bieten auch entsprechend geschultes Personal an. Sie sind jedoch aus rechtlichen Gründen in aller Regel

---

95 Der bekannteste Standard zur Umschreibung des E-Discovery-Prozesses in den USA ist wohl das "Electronic Discovery Reference Model" (EDRM), erläutert unter http://edrm.net; vgl. jedoch die Standardprozedur zur Durchführung einer E-Discovery in Europa nachstehend in Kapitel 3.3.2.

96 Zum Beispiel sog. Early-Case-Assessment–Software.

durch die mit der Vertretung eines Falls betrauten Anwälte mandatiert und unterliegen entsprechend einzig deren Instruktion und nicht jener ihrer Klienten.

In der Praxis führt dies erfahrungsgemäß leider häufig dazu, dass dem Aspekt der Kostenminimierung weniger Rechnung getragen wird, als sich dies viele Unternehmen und Auftraggeber wohl wünschen würden: Je weniger sorgfältig und intensiv die erste Phase der semi-automatischen Filtrierung der für eine Discovery eingesammelten Daten betrieben wird, desto grösser sind die resultierend Datenmengen für die nachfolgende manuelle Sichtung der Datensätze durch die Anwälte – und entsprechend höher fallen die Kosten für den Auftraggeber aus. Ein gründliches Einschränken und Testen der Suchbegriffe (*keyword refinement*) entfällt häufig, weil entweder die nötige Expertise fehlt, für diesen Vorgang nützliches Wissen, das im Unternehmen oft vorhanden ist, nicht beigezogen wird, es aus der Optik des US-Prozessanwalts nicht stört, wenn mehr irrelevante Unterlagen offengelegt werden als nötig ist, oder alle drei Gründe gegeben sind. Weil ein ausgeprägtes *keyword refinement* in der Praxis sich aber als äußerst wirksames Instrument zur Kostenreduktion – und im gleichen Zug auch zur datenschutzrechtlich erwünschten Reduktion der offenzulegenden Daten – erwiesen hat, sehen sich immer mehr multinational tätige Unternehmen mit der Herausforderung konfrontiert, diese Prozesse in die eigene Unternehmung zu verlagern und eine entsprechende Expertise intern aufzubauen.

3. Lösungsansätze für multinationale Konzerne

3.1 Vorbemerkungen

Während sich die organisatorischen Herausforderungen mit entsprechendem Aufwand und guten Willen bewältigen lassen, erscheint es jedenfalls auf den ersten Blick illusorisch, eine E-Discovery in Europa durchzuführen und dabei sowohl den Anforderungen des US-Rechts als auch des Datenschutzes und der weiteren rechtlichen Anforderungen vollumfänglich gerecht zu werden.

Auf den zweiten Blick wird klar, dass mit etwas Flexibilität und Offenheit sich für die Praxis durchaus allseitig vertretbare Lösungsansätze finden lassen. Sie werden inzwischen denn auch in den entsprechenden internationalen Gremien wie etwa der Sedona-Konferenz diskutiert[97] und stoßen bei Verfechtern einer umfassenden Offenlegung im Prozess wie auch Datenschützern zusehends auf Anerkennung[98]. Solche Lösungsansätze, wie sie auch nachfolgend dargestellt werden, setzen allerdings drei Dinge voraus:

---

97 So jüngst an der 2nd Annual Sedona Conference International Programme on Cross-Border Discovery and Data Privacy, vom 15. bis 16. September 2010 in Washington D.C., USA.

98 Vgl. zur Historie von „The Sedona Conference®“ und den Ergebnissen der Arbeitsgruppen die beiden Beiträge in diesem Herausgeberband.

Erstens muss die Partei, welche eine Discovery in Europa durchführen soll, zur Offenlegung der betreffenden Dokumente grundsätzlich bereit sein, soweit es das jeweilige Recht zulässt. Diese Kooperationsbereitschaft wird vom US-Prozessrecht zwar verlangt bzw. vorausgesetzt, ist aber aus europäischer Warte nicht selbstverständlich, widerspricht der Grundsatz der totalen Transparenz im Rahmen einer Discovery doch einerseits fundamental der kontinentaleuropäischen Rechtstradition und kann insbesondere eine E-Discovery mit anschließender Auswertung der Ergebnisse massive Kosten verursachen (alleine in den USA kann die E-Discovery für einen größeren Prozess für eine Partei Kosten von einer halben bis drei Millionen USD mit sich bringen[99]). Fälschlicherweise werden der Datenschutz und weitere Rechtsbestimmungen in den einzelnen Staaten Europas von Prozessparteien zuweilen instrumentalisiert, um einer Offenlegung scheinbar unüberbrückbare Steine in den Weg zu legen. Die Erfahrung der letzten Jahre zeigt allerdings, dass die Mehrheit der europäischen Unternehmen in den meisten Fällen (wenn auch widerwillig) kooperationsbereit sind, wenn sie wegen geschäftlichen Aktivitäten im angelsächsischen Raum in einen Zivilprozess verwickelt sind. Das gilt für multinationale Konzerne, die über permanente Niederlassungen in den USA verfügen, erst recht; dass eine europäische Konzerngesellschaft oder Konzernmutter ihrer US-Landesgesellschaft in einem dortigen Streit nicht beistehen will, wenn es ihr vernünftigerweise möglich ist, kommt kaum vor. Schließlich darf auch der Einfluss der Rechtsberater nicht unterschätzt werden: Wird ein europäisches Unternehmen in den USA in einen Prozess verwickelt, wird es jedenfalls bei Verfahren vor staatlichen Gerichten (im Bereich der internationalen Schiedsgerichtsbarkeit[100] finden Offenlegungen wesentlich zurückhaltender statt, obwohl auch in diesem Bereich – getrieben vorwiegend durch Anwälte mit US-amerikanischer Tradition – Tendenzen zu einer Ausweitung zu beobachten sind) regelmäßig Prozessvertreter in den USA mandatieren. Für den US-Anwalt aber ist die Verweigerung der Offenlegung aus taktischen Gründen, aufgrund seiner eigenen Rechtstradition und seines Rollenverständnisses als Diener des Rechtssystems praktisch nicht denkbar; er wird im Rahmen einer Discovery erfasste Unterlagen nötigenfalls (letztlich zum eigenen Schutz) auch gegen den Willen seines Klienten offenlegen, sollte er ihrer habhaft werden.

Zweitens sollten sich europäische Unternehmen, bei welchen ein nicht vernachlässigbares Risiko besteht, in einen US-Zivilprozess und damit in ein Discovery-Verfahren verwickelt zu werden, auf einen solchen Fall vorbereiten und entsprechende Vorkehrungen treffen. Nur so kann sichergestellt werden, dass im konkreten Fall geordnet, richtig und einigermaßen effizient reagiert wird: Eine Pre-trial-Discovery – dem häufigsten Anlass einer E-Discovery – ist kein langfris-

---

99 Die Kosten sind fallspezifisch und insbesondere vom Datenvolumen (volume times fees) abhängig sowie der Effizienz der eingesetzten Prozesse (z.B. Reduktion der Datenmengen vor einer manuellen Sichtung).

100 Vgl. zu den Möglichkeiten der Schiedsgerichtsbarkeit den Beitrag von Wilske in diesem Herausgeberband.

tiges Projekt, sondern muss typischerweise innert Wochen organisiert und weniger Monate durchgeführt sein, wobei die ersten Vorbereitungsmaßnahmen – namentlich die *legal hold* – schon vor Einreichung einer Klage konzernweit eingeleitet worden sein müssen oder dies jederzeit ohne Verzug in geordneter und dokumentierter Weise möglich sein muss[101]. Zeit für eingehende Abklärungen der rechtlichen Anforderungen und zum Üben bleibt in einem solchen Fall leider kaum. Zwar ist es richtig, dass der Datenschutz und weitere Rechtsnormen in Europa die Durchführung einer E-Discovery erschweren und einschränken können. Auch haben das Verständnis und die Rücksicht der US-Gerichte bezüglich solcher Hindernisse in den vergangenen Jahren deutlich zugenommen. Die Erfahrungen aus konkreten Fällen als auch die laufenden Diskussion in den Fachgremien und der Literatur zeigen ihnen jedoch auch, dass sich viele dieser Hindernisse mit etwas gutem Willen durchaus aus teilweise dem Weg räumen lassen. Diesen guten Willen setzen sie – ob zu Recht oder zu Unrecht – stillschweigend voraus. Auch europäische Unternehmen sind somit gut beraten, diesen guten Willen zu demonstrieren und darzulegen, dass das Bestehen etwaiger rechtliche Hindernisse in der Durchführung einer Discovery nicht daran liegt, dass das Unternehmen seine Hausaufgaben nicht gemacht hat. Zwar stellen nicht alle US-Gerichte die gleich hohen Anforderungen an die Fähigkeit von Unternehmen, eine E-Discovery *lege artis* durchzuführen. Wer dies jedoch nicht tut, weil er sich nicht entsprechend vorbereitet hat, muss in gewissen Gerichtsbezirken inzwischen leider damit rechnen, dass dies als grob fahrlässiges Verhalten gewertet und entsprechend sanktioniert wird, selbst wenn es nicht bösgläubig erfolgen sollte. Dies gilt insbesondere für multinational tätige Konzerne, die in den Augen eines jeden US-Richters ohne Weiteres über die erforderlichen Ressourcen und das nötige Wissen verfügen sollten, um eine E-Discovery auch im internationalen Bereich umfassend und effizient durchführen zu können. Es wird mit anderen Worten von immer mehr Richtern in den USA inzwischen erwartet, dass solche Unternehmen wissen, was im Bereich E-Discovery auf sie zukommen kann und sie sich entsprechend vorbereitet haben.

Drittens ist es unabhängig von konkreten Maßnahmen wichtig, dass alle Beteiligte sich ein Bewusstsein für die Rechtstradition und Denkweise der Gegenseite schaffen. Dies ist nicht selbstverständlich, im transatlantischen Kontext jedoch unverzichtbar. Hierbei kann insbesondere dem *inhouse counsel* bzw. Case Handler der betroffenen Unternehmen bzw. des betroffenen Konzerns die wichtige Rolle zukommen, im eigenen Lager dafür zu sorgen, dass die Vertreter der verschiedenen Rechtskulturen – sprich: die beigezogenen externen Anwälten – an einem Strick ziehen und sich frühzeitig miteinander abstimmen, also beispielsweise noch bevor der Umfang, die Fristen und die Prozeduren einer E-Discovery in einem konkreten Fall mit der Gegenseite in den *meet-and-confer*-Gesprächen festgelegt werden. Doch auch im externen Verkehr tut ein Unternehmen gut daran, frühzeitig bei Gericht und Gegenpartei Aufklärungsarbeit bezüglich der Anforderungen des euro-

[101] Dazu vorne Kapitel 1.

päischen Rechts zu betreiben, wenn im Rahmen einer Discovery – wie im Falle multinationaler Konzerne fast immer der Fall – eine Beschaffung von Daten und Dokumenten auch in Europa und anderen Regionen außerhalb den USA zur Diskussion stehen kann. Dies ist trotz des in den USA in den letzten Jahren stark gewachsenen Bewusstseins für die Herausforderungen des europäischen Datenschutzes im US-Zivilprozess nach wie vor eine Bringschuld, die möglichst früh erfüllt werden sollte.

3.2 Den eigenen Fall kennen

Jedes Unternehmen hält aufgrund des seines eigenen Geschäftszwecks unterschiedlichste Arten von Daten vor. Jedes Unternehmen ist auch anders organisiert. Auch wird der Grad der Globalisierung selbst in multinational tätigen Konzernen hinsichtlich ihrer Geschäftsprozesse, der länderübergreifenden Zusammenarbeit der einzelnen Konzerngesellschaften und der Zentralisierung der IT-Infrastruktur unterschiedlich weit vorgeschritten sein.

Will ein Konzern daher eine firmeninterne Einschätzung vornehmen, in welchem Ausmaß eine grenzüberschreitende E-Discovery in einem konkreten US-Rechtsfall möglich werden kann und welches die Konsequenzen sind, muss das Unternehmen daher zunächst die eigene Situation bezüglich der relevanten Parameter kennen. Es muss verstehen, wie seine eigenen Prozesse nicht nur auf dem Papier, sondern in Tat und Wahrheit funktionieren, welche Art von Daten wo fließen, und wo und wie und wie lange gespeichert werden.

Wie vorstehend bereits mehrfach gezeigt, ist es unumgänglich die eigene Situation schon vor den jeweiligen *meet-and-confer*-Gesprächen mit der Gegenseite zu Beginn eines US-Rechtsfalles zu kennen, damit das Unternehmen sich auf diese Gespräche richtig vorbereiten kann. Hierzu muss ein Unternehmen nicht nur den standardmäßig von der Gegenseite für solche Gespräche angeforderten Katalog an relevanten Datensystemen und deren Zugänglichkeit vorlegen können. Auch eine vorgängige Klärung des möglichen geografischen Ausmaßes einer E-Discovery und der betroffenen rechtlichen Entitäten des Konzerns ist unerlässlich, um frühzeitig auf potentielle Probleme rechtlicher und anderer Natur hinweisen zu können. Schließlich muss das Unternehmen ebenfalls in der Lage sein abzuschätzen, wie sensitiv die verschiedenen Datenkategorien bezüglich der diversen erkannten rechtlichen Anforderungen tatsächlich sind, denn es wird immer Datenbestände geben, die stärker von entsprechenden Einschränkungen betroffen sind als andere. Nur wer auch hier seine Hausaufgaben getätigt hat, kann entsprechend effizient und zeitnah reagieren, wie dies im Rahmen der Gespräche mit der Gegenpartei und in der Durchführung der eigentlichen E-Discovery erforderlich ist.

Im Folgenden werden zunächst für organisatorische und technische Sonderaspekte multinationaler Konzerne beleuchtet, die für eine fallspezifische Analyse einer grenzüberschreitenden E-Discovery erfahrungsgemäß besonders wichtig sind. Es folgen Ausführungen dazu, wie eine solche Analyse vorzunehmen ist. Schließ-

lich wird auf zwei weitere Entwicklungen bzw. Hilfestellungen hingewiesen, die multinationalen Konzernen helfen können, den eigenen Fall besser zu kennen und damit umzugehen.

3.2.1 Besondere organisatorische Aspekte multinationaler Konzerne

Zunächst muss ein Unternehmen wissen, wie und wo seine Wertschöpfungskette bearbeitet wird[102]. In vielen multinationalen Konzernen ist dieser Vorgang auf unterschiedlichste Länder verteilt. Dementsprechend können Forschung und Entwicklung, Produktion, Vertrieb, Marketing und zentrale Konzernfunktionen auf Gesellschaften in unterschiedlichsten Ländern verteilt sein, jedoch in einem konkreten Rechtsfall alle von Belang werden.

In vielen Konzernen ist selbst die Ausführung einzelner Wertschöpfungsschritte weltweit verteilt: Statt durch landesspezifische Teams erfolgt diese durch Teams aus global verteilten Mitarbeitern zum Beispiel in Form einer Matrixorganisation. Diese Teams sind auf verschiedene Länder und Konzerngesellschaften verteilt; während sich der Abteilungsleiter an einem Standort befinden kann, kann ein Teil seiner Mitarbeiter auch an zwei, drei oder mehr anderen Standorten tätig sein.

Die immer stärkere Nutzung asynchroner Kommunikationsmedien wie etwa E-Mail und anderer Software zur elektronischen Kollaboration (elektronische Foren und Plattformen in konzernweiten Netzwerken) verstärken diese Entwicklung zusätzlich und führen dazu, dass auch eine E-Discovery entsprechend aufwändiger und globaler wird.

Hinzu kommt der wachsende Einsatz des Offshorings, Nearshorings oder des klassischen Outsourcings selbst bei Kernprozessen im Konzern. Diese Organisationsformen haben eine hohe Auswirkung auf die Fragen der Datenkontrolle und des Datenzugriffs. Sie müssen daher für eine E-Discovery ebenfalls bekannt und dokumentiert sein und entsprechend kontrolliert werden können.

3.2.2 Besondere IT-Aspekte multinationaler Konzerne

Wie das Organisationsmodell einer international operierenden Unternehmung kann die technische Datenhaltung in multinationalen Konzernen sehr unterschiedlich organisiert sein.

Eine Zentralisierung der Datenhaltung pro Kontinent oder der Einsatz von Cloud Computing für weniger kritische Daten ist allerdings für viele Unternehmen aus Gründen der Effizienz und Kosten entweder bereits Realität oder aber in Planung. Befanden sich früher an jedem physischen Standort eines Konzerns lokale E-Mail- und File-Server, werden diese inzwischen immer häufiger pro Region kon-

---

[102] Vgl. zur Betrachtung der Wertschöpfungskette sowie der IT-Architektur im Kontext einer E-Discovery den Beitrag von Schmid in diesem Herausgeberband.

solidiert und in einem einzigen Land zusammengefasst. Dieselbe Entwicklung findet bei geschäftlichen Datenbanken ebenfalls statt.[103]

Die Folge dieser Entwicklungen ist unter anderem, dass eine in der Vergangenheit möglicherweise strikte Trennung von Daten aus den USA und Daten anderer Ländern mehr und mehr verschwindet oder nur noch für wenige Systeme wie etwa des Personalwesens gilt oder aber dort, wo bereits im operativen Alltagsgeschäft das geltende Recht den Export von Daten untersagt.

Diese Tendenzen bedeuten umgekehrt, dass in Konzernen auch den Mitarbeitern in den USA immer häufiger auch im ordentlichen Geschäftsbetrieb Zugang zu Daten gewährt wird, die außerhalb der USA entstanden sind und aufbewahrt werden. Auch hier muss das Unternehmen genau wissen (und dokumentieren), wem es welche Zugriffe gewähren will, weil es einen direkten Einfluss auf die Pflicht zur Offenlegung von Unterlagen haben kann, wenn einem US-Mitarbeiter bestimmte Daten nur schon im Fernzugriff zur Verfügung stehen. Die gesellschafts- und landesübergreifenden Zugriffsberechtigungen im Konzern sollten daher entsprechend geregelt und dokumentiert sein, nicht nur jene innerhalb eines Betriebs.

Nebst den Zugriffsrechten ist für das geographische *scoping* und Ermittlung der relevanten rechtlichen Rahmenbedingungen einer E-Discovery zu erheben und zu dokumentieren, wo ein Konzern seine elektronischen Dokumente und Daten physisch speichert bzw. wo sich die betreffenden Anwendungen befinden. Besonderes Augenmerk ist hierbei auf die Frage zu richten, ob bestimmte Daten gegebenenfalls in mehreren Ländern parallel verfügbar sind, was deren Offenlegung im Falle unterschiedlicher Hindernisse in den einzelnen betroffenen Rechtsordnungen stark vereinfachen kann; unter Umständen können gestützt auf solche Informationen auch entsprechende Vorsichtsmaßnahmen getroffen werden, wie z.B. der rechtzeitige konzerninterne Export von Kopien relevanter Daten, falls deren Herausgabe ansonsten durch *blocking statutes* ungewollt verhindert werden könnte[104].

3.2.3 Analyse einer grenzüberschreitenden E-Discovery im multinationalen Konzern

Die Analyse der eigenen Situation im Bezug auf den Fall einer grenzüberschreitenden E-Discovery[105] erfolgt grundsätzlich in mehreren Schritten:

Der *erste Schritt* ist die Ermittlung des Umfangs der offenzulegenden Daten: Welche Art der Dokumente werden in Anbetracht des Falls benötigt? Über welche

---

103 Vgl. zur Zentralisierung der Daten in einem Cloud Computing für Zwecke der E-Discovery den Beitrag von Hartmann und Venhofen in diesem Herausgeberband.

104 Dazu vorstehend Kapitel 2.2.1.

105 Siehe dazu ausführlich: Zeunert, et al., Working Through the Maze Part 2, Cross-border Discovery Preparedness & Protocols, Arbeitspapier erstellt im Rahmen der 2nd Annual Sedona Conference International Programme on Cross-Border Discovery and Data Privacy vom 15. bis 16. September 2010 in Washington D.C., USA (Veröffentlichung vorgesehen im Sedona Conference Journal im Jahre 2011).

dieser Daten verfügt der Konzern und wo? Welches wären vernünftige Kriterien, mit denen solche möglicherweise relevanten Dokumente von anderen Dokumenten im Konzern abgrenzen und die offenzulegenden Daten letztlich isoliert werden könnten? Verschiedene Aspekte, die im multinationalen Konzern hierbei zusätzlich beachten werden müssen, wurden vorstehend bereits erwähnt[106].

Im Ergebnis sollte aufgrund der entsprechenden Abklärungen Klarheit darüber geschaffen werden, welche Rechtsordnungen und welche Konzerngesellschaften von einer E-Discovery in einem konkreten Rechtsfall betroffen sind, was sich wiederum daraus ergibt, in welchen Rechtsordnungen und Konzerngesellschaften sich die von einem Fall (direkt und indirekt) betroffenen (ehemaligen und aktiven) Mitarbeiter befinden bzw. angestellt sind, wo die möglicherweise relevanten Daten gespeichert sind und welche Gesellschaften selbst Partei des betreffenden Rechtsfalles sind, welche hingegen nur mit betroffen sind.

Auch die Natur der möglicherweise relevanten Daten sollte in diesem ersten Schritt der Analyse ermittelt werden, wobei geeignete Kategorien zu bilden sind. Handelt es sich um sensitive persönliche Daten von Mitarbeitern, von Kunden oder anderen Personen? Sind es Daten von ehemaligen Mitarbeitern, bei welchen möglicherweise weniger strenge Anforderungen punkto Datenschutz bestehen? Sind Geschäftsleitungsmitglieder oder andere Mitarbeiter betroffen, die Träger von Geschäftsgeheimissen sind? Sind Daten von Dritten betroffen, denen eine besondere Geheimhaltung oder besondere Vorkehren bezüglich des Datenschutzes zugesichert wurden oder von Gesetzes wegen garantiert werden?

In einem *zweiten Schritt* ist zu ermitteln, wo der erwartete US-Rechtsfall ausgetragen werden wird und nach welchen Regeln. Auch innerhalb den USA gibt es unterschiedliche Regeln bzw. Standards und Praktiken im Bereich E-Discovery; je nach den Umständen kann ein bestimmter Fall je nach Wahl des Klägers zum Beispiel vor ein Bundesgericht (*federal district court*) oder das Gericht eines bestimmten Bundesstaates (*state court*) gebracht werden, während der Beklagte wiederum gewisse Möglichkeiten hat, dass ein Fall vor ein Gericht verlagert wird, das ihm besser passt.

In einem *dritten Schritt* sind schließlich in Anbetracht der offenzulegenden Dokumente und relevanten Regeln des US-Prozessrechts die rechtlichen Rahmenbedingungen zu ermitteln, die für eine solche Offenlegung außerhalb den USA zu beachten sind, so etwa das europäische Datenschutzrecht im Falle von Dokumenten aus europäischen Ländergesellschaften oder andere Rechtsnormen wie etwa die erwähnten *blocking statutes*. Auch die Möglichkeiten zur Erfüllung dieser Anforderungen (wie etwa entsprechende Verträge oder Schutzverfügungen[107]) sind in diesem dritten Schritt zu analysieren. In diesem Schritt ist ebenfalls zu ermitteln, wer im Konzern für diese begleitenden Maßnahmen zuständig ist bzw. inwiefern sogar Behörden (z.B. nationale Datenschutzbehörden) involviert werden müssen.

---

106 Kapitel 3.2.1 und 3.2.2.

107 Dazu nachstehend Kapitel 3.4.

Einsatz interner E-Discovery-Spezialisten

Während in vielen Bereichen der Trend zum Outsourcing[108] anhält, spielt sich im Bereich E-Discovery in multinationalen Konzernen derzeit genau das Gegenteil ab: Es findet ein konsequentes Insourcing von E-Discovery-Spezialisten und -Systemen statt[109/110].

Dies hat nicht nur Kostengründe. Immer mehr Unternehmen, welche in den USA latent dem Risiko von Rechtsfällen ausgesetzt sind und eine gewisse Größe bzw. globale Präsenz aufweisen, bauen interne Kompetenzen im Bereich E-Discovery auch aus anderen Gründen auf: Sie erhoffen sich nebst einer besseren Effizienz und Effektivität in der Bewältigung der Herausforderungen grenzüberschreitender E-Discovery-Vorhaben eine Risikominimierung im internationalen Bereich. Das scheint vor allem eine wachsende Zahl von multinationalen Konzernen mit Hauptsitz in Europa zu diesem Schritt zu bewegen: Sie versprechen sich durch den gezielten Aufbau interner E-Discovery-Spezialisten eine bessere zentrale Kontrolle des Prozesses und somit eine verstärkte und vor allem auch frühzeitige Beachtung der internationalen Aspekte einer E-Discovery[111]. Dementsprechend sind die betreffenden Positionen auch keineswegs nur in den USA zu finden, sondern stehen im Gegenteil in europäischen Konzernen oftmals sogar unter europäischer Führung.

Die Schaffung einer unternehmensinternen E-Discovery-Organisation mit entsprechenden Spezialisten ist auch eine wichtige Voraussetzung für eine konzernweite Zentralisierung und Standardisierung des *legal-hold-* und E-Discovery-Prozesses als solcher[112], was nicht nur dem Anliegen des europäischen Datenschutzes, sondern letztlich auch des US-Prozessrechts dient.

Der internen E-Discovery-Organisation kommt schließlich auch eine Schnittstellenfunktion zu. Sie kann dabei nicht nur die Anliegen der Rechtabteilung, der externen Anwälte und er IT koordinieren, sondern ebenso auch ein gutes Verbindungsglied zu den für das Records Management, die Informationssicherheit und der konzerninternen Datenschutzanliegen zuständigen Stellen.

---

108 Vgl. zum E-Discovery-Datenschutz im IT-Outsourcing den Beitrag von Brunsch sowie den Anforderungen an E-Discovery-Dienstleister den Beitrag von Murray in diesem Herausgeberband.

109 Vgl. z.B. Hill/Owens, Searching For eDiscovery Cost Control, Forrester Research, Inc., April 27, 2009; Tero, Corporate eDiscovery Technology Trends 2009: Doing More with Less While Facing Increasing Complexity in eDiscovery, IDC Information and Data sponsored by FTI Technology, November 2009; sowie Kaplan, Advice from Counsel: Best Practices on Controlling E-Discovery Costs, FTI Consulting, 2009.

110 Vgl. zum Aufbau unternehmenseigener Kompetenzen für E-Discovery die Beiträge von Hartmann/Venhofen sowie von Kiemes/Pauseback in diesem Herausgeberband.

111 Dazu vorstehend Kapitel 2.3.2.

112 Dazu nachstehend Kapitel 3.3.2.

Einsatz interner E-Discovery-Systeme

In multinationalen Konzernen kommen auch immer häufiger workflowbasierte *legal-hold*-Systeme[113] zum Einsatz. Der Grund hierfür ist, dass solche Systeme nicht nur dazu dienen, einen *legal hold* effizienter und sicherer abzuwickeln, sondern sie auch nicht zu unterschätzende Vorteile in der Vorbereitung einer Offenlegung von Unterlagen im Rahmen einer grenzüberschreitenden E-Discovery haben. Mit ihnen können somit nicht nur die sichere Aufbewahrung von Dokumenten (*preservation*) und deren Einsammlung (*collection*) abgewickelt, rechtsgenüglich dokumentiert und überwacht werden. Sie können auch benutzt werden, den Umfang der offenzulegenden Dokumente (*scoping*) mit Bezug auf Mitarbeiter, Datenquellen und Zeiträume besser zu definieren und damit einzuschränken, was letztlich nicht nur Kosten senkt, sondern auch dem Datenschutz dient.

Auch Systeme zur Archivierung von E-Mails können, sofern sie über entsprechende Funktionalitäten verfügen, nebst der Aufbewahrung elektronischer Korrespondenz zwecks Erfüllung gesetzlicher und geschäftlicher Vorgaben für die Zwecke eines *legal holds* und einer E-Discovery eingesetzt werden. Das gilt insbesondere für Unternehmen, welche zur Entlastung der dezentralen E-Mail-Server und aus Kostengründen immer häufiger zentralisierte E-Mail-Archivsysteme einsetzen. Solche Archive können sich hervorragend für ein *preserve-in-place,* also der fallspezifischen Aufbewahrung im Archiv ohne jeglichen zusätzlichen Datentransfer eignen, was entsprechende Kostenvorteile und eine zentrale, transparente Sicherstellung der Umsetzung eines *legal holds* erlaubt. Gleichzeitig können solche Systeme benutzt werden, um betreffende Daten vor der Weitergabe und Offenlegung bezüglich ihres geographischen Bezugs zu kennzeichnen.

Werden solche Archiv-Systeme zudem mit entsprechend effizienten und leistungsstarken Suchmaschinen verknüpft, können sie auch zur Vorbereitung einer E-Discovery dienen, indem sich mögliche Suchbegriffe für die Zwecke der *meet-and-confer*-Gespräche testen und verfeinern lassen, ohne dass die gesammelten Daten in separate Systeme umkopiert oder exportiert werden müssen. Auch dies spart nicht nur Kosten und Zeit, sondern dient letztlich dem Datenschutz.

3.3 Pragmatische Kompromisse akzeptieren

3.3.1 Vorbemerkungen

Der zweite Bereich zur Lösung der Herausforderungen, mit denen multinationale Konzerne im Rahmen von Discovery-Vorhaben konfrontiert sind, besteht darin, durch technische und organisatorische Maßnahmen praktikable Kompromisse bezüglich der datenschutzrechtlichen Anforderungen zu suchen.

---

[113] Logan/Andrews/Bace, MarketScope for E-Discovery Software Product Vendors, Gartner Report, December 21, 2009.

Wie solche Kompromisse aussehen können, lässt sich am Beispiel des datenschutzrechtlichen Grundsatz der Verhältnismäßigkeit zeigen[114]. Würde namentlich den Empfehlungen der Artikel-29-Arbeitsgruppe gefolgt, müssten demnach alle offenzulegenden Daten vorgängig von einer Drittperson überprüft und – soweit es der Streitgegenstand zulässt – vor der Offenlegung, ja sogar vor der Übermittlung in ein Drittland pseudonymisiert oder anonymisiert werden[115]. Dies ist aber in der zur Verfügung stehenden Zeit normalerweise nicht möglich, würde auch finanziell jeden vernünftigen Rahmen sprengen und eine weitere Analyse der Daten durch die eigenen Anwälte (einschließlich dem Aussondern irrelevanter Daten) letztlich verunmöglichen. Würde hingegen der klassische Weg einer Discovery nach US-amerikanischem Verständnis beschritten, würden die im Rahmen einer E-Discovery erhobenen Daten vor einer Offenlegung bestenfalls auf mit einem *legal privilege* beschlagenen Inhalte untersucht. Maßnahmen zum Schutz der Privatsphäre etwa der Mitarbeiter würden keine getroffen, denn sämtliche Dokumente und Daten, die sich auf den Anlagen des Arbeitgebers befinden, gehören nach US-Rechtsverständnis ausschließlich dem Arbeitgeber: Er darf darüber mehr oder weniger frei verfügen, auch im Prozess und selbst dann, wenn dies die Publikation dieser Dokumente und Daten zur Folge hat.

Das europäische Rechtsverständnis ist hier abermals anders: Selbst am Arbeitsplatz wird dem Mitarbeiter ein gewisser Schutz der Privatsphäre zugesprochen: So darf der Arbeitgeber zwar über geschäftliche E-Mails verfügen, doch private Korrespondenz in den Postfächern seiner Mitarbeiter geht ihn – selbst wenn sie untersagt sein sollten – grundsätzlich nichts an. Wo wie etwa beim persönlichen E-Mail-Postfach mit solchen privaten Inhalten gerechnet werden muss, unterliegt der Zugriff des Arbeitgebers häufig entsprechenden Restriktionen, die sich je nach Auslegung des betreffenden Datenschutzrechts in der Praxis nicht erfüllen lassen.

3.3.2 Standardprozedur zur Durchführung einer E-Discovery in Europa

Die Erkenntnis, dass zwischen europäischem Datenschutz und dem US-amerikanischen Erfordernis der vollumfänglichen Offenlegung ein Spannungsverhältnis besteht, hilft dem multinationalen Konzern freilich wenig: Er sieht sich ungeachtet dieses Spannungsverhältnisses regelmäßig mit der Aufgabe konfrontiert, trotzdem auch in seinen europäischen Betrieben breitangelegte Discovery-Verfahren durchzuführen. Er kommt somit nicht umhin, einen Mittelweg zu suchen.

Vor diesem Hintergrund hat sich in den letzten Jahren eine Standardprozedur für E-Discovery-Verfahren in Europa entwickelt, die inzwischen etliche multinationale Konzerne einsetzen, um den Anforderungen möglichst beider Rechtsord-

---

114 Dazu vorstehend Abschnitt S. 38ff.

115 Ebd.

nungen gerecht zu werden[116]. Sie ist bereits in verschiedenen Ausprägungen in der Fachliteratur und einschlägigen Fachgremien beschrieben und diskutiert worden[117].

Wie die praktische Erfahrung zeigt, funktioniert dieses Verfahren erstaunlich reibungslos. Von datenschutzrechtlichen Zwischenfällen oder nennenswerte Interventionen seitens der Datenschutzbehörden sind nicht bekannt. Die Prozedur wurde sogar mit Vertretern der Artikel-29-Datenschutzgruppe diskutiert und von diesen positiv aufgenommen, auch wenn sie deren (jedenfalls ursprünglich kommunizierten[118]) Anforderungen nicht erfüllt und letztlich nur (aber immerhin) eine Kompromisslösung darstellt. Genau dies dürfte freilich das Erfolgsrezept der Prozedur sein: Sie will praktikabel, nicht perfekt sein.

Die Prozedur kann in vielerlei Hinsicht variiert und den konkreten Umständen angepasst werden. Sie lässt sich jedoch grob in die folgenden fünf Schritte aufteilen:

In einem **ersten Schritt** werden in allen europäischen Ländergesellschaften, die über möglicherweise relevante Daten verfügen, forensisch korrekte Kopien der zuvor identifizierten Daten gesammelt (*targeted collection*). Im Nachgang zur schriftlichen *legal-hold*-Mitteilung werden die Mitarbeiter mittels eines Fragebogens aufgefordert die Systeme zu identifizieren, auf denen sie für den Fall potenziell relevante Dokumente und Informationen gespeichert haben[119]. Sie werden aufgefordert Angaben zu machen, die so spezifisch wie möglich und so breit wie nötig sind. So kann schon im Ansatz vermieden werden, dass es nachfolgend zu einem unverhältnismäßigen Einsammeln irrelevanter Daten kommt. Die Mitarbeiter sollen möglichst genau den Teilbereich der ihnen bekannten Systeme im Unternehmen identifizieren, der aus ihrer Sicht potenziell relevant ist. So sollen sie beispielsweise angeben, welche Ordner sie auf ihrem lokalen Computer und auf den von ihnen benutzten Netzwerklaufwerken von ihnen zur Speicherung von Unterlagen benutzt wurden, sodass nicht der gesamte Computer oder Server in das Einsammeln von Daten einbezogen wird, wie dies sonst oft üblich ist. Wichtig ist hierbei, dass genau instruiert, aber auch verifiziert und nachgefragt wird, um der Gefahr einer zu fokussierten Einsammlung von Daten und somit eines *non-disclosures* vorzubeugen. Sind die Mitarbeiter nicht schon im Rahmen der schriftlichen *legal-hold-Mitteilung* darüber informiert worden, dass der Konzern für einen konkreten Streitfall be-

---

116 Statistiken hierzu existieren keine, doch lässt sich diese Aussagen einerseits auf Erkenntnisse aus dem direkten Erfahrungsaustausch solcher Konzerne in einschlägigen E-Discovery-Fachgremien stützen und andererseits auf Erfahrungswerte von in diesem Bereich tätiger Wirtschaftskanzleien aus verschiedenen europäischen Ländern und den USA.

117 Zeunert/Kos/Daley/Rosenthal, Working Through the Maze, Part 2: Cross-border Discovery Preparedness & Protocols, Konferenartikel zur 2nd Annual Sedona Conference International Programme on Cross-Border Discovery and Data Privacy, 15. bis 16. September 2010, Washington D.C., USA; ROSENTHAL, E-discovery in Switzerland: How to deal with DP restrictions, in: Privacy Laws & Business International, October 2007, S. 9 ff.

118 WP158, Fn. 44.

119 Dies kann entweder effizient über legal-hold-Workflows unterstützende Spezialsoftware geschehen, oder im klassischen Interview-Prozess.

stimmte Daten vorsorglich beziehungsweise zur Durchsicht zusammentragen muss, so werden die Mitarbeiter im Rahmen dieses Befragungsprozesses und somit noch vor dem Einsammeln dieser Daten informiert. Mit der *legal-hold-Mitteilung* und solchen Interviews kann somit nicht nur vermieden werden, dass möglicherweise relevante Dokumente gelöscht oder verändert wurden, sondern auch, dass klar irrelevante Daten gar nicht erst eingesammelt werden. Die Information und der Befragungsprozess der Mitarbeiter dient so auch dem Datenschutz und erlaubt es dem Unternehmen, gleichzeitig seinen datenschutzrechtlichen Transparenzpflichten nachzukommen; eine besondere Einwilligung der Mitarbeiter wird unter solchen Umständen jedenfalls aus Gründen des Datenschutzes meist nicht mehr erforderlich sein. Die Information der Mitarbeiter wird häufig auch genutzt, um das Problem der privaten Inhalte zu lösen: Mitarbeiter werden entweder daran erinnert, dass sie ihre privaten Inhalte entsprechend der im Betrieb geltenden Richtlinien gar nicht oder nur an bestimmten Stellen (z.B. in besonderen Verzeichnissen auf der lokalen Festplatte) speichern dürfen (die im Rahmen der Datensammlung für die Zwecke einer E-Discovery nicht erfasst werden) oder aber private Daten rechtzeitig entfernen sollen, da sie ansonsten miterfasst würden.

In einem **zweiten Schritt** werden die in den europäischen Ländergesellschaften gesammelten Daten häufig an einer zentralen Stelle in Europa in einer konzerneigenen oder von einem E-Discovery-Service-Provider angebotenen Datenbank (*early case assessment database*) zusammengetragen; der Datentransfer innerhalb Europas ist datenschutzrechtlich normalerweise unproblematisch[120]. Besteht im betreffenden Unternehmen bereits eine Archiv-Lösung für die betreffenden Daten (zum Beispiel für E-Mails) kann unter Umständen auf eine separate Sammlung der Daten für die Zwecke der Discovery verzichtet werden. Voraussetzung ist allerdings, dass diese Lösung bereits herstellerseitig so konzipiert ist, dass sie auch als *early case assessment database* für Discovery-Zwecke genutzt werden kann, also etwa über die nötigen Schutzvorkehrungen, Filterfunktionen und Exportschnittstellen verfügt. Diese Datenbank enthält naturgemäß auch zahlreiche nicht relevante Informationen und möglicherweise auch private Daten. Unabhängig davon, ob für die Sicherstellung ein eigenes System oder aber eine Archiv-Lösung benutzt wird, musst sichergestellt sein, dass keine unerlaubten oder unerwünschten Löschungen, Änderungen oder Verluste vorkommen können (im Falle einer Parallelnutzung einer Archiv-Lösung muss insbesondere dafür gesorgt werden, dass die oft übliche automatische Löschung von Dokumenten nach Ablauf der definierten Aufbewahrungsdauer ausgeschaltet wird, sodass die Dokumente auf unbestimmte Zeit aufbewahrt werden). Der Zugriff auf die sichergestellten Dokumente sollte daher, aber auch aus Gründen des Datenschutzes, nur einem kleinen Kreis von entsprechend geschulten und pro Fall autorisierten Personen erlaubt sein. Alle Aktionen auf der

[120] Auch hier gibt es allerdings Ausnahmen. So lässt das französische Datenschutzrecht den Export von Personendaten von Mitarbeitern nur unter strengen Voraussetzungen zu.

Datenbank sollten aus Gründen der Nachvollziehbarkeit automatisch pro Fall protokolliert und in Form von ad hoc Berichten bei Bedarf abrufbar sein.

Bahnt sich eine Offenlegung im Rahmen einer Pre-trial Discovery an, werden die gesammelten Informationen in einem **dritten Schritt** typischerweise in der *early case assessment database* einer oder mehreren semi-automatischen Filtrierungen unterzogen mit dem Ziel, irrelevante Dokumente zu identifizieren und physisch oder zumindest logisch entfernen[121]. Diese Filtrierungen (*culling*) erfolgen einerseits manuell, indem E-Discovery-Experten zusammen mit Personen, die über das entsprechende Fallwissen verfügen, Filter- und Suchparameter definieren, diese testen und soweit nötig präzisieren (z.B. Stichwörter, Datumangaben, Speicherordner, Dokumentenbezeichnungen, Sender- und Empfängernamen). Das Ziel ist es, die für den Fall tatsächlich relevanten Dokumente bzw. klar irrelevante Dokumente auch mit nur exemplarischer Sichtung von Dokumenten möglichst gut identifizieren und extrahieren zu können. Als effiziente Maßnahme zur Präzisierung der Suchwörter (*keyword refinement*) hat sich in der Praxis der Einsatz von Ausschlussbegriffen (Operator „NOT") sowie die Gruppierung von Begriffen (Operator „AND") erwiesen[122]. Häufig werden Suchläufe aus nachvollziehbaren Gründen mit zunächst sehr breit angelegten Suchbegriffen durchgeführt, wie etwa allgemeine, beschreibende Begriffe sowie Vornamen und falltypische Abkürzungen. Um in den Suchtreffern enthaltene, aber tatsächlich irrelevante Dokumente (*false positives*) unterdrücken zu können, sind oft zahlreiche Variationen mit unterschiedlichen Suchbegriffen und deren Verknüpfungen erforderlich, um letztlich eine geeignete Kombination von Suchbegriffen für die Extraktion der offenzulegenden Dokumente zu erhalten. Dieses Vorgehen dient nicht nur dem Datenschutz, sondern ist letztlich auch eine Maßnahme zur Kostensenkung, denn je geringer die Menge an Daten, desto tiefer werden letztlich auch die Kosten deren Sichtung sein. Daher ist der Prozess des *culling* auch in den USA bekannt und akzeptiert[123]. Er sollte dennoch im Rahmen der *meet-and-confer*-Gespräche von den Parteien ausdrücklich und schriftlich vereinbart, namentlich auch die letztendlich maßgeblichen Filterkriterien (daher ist es wichtig, entsprechende Suchläufe und Vorschläge mit den diesbezüg-

---

121 Nicht immer ist eine physische Löschung (d.h. Entfernung des Datensatzes aus der physischen Kopie der Datenbank) zulässig oder möglich. So kann es im späteren Zivilprozess unter Umständen erforderlich werden, die Filterkriterien nachträglich anzupassen und einen neuen Satz an Dokumenten offenzulegen. In solchen Fällen wird das betreffende Dokument lediglich als „irrelevant" oder „herausgefiltert" markiert und in entsprechenden Abfragen zum Bespiel für den Export nicht mehr angezeigt. Er wird zwar nicht offengelegt, befindet sich aber weiterhin in der Datenbank (early case assessment database) der offenlegenden Partei. Die Korrektheit der Filtrierung sollte hingegen in ausreichender Form mit Hilfe der von den betreffenden Filterprogrammen automatisch generierten Protokolle und der manuell zu erstellenden Dokumentationen belegt werden können.

122 Beispiel für den Einsatz solcher sog. boolscher Operatoren: – Ausschluss: John NOT (Doe OR Miller OR Smith); – Gruppierung: Alliance AND Star (oder alternative) "Star Alliance".

123 The Sedona Conference Commentary on Achieving Quality in the E-Discovery Prozess, Mai 2009

lichen Ergebnissen schon vor solchen Gesprächen durchzuführen). Unterstützt werden die Spezialisten durch immer mächtigere Such- und Filterwerkzeuge, welche die Hersteller diverser E-Discovery-Programme inzwischen anbieten. Der Prozess einer ersten Filtrierung sollte mit Rücksicht auf den Datenschutz noch in Europa und in der *early case assessment database* selbst stattfinden. Das Ergebnis ist eine deutlich reduzierte Datensammlung „vermutlich relevanter Daten". Diese Daten sind allerdings weder geschwärzt noch manuell aussortiert. Eine vollständige manuelle Sichtung vor einem Export der *early case assessment database* bzw. der darin einfließenden Dokumente wird normalerweise nur dann durchgeführt, wenn bereits der Export der Daten zu strafrechtlichen Konsequenzen führen kann, was wie erwähnt in gewissen europäischen Ländern zum Beispiel bei bestimmten Geschäftsgeheimnissen der Fall sein kann[124].

In einem **vierten Schritt** werden die für den US-Prozess gesammelten und vorfiltrierten „vermutlich relevant" (*likely relevant*) Daten normalerweise den eigenen Anwälten in den USA übermittelt oder diesen dort via Fernzugriff auf das Review-System eines E-Discovery-Service-Providers in den USA oder Europa zugänglich gemacht[125]. Diese letztere Variante in Kombination mit einer Datenhaltung in Europa greift nach dem Verständnis vieler Datenschützer weniger weit in das Datenschutzinteresse der betroffenen Personen und ist daher der Übermittlung einer vollständigen Kopie der vermutlich relevanten Daten in die USA bevorzugen, wird aber erfahrungsgemäß bis zu 50% höhere Kosten als im Falle einer Inanspruchnahme eines in den USA ansässigen E-Discovery-Service-Providers mit sich bringen; erforderlich ist die europäische Variante mit bloßem Fernzugriff aus den USA nach der hier vertretenen Auffassung aber nicht. Sie ist freilich immer noch wesentlich günstiger als das Einfliegen von US-Anwälten zum Zweck einer Dokumentensichtung (*review*) in Europa, was wiederum aus reinen Datenschutzgründen unverhältnismäßig wäre. Erst in diesem vierten Schritt werden die nach der Filterung verbliebenen Daten im Hinblick auf den Fall manuell gesichtet. Diese Sichtung dient verschiedenen Zwecken: Zum einen werden Dokumente, die aus Gründen des *legal privilege* nicht offengelegt werden müssen (oder die klar irrelevant sind), ausgesondert. Zum anderen dient die Sichtung der eigentlichen Ermittlung des Sachverhalts für den späteren Prozess. Die Sichtung kann jedoch auch benutzt werden, um datenschutzrechtlich problematische Dokumente auszusondern, so etwa private oder sonst irrelevante Dokumente. Dies setzt allerdings voraus, dass den mit der Sichtung betrauten Personen entsprechende (und zum Zweck des Nachvollzugs jeweils dokumentierte) Anweisungen erteilt wurden und diese in der Lage sind, sie auch umzusetzen, also über die erforderlichen Kenntnisse und Fertigkeiten verfügen. Ist im Falle privater (d.h. nicht-geschäftlicher) Inhalte eine Aussonderung nicht zulässig, weil sie sich in an sich relevanten Dokumenten befinden, muss ggf. mit Schwärzungen (*redactions*) gearbeitet werden.

---

124 Dazu vorne Kapitel 2.2.1.

125 Zu den rechtlichen Voraussetzungen siehe nachfolgend Kapitel 3.4.2.

Ob die Aussonderung privater Inhalte, die nicht schon im Rahmen der semi-automatischen Filterung ausgesondert wurden, genügt, muss anhand des konkreten Einzelfalls beurteilt werden. Mitunter kann aus Datenschutzgründen eine vorgängige separate Sichtung (*privacy review*) angezeigt sein, was unter anderem davon abhängt, inwieweit der Betrieb, aus welchem die Daten stammen, seine Mitarbeiter vorgängig über die mögliche Verwendung ihrer Daten informiert hat. Wer also mit anderen Worten seine Mitarbeiter nicht vorgängig informiert hat, ist unter Umstände später zu zusätzlichen Aufwendungen im Bereich der Sichtung von Daten gezwungen.

Auch die Schwärzung von Namen betroffener Personen kann angezeigt sein. Von einer generellen Pflicht kann jedoch auch nach europäischem Datenschutzrecht nach der hier vertretenen Auffassung vernünftigerweise nicht ausgegangen werden. Sie wird denn auch in aller Regel nicht praktiziert. Ausnahmen können dort angezeigt sein, wo die Offenlegung eines Personennamens für den betreffenden Mitarbeiter mutmaßlich gewichtige negative Konsequenzen wie zum Beispiel persönliche Ansprüche oder Strafverfolgung durch ausländische Behörden haben können. Hier kann schon eine etwaige (arbeitsrechtliche) Fürsorgepflicht des Arbeitgebers, soweit das nationale Recht eine solche vorsieht, die Schwärzung der entsprechenden Mitarbeiternamen erfordern, sofern die betreffende Person nicht ohnehin bereits exponiert ist (wie dies etwa bei Personen in Führungspositionen typischerweise der Fall sein wird).

Solche Fälle sind jedoch selbst im Alltag multinationaler Konzerne klar die Ausnahme. In den allermeisten kommerziellen Streitigkeiten wird es für den einzelnen, in einer E-Mail namentlich genannten Mitarbeiter eines Unternehmens letztlich keine persönlichen Konsequenzen haben, wenn seine Identität im Rahmen einer E-Discovery offengelegt wird – abgesehen von der Möglichkeit, allenfalls als Zeuge im fraglichen Verfahren aussagen zu müssen. Wenn aber die Offenlegung der Identität einer Person keine nennenswerten Nachteile für diese Person mitbringt, ihre Entfernung jedoch normalerweise mit erheblichen Aufwänden verbunden ist und im Rahmen einer Discovery immer auch die Frage ihrer Berechtigung aufwirft, dann stellt sich die Frage der Verhältnismäßigkeit einer Schwärzung. Es darf nicht vergessen werden, dass auch im Datenschutzrecht letztlich eine Interessenabwägung zwischen den Datenschutzinteressen der betroffenen Person und dem Interesse an der Bearbeitung ihrer Daten vorgenommen werden muss. In diesem Sinne ist denn auch die oben zitierte Stellungnahme der Artikel-29-Datenschutzgruppe bezüglich der Anonymisierung von Personennamen inzwischen eher als Empfehlung denn als datenschutzrechtliche Pflicht verstanden.

In einem **fünften Schritt** erfolgt schließlich durch die Anwälte in den USA die Offenlegung der im vierten Schritt manuell gesichteten und ggf. geschwärzten Daten an die Gegenpartei. Die Daten verlassen hierbei den Herrschaftsbereich der Partei, welche die Daten offenlegt. Immerhin können und sollten Vorkehrungen ge-

troffen werden, welche die Daten auch nach der Offenlegung in einem gewissen Maß schützen[126].

3.4 Dokumentation & Reglementierung des grenzüberschreitenden Datentransfers

3.4.1 Vorbemerkung

Die vorstehend beschriebene Standardprozedur der schrittweisen Filterung und Übermittlung von Daten im Rahmen eines E-Discovery-Verfahrens erlaubt es einem europäischen Unternehmen vor allem, die beiden zentralen Datenschutzgrundsätze der Verhältnismäßigkeit und Transparenz auch in einem Discovery-Verfahren vor einem US-Gericht mit gewissen Kompromissen zu erfüllen. Andere Herausforderungen des Datenschutzes im Zusammenhang mit einer E-Discovery löst dieses Standardprozedere allerdings nicht. Hierzu sind weitere Schritte nötig. Auch hierfür konnten in der Praxis pragmatische Lösungen entwickelt werden, die sich auch für multinationale Konzerne eignen.

3.4.2 Grenzüberschreitende Bekanntgabe

Dies betrifft zunächst die Herausforderung der datenschutzrechtlichen Anforderungen an die grenzüberschreitende Bekanntgabe von Personendaten. Ohne eine solche ist ein Discovery-Verfahren in Europa nicht möglich. Zugleich sind die rechtlichen Handlungsoptionen wie bereits dargelegt beschränkt[127]. Hierbei ist zwischen den verschiedenen Verfahrensstadien zu unterscheiden. Wird das vorstehend beschriebene E-Discovery-Standardverfahren befolgt, so kommt es zu einer ersten grenzüberschreitenden Bekanntgabe von Personendaten bereits im Rahmen der innereuropäischen Datenkonsolidierung. Diese unterliegt jedoch in aller Regel keinen kostentreibenden oder sonst besonderen datenschutzrechtlichen Restriktionen, da der Datentransfer jeweils im Binnenmarkt des EWR oder aber in ein sicheres Drittland wie die Schweiz erfolgt.

Konkreter Regelungsbedarf entsteht erst mit der Übermittlung der konsolidierten eigenen E-Discovery-Daten in die USA. Da die USA bisher nicht als sicheres Drittland gelten, liegt es in den meisten Fällen nahe, das erforderliche Datenschutzniveau durch Vereinbarung der Musterklauseln der Europäischen Kommission (die *EU model clauses*) auf vertraglichem Wege zu erreichen. In der Praxis dürfte dies zwar die beliebteste Methode zur Absicherung der Datenbekanntgabe in die USA darstellen.

Erfahrungsgemäß kann es sich jedoch lohnen, auch andere Methoden zu überprüfen und selbst beim Einsatz der Musterklauseln der Kommission verschiedene

---

126 Dazu nachfolgend Kapitel 3.4.3.

127 Dazu vorne Abschnitt S. 41ff.

denkbare Szenarien zu überprüfen. Das gilt vor allem für Konzerne, die in verschiedenen Ländern – mitunter auch in den USA – über eigene Niederlassungen verfügen. Das eröffnet bezüglich der möglichen Datenexporteure und Importeure zusätzliche Optionen: So kann es unter Umständen einfacher und effizienter sein, in Europa gesammelte Daten von den europäischen Ländergesellschaften zunächst einer betroffenen Schwester- oder Muttergesellschaft in den USA zu übermitteln und erst dann den dortigen Anwälten zugänglich zu machen statt diese von jeder Ländergesellschaft direkt der Anwaltskanzlei zu übertragen. Dies wird etwa dann der Fall sein, wenn mit der betreffenden US-Gesellschaft bereits eine passende Datenübermittlungsvereinbarung besteht, im Konzern hinreichende *binding corporate rules* existieren[128] oder die US-Gesellschaft über eine auf die Daten passende Safe-Harbor-Zertifizierung verfügt[129].

Allerdings ist in allen Fällen darauf zu achten, dass die betreffende Datenschutzregulierung nicht nur die Weitergabe der Discovery-Daten an die eigenen Anwälte zulässt, sondern auch deren Offenlegung im Prozess. Dieser Aspekt wird zum Beispiel beim Einsatz der EU-Musterklauseln in der Praxis häufig übersehen oder übergangen: Die erfahrungsgemäß beliebtesten Klauseln für die Datenübermittlung zwischen für die Datenbearbeitung Verantwortlichen (*controllern*) vom Dezember 2004[130] erlauben dem Datenempfänger außerhalb des EWR zum Beispiel eine Weitergabe der Daten gemäß ihrer Ziff. II (i) nur, wenn diese in ein sicheres Drittland erfolgt (was die USA für Unternehmen ohne passende Safe-Harbor-Zertifizierung ausschließt), der Empfänger die Klauseln ebenfalls unterzeichnet (was die Gegenpartei oder das Gericht in einem US-Prozess normalerweise nicht tun wird) oder den betroffenen Personen die Möglichkeit gegeben wurde, die Bekanntgabe nach entsprechender Information abzulehnen (was allenfalls bezüglich der eigenen Mitarbeiter, nicht aber bezüglich anderer betroffener Personen möglich ist). Werden Discovery-Daten somit gestützt auf eben diese Klauseln in die USA übermittelt, führt deren Offenlegung zwangsläufig zu einer Vertragsverletzung; weiß der Exporteur bereits vorgängig, dass es dazu kommen wird, dürfte er die Daten somit genau genommen trotz Vereinbarung der Klauseln nicht übermitteln. Die Verwendung der EU-Musterklauseln für Datenübermittlungen an einen Auftragsverarbeiter (*processor*) vom Februar 2010[131] sind diesbezüglich zwar weniger restriktiv, können aber je nach Fallkonstellation andere Komplikatio-

---

128 Die in der EU allerdings von der Datenschutzbehörde im betreffenden Land regelmäßig vorgängig geprüft und genehmigt sein müssen, sofern keine gegenseitige Anerkennung möglich ist.

129 Vgl. die unter www.export.gov/safeharbor abrufbaren Listen für Daten aus der EU und der Schweiz.

130 Entscheidung der Kommission vom 27. Dezember 2004 zur Änderung der Entscheidung 2001/497/EG bezüglich der Einführung alternativer Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer, 2004/915/EG, Az. K(2004) 5271.

131 Beschluss der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates, 2010/87/EG, Az. K(2010) 593.

nen verursachen, weil in bestimmten EU-Staaten im Falle einer Übermittlung an einen Auftragsdatenbearbeiter zusätzliche Anforderungen erfüllt werden müssen[132]. Sehr viel mehr Flexibilität besteht hingegen in Fällen, in denen eine Datenübermittlung auf eine Safe-Harbor-Zertifizierung gestützt werden kann; hier kann das Unternehmen im Rahmen seiner Datenschutzrichtlinien bzw. Zertifizierung weitgehend in Eigenregie bestimmen, wie es den Datenschutz im Falle einer Weitergabe (*onward transfer*) sicherstellen will (freilich wird der Fall der Übermittlung von Daten zwecks Offenlegung in einem Zivilprozess oft nicht bedacht, wenn Unternehmen ihre Datenschutzrichtlinien formulieren). Inzwischen haben sich auch eine Reihe von namhaften US-Anwaltskanzleien und E-Discovery-Service-Provider im Rahmen des Safe-Harbor-Privacy-Framework selbstzertifiziert, was direkte Datenübermittlungen an diese Kanzleien aus dem EWR-Raum und der Schweiz erheblich erleichtern kann.

Auch die Konsolidierung von europäischen Discovery-Daten in einem europäischen Staat mit günstigen Bestimmungen zur grenzüberschreitenden Bekanntgabe kann eine solche erheblich vereinfachen. Die Schweiz ist ein solches Beispiel: Anders als in der EU üblich besteht in der Schweiz weder rechtlich noch faktisch ein Formzwang bezüglich der Sicherstellung des Datenschutzes in einem unsicheren Drittland[133]. Zwar sind die EU-Musterklauseln auch in der Schweiz anerkannt, doch steht es einem Datenexporteur aus der Schweiz frei, eine beliebige andere (mitunter auch wesentlich kürzere und einfachere bzw. auf den konkreten Sachverhalt passendere) Regelung zu treffen, sofern diese ein angemessenes Datenschutzniveau seitens des Empfängers im Ausland sicherstellt[134]. Der Export der in der EU im Rahmen einer E-Discovery gesammelten Daten in die Schweiz ist wiederum aufgrund des Status der Schweiz als sicheres Drittland[135] in aller Regel problemlos möglich. Sind die Daten erst einmal in der Schweiz konsolidiert, finden auf deren Export nur noch die Bestimmungen des Schweizer Datenschutzrechts Anwendung, welche wie gezeigt mehr Spielraum lassen als das entsprechende EU-Recht. Kann beispielsweise gezeigt werden, dass die in Europa gesammelten Personendaten für einen Prozess in den USA erforderlich sind und sichergestellt ist, dass sie dort nicht zu anderen Zwecken verwendet werden (dazu sogleich), ist der Export nach schweizerischem Recht in aller Regel auch ohne Safe-Harbor-Registrierung oder

---

132 So etwa Art. 11 des deutschen Bundesdatenschutzgesetzes, welcher solche Übermittlungen nur zulässt, wenn die Auslagerung durch einen detaillierten Vertrag geregelt ist. Dabei ist noch unklar, ob die EU-Musterklauseln diesen Anforderungen genügen, auch wenn dies vernünftigerweise angenommen werden müsste. Dementsprechend wird in Deutschland das Konstrukt der Auftragsdatenbearbeitung im vorliegenden Zusammenhang eher gemieden.

133 ROSENTHAL, Fn. 53, Art. 6 DSG, N 38.

134 Art. 6 Abs. 2 Bst. a des schweizerischen Datenschutzgesetzes.

135 Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzes personenbezogener Daten in der Schweiz, 2000/518/EG, Az. K(2000) 2304.

Datenübermittlungsvertrag möglich[136]; auch verschiedene EU-Staaten bieten diese Möglichkeit[137].

Allerdings können auch solche Lösungen ihre Haken haben: Die Schweiz bietet zwar im Bereich des Datenschutzes wesentlich flexiblere und damit attraktivere Regelungen an als die meisten EU-Staaten, doch schützt sie umgekehrt ihr Territorium sehr viel stärker vor Zugriffen ausländischer Behörden als manche andere Rechtsordnungen dies tun. Während dies der freiwilligen Teilnahme eines Unternehmens an einer Pre-trial Discovery normalerweise nicht entgegensteht, kann eine Offenlegung derselben Daten, sofern sie im Rahmen einer zwangsweisen Anordnung eines US-Gerichts geschieht, unter Strafe verboten sein[138].

Die genannten Beispiele und Ausführungen zeigen, dass die Schwierigkeit der datenschutzkonformen grenzüberschreitenden Bekanntgabe von Daten einer E-Discovery nicht darin besteht, *ob* sie möglich ist, sondern auf welchem Weg sie am besten durchgeführt wird. Hier können die verschiedenen Kommunikationswege, die gerade international tätige Konzerne häufig bieten können, ein Vorteil sein, da die rechtliche Lösung dieser Herausforderung eine entsprechende Lenkung der Datenströme voraussetzen kann.

3.4.3 Schutz der Daten nach ihrer Offenlegung

Dass der Schutz der Personendaten auch nach ihrer Übermittlung in die USA sichergestellt bleiben muss, wurde bereits ausgeführt. Während sich dies bei ihrer Verarbeitung innerhalb des Konzerns oder durch die vom Konzern beauftragten Anwälte noch durch Weisungen und Vereinbarungen einigermaßen sicherstellen lässt, ist dies nach der Bekanntgabe der Daten an die Gegenpartei (und später ggf. an das Gericht) naturgemäß nicht mehr möglich.

Doch auch für dieses Problem hat sich in den letzten Jahren ein Standardprozedere etabliert. Es kann den Anforderungen des Datenschutzes zwar wiederum nicht in allen Punkten gerecht werden, adressiert jedoch das datenschutzrechtliche Kernanliegen im Rahmen einer Discovery: Der Verhinderung einer Nutzung der Personendaten außerhalb des Gerichtsverfahrens oder für andere Zwecke.

Das Standardprozedere besteht im Erlass einer entsprechenden Schutzverfügung durch das zuständige US-Gericht (*protective order*). Sie wird in aller Regel von den Parteien gemeinsam vorbereitet und ausgehandelt, vom Gericht erlassen und deckt alle offengelegten Daten ab. Im US-Zivilprozess sind *protective orders* weit verbreitetet. Sie dienten bis anhin jedoch in erster Linie dazu, im Prozess offengelegte Geschäftsgeheimnisse vor einer Preisgabe durch die Gegenpartei und weitere beteiligte Personen wie etwa Zeugen oder Sachverständige zu schützen. Gleichzeitig sorgt sie dafür, dass das Gericht die betreffenden Dokumente nicht der

---

136 Art. 6 Abs. 2 Bst. d des schweizerischen Datenschutzgesetzes.

137 So etwa das Vereinigte Königreich.

138 Art. 271 des schweizerischen Strafgesetzbuches; vgl. dazu Kapitel 2.2.1 vorne.

Öffentlichkeit zugänglich macht (wie dies mit Parteieingaben und eingereichten Urkundenbeweisen in einem US-Zivilprozess normalerweise geschieht[139]), sondern sie unter Verschluss (*under seal*) hält.

Eine Alternative zur Schutzverfügung kann auch die rein vertragliche Vereinbarung der Vertraulichkeit sein (*confidentiality agreement*). Sie hat den Vorteil, dass sie rascher und ohne Mitwirkung des Gerichts umgesetzt werden kann. Ihr Nachteil besteht darin, dass sie nur gegen die Parteien der Vereinbarung durchgesetzt werden können (also nicht gegen etwaige in den Prozess einbezogene Dritte) und auch dann lediglich als Vertragsverletzung, nicht als Missachtung einer gerichtlichen Anweisung. In der Praxis kommen Vertraulichkeitsvereinbarungen typischerweise im Vorfeld einer Offenlegung zum Einsatz, etwa wenn es um die Aushandlung der Offenlegung oder den Austausch erster Vorabdaten geht, während die Schutzverfügung für die Absicherung der eigentlichen Offenlegung benutzt wird.

Weil jeder US-Anwalt und jedes Gericht das Instrument des *protective order* und des *confidentiality agreements* kennt und akzeptiert, erwiesen sie sich in den letzten Jahren denn auch als ideale Werkzeuge auch zur Sicherstellung des Datenschutzes von vor oder im Prozess offengelegten Personendaten. Zu diesem Zwecke werden einerseits sämtliche Personendaten (nach europäischer Definition) pauschal dem gleichen Schutz wie Geschäftsgeheimnisse unterstellt[140] und andererseits die Empfängers solcher Geheimnisse nicht nur zur Geheimhaltung verpflichtet, sondern ihnen – so nicht schon der Fall – auch die Verwendung zu anderen Zwecken als für den Prozess untersagt. Werden die Unterlagen Dritten zugänglich gemacht, ist sicherzustellen, dass diese ebenfalls unter die Restriktionen des *protective order* (bzw. im Rahmen einer Vertraulichkeitsvereinbarung die Offenlegung gegenüber Dritten untersagt oder nur unter bestimmten Bedingungen erlaubt wird) fallen. Schutzverfügungen legen in der Regel auch fest, dass die Unterlagen nach Prozessende bzw. nach Gebrauch vernichtet bzw. zurückgegeben werden müssen.

Einzig für die Durchsetzung der Auskunfts-, Berichtigungs- und Löschrechte der betroffenen Person ist ein *protective order* nicht unbedingt geeignet. Häufig werden US-Gegenparteien nicht bereit sein, betroffenen Personen entsprechende Rechte verbindlich einzuräumen, weil sie ihnen in letzter Konsequenz zu weit gehen (warum etwa sollte eine Partei sich der Anweisung einer Person aus dem gegnerischen Lager unterwerfen, wenn diese von ihr verlangt, bestimmte Beweismittel nicht mehr oder nur noch in anonymisierter Form zu verwenden?). Sie werden sich allenfalls bereit erklären, entsprechende Forderungen betroffener Personen wohlwollend zu prüfen. Will also eine betroffene Person Auskunfts-, Berichti-

---

139 Vgl. etwa www.pacer.gov für den Online-Zugang zu den Akten der US-Bezirks-, Konkurs- und Berufungsgerichte.

140 Normalerweise sehen Schutzverfügungen zwei Klassen vertraulicher Dokumente vor: Vertrauliche (confidential) Dokumente und streng vertrauliche (highly confidential) Dokumente (mit eingeschränktem Zugang). Personendaten im Sinne des Datenschutzes werden in der Praxis grundsätzlich der ersten Klasse zugeordnet.

gungs- oder Löschrechte bzw. das Recht auf Widerspruch geltend machen, so wird sie sich letztlich nur an jene Partei wenden können, welche die betreffenden Personendaten im Verfahren offengelegt hat, damit diese im eigenen Namen den Richter um entsprechende Anordnungen bittet oder ihr die nötigen Auskünfte erteilt (etwa über den Umfang der offengelegten, die betroffene Person betreffende Unterlagen).

Solche Situationen sind jedoch eher theoretischer Natur und kommen so gut wie nie vor, weshalb sie in der Praxis einer Offenlegung von Personendaten in einem US-Zivilprozess in aller Regel auch nicht entgegenstehen. Auch hier gilt: Die Lösung muss praktikabel, nicht perfekt sein.

Literaturverzeichnis

Artikel-29-Arbeitsgruppe, Arbeitsunterlage 1/2009 über Offenlegungspflichten im Rahmen vorprozessualen Beweiserhebungen bei grenzübergreifenden zivilrechtlichen Verfahren (pre-trial discovery) vom 11. Februar 2009, WP 158.

Hill, Brian W., Owens, Leslie, Searching For eDiscovery Cost Control, Forrester Research, Inc., April 27, 2009.

Kaplan, Ari, Advice from Counsel: Best Practices on Controlling E-Discovery Costs, FTI Consulting, 2009.

Kravitz, Mark R, Memo from Honorable Mark R Kravitz, Chair, Advisory Committee on Federal Rules of Civil Procedure to Honorable Lee H. Rosenthal, Chair, Standing Committee on Rules of Practice and Procedure RE: Report of the Civil Rules Advisory Committee (May 17, 2010).

Logan, Debra, Andrews, Whit, Bace, John, MarketScope for E-Discovery Software Product Vendors, Gartner Report, December 21, 2009.

NIST, US Department of Commerce, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), Special Publication 800-122.

Rosenthal, David, E-discovery in Switzerland: How to deal with DP restrictions, in: Privacy Laws & Business International, October 2007, S. 9 ff.

Rosenthal, David, Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich 2008.

The Sedona Conference Working Group 6, Comment of The Sedona Conference Working Group 6 to Article 29 Data Protection Working Party Working Document 1/2009 („WP 158"), Oktober 2009.

The Sedona Conference Commentary on Achieving Quality in the E-Discovery Prozess, Mai 2009.

Tero,Vivian, Corporate eDiscovery Technology Trends 2009: Doing More with Less While Facing Increasing Complexity in eDiscovery, IDC Information and Data sponsored by FTI Technology, November 2009.

Zeunert, Christian, Kos, Patrick, Daley, James, Rosenthal, David (The Sedona Conference), Working Through the Maze, Part 2: Cross-border Discovery Preparedness & Protocols, 2nd Annual Sedona Conference International Programme on Cross-Border Discovery and Data Privacy, 15. bis 16. September 2010, Washington D.C., USA.

Literaturverweise auf Beiträge innerhalb dieses Herausgeberbandes

Banaschik, Meribeth: Leitfaden für Unternehmensjuristen zur Reaktion auf Anforderungen der U.S.-Discovery aus der amerikanischen Perspektive
Brunsch, Elmar: Safe in Germany. E-Discovery-Datenschutz im IT-Outsourcing
Hartmann, Matthias H.: Systematische E-Discovery und Information Governance
Hartmann, Matthias H.; Venhofen, Jürgen: Strategisches Innovations- und Technologie-Management für E-Discovery
Kiemes, Sandra; Pauseback, Jörg: Prozess der E-Discovery in der technischen Umsetzung
Laue, Philipp: E-Discovery und Prüfschema zum internationalen Datentransfer
Meyer, Stephan: Deutsches Datenschutzrecht und Betriebsratsbeteiligung bei E-Discovery in den USA
Murray, Nigel: E-Discovery-Strategien für international agierende Unternehmen
Paknad, Deidre; Jung, Wolfgang; Hampp, Thomas: Information Governance als Erfolgsfaktor für Electronic Discovery
Schmid, Claus: E-Discovery im Kontext IT-Management und Enterprise Data Management
The Sedona Conference®: Historie „The Sedona Conference®“
The Sedona Conference®: Ergebnisse von „The Sedona Conference®“ Working Group „International Electronic Information Management, Discovery and Disclosure” (WG6)
Wilske, Stephan: E-Discovery im kontinentaleuropäischen Rechtsraum: Discovery-Verfahren in der Schiedsgerichtsbarkeit

E-Discovery verstehen – Risiken im Unternehmen begrenzen

Ob Produkthaftung, Patentrecht oder M&A-Fragen – weltweit agierende Unternehmen sind verstärkt mit der Gefahr eines internationalen Rechtsstreits und harter Sanktionen konfrontiert. Wie gelingt es in diesem Kontext, elektronische Beweismittel von Beginn an systematisch zu sichern und Verfahrensfehler zu vermeiden?

Internationale Experten informieren Sie in diesem Werk umfassend über die **Risiken und Chancen von E-Discovery** – dem Ermitteln, Sammeln und Zusammenstellen von Informationen für gerichtliche Prozesse in den USA und Europa:

- Sie lernen sowohl rechtliche als auch technologische und betriebswirtschaftliche Konsequenzen kennen.
- Sie erkennen anhand einer Darstellung juristischer Optionen, wie Sie komplexe Rechtsstreitigkeiten lösen können.
- Sie erfahren, wie Sie Leitlinien für den Schutz sensibler Unternehmensdaten erarbeiten und umsetzen.
- Sie erhalten einen detaillierten Einblick in die IT-Prozesskette einer E-Discovery.

Zahlreiche Praxisbeispiele veranschaulichen die unterschiedlichen Perspektiven beteiligter Anwaltskanzleien, beratender IT-Unternehmen sowie betroffener Unternehmen!

9 783503 130740 € (D) 44,95

www.ESV.info