

Hinweise zur verwaltung elektronischer daten

April 2005

Einführung

Die Unterlagen eines Unternehmens sind eine notwendige und wertvolle Ressource sowohl als Informationsquelle als auch zum Beleg von Aktivitäten, Rechten und Pflichten des Unternehmens. Mit dem wachsenden Vertrauen auf elektronische Dokumente wird es für ein Unternehmen lebensnotwendig vorhandene Richtlinien zur Dokumentenverwaltung zu überarbeiten, um den neuen Arbeitsmethoden und Pflichten des Unternehmens Rechnung zu tragen.

Es entspricht schon seit langem der guten betrieblichen Praxis von Unternehmen, dass es Richtlinien zur Verwaltung von Dokumenten gibt, welche sowohl für Mitarbeiter, als auch Vertragspartner oder Berater des Unternehmens gelten. Eine solche Richtlinie betrifft die Speicherung, Bereitstellung, Aufbewahrung und Vernichtung von Unterlagen aller Art.

„Unterlagen“ meint dabei sowohl förmliche Aufzeichnungen von Transaktionen wie Buchhaltungsunterlagen und Verträge, aber auch formlose Unterlagen wie

Korrespondenz, interne Memoranden, e-mails oder persönliche Notizen. Alle diese Unterlagen können als Beweis in einem Gerichtsverfahren relevant werden und müssen eventuell, wenn sie noch existieren, im Rahmen von Prozessen oder einer regulatorischen oder behördlichen Untersuchung vorgelegt werden. Dabei ist es bisher zwar noch so, dass bei deutschen Gerichten elektronische Dokumenten nur dann als Anscheinsbeweis ausreichen, wenn sie eine qualifizierte elektronische Signatur erhalten. Die Fotokopie oder das elektronische Dokument kann aber im Rahmen der freien Beweiswürdigung durch den Richter ebenso relevant sein.

Die Art und Weise in der eine Unternehmens-Richtlinie das Thema der elektronischen Dokumente behandelt, bedarf sorgfältiger Überlegungen. Die Daten existieren wahrscheinlich an einer Vielzahl von Orten. Zum Beispiel kann es tägliche, wöchentliche oder monatliche Sicherungskopien von Computerdateien geben. Diese Dateien sind dann nicht nur auf Band vorhanden, sondern können immer noch auf der Festplatte eines Computers oder in einer temporären Datei, auf einer Floppy Disk, im

Netzwerk oder auf mobilen Geräten vorhanden sein. Elektronische Dokumente, SMS- oder E-mail-Nachrichten können darüber hinaus einen größeren Empfängerkreis haben als nur die bekannten Empfänger. Auch können elektronische Informationen länger als Papier gespeichert sein, da sie weniger Platz in Anspruch nehmen.

Die große Herausforderung ist es daher, eine Aufbewahrungsrichtlinie auszuarbeiten, die im elektronischen Umfeld kaufmännisch praktikabel ist und welche die rechtlichen und regulatorischen Anforderungen an das Unternehmen berücksichtigt.

Die nachfolgenden Hinweise sollen dazu dienen, über die rechtlichen und regulatorischen Anforderungen im Zusammenhang mit elektronischem Dokumentenmanagement aus globaler, europäischer und nationaler Sicht zu informieren.



Globale anforderungen

Im Nachgang zum weithin bekannten Enron-Skandal, haben internationale Gesetzgeber sowie Aufsichtsbehörden regulative Maßnahmen getroffen, um das Vertrauen in die Unternehmen wieder herzustellen.

Sarbanes-Oxley

Obwohl es sich bei dem sog. Sarbanes-Oxley Act aus dem Jahre 2002 ("SOX") um ein amerikanisches Gesetz handelt, wirkt sich dieses Gesetz generell für Unternehmen auf globaler Ebene aus. Dies liegt daran, dass von Unternehmen, die in den USA Geschäfte machen, verlangt wird, dass sie ihre Richtlinien zum Datenmanagement mit den Regeln des SOX in Einklang bringen.

Hintergrund

Im Dezember 2001 meldete Enron eine der größten Insolvenzen in der US Geschichte an, als bekannt wurde, dass Enron angeblich in verschiedene fragwürdige Praktiken verwickelt war, die insgesamt in Abschreibungen von Investitionen von über einer Milliarde US-Dollar sowie entsprechende Wertberichtigungen bei den

Einkünften mündeten. Diese Praktiken betrafen zahlreiche Investment Strategien, Transaktionen außerhalb der Bilanz, Zweckgesellschaften zum "Verstecken" von Schulden, Geschäfte mit nahe stehenden Personen oder Gesellschaften, durch Enron-Aktien abgesicherte Darlehen, falsche, unvollständige oder irreführende Angaben, aggressive Rechnungslegungspolitik, und verschiedene andere fragwürdige Praktiken.

Vor Anmeldung der Insolvenz hatten Enron's Wirtschaftsprüfer damit begonnen Dokumente zu vernichten. Sie fuhren damit fort bis Arthur Andersen schließlich einer gerichtliche Verfügung erhielt, wonach diese und andere Dokumente vorzulegen waren. Im Ergebnis wurde Arthur Andersen wegen Rechtsbehinderung verurteilt. Im Prozess hatte nämlich der leitende Prüfer zugegeben, dass Dokumente betreffend Enron geschreddert worden waren.

Management von Daten und SOX

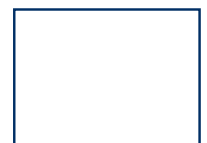
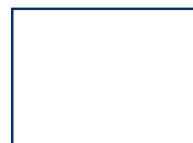
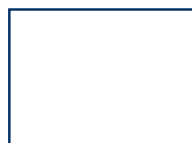
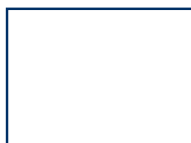
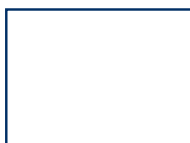
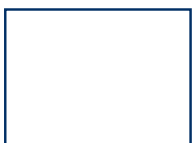
SOX findet Anwendung auf Unternehmen, deren Aktien bei der Security and Exchange Commission ("SEC") gelistet oder registriert sind.

Folglich können sowohl US als auch Nicht-US Unternehmen (z.B. Töchter von US-Unternehmen) unter SOX fallen.

Vor SOX gab es recht wenig Richtlinien im Zusammenhang mit der Aufbewahrung von Dokumenten. SOX hat diese Thema in den Mittelpunkt gerückt, indem es die Anwendbarkeit der Gesetze zur Rechtsbehinderung auf die Aufbewahrung von Daten ausgedehnt und die Strafen in diesem Zusammenhang merklich angehoben hat. Aus diesem Grund ist SOX inzwischen zu einer Bezugsgröße für die Transparenz eines Unternehmens geworden.

Aufbewahrung (§ 802)

Gemäß SOX ist es jetzt eine Straftat, wenn Dokumente eines Unternehmens in Anbetracht einer Untersuchung des Bundes oder einer jeglichen Verwaltungsmaßnahme zerstört werden. Als Strafe können bis zu 20 Jahre Gefängnis und Bußgelder bis zu 10 Millionen US-Dollar verhängt werden, wenn jemand:



"bewusst eine Akte, ein Dokument oder eine Sache verändert, zerstört, verstümmelt, versteckt, vertuscht, fälscht, oder einen falschen Eintrag in der Absicht macht, eine Untersuchung oder ordnungsgemäßen Administration einer Angelegenheit innerhalb der Zuständigkeit einer Bundesbehörde der Vereinigten Staaten oder eines Insolvenzverfahrens [nach dem Bankruptcy Code] oder im Zusammenhang oder in Erwägung einer solchen Angelegenheit oder eines solchen Verfahrens, zu behindern, zu verhindern oder zu beeinflussen." (§ 802 SOX)

Offenlegung (§ 302 und 906)

Zusätzlich zu den Anforderungen an eine Aufbewahrung nach § 802, regelt SOX Verpflichtungen im Zusammenhang mit der Offenlegung von Daten.

Nach § 302, müssen der CEO und der CFO eines Unternehmens persönlich jeden "eingereichten Jahres- oder Quartalsbericht" bestätigen. Ferner müssen sie versichern, dass die internen Kontrollen in Bezug auf die Offenlegung ausreichend sind.

Wie bei § 802 drohen Strafen von bis zu 10 Jahren Gefängnis und/oder 1 Million US-Dollar Bußgeld, oder 20 Jahre Gefängnis und/oder 5 Millionen US-Dollar Geldbuße wenn "wissentlich" oder "absichtlich" falsch bestätigt wird. Zudem kann die SEC eine Zivilklage anstrengen.

Der Effekt von diesen und anderen rechtlichen Bedingungen ist, dass der Umfang der Aufbewahrung und Offenlegung von Dokumenten sehr weit ist. Unternehmen sollten daher sehr genau ihre allgemeinen Richtlinien zur Aufbewahrung von Dokumenten prüfen, insbesondere wenn formlose Aufzeichnungen existieren. Es sind Fälle denkbar, in denen die Lösung einer formlosen Aufzeichnung (z.B. eine E-mail) unzulässig ist, auch wenn es kein spezielles Gesetz oder eine Verordnung gibt, welche(s) die Aufbewahrung anordnet.

Anforderungen innerhalb der EU

Basel II

Innerhalb der EU hat die Europäische Kommission vorgeschlagen, zwei Richtlinien betreffend das Geschäft von Kreditinstituten und die angemessene Kapitalausstattung von Investmentfirmen und Kreditinstituten (Kapitalausstattungs-Richtlinie) umzugestalten, um Basel II zu implementieren.

Basel II ist ein internationales Abkommen, welches vom Baseler Komitee für die Bankenaufsicht entwickelt wurde. Es zielt darauf ab, neue, globale Standards dafür zu kreieren, wie Banken und bestimmten andere Finanzinstitute Risiken bewerten und Kapital verteilen.

Basel II beinhaltet drei sich gegenseitig stützende Säulen (d.h. Ziele), welche die Sicherheit und Zuverlässigkeit der Finanzsysteme sichern sollen. Die dritte Säule (Marktdisziplin) beschreibt den Rahmen für die Marktoffenlegung durch Banken und Finanzinstitute. Insbesondere, verlangt Basel II von den Unternehmen die Offenlegungen



im Markt um die Marktdisziplin zu verbessern. Derartige Pflichten zur Offenlegung schließen Schlüsselinformationen über Risiken der die Gesellschaft ausgesetzt ist, die Risiko Management-Prozesse sowie ausreichendes Kapital mit ein. Die Offenlegung wird alle sechs Monate gefordert.

Folglich besteht das Risiko, dass unzureichendes Datenmanagement durch welches ein Unternehmen nicht in der Lage ist den Anforderungen der Richtlinie zu entsprechen, die finanzielle Stellung einer Bank oder einer Finanzinstitution in Frage stellen kann.

Es wird erwartet, dass die Richtlinie über ausreichende Kapitaldeckung von der EU im Sommer 2005 verabschiedet wird. Die Mitgliedstaaten werden dann diese aller Voraussicht nach bis Ende 2006 in nationales Recht umsetzen, d.h. Unternehmen müssen bis dahin konform sein. Aus diesem Grund gibt es nur noch eine begrenzte Zeit, bis ein Unternehmen konform sein muss.

Die Datenschutz-Richtlinie

Die EU Datenschutz-Richtlinie regelt verschiedene Pflichten eines Unternehmens bei der Verarbeitung personenbezogener Daten. Personenbezogene Daten meint Information über Einzelpersonen, nicht nur in Bezug auf ihr Privatleben, sondern auch im Rahmen ihres Arbeitsverhältnisses.

Ein innerhalb der EU operierendes Unternehmen muss im Zusammenhang mit elektronischen Daten die Datenschutzgesetze beachten soweit diese personenbezogene Daten enthalten (z.B. E-mails).

Nach Artikel 17 (1) der Datenschutz-Richtlinie muss ein Unternehmen insbesondere:

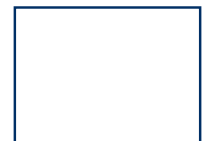
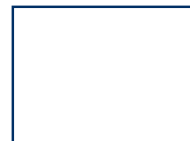
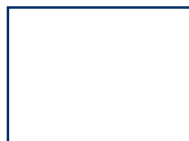
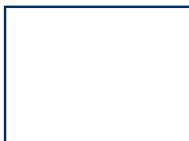
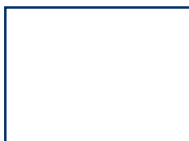
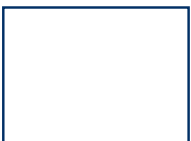
„geeignete technische und organisatorische Maßnahmen durchführen ... die für den Schutz gegen zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder

den unberechtigten Zugang - insbesondere wenn im Rahmen der Verarbeitung Daten in einem Netz übertragen werden - und gegen jede andere Form der unrechtmäßigen Verarbeitung personenbezogener Daten erforderlich sind.“

Dies bedeutet im Ergebnis, dass ein Unternehmen gesetzlich verpflichtet ist, gute Richtlinien und Praktiken zur Sicherheit von und dem Umgang mit Informationen zu haben.

Zusätzlich muss ein Unternehmen nach Artikel 12 jedem Betroffenen das Recht gewähren, in angemessenen Abständen und ohne unzumutbare Verzögerung oder übermäßige Kosten, Auskunft über die Verarbeitung und Übermittlung seiner Daten zu erhalten.

Daher gibt es innerhalb der gesamten EU ein Recht auf Auskunft über personenbezogene Daten, einschließlich E-mails, wobei es (fast) nicht darauf ankommt, ob dies für das Unternehmen eine Unannehmlichkeit darstellt oder nicht.



Deutsche anforderungen an die dokumentenverwaltung

Pflichten im Rahmen der Dokumenten-Verwaltung

Aufbewahrungspflichten

Eine Unternehmensrichtlinie zu Dokumentenverwaltung muss gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungspflichten und -fristen berücksichtigen. Interne Richtlinien, rechtliche Vorschriften oder Verträge sowie die Eventualität von Rechtsstreitigkeiten erfordern es, dass die Unterlagen für eine bestimmte Zeit aufbewahrt werden.

So ist beispielsweise jeder Kaufmann verpflichtet, Handelsbücher, Inventare, Eröffnungsbilanzen, Jahresabschlüsse, Lageberichte, Konzernabschlüsse, Konzernlageberichte sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen 10 Jahre aufzubewahren. Handelsbriefe sowie Buchungsbelege sind 6 Jahre aufzubewahren.

Ein Arbeitgeber ist ferner verpflichtet Beitragsabrechnungen der Sozialversicherungsträger, Fahrtkostenerstattungsbelege, Gehaltlisten, Lohnbelege, Prozessakten und Reisekostenabrechnungen 10 Jahre aufzubewahren. Essenmarkenabrechnungen, Geschenknachweise, Lohnlisten, Steuerunterlagen und Unterlagen über vermögenswirksame Leistungen wiederum müssen über einen Zeitraum von 6 Jahren aufbewahrt werden. Für Buchungsbelege zu vermögenswirksamen Leistungen gilt eine 10-jährige Aufbewahrungsfrist.

Dienstleister im Bereich Telekommunikation müssen auf staatsanwaltliche und andere gesetzliche Auskunftersuchen in der Lage sein, Bestandsdaten der Kunden zu übermitteln. Diese Verpflichtung besteht auch für innerbetriebliche Telekommunikationsdienste, soweit diese geschäftsmäßig erbracht werden.

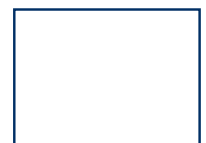
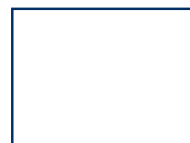
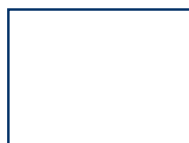
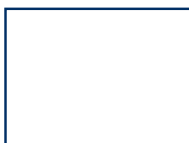
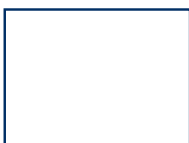
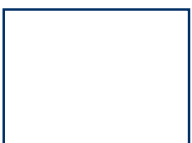
Darüber hinaus müssen Unternehmen eventuell auf sie anwendbare Spezialgesetze sowie aufsichtsrechtliche Vorgaben beachten. So sieht beispielsweise das Geldwäschegesetz für den Bankenbereich bestimmte

Aufzeichnungs- und Aufbewahrungspflichten vor, die teilweise durch Verlautbarungen des Bundesaufsichtsamtes für das Kreditwesen weiter konkretisiert werden.

Aber auch, wenn ein Dokument nicht aus gesetzlichen Gründen aufbewahrt werden muss, ist es oft sinnvoll, bestimmte Unterlagen aufzubewahren, beispielsweise um Unternehmensentscheidungen zu rechtfertigen oder um im Rahmen eines Rechtsstreits Beweismaterial, wie Verträge und Korrespondenz, an der Hand zu haben (siehe unten).

Fallstudie 1 - Wo ist das E-mail?

Ein Unternehmen beauftragt seinen Lieferanten regelmäßig per E-mail. Als der Lieferant dem Unternehmen eine Rechnung stellt, räumt es nicht den vereinbarten Rabatt ein. Die E-mail, in welcher ein Rabatt vom Standardpreis vereinbart war, kann nicht mehr aufgefunden werden. Im Ergebnis konnte das Unternehmen daher den vereinbarten Rabatt nicht durchsetzen.



Speicherung von Daten, technische und organisatorische Maßnahmen zum Schutz der Daten, Auskunft, Sperrung und Löschung

Aus datenschutzrechtlicher Sicht ist es erforderlich, dass bei der Speicherung von personenbezogenen Daten der Betroffene von der Speicherung, der Art der Daten, der Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und der Identität der verantwortlichen Stelle benachrichtigt wird. "Personenbezogene Daten" sind Einzelangaben über persönliche oder sachliche Verhältnisse einer natürlichen Person.

Darüber hinaus ist das Unternehmen verpflichtet, technische und organisatorische Maßnahmen zu treffen, um personenbezogene Daten insbesondere vor unbefugtem Zugriff zu schützen. Insoweit sollte eine Unternehmensrichtlinie zur Dokumentenverwaltung Angaben zu Sicherungsmaßnahmen gem. der Anlage zu § 9 BDSG enthalten.

Auch muss es dem Unternehmen möglich sein, dem Betroffenen Auskunft über die zu seiner Person gespeicherten Daten zu erteilen. Dies betrifft z.B. sowohl Kundendaten, als auch Daten von Mitarbeitern. Ferner sehen die Datenschutzgesetze Lösungs- und Sperrungspflichten vor, wenn z.B. personenbezogene Daten unberechtigt gespeichert worden sind. Schließlich sind unrichtige Daten zu berichtigen, wobei die Beweislast für die Richtigkeit grundsätzlich bei dem speichernden Unternehmen liegt. Eine Richtlinie zur Dokumentenverwaltung sollte daher Angaben zu Verfahren zur Umsetzung dieser Verpflichtungen enthalten.

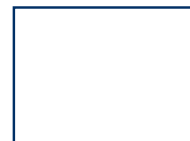
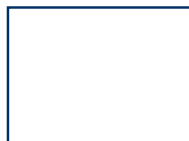
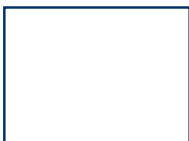
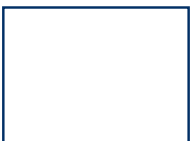
Fallstudie 2 - Was kosten Altdaten?
Ein ehemaliger Angestellter bittet um Auskunft über seine Personalakte. Das Personalverwaltungssystem des Unternehmens wurde gerade auf eine neue Version migriert, so dass Teile der Akte nur im Altdatenbestand erhältlich waren. Um der Nachfrage des ehemaligen Angestellten nachzukommen, musste das Altdatensystem für zehntausende Euro zum Laufen gebracht werden. Diese Kosten hatte allein das Unternehmen zu tragen.

Beweispflichten

Das Erfordernis bestimmte Dokumente aufzubewahren ergibt sich nicht nur aus dem Gesetz. Vielmehr ist auch zu berücksichtigen, dass für den Fall einer Rechtstreitigkeit bestimmte Dokumente zu Beweis Zwecken aufbewahrt werden sollten. Insoweit sind für die Dauer der Aufbewahrung von Dokumenten die Verjährungsfristen von möglichen Ansprüchen relevant.

Grundsätzlich verjähren zivilrechtliche Ansprüche binnen 3 Jahren mit Entstehung des Anspruchs, dies sind z.B. vertragliche Erfüllungsansprüche, Schadensersatzansprüche, Bereicherungsansprüche, Ansprüche aus Geschäftsführung ohne Auftrag. Teilweise kann aber auch vertraglich eine kürzere Verjährungsfrist vorgesehen sein.

Herausgabeansprüche aus Eigentum und anderen dinglichen Ansprüchen verjähren dagegen erst binnen 30 Jahren. Ansprüche auf Übertragung des Eigentums an einem Grundstück sowie auf Begründung und Übertragung eines Rechts an einem Grundstück verjähren binnen 10 Jahren.



Unabhängig also von einer gesetzlichen oder aufsichtsrechtlichen Verpflichtung sollte eine Richtlinie zum Dokumentenmanagement Verjährungsfristen für rechtliche Ansprüche berücksichtigen. Beispielsweise sollten Unterlagen im Zusammenhang mit dem Abschluss und der Abwicklung von Verträgen zumindest über die Zeit der Vertragsabwicklung hinaus bis zum Ablauf der Verjährungsfrist eventuell möglicher Ansprüche aufbewahrt werden.

Grundsätzlich können auch elektronische Dokumente als Beweismittel in ein Gerichtsverfahren eingebracht werden. Es ist jedoch möglich, dass die Echtheit des Dokuments von der Gegenseite bestritten wird. Eine Beweiserleichterung gibt es dann, wenn das Dokument mit einer sog. qualifizierten elektronischen Signatur versehen ist. In diesem Fall muss die Gegenseite Tatsachen vortragen, die ernsthafte Zweifel daran begründen, dass die Erklärung mit dem Willen des Signaturschlüssel-Inhabers abgegeben worden ist.

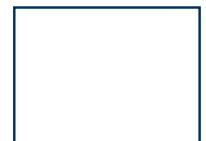
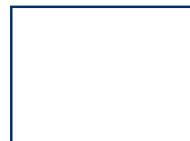
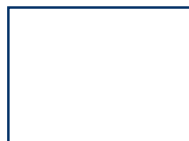
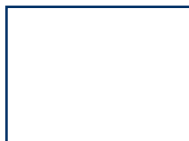
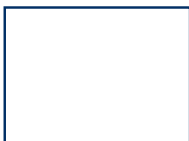
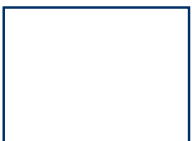
Fallstudie 3 - Was kostet die Aufbewahrung von Daten?

Ein US Unternehmen löschte automatisch sämtliche E-mails, die älter als 60 Tage waren, obwohl die Gesellschaft in ein Gerichtsverfahren involviert war. Im Gerichtsprozess verhängte der Richter eine Geldbuße von US\$ 2.750.000 und verweigerte die Vernehmung eines Schlüsselzeugen, da das Unternehmen es versäumt hatte für den Prozess relevante elektronische Dokumente aufzubewahren.

Vernichtung von Dokumenten

Grundsätzlich kann ein Gericht in einem Rechtsstreit die Vorlage von Dokumenten verlangen. Wird diese Anordnung nicht befolgt und ist das Gericht aber der Auffassung, dass das Unternehmen im Besitz dieser Unterlagen sein sollte, kann es diesen Umstand zu Lasten des Unternehmens werten. Insofern ist in jedem Fall sicherzustellen, dass Dokumente nicht vor Ablauf der gesetzlichen Aufbewahrungsfristen vernichtet werden.

Soweit ein Unternehmen keine Verpflichtung mehr hat, bestimmte Dokumente aufzubewahren, sollte überprüft werden, ob umgekehrt die Verpflichtung besteht, diese zu vernichten. Beispielsweise sollten Bewerbungsunterlagen grundsätzlich nur für die Dauer des Bewerbungsverfahrens aufbewahrt werden. Etwas anderes gilt, wenn es ein berechtigtes Interesse des Unternehmens an der Aufbewahrung der Unterlagen gibt, z.B. wenn die Bewerbung im Einverständnis beider Parteien in absehbarer Zeit wiederholt werden soll oder wenn der Arbeitgeber wegen der Bewerbung mit einer Rechtsstreitigkeit über die negative Entscheidung des Bewerbers oder eines Dritten rechnen muss. Letzteres könnte zukünftig insbesondere dann eine Rolle spielen, wenn die Antidiskriminierungsrichtlinie in deutsches Recht umgesetzt wird und der Arbeitgeber zukünftig seine Auswahl rechtfertigen muss. Nicht ausreichend ist dagegen das Interesse des Arbeitgebers wegen einer lediglich eventuellen zukünftigen erneuten Bewerbung die Unterlagen des Bewerbers aufzubewahren.



Auch Spezialgesetze können eine Lösungsverpflichtung vorsehen, so verlangt z.B. das Teledienstschutzgesetz, das personenbezogene Daten nach der Beendigung der Nutzung gelöscht werden. An die Stelle der Löschung tritt die Sperrung, wenn gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen dagegen stehen.

Gibt es keine Pflicht zur Vernichtung, wird sich die Entscheidung vor allem danach ausrichten, wie viel Speicherplatz das Unternehmen zur Verfügung hat und wie wahrscheinlich es ist, dass die Dokumente noch gebraucht werden. Die im Rahmen des Entwurfs einer Richtlinie für das Dokumentenmanagement vorzunehmende Abwägung zwischen Vernichten und Aufbewahren ist letztlich eine Managemententscheidung, die im Rahmen des ohnehin erforderlichen Risiko-Managements zu erfolgen hat.

Generell empfiehlt es sich, dass jedes Unternehmen bzw. jede Abteilung eine bestimmte Person benennt, die für die Implementierung der Richtlinie zum Dokumentenmanagement verantwortlich ist. Dabei sollten die Verantwortlichen ermuntert werden, ihr Wissen und ihre Erfahrung untereinander auszutauschen.

In jedem Fall sollte die Methode der Vernichtung von Unterlagen die Sensitivität der Informationen berücksichtigen. So können elektronische Daten gelöscht, überschrieben oder unlesbar gemacht werden. Insbesondere ist es wichtig, dass bei sensiblen personen- oder unternehmensbezogenen sämtliche Datenspuren gelöscht werden.

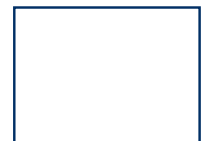
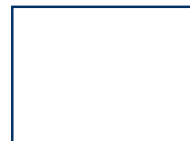
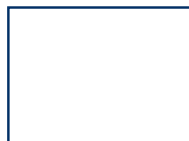
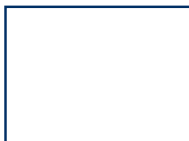
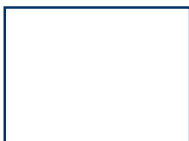
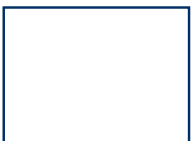
Fallstudie 4 - Was sagt Dein Computer über Dich?

In einer kürzlich durchgeführten Untersuchung haben Wissenschaftler auf gebrauchten Computern Unternehmensdaten und sensible personenbezogene Daten gefunden. Man hatte versäumt, diese vor dem Verkauf zu entfernen. Die ehemaligen Eigentümer der Geräte waren in 50% der Fälle identifizierbar. 20% der Geräte enthielten bankrelevante Daten. Lediglich in zwei von neunzig Fällen waren überhaupt keine Daten auf der Festplatte enthalten, eine davon war neu.

Über Bird & Bird

Bird & Bird ist eine internationale Wirtschaftskanzlei, die rechtliche Expertise mit einer vertieften Branchenkenntnis in den folgenden Schlüsselindustrien kombiniert: Informationstechnologie, E-commerce, Telekommunikation, Life Science, Medien, Sport, Luftverkehr, Banken- und Finanzdienstleistungen. Wir sind stolz darauf, dass wir mit einigen der innovativsten und technologisch führenden Unternehmen zusammenarbeiten, die auf topaktuellen Rechtsrat vertrauen, um ihre Geschäftsziele zu erreichen.

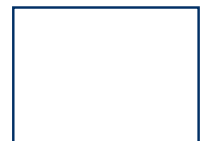
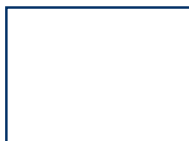
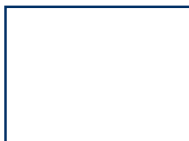
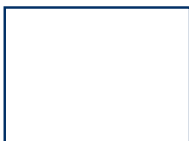
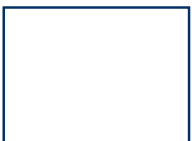
Mit unseren Büros in Europa, Hongkong und China sowie engen Kontakten zu führenden Rechtsanwaltskanzleien im Rest der Welt, sind wir in der Lage unseren Mandanten Rechtsrat in globalem Zusammenhang anzubieten. Anwälte aus jedem unserer Büros arbeiten zusammen, um dem Mandanten einen auf seine Bedürfnisse zugeschnittenen, nahtlosen und internationalen Service zu bieten. In allen unseren Büros haben wir lokale Anwälte, die einen ausgezeichneten Einblick in die Marktkultur und -konditionen haben, gepaart mit einem vertieften Verständnis der Branche sowie des jeweiligen Rechtsgebiets in dem sie arbeiten.

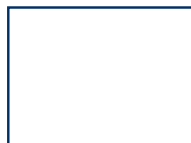
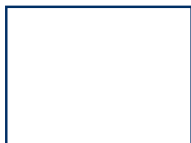
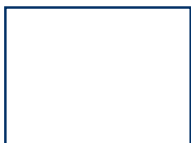
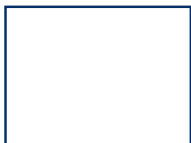
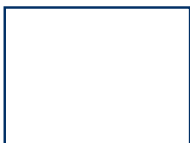
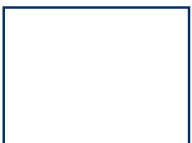


Über VERITAS Software

VERITAS Software, eines der zehn größten Softwareunternehmen der Welt, ist ein führender Anbieter von Software und Services zur Ermöglichung von Utility Computing. In einem Utility Computing-Modell werden IT Ressourcen auf den Geschäftsbedarf angepasst und es werden Geschäftsapplikationen mit optimaler Leistung und Verfügbarkeit geliefert. Dies zusätzlich zu einer sog. shared IT-Infrastruktur, welche Hardware und Arbeitskosten minimiert. Mit einem Umsatz von 2.04 Milliarden US-Dollar in 2004 liefert VERITAS Produkte und Services für die Bereiche Datenschutz, Speicher & Server Management, Hochverfügbarkeit und Applikationsperformance-Management, welche von 99 Prozent der Fortune 500 genutzt werden.

Mehr Informationen über VERITAS Software finden Sie unter www.veritas.com.





BIRD & BIRD

www.twobirds.com

Beijing

3614, China World Trade
Centre, Tower 1
1 Jianguomenwai Dajie
Chaoyang District
Beijing 100004
PRC
Tel: +86 10 6505 6667
Fax: +86 10 6505 9469

Brussels

Avenue d'Auderghem 22-28
1040 Brussels
Belgium
Tel: +32 (0)2 282 6000
Fax: +32 (0)2 282 6011

Düsseldorf

Karl-Theodor-Strasse 6
D 40213 Düsseldorf
Germany
Tel: +49 (0)211 2005 6000
Fax: +49 (0)211 2005 6011

The Hague

Parkstraat 31
2514 JD The Hague
P.O. Box 30311
2500 GH The Hague
The Netherlands
Tel: +31 (0)70 353 8800
Fax: +31 (0)70 353 8811

Hong Kong

6/F ICBC Tower
Citibank Plaza
3 Garden Road
Hong Kong
Tel: +852 2248 6000
Fax: +852 2248 6011

London

90 Fetter Lane
London
EC4A 1JP
UK
Tel: +44 (0)20 7415 6000
Fax: +44 (0)20 7415 6111

Milan

Via Montenapoleone, 10
20121 Milan
Italy
Tel: +39 02 30 35 6000
Fax: +39 02 30 35 6011

Munich

Pacellistrasse 14
80333 Munich
Germany
Tel: +49 (0)89 3581 6000
Fax: +49 (0)89 3581 6011

Paris

Centre d'Affaires
Edouard VII
3 square Edouard VII
75009 Paris
France
Tel: +33 (0)1 42 68 6000
Fax: +33 (0)1 42 68 6011

Stockholm

Norrandsgatan 15
Box 7714
SE-103 95 Stockholm
Sweden
Tel: +46 (0)8 506 320 00
Fax: +46 (0)8 506 320 90
