

# *Compliance*

## *Ein PROJECT CONSULT Whitepaper*

Der Begriff Compliance sorgt bei vielen Anwendern für Verunsicherung. Zahlreiche Anbieter vermarkten inzwischen Ihre Produkte unter dem Etikett „Compliance“ – nicht nur herkömmliche Anbieter von DMS- und ECM-Lösungen, sondern auch Hersteller von Speichersystemen, Management-Informationen-Programmen und ERP-Lösungen. Mit dem Begriff Compliance hat sich zugleich ein neues Marktsegment gebildet. In Deutschland wird der englische Begriff Compliance bisher nur selten verwendet. Rechtliche und regulative Vorgaben für Dokumentationspflichten nehmen aber, wenn man an Beispiele wie die GDPdU oder Basel II denkt, stetig zu. Es liegt also am Kunden, sich zwischen spezialisierten Insellösungen zur Erfüllung bestimmter Compliance-Anforderungen oder übergreifenden Lösungen, die auch Compliance-Anforderungen mit abdecken, zu entscheiden.

Das Whitepaper bietet einen Überblick über Hintergründe und notwendige Maßnahmen zur Erfüllung der zunehmenden Compliance-Anforderungen.

### Inhaltsverzeichnis

<i>Was verbirgt sich hinter dem Begriff Compliance</i>	3
<i>Die USA: Ursprung des Compliance-Trends</i>	4
<i>Europa</i>	6
<i>Gibt es Compliance auch in Deutschland?</i>	6
<i>Compliance-Anforderungen treiben den Markt für Dokumenten-Technologien</i>	8
<i>Information Compliance Policy</i>	10
<i>Anforderungen an ein elektronisches Archivsystem</i>	11
<i>Speichertechnologien für die Archivierung</i>	12
<i>10 Compliance-Merksätze</i>	14
<i>Documentum</i>	15





Die Information des Whitepapers wurde mit größter Sorgfalt erarbeitet. Dennoch können Fehler nicht vollständig ausgeschlossen werden. Die Autoren übernehmen keine juristische Verantwortung oder Haftung für eventuell verbliebene Angaben und deren Folgen.

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Autors unzulässig und strafbar. Alle Rechte, wie Vervielfältigung, Übersetzung, Mikroverfilmung sowie digitale Einspeicherung, Verarbeitung und Verbreitung sind dem Autor vorbehalten.

#### **Autorenrecht und CopyRight**

Autor: Dr. Ulrich Kampffmeyer  
PROJECT CONSULT Unternehmensberatung GmbH  
Breitenfelder Str. 17  
D-20251 Hamburg  
Tel.: 040 / 460 762 20  
Fax: 040 / 460 762 29  
E-Mail: [Presse@PROJECT-CONSULT.com](mailto:Presse@PROJECT-CONSULT.com)  
Web: [www.PROJECT-CONSULT.com](http://www.PROJECT-CONSULT.com)

© PROJECT CONSULT Unternehmensberatung GmbH 2004. Alle Rechte vorbehalten

© Documentum GmbH 2004. Alle Rechte vorbehalten

Der gesamte Inhalt ist, sofern nicht gesondert zitiert, ein Originaltext des Autors. Jeglicher Abdruck, auch auszugsweise oder als Zitat in anderen Veröffentlichungen, ist durch den Autor vorab zu genehmigen. Die Verwendung von Texten, Textteilen, grafischen oder bildlichen Elementen ohne Kenntlichmachung der Autorenschaft ist ein Verstoß gegen geltendes Urheberrecht. Belegexemplare, auch bei auszugsweiser Veröffentlichung oder Zitierung, sind unaufgefordert einzureichen.



# ***Was verbirgt sich hinter dem Begriff Compliance***

Zu den häufig, zumindest für deutsche Ohren, schwer verständlichen Begriffen aus den USA muss auch der Begriff „Compliance“ gezählt werden. Ein einzelnes Wort reicht bei der Übersetzung nicht aus, man benötigt schon einen ganzen Satz:

## ***Übereinstimmung mit und Erfüllung von rechtlichen und regulativen Vorgaben.***

Auch wenn es Compliance-Anforderungen schon immer, auch im Ursprungsland des Begriffes, den USA, gab, so haben sie nach den Skandalen um ENRON und WorldCom eine brisante Qualität erhalten: neue, strafbewehrte Anforderungen zur Aufbewahrung geschäftsrelevanter elektronischer Informationen. In der Vergangenheit gab es schon immer eine Reihe von rechtlichen Anforderungen; so mussten z.B. Finanzbuchhaltungssoftware schon immer Compliance-Standards erfüllen. Mit dem steigendem Aufkommen und der wachsenden Bedeutung von E-Mails und E-Commerce gewann die Notwendigkeit der Dokumentation und elektronischen Archivierung von Geschäftsvorgängen immer mehr Bedeutung.

Betrachtet man die einzelnen Begriffe der deutschen Übertragung der Definition von Compliance „Übereinstimmung mit und Erfüllung von rechtlichen und regulativen Vorgaben“, dann werden unterschiedliche Aspekte von Compliance-Anforderungen deutlich.

- **„Übereinstimmung“**  
Zur Erreichung der „Übereinstimmung“ wird vorausgesetzt, dass es nachlesbare, definierte, offizielle Vorgaben gibt, die die Regeln enthalten, was zu tun ist. Hier ist „Übereinstimmung“ gefordert, ohne dass die Regeln meistens eine technische Vorgabe enthalten, wie die Anforderung umzusetzen ist. Dies ist auch sinnvoll, da sich solche Vorgaben nicht an einer Technologie festmachen sollten, die in ein paar Jahren schon wieder obsolet ist.  
Die Übereinstimmung ist der „statische Aspekt“ von Compliance.
- **„Erfüllung“**  
Der Begriff „Erfüllung“ impliziert zweierlei: Einmal, dass die Anforderungen in einer Lösung umgesetzt werden müssen, und zum Zweiten, dass dies ein Prozess ist, keine einmalige Aktion. Das Unternehmen oder die Organisation muss kontinuierlich für die Einhaltung der Vorgaben Sorge tragen. „Erfüllung“ geht dabei meistens über eine rein technische Lösung hinaus und beinhaltet auch organisatorische und Management-Aspekte.  
Die kontinuierliche Erfüllung ist der „dynamische Aspekt“ von Compliance.
- **„Rechtliche Vorgaben“**  
Hierbei handelt es sich um Gesetze oder behördliche Verordnungen, die bestimmte Unternehmen, Organisationen oder Personen verpflichten, die jeweils aufgeführten Regelungen einzuhalten. Hier kann man sich auch nicht um die Erfüllung „drücken“, lediglich in Hinblick auf Auslegung, Umfang und Umsetzungsweise besteht Handlungsspielraum.
- **„Regulative Vorgaben“**  
Warum unterscheidet man hier noch zwischen „rechtlich“ und „regulativ“? Es gibt eine Reihe von Vorgaben, die sich nicht auf Gesetze berufen wie z.B. Normen, Standards, Codes of Best Practice von Branchen oder andere Vorgaben. Vielfach ergeben sich aus gesetzlichen Vorgaben für einen Anwendungsfall auch Auswirkungen und implizite Anforderungen für andere Fälle. Diese werden als „regulative Vorgaben“ abgegrenzt.

Der bindende Charakter einer Vorgabe kann also sehr unterschiedlich sein. Steckdosen, Lebensmittel, Flugzeuge, elektrische Geräte, Medikamente, Kindergärten, Bildschirme usw. müssen auch bestimmte Compliance-Anforderungen erfüllen, die sich beispielsweise in Prüfsiegeln wieder finden. Ein Vergleich dieser Anforderungen mit dem, was heute unter dem Schlagwort „Compliance“ bei informationstechnologischen Lösungen verstanden wird, zeigt aber große Unterschiede. Daher scheint es sinnvoller, in diesem Fall konkreter von „Information Management Compliance“ zu sprechen.



## Die USA: Ursprung des Compliance-Trends

In den USA gab es schon sehr lange Compliance-Anforderungen an Softwaresysteme. So ist die FDA Federal Drug Administration, mit ihren bindenden Regularien für die Herstellung von Lebensmitteln, Pharmazeutika und Medikamenten auch über die Grenzen der Vereinigten Staaten bekannt. Bei der Beantragung eines neuen Medikamentes, mit Vorlage von allen Testnachweisen und Produktionsverfahren, hat sich die Anschaffung eines Dokumentenmanagementsystems meistens bereits gelohnt.

### Sarbanes-Oxley-Act

Das Gesetz findet Anwendung für alle Unternehmen, die an der New York Stock Exchange gelistet sind.

SOA hat die Aufgabe, die Transparenz und Nachvollziehbarkeit in den Unternehmen bei Prüfungen durch die SEC, Securities and Exchange Commission, zu verbessern. Unternehmen werden verpflichtet, u. a. ein internes Kontrollsystem für die Rechnungslegung zu unterhalten, die Wirksamkeit der Systeme zu beurteilen und die Richtigkeit der Jahres- und Quartalsberichte beglaubigen zu lassen.

Quelle: Sarbanes-Oxley Act of 2002 (H.R.3763)

Durch die Skandale um ENRON, WorldCom und einige andere Unternehmen, die unter Zurücklassung von zahllosen Arbeitslosen und riesigen Schulden insolvent wurden, rückte das Thema Compliance in den Mittelpunkt des allgemeinen Interesses. Anlass waren „geschönte“ Prüfungen von Wirtschaftsprüfern und die Geschäftsberichte der Unternehmen. E-Mail wurde dabei als eine der möglichen Nachweisquellen für ungesetzliches Handeln entdeckt. Dies führte im Jahr 2002 zum Sarbanes-Oxley-Act, allgemein SOA oder SOX abgekürzt. Typisch amerikanisch wurde es nach den beiden Leitern der Kommission benannt, die das Gesetz entworfen haben. SOA hat die Aufgabe, die Transparenz und Nachvollziehbarkeit in den Unternehmen bei Prüfungen durch die SEC, Securities and Exchange Commission, zu verbessern. Äquivalent wären in Deutschland die Steuerbehörden mit Steuerprüfung und Steuerfahndung.

### **SOA ist nur die groß gedruckte Hauptaufschrift auf dem Compliance-Banner**

SOA hat in den USA besonders auf Grund von Abschnitt 802 Bedeutung erlangt, weil hier empfindliche Strafen in der Strafgesetzgebung verankert worden sind. Die Zerstörung oder Veränderung von aufbewahrungspflichtigen Unterlagen kann mit bis zu 20 Jahren Gefängnis bestraft werden. Dieser Abschnitt schreckte alle amerikanischen Unternehmensführer auf und machte den zurzeit zu beobachtenden Boom von Compliance-Lösungen erst möglich. Aber auch besonders die Wirtschaftsprüfer legen in ihrer Beratung nunmehr sehr viel Wert auf Compliance, da im Rahmen der Skandale große, namhafte Wirtschaftsberatungsfirmen wie Andersen vom Markt verschwanden.

SOA besitzt eine erhebliche Bedeutung für Unternehmen mit amerikanischer Muttergesellschaft oder mit Niederlassungen in den USA, da auch Unterlagen und Daten außerhalb der USA einer Nachweispflicht nach amerikanischem Recht und einem möglichen Zugriff amerikanischer Behörden unterliegen können. Für US-Firmen wird der SOA am 15. 11.2004 verbindlich.



### Dave DeWalt

President  
Documentum & LEGATO

Executive Vice President  
EMC Software Group

*"CIOs continue to name compliance as a top reason for selecting and implementing enterprise content management solutions, as almost every company must address some form of legislation, regulation or requirement around data security - postponement is not an option as it can result in product delays, stiff penalties and even risk of shut down."*

### CFR 17

#### Code of Federal Regulations

CFR 17, § 240 beinhaltet harte Regularien für Börsenmakler.

Hieraus leiten sich Dokumentationsanforderungen für alle prüfungsrelevanten Daten und Dokumente ab.

Quelle: Code of Federal Regulations

Es ist aber nicht allein SOA, der den Druck im Umfeld der Steuerprüfung und Steuerfahndung erhöht. Aus den CFR Code of Federal Regulations lassen sich inzwischen eine Vielzahl weiterer Anforderungen für spezielle Branchen und Geschäftstätigkeiten ableiten. Ein Beispiel ist der CFR 17, § 240, mit harten Regularien für Börsenmakler. Die Regeln der US-Börsenaufsicht für Aktien-Broker SEC 17A-3 und SEC 17A-4 definieren exakt, welche Aufzeichnungen und Belege bei einer Transaktion aufgehoben und auf welchem Medium sie gespeichert werden



müssen. Bislang waren ausschließlich optische Medien mit der so genannten WORM-Funktion (Write Once Read Many) erlaubt. Seit verganginem Jahr akzeptiert die SEC auch magnetische Speichermedien, sofern sie WORM-Verfahren unterstützen. Die Steuerfahndung der SEC hat inzwischen erste harte Maßnahmen in Bezug auf die Einhaltung ergriffen und es wurden bereits Unternehmen zu Geldstrafen verurteilt, weil sie ihre elektronische Dokumentation nicht in Ordnung gehalten hatten. Ähnliche Regeln für die Finanzwelt hat die National Association of Securities Dealers (NASD) entwickelt. NASD 3010 und NASD 3110 beispielsweise verlangen, dass Broker und Händler externe Transaktionen von registrierten Stellvertretern überwachen.

#### FDA 21 CFR Part 11

##### Food and Drug Administration

Seit dem 20.03.1997 ist in den USA die elektronische Datenverwaltung und die Benutzung elektronischer Unterschriften in Datenüberwachungs- und Steuerungssoftware in bestimmten Industriezweigen gesetzlich geregelt. Dieses Gesetz ist auch auf Maschinen, die in die USA exportiert werden, anzuwenden.

Eine grundsätzliche Forderung der FDA ist, dass elektronische Aufzeichnungen äquivalent zu Papieraufzeichnungen sind und elektronische Unterschriften die gleiche Aussagekraft und Eindeutigkeit wie handgeschriebene Unterschriften haben.

Quelle: Federal Register Part II, 21 CFR Part 11.

Regelungen, die weltweit alle Pharma-Hersteller betreffen, sind die FDA-Kriterien, auch abgekürzt unter FDA Part 11 bekannt. Um Herstellungsmethoden zu standardisieren hat die FDA ein Regelwerk mit der Bezeichnung CGMP herausgebracht. Die Current Good Manufacturing Practices sollen dafür sorgen, dass beispielsweise Laborergebnisse nicht mehr nachträglich verändert werden können. Sie regeln auch die Audit- und Zertifizierungsverfahren für Bestandteile, Produkte, Maschinen und ganze Fertigungsstätten im Umfeld der Lebensmittel- und Medikamentenherstellung. Ohne eine entsprechende Zulassung kann ein Produkt quasi nicht vertrieben werden. Der Einsatz von Dokumenten-

management-Lösungen für die Anmeldung von neuen Medikamenten ist auch deshalb essentiell wichtig für die Unternehmen, da er das Verfahren kontrollierbar macht, beschleunigt und so schneller Produkte an den Markt bringt.

In anderen Bereichen gibt es ebenfalls rechtliche und regulative Vorgaben. Besondere Aufmerksamkeit verdient z.B. HIPAA. HIPAA zieht sowohl im Krankenhaus- als auch im Versicherungsbereich Investitionen in Milliardenhöhe für Dokumentenmanagementlösungen nach sich. Im Bereich der Fertigungsindustrie macht sich inzwischen der Tread Act mit umfangreichen Anforderungen zur Produkt-, Qualitäts- und Herstellungsdokumentation im Rahmen des Supply Chain Management bemerkbar. Auch die EPA, Environmental Protection Agency, macht mit neuen Dokumentationspflichten auf sich aufmerksam.

Viele dieser Regelwerke beziehen sich auf die neu gefassten FSG, Federal Sentencing Guidelines von 2002, so dass Verstöße mit erheblichen Strafen belegt werden können.

#### HIPAA

##### Health Insurance and Accountability Act.

HIPAA (Gesetz zur Krankenversicherungsübertragbarkeit und Verantwortlichkeit) von 1996 wurde eingeführt, um die Gesundheitspflege-Industrie zu reformieren.

Die Gesetzgebung strebt nach größerer Wirtschaftlichkeit, Verringerung von Schreibearbeiten und einfacher Identifizierung und Weiterverfolgung von Betrug durch die Auferlegung von unterschiedlichen Normen und Sicherheitsmaßnahmen gegen den Missbrauch von gesundheitsbezogenen Angaben des Bürgers.

Bei den Regeln handelt es sich besonders um Normen der Adress-Transaktion, Code-Sets, Vertraulichkeit und Sicherheit.

Quelle: Health Insurance Portability and Accountability Act of 1996

#### DoD 5015.2

Der DoD 5015.2 Standard des Departement of Defense definiert die grundsätzlichen rechtlichen Anforderungen an DM-Systeme.

Die Einhaltung der Standards ist für alle Hersteller erforderlich, die für die Bundesverwaltung in den USA im militärischen und angrenzenden Bereich anbieten wollen.

Quelle: DoD 5015.2-STD, June 19, 2002

Zu den regulativen Vorgaben gehört in den USA z.B. die Richtlinie des Department of Defense, DoD 5015.2. Hierbei handelt es sich um eine Vorgabe für die Anbieter von Dokumentenmanagement-Lösungen. Produkte ohne eine DOD 5015.2 Compliance haben kaum eine Chance im öffentlichen Sektor in den USA platziert zu werden. Auch andere Gesetze wie der Patriot Act ziehen inzwischen Dokumentationspflichten nach sich. Ein Ende der Flut von Regularien ist nicht abzusehen. Und man darf eines nicht übersehen: Die

Regularien für die elektronische Bereitstellung und Dokumentation von Informationen sind unerlässlich, weil immer mehr Information originär elektronisch entsteht und sich nicht mehr in Papier niederschlägt.

Man kann es in einem Satz fassen: Ohne Information Management Compliance kann die Informationsgesellschaft nicht funktionieren.



## Europa

In den Mitgliedstaaten der europäischen Union muss jede Richtlinie der Europäischen Kommission früher oder später in nationales Recht überführt werden. Mittlerweile haben viele der neuen nationalen Vorgaben in Europa ihren Ursprung in der europäischen Gesetzgebung, für zukünftige Entwicklungen ist ein Blick auf die Entwicklungen und Richtlinien in Brüssel daher immer lohnend. Bereits durch die Richtlinien zum E-Commerce und zur elektronischen Signatur sind eine Reihe von Anforderungen für Compliance in Deutschland entstanden. Erinnerung sei hier nur an die elektronische Rechnung, die nur zum Vorsteuerabzug berechtigt, wenn sie qualifiziert elektronisch signiert wurde. Auch eine europäische Variante von SOA wird sich kaum vermeiden lassen.

Der elektronische Geschäftsverkehr und die Umstellung der öffentlichen Verwaltung auf elektronisch unterstützte Verfahren wird weitere Compliance-Anforderungen nach sich ziehen. Auch deshalb ist es wichtig, nicht nur auf eine Einzellösung für ein bestimmtes Problem zu schauen, sondern eine IT-Strategie zu entwickeln, die mit einer Lösung möglichst viele Compliance-Anforderungen erfüllt und darüber hinaus für das Unternehmen auch im Geschäftsbetrieb nutzbringend eingesetzt werden kann.

### Europäische Richtlinien

- **E-Commerce**

E-Commerce-Richtlinie der EU die genau festgelegt, was im elektronischen Geschäftsverkehr erlaubt und verboten ist.

Quelle: E-Commerce-Richtlinie, 2000/31/EG

- **E-Signatur**

Europäische Richtlinie (RLeS) zur elektronischen Signatur. Der Einsatz der elektronischen Signatur ersetzt unter bestimmten Voraussetzungen das Papier. Die elektronische Signatur ist daher Bestandteil zahlreicher Compliance-Regelungen.

Quelle: RLeS, 99/93/EG

### Basel II

Mit „Basel II“ wird die Neugestaltung der Eigenkapitalvorschriften der Kreditinstitute bezeichnet.

Ziel von "Basel II" ist es, die Stabilität des internationalen Finanzsystems zu erhöhen. Dazu sollen die Risiken im Kreditgeschäft besser erfasst und die Eigenkapitalvorsorge der Kreditinstitute risikogerechter ausgestaltet werden.

Quelle: Eigenkapitalempfehlung für Kreditinstitute (Basel II)

Als gutes Beispiel für direkte und indirekte Auswirkungen der Gesetzgebung kann Basel II angeführt werden. Finanzdienstleister müssen umso mehr Eigenkapital vorhalten, je höher das Risiko des Kreditnehmers ist. Auch wenn man in Bezug auf die Kreditvergabe und die Dokumentationspflichten hier zunächst nur an die Banken denkt, hat Basel II auch erhebliche Auswirkungen auf alle Unternehmen. Kaum ein Unternehmen kommt ohne Kredite der Banken aus. Da sich die Kreditnehmer einem Rating unterziehen müssen, schlagen die Transparenzanforderungen von Basel II praktisch auf die Unternehmen durch. Wenn ein Unternehmen also einen Kredit haben will, sollte es Geschäftsdokumente und alle Informationen, die für die Kreditvergabe

relevant sein können, gesichert abgelegt haben. Ohne die Vorhaltbarkeit der geforderten Dokumente setzen sich Unternehmen dem Risiko aus, einen Kredit nicht zu erhalten. Um einen Kredit überhaupt noch oder zu günstigen Konditionen zu erhalten, müssen sich die Unternehmen neu aufstellen.

Hinter Schlagworten wie Corporate Governance, Enterprise Information Policy oder Records Management Policy und Projekten zur Erarbeitung und Einführung solcher Regelwerke verbergen sich auch viele Ansätze zur Lösung von Compliance-Anforderungen.

## Gibt es Compliance auch in Deutschland?

In Deutschland wird der Begriff „Compliance“ zwar noch selten verwendet, folgende Beispiele sollen aber verdeutlichen, dass es vergleichbare Anforderungen schon längst gibt.

Die GDPdU Grundsätze des Datenzugriffs und der Prüfbarkeit digitaler Unterlagen sind ein typisches Beispiel für Compliance-Vorgaben. Zwar sind die GDPdU noch nicht strafbewehrt wie SOA, aber durchaus mit anderen Anforderungen des SEC in den USA vergleichbar. Die Bereithaltung von steuerlich relevanten Daten in auswertbarer Form ist eine Pflichtvorgabe, die alle Unternehmen in Deutschland erfüllen müssen.

<b>GDPDU</b>
<p><b>Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen</b></p> <p>Es handelt sich um bundesweit gültige Vorschriften zur Sicherstellung des Zugriffs der Finanzverwaltung im Rahmen von Außenprüfungen auf die steuerrelevanten DV-Daten eines Unternehmens. Dabei sind ein direkter (Z1) und indirekter Zugriff (Z2) sowie die Datenträgerüberlassung (Z3) vorgesehen.</p> <p>Die Daten müssen entsprechend den Aufbewahrungsfristen bis zu 10 Jahre auswertbar vorgehalten werden.</p> <p>Quelle: BStBl. 2001 I S. 415</p>

Die GDPdU selbst sind eine Verordnung, die auf den Änderungen im Steueränderungsgesetz und HGB Abgabenordnung, §§ 146, 147 und 200, basiert. Sie stellen eine Richtlinie für das Vorgehen der Finanzbehörden bei Außenprüfungen dar. Die Unternehmen müssen sicherstellen, dass alle steuerrelevanten Daten identifiziert, unverändert und vollständig und über einen Zeitraum von 10 Jahren aufbewahrt werden. Entscheidend dabei ist, dass die Daten auswertbar vorgehalten werden müssen. Die originalen Daten müssen vollständig, richtig und auswertbar entweder in den sie erzeugenden Systemen vorgehalten oder aber in elektronische Archive ausgelagert werden. Auch bei den GDPdU spielen inzwischen Dokumente und E-Mails neben den Daten aus ERP- und Buchhaltungssystemen eine zunehmend wichtigere Rolle.

In eine ähnliche Kerbe wie die GDPdU schlägt auch das Gesetz zu den Dokumentationspflichten bei Verrechnungspreisen, das anders als die GDPdU bereits direkt strafbewehrt ist. Auch hier ist es das Ziel, den Nachweis einer ordnungsgemäßen, nachvollziehbaren und prüfbareren Dokumentation aller steuerrelevanten Daten zu ermöglichen.

Die Vorgaben für die Anforderungen wie die Nachvollziehbarkeit, die Ordnungsmäßigkeit oder die Prüfbarkeit bestehen schon seit langem und sind im Handelsgesetzbuch §§ 239 und 257 nachzulesen. Die Anforderungen, die sich ursprünglich an einer papiergebundenen Dokumentation orientierten, sind in die elektronische Welt zu übertragen und dort gleichermaßen anzuwenden.

<b>Verrechnungspreisdokumentation</b>
<p>Verordnung zu Art, Inhalt und Umfang von Aufzeichnungen im Sinne des §90 Abs. 3 der Abgabenordnung (AO).</p> <p>Sie legt fest, welche Unterlagen und Dokumentationen zu erstellen sind, wenn Leistungen mit "nahe stehenden Personen und Unternehmen" verrechnet werden.</p> <p>Inhalt, Art und Umfang der Dokumentationspflichten werden durch eine Rechtsverordnung (GAufzV) näher bestimmt, die mit Rückwirkung zum 30. Juni 2003 in Kraft getreten ist.</p> <p>Quelle: StVergAbG §90 Abs. 3 AO</p>

<b>GOBS</b>
<p><b>Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme</b></p> <p>Bei den GoBS handelt es sich um eine Verordnung mit bundesweiter Gesetzeskraft.</p> <p>Sie schreiben bei elektronischer Buchführung die Dokumentation betroffener Geschäftsvorfälle und des Gesamtsystems vor. In den GoBS sind die Grundsätze für das interne Sicherheitssystem, die revisionssichere Archivierung und die Verfahrensdokumentation festgelegt.</p> <p>Handels- und Steuerrecht fordern die Einhaltung der GoBS ein.</p> <p>Quelle: BStBl 1995 I S. 738</p>

Aber auch bereits vor den GDPdU gab es verbindliche Vorgaben. Es sei hier nur an die GoBS erinnert, die die Aufbewahrung von kaufmännischen Unterlagen in elektronischer Form regelt. Neben sicheren Systemen wird hier auf die Prozesse und die Verfahrensdokumentation besonderes Augenmerk gelegt.

Bei diesen Vorgaben geht es aber nicht darum, die Unternehmen mit bürokratischen Auflagen zu behindern, sondern die Voraussetzungen für E-Commerce und E-Business und eine effektive elektronische Informationsverwaltung zu schaffen.

In diesem Umfeld kommt der elektronischen Signatur eine besondere Bedeutung zu. Der Einsatz der elektronischen Signatur findet sich inzwischen in

nahezu allen neueren Gesetzen. So z.B. auch bei der elektronischen Rechnung. Zum Vorsteuerabzug berechtigen den Empfänger nach § 14 Abs. 4 Satz 2 UStG nur elektronisch signierte Rechnungen. Da die elektronische Rechnung das Original darstellt, ist es auch elektronisch aufzubewahren. Hier greifen die verschiedenen neuen Gesetze und Regelungen ineinander. Das Signaturgesetz und die Änderungen von BGB Bürgerlichem Gesetzbuch und ZPO Zivilprozessordnung zur Verankerung der elektronischen Signatur finden ihren Widerhall in der Handels- und Steuergesetzgebung. Die gesamte Gesetzgebung und Rechtsprechung befindet sich auf dem Weg ins Informationszeitalter und zieht damit automatisch immer mehr Compliance-Anforderungen für das Management von Informationen nach sich.

### **Österreich und die Schweiz**

In Österreich sieht die Situation nicht viel anders aus als in Deutschland. Die Unterschiede liegen nur im Detail. Dies ist darauf zurückzuführen, dass die wesentlichen Compliance-Anforderungen auf den europäischen Richtlinien basieren. Auch in Österreich ist analog zum BGB in Deutschland die elektronische Signatur verankert, auch Österreich kennt im



Handelsrecht und in der Abgabenordnung ähnliche Bestimmungen wie in Deutschland. Dies gilt z.B. für die Aufbewahrung von elektronischen Informationen in Bezug auf Vollständigkeit, Inhaltsgleichheit, Geordnetheit und Urschriftstreue. Auch wenn die Bereithaltung von Daten zur steuerlichen Prüfung in Österreich in Listenform ausreichend erscheint, ist die Forderung der Auswertbarkeit die Gleiche. Zur Vermeidung des Umsatzsteuerbetruges finden sich natürlich auch die Regelungen zur elektronischen Rechnung wieder.

Selbst die Schweiz hat als nicht EU-Mitglied inzwischen die wesentlichen Gesetze und Verordnungen an die europäischen Vorgaben schrittweise angeglichen. Dies zeigt sich z.B. im Obligationenrecht in den Bestimmungen über die Buchführung OR Art. 957ff, die die Aufbewahrung von Geschäftskorrespondenz, der Bücher und der Buchungsbelege in elektronischer Form regeln.

Angesichts des Zusammenwachsens der europäischen Union und ihrer Mitgliedsstaaten wird durch den grenzüberschreitenden Geschäftsverkehr und über das Internet abrufbare elektronische Dienstleistungen ein einheitlicher Rechtsraum insbesondere im Handels- und Steuerrecht unerlässlich. Dementsprechend werden sich auch die daraus abgeleiteten Compliance-Anforderungen immer einheitlicher und europaweit ausgreifender gestalten.

## ***Compliance-Anforderungen treiben den Markt für Dokumenten-Technologien***

Anbieter von Dokumentenmanagement-Lösungen wittern, aufgrund der in nahezu allen Staaten steigenden Compliance-Anforderungen, das große Geschäft. Compliance-Angebote sind bei den meisten ECM Enterprise-Content-Management-Anbietern mittlerweile fester Bestandteil des Produktangebotes. Nach aktuellen Marktuntersuchungen ist Compliance in den USA eines der Hauptargumente für neue Investitionen in Informationstechnologie. In Europa ist dies noch nicht so deutlich zu merken.

Bei Umfang und Zielsetzung der angebotenen Software und Systeme sind aber noch Unterschiede zu finden. Die größeren Anbieter setzen auf eine vollständige Kontrolle und Dokumentation des Informationsflusses und beschränken sich nicht nur auf das Thema Archivierung oder Records Management. Andere Anbieter preisen Lösungen für E-Mail-Archivierung an, was für Anwender die Gefahr birgt, auf einer Compliance-Insellösung sitzen zu bleiben. E-Mails und ihre Anhänge gehören in einen fachlichen Zusammenhang, in elektronische Kunden-, Produkt- oder Vorgangsakten. E-Mails separat zu archivieren bringt mittelfristig mehr Probleme denn Vorteile.

Vergleichbar sieht es bei der Erfüllung der Vorgaben der GDPdU aus, wenn Archive nur angeschafft werden, um die steuerrelevanten Daten zu sichern. Hier sollte das Ziel die Einführung von Lösungen sein, die alle Informationen des Unternehmens verwalten und bereithalten – und dabei die Anforderungen der GDPdU so „nebenbei“ erfüllen. Steuerrelevante Daten sind nur ein kleiner Ausschnitt aus allen Daten und ihre Archivierung ist schwer wirtschaftlich zu rechnen, wenn nur der Steuerprüfer alle paar Jahre mal ein paar Daten sehen will.

### **ECM Enterprise Content Management - ein umfassender Ansatz auch für Compliance**

ECM umfasst herkömmliche dokumentenorientierte Informationstechnologien wie Scanning, Dokumentenmanagement, Knowledge Management, Workflow, Archivierung etc. und integriert die Host- und Client/Server-Welt mit Web-Content-Management-, Portal- und anderen Internet-Technologien.

Ziel von ECM ist es, Daten- und Dokumentenredundanz zu vermeiden (jede Information existiert nur einmal), den Zugriff einheitlich zu regeln, unabhängig von Quelle und Nutzung beliebige Informationen bereitzustellen und als Dienst allen Anwendungen gleichförmig zur Verfügung zu stehen. ECM ist eine Basistechnologie von eBusiness zur Bereitstellung der erforderlichen Informationen und Steuerung der Prozesse. ECM umfasst dabei auch diejenigen Technologien, die in Deutschland unter dem Begriff elektronische Archivsysteme subsumiert werden. Nach der Klassifikation der AIIM handelt es

<b>ECM</b>
<b>Enterprise Content Management</b>
Enterprise Content Management sind die Technologien und Methoden zur Erfassung, Verwaltung / Verarbeitung, Bereitstellung, Speicherung und Archivierung von Informationen zur Unterstützung der Geschäftsprozesse im Unternehmen.
Die Komponente Verwaltung/Verarbeitung beinhaltet Document Management, Records Management, Business Process Management / Workflow, Web Content Management und Collaboration.
Quelle: AIIM international 2003



sich bei einem Archivsystem um Anwendungen, die die Komponenten Datenbank, Records Management, Document Management, Store und Preserve umfassen. In Verbindung mit Workflow und durch die Integration in bestehende Anwendungen sind ECM-Systeme einer der wichtigsten Bestandteile einer Compliance-Lösung. Viele ECM-Anbieter kombinieren daher ihre Komponenten, um sie als spezielles „Compliance-Produkt“ anzubieten.

## Records Management – Voraussetzung für viele Compliance-Lösungen

Um alle Informationen in einem Unternehmen, einer Behörde oder einer Organisation effektiv verwalten zu können, ist der Einsatz von RM Records Management Lösungen (auch ERM Electronic Records Management oder EDRM Electronic Document and Records Management) erforderlich. Records Management geht dabei über den Ansatz der elektronischen Archivierung hinaus:

- Records Management Systeme verwalten über Referenzen auch Informationen auf Papier in Aktenordnern oder auf Mikrofilm. Dies ermöglicht die vollständige Kontrolle auch „gemischter“ Verfahren, in denen ein Parallelbetrieb mit unterschiedlichen Medien erforderlich ist.
- Records Management Systeme besitzen elektronische Ablagepläne und Thesauri, die eine strukturierte, geordnete, nachvollziehbare und eindeutige Zuordnung der Informationen sicherstellen. Hierbei werden Mehrfachzuordnungen nach unterschiedlichen Sachzusammenhängen und die Verwaltung unterschiedlicher Versions- und Historienstände der Ordnungssystematik unterstützt.

Records Management ist daher eine Basiskomponente für die Abbildung elektronischer, virtueller Akten und für die elektronische Vorgangsbearbeitung, die auch diejenigen Informationen bereitstellen, die Compliance-Anforderungen unterliegen.

Records Management stellt eine Wissens-Infrastruktur in der elektronischen Ablage bereit. In den 90er Jahren entstanden elektronische Dokumentenmanagement-Systeme mit Ablage nach Abteilungen und einfachen Index-Strukturen, so z.B. Kundenname/Kontonummer, wobei jede Abteilung oder Service-Einheit anders ablegte, beispielsweise nach Produkt/Kunden im Kundendienst, aber nach Region/Kunden/Produkt im Verkauf. Das Records Management gibt einen Rahmen zur Entwicklung einer unternehmensweiten Ablagestruktur.

### ISO 15489

#### Records Management

Die ISO 15489 Records Management stellt Management-Richtlinien zur Unternehmenspolitik und Vorgehensweisen für das Records Management des Unternehmens auf und dient als Anleitung zur Implementierung bei der Einführung von Records Management.

Quelle: PROJECT CONSULT 2000

Die Grundprinzipien des Records Management sind in zahlreichen nationalen Regelungen der öffentlichen Verwaltung und Archive sowie in einer internationalen Norm niedergelegt. Die ISO-Norm 15489 „Records Management“ gibt in Teil 1 Hilfestellungen zum:

- Festlegen, welche Dokumente erzeugt und welche Information in die Dokumente eingefügt werden müssen sowie welcher Genauigkeitsgrad erforderlich ist
- Entscheiden, in welcher Form und Struktur Dokumente erzeugt und erfasst werden sollen
- Festlegen der Anforderungen zum Retrieval und Gebrauch von Dokumenten und wie lange sie archiviert sein müssen, um diesen Anforderungen zu genügen
- Festlegen, wie Dokumente zu organisieren sind, um die Anforderungen für den Gebrauch zu unterstützen.

Die ISO 15489 Teil 2 legt die Schritte für das Vorgehen der Umsetzung fest: Von der ersten Analyse und Identifizierung der Anforderungen bis zur Implementierung eines Records Management Systems und unternehmenspolitischen Maßnahmen.

Auch wenn diese ISO-Norm keine konkreten Kriterien für eine technische Prüfbarkeit von Systemen beinhaltet, ist sie jedoch ein wertvoller Leitfaden, um Information im Unternehmen geordnet und nachvollziehbar zu verwalten. Professionelles Records Management ist damit eine Grundvoraussetzung zur Erfüllung von Compliance-Vorgaben.

### RM

#### Records Management

Elektronisches Records Management sind die Methoden, Verfahren und Anwendungen, die zur geordneten Verwaltung, Erschließung, Bewahrung, Sicherung und Aussonderung von elektronischen Informationen dienen, die Geschäftsvorfälle, Rechtshandlungen und die Einhaltung rechtlicher und regulatorischer Vorgaben vollständig, richtig, authentisch, beweiskräftig und nachvollziehbar dokumentieren.

Quelle: PROJECT CONSULT 2001



## **Information Lifecycle Management – ein neuer Trend zur Erfüllung von Compliance-Anforderungen**

Die Compliance-Anforderungen zogen Verwerfungen im Markt nach sich und kurbelten die Konsolidierung nach einer kurzen Periode der Ruhe wieder an. Inzwischen haben alle Anbieter von Storage-Technologien nachgezogen und mit ILM Information Lifecycle Management auch gleich ein eigenes Etikett etabliert. Die Speichersysteme werden um immer mehr Software ergänzt und dringen damit in die traditionellen Bereiche von Records Management, Archivierung und Dokumentenmanagement vor. Dabei konnte man entweder Unternehmen oder Produkte kaufen, sie selbst entwickeln oder eine Partnerschaft mit den traditionellen Anbietern abschließen. Der Markt für Compliance-Lösungen bot die Chance, aus dem engen, hart umkämpften Hardwaresegment für Speicherlösungen ins Lösungsgeschäft auszubrechen. Da jedes Unternehmen sich zurzeit mit dem Thema Compliance in der einen oder anderen Form auseinandersetzt und die Konsolidierung von IT-Plattformen ebenfalls auf den Wunschlisten der CIOs steht, ist der Zeitpunkt gut gewählt.

### **ILM**

#### **Information Lifecycle Management**

Information Lifecycle Management sind Strategien, Methoden und Anwendungen um Information automatisiert entsprechend ihrem Wert und ihrer Nutzung optimal auf dem jeweils kostengünstigsten Speichermedium bereitzustellen, zu erschließen und langfristig sicher aufzubewahren.

Quelle: PROJECT CONSULT 2003

### **Zertifizierungen für Compliance-Lösungen?**

Dass Anwender sich derzeit immer schwieriger orientieren können, liegt nicht nur an den Anglizismen, den Akronymen und den immer neuen Begriffen. Häufig wissen sie selbst nicht, was sie genau wollen bzw. was sie tun müssen. Zu undurchsichtig sind viele der Vorgaben und die Werbeschlacht der Anbieter irritiert mehr, als sie hilft. So schaut sich der potentielle Kunde gerade im Umfeld von Compliance-Lösungen nach Stempeln, Siegeln und Zertifikaten um, die ihm Sicherheit in seiner Entscheidung geben sollen. Er geht vielfach davon aus, dass Gesetze mit Vorgaben auch überprüft werden, und so die Konformität festgestellt und den Produkten bestätigt wird. Dem ist aber häufig nicht so. Es gibt keine Zertifikate für Produkte wie z.B. von Anbietern für GDPdU-konforme Lösungen suggeriert wird. Eine Lösung kann auch nur im Zusammenhang mit den Prozessen und den eingesetzten Verfahren im Unternehmen selbst geprüft werden. Solche Prüfungen führen z.B. Wirtschaftsprüfer durch. Diese individuellen Prüfungen ermöglichen jedoch keine generelle Aussage, ob ein Produkt an sich auch geeignet ist, denn es muss auch entsprechend den Vorgaben eingesetzt und betrieben werden. Auch wenn es wünschenswert wäre, offizielle Zertifikate auf den Verpackungen der Produkte zu finden, die Komplexität der Lösungen und die Individualität des Einsatzes sprechen dagegen.

So bleibt dem Anwender nur der Rückzug auf Standards, Codes of Best Practice und Richtlinien, wie z.B. das Grundschutzhandbuch des BSI, um zu einer sicheren Lösung zu kommen, die technologisch die Compliance-Anforderungen abdeckt.

Eines darf man aber in keinem Fall vergessen: Compliance ist nicht nur ein Thema für Dokumentenmanagement und Archivierung, Compliance zieht sich durch alle Softwarekomponenten, in denen aufbewahrungspflichtige Daten, Informationen und Dokumente entstehen und verwaltet werden. Deshalb sind auch übergreifende Richtlinien erforderlich, die alle Quellen und alle Formen der Nutzung von Informationen berücksichtigen.

## **Information Compliance Policy**

Basis für die Planung, Durchführung und kontinuierliche Umsetzung von Information Compliance Management (IMC) im Unternehmen ist eine so genannte Information Compliance Policy. Die Inhalte einer solchen Richtlinie und ihrer Umsetzung kann man in vier Punkten zusammenfassen:

### **1. Information Management Policy**

Grundregeln und Verhaltensweisen für den Umgang mit Prozessen und Informationen, die sich in der „Corporate Governance“ niederschlagen. Dies schließt das Bewusstmachen, die Zuordnung der Verantwortung und die Verankerung der Policy im Management der Organisation ein. Das Management trägt hier nicht nur die eigene Verantwortung für die Einhaltung der Regelwerke, sondern auch für die Umsetzung im Unternehmen mit Vorbildfunktion.

2. Delegation  
Zuordnung von Verantwortlichkeiten und entsprechende Ausbildung auf den nachgeordneten Ebenen, die allen Betroffenen die Bedeutung von Compliance-Regeln deutlich macht. Dies schlägt sich auch in den Arbeitsprozessen, Arbeitsplatzbeschreibungen, Verträgen und Arbeitsanweisungen nieder. Auf den verschiedenen Ebenen einer Organisation muss abhängig von Aufgaben und Zuständigkeiten der Mitarbeiter eine Durchgängigkeit erzeugt werden.
3. Nachhaltigkeit  
Die Einhaltung der Regeln muss regelmäßig überprüft werden. Hierzu gehören z.B. Qualitätssicherungsprogramme ebenso wie Audits. Hierbei ist auf eine ständige Verbesserung der Prozesse und auf die Nachführung der Dokumentation zu den durchgeführten Maßnahmen Wert zu legen.
4. Sichere Systeme  
Die IT-Systeme müssen den Anforderungen mit ihrer Funktionalität, Sicherheit und Verfügbarkeit genügen und die Nachvollziehbarkeit unterstützen. Compliance beschränkt sich hier nicht nur auf die Anwendungsfunktionalität und das Dokumentenmanagement, sondern schließt den gesamten Betrieb der Lösung ein.

Obwohl Compliance sehr viel mit Dokumenten und Dokumentation zu tun, gilt es bei den Anforderungen immer in Prozessen zu denken. Das Hauptproblem von Compliance ist dabei, dass die Maßnahmen zunächst einmal viel Geld und organisatorischen Aufwand kosten, ohne dass hierdurch mehr Geschäft generiert wird. Compliance ist daher den meisten ein ungeliebtes Kind. Wenn man aber sein Unternehmen konsequent und strukturiert organisiert, ist durch die Transparenz, die Nachvollziehbarkeit und die integrale Verfügbarkeit von Information ein hoher qualitativer Nutzen gegeben, der sich auf längere Sicht auch betriebswirtschaftlich auszahlt.

## ***Anforderungen an ein elektronisches Archivsystem***

<p><b>Elektronische Archivierung</b></p> <p><b>Langzeitarchivierung &amp; Revisionssichere Archivierung</b></p> <p>Unter elektronischer Langzeitarchivierung versteht man Archivsysteme, die Daten und Dokumente über einen Zeitraum von mindestens 10 Jahren verfügbar halten.</p> <p>Unter revisionssicherer elektronischer Archivierung versteht man Archivsysteme, die nach den Vorgaben von HGB § 239, AO §147 und GoBS Daten und Dokumente sicher, unverändert, vollständig, ordnungsgemäß, verlustfrei reproduzierbar und datenbankgestützt recherchierbar verwalten.</p> <p>Quelle: PROJECT CONSULT 1996</p>
--

Basis für die sichere Aufbewahrung von Information sind meistens elektronische Archivsysteme. Sie sind keineswegs einfach mit hierarchischem Speichermanagement gleichzusetzen, sondern zeichnen sich durch eine Reihe eigenständiger Merkmale aus. Zweck eines elektronischen Archivsystems ist es, unabhängig von Quelle, Erzeuger und späterer Nutzung Information sicher aufzubewahren und datenbankgestützt auf Anforderung wieder bereit zu stellen. Archivsysteme sind daher Dienste, die allen Anwendungen zur Verfügung stehen, die Informationen erzeugen, die langfristig unverändert und sicher aufbewahrt werden müssen.

Elektronische Archivsysteme zeichnen sich durch folgende eigenständige Merkmale aus:

- Programmgestützter, direkter Zugriff auf einzelne Informationsobjekte, landläufig auch Dokumente genannt, oder Informationskollektionen, z.B. Listen, Container mit mehreren Objekten etc.
- Unterstützung verschiedener Indizierungs- und Recherchestrategien, um auf die gesuchte Information direkt zugreifen zu können
- Einheitliche und gemeinsame Speicherung beliebiger Informationsobjekte, vom gescannten Faksimile über Word-Dateien bis hin zu komplexen XML-Strukturen, Listen oder ganzen Datenbankinhalten
- Verwaltung von Speichersystemen mit nur einmal beschreibbaren Medien einschließlich dem Zugriff auf Medien, die sich nicht mehr im Speichersystem direkt befinden
- Sicherstellung der Verfügbarkeit der gespeicherten Informationen über einen längeren Zeitraum, der Jahrzehnte betragen kann



- Bereitstellung von Informationsobjekten, unabhängig von der sie ursprünglich erzeugenden Anwendung auf verschiedenen Clients und mit Übergabe an andere Programme
- Unterstützung von „Klassen-Konzepten“ zur Vereinfachung der Erfassung durch Vererbung von Merkmalen und Strukturierung der Informationsbasis
- Konverter zur Erzeugung von langfristig stabilen Archivformaten und Viewer zur Anzeige von Informationsobjekten, für die die ursprünglich erzeugende Anwendung nicht mehr zur Verfügung steht
- Absicherung der gespeicherten Informationsobjekte gegen unberechtigten Zugriff und gegen Veränderbarkeit der gespeicherten Information
- Übergreifende Verwaltung unterschiedlicher Speichersysteme, um z.B. durch Zwischenspeicher (Caches) schnellen Zugriff und zügige Bereitstellung der Informationen zu gewährleisten
- Standardisierte Schnittstellen, um elektronische Archive als Dienste in beliebige Anwendungen integrieren zu können
- Eigenständige Wiederherstellungsfunktionalität (Recovery), um inkonsistent gewordene oder gestörte Systeme aus sich heraus verlustfrei wieder aufbauen zu können
- Sichere Protokollierung von allen Veränderungen an Strukturen und Informationsobjekten, die die Konsistenz und Wiederauffindbarkeit gefährden können und dokumentieren, wie die Informationen im Archivsystem verarbeitet wurden
- Unterstützung von Standards für die spezielle Aufzeichnung von Informationen auf Speichern mit WORM-Verfahren, für gespeicherte Dokumente und für die Informationsobjekte beschreibende Meta-Daten, um eine langfristige Verfügbarkeit und die Migrationssicherheit zu gewährleisten

All diese Eigenschaften sollten deutlich machen, dass es nicht um hierarchisches Speichermanagement oder herkömmliche Datensicherung geht. Elektronische Archivsysteme sind eine Klasse für sich, die als nachgeordnete Dienste heute in jede IT-Infrastruktur gehören.

## ***Speichertechnologien für die Archivierung***

Eine wesentliche Komponente von Archiv- und Compliance-Lösungen sind die Speichersysteme zur sicheren Aufbewahrung der Daten und Dokumente. Bei den Speichertechnologien muss man heute eine Trennung zwischen der Verwaltungs- und Ansteuerungssoftware einerseits und den eigentlichen Medien andererseits machen. Die Kombination unterschiedlicher Speichertechnologien für die kostengünstige und effiziente Verwaltung von Informationen ist ein wesentliches Merkmal des ILM Information Lifecycle Management Konzeptes.

Für die unveränderbare Langzeitarchivierung wurden Speichertechnologien geschaffen, die nur das einmalige Beschreiben erlauben. Dieses Verfahren nennt man WORM: „Write Once, Read Many“. Ursprünglich wurde dieser Begriff nur für digital-optische Speichertechnologien verwendet. Die Speichermedien selbst waren dabei durch ihre physikalischen Eigenschaften gegen Veränderungen geschützt und boten eine wesentlich höhere Lebensdauer als die bis dahin bekannten magnetischen Medien. In diese Kategorie von Speichermedien fallen heute folgende Typen:

- CD-WORM  
Nur einmal beschreibbare Compact Disk Medien mit ca. 650 MegaByte Speicherkapazität. Die Speicherfläche im Medium wird beim Schreiben irreversibel verändert. CD-Medien sind durch die ISO 9660 standardisiert und kostengünstig. Die Qualität mancher billiger Medien ist aber für eine Langzeitarchivierung als nicht ausreichend zu erachten. Für Laufwerke und Medien gibt es zahlreiche Anbieter. Die Ansteuerung der Laufwerke wird von den Betriebssystemen direkt unterstützt.

- DVD-WORM  
Ähnlich wie die CD wird bei der DVD die Speicheroberfläche irreversibel im Medium verändert. DVD sind derzeit noch nicht einheitlich genormt und bieten unterschiedliche Speicherkapazitäten zwischen 4 und 12 GigaByte. Beim Einsatz für die Archivierung ist daher darauf zu achten, dass Laufwerke und Medien den Anforderungen der langzeitigen Verfügbarkeit gerecht werden. Es gibt auch hier zahlreiche Anbieter und die meisten Laufwerke werden auch direkt von den gängigen Betriebssystemen unterstützt.
- 5¼" WORM  
Bei diesen Medien und Laufwerken handelt es sich um die traditionelle Technologie, die speziell für die elektronische Archivierung entwickelt wurde. Die Medien befinden sich in einer Schutzhülle und sind daher gegen Umwelteinflüsse besser gesichert, als CD und DVD, die für den Consumer-Markt entwickelt wurden. Die Medien werden mit einem Laser beschrieben und bieten eine äußerst hohe Verfälschungssicherheit. Der derzeitige Stand der Technik sind so genannte UDO-Medien, die einen blauen Laser verwenden und eine Speicherkapazität von 50 GigaByte bieten. Zukünftig ist mit noch deutlich höheren Kapazitäten je Medium zu rechnen. Solche Laufwerke und Medien werden von Unternehmen wie Plasmon und HP angeboten. Nachteilig ist, dass Medien der vorangegangenen Generationen von 5¼"-Medien in den neuen Laufwerken nicht verwendet werden können. Von diesen sind noch mehrere verschiedene Technologien am Markt verfügbar. Für den Anschluss von 5¼"-Laufwerken ist spezielle Treibersoftware notwendig.

Für die Verwaltung und Nutzung der Medien sind so genannte Jukeboxen, Plattenwechselautomaten, gebräuchlich. Diese stellen softwaregestützt die benötigten Informationen von Medien bereit. Die Software ermöglicht es in der Regel auch, Medien mit zu verwalten, die sich nicht mehr in der Jukebox befinden und auf Anforderung manuell zugeführt werden müssen. Die Software zur Ansteuerung von Jukeboxen wird direkt in die Archivsoftware integriert, aber auch als unabhängige Ansteuerungssoftware angeboten. Zum Anschluss von Jukeboxen bedient man sich in der Regel eigener Server, die auch die Verwaltung und das Caching übernehmen. Inzwischen können solche Systeme aber auch als NAS Network Attached Storage oder integriert in SAN Storage Area Networks genutzt werden. Die Software ermöglicht dabei respektable Zugriffs- und Bereitstellungszeiten, die im Regelfall ein ausreichendes Antwortzeitverhalten garantieren. Neben diese klassischen Archivspeicher, die auf rotierenden, digital-optischen Wechselmedien basieren, treten inzwischen zwei weitere Technologien:

- CAS Content Addressed Storage  
Hierbei handelt es sich um Festplattensysteme, die durch spezielle Software die gleichen Eigenschaften wie ein herkömmliches WORM-Medien erreichen. Ein Überschreiben oder Ändern der Information auf dem Speichersystem wird durch die Kodierung bei der Speicherung und die spezielle Adressierung verhindert. Bei diesen Speichern handelt es sich um abgeschlossene Subsysteme, die allerdings nahezu wie herkömmliche Festplattensysteme direkt in die IT-Umgebung integriert werden können. Solche Systeme sind derzeit noch relativ teuer und werden von wenigen Herstellern wie EMC (Centera) angeboten. Sie bieten Speicherkapazitäten mit hoher Performance im TeraByte-Bereich.
- WORM-Tapes  
WORM-Tapes sind Magnetbänder, die durch mehrere kombinierte Eigenschaften ebenfalls die Anforderungen an ein herkömmliches WORM-Medium erfüllen. Hierzu gehören spezielle Bandmedien sowie geschützte Kassetten und besondere Laufwerke, die die Einmalbeschreibbarkeit sicherstellen. Besonders in Rechenzentren, in denen Bandroboter und Librarysysteme bereits vorhanden sind, stellen die WORM-Tapes eine einfach zu integrierende Komponente für die Langzeitarchivierung dar. Die vorhandene Steuerungssoftware kann mit den Medien umgehen und auch entsprechendes Umkopieren und Sichern automatisieren. Solche Laufwerke und Bandmedien werden z.B. von StorageTek, Sony, IBM und anderen angeboten.

Besonders für größere Unternehmen und Verwaltungen mit Rechenzentren stellen Festplatten- oder WORM-Tape-Archive eine Option dar, da sie sich einfach in den laufenden Betrieb integrieren lassen.



## ***10 Compliance-Merksätze***

Fassen wir das Thema Compliance unter dem Gesichtspunkt Information Management Compliance zum Schluss in einer Reihe von Merksätzen zusammen:

1. Compliance-Themen gehören auf die Entscheidungsebene, die die Verantwortung für die Einhaltung und Umsetzung der Anforderungen haben
2. Compliance-Anforderungen sind ein Bestandteil jedweder Corporate Governance Strategie
3. Unternehmen benötigen eine Richtlinie zum Umgang mit Informationen, eine Information Policy, die die Compliance-Anforderungen und die Lösung zur Umsetzung der Anforderungen beinhaltet
4. Compliance muss durchgängig im Unternehmen implementiert werden, um wirksam zu sein
5. Die Erfüllung von Compliance-Anforderungen ist kein einmaliges Projekt, sondern ein kontinuierlicher Prozess
6. Die Erfüllung von Compliance-Anforderungen muss regelmäßig nach definierten Verfahren überprüft werden
7. Information Management Compliance betrifft nicht nur Software und Systeme, sondern die Prozesse im Unternehmen, die Organisation und den Umgang mit den Systemen
8. Compliance-Anforderungen betreffen nicht nur elektronische Archive, sondern alle Systemkomponenten, in denen aufbewahrungspflichtige Daten, Informationen und Dokumente erzeugt, genutzt und verwaltet werden
9. Die Erfüllung von Compliance-Anforderungen muss auch für den eigenen Nutzen im Unternehmen genutzt werden, um mehr Transparenz und Sicherheit zu schaffen und um das Unternehmen auf das Informationszeitalter einzustellen.
10. Man darf sich nicht durch den Begriff Compliance verunsichern oder gar verängstigen lassen, sondern muss zunächst im Unternehmen prüfen, welche Regelungen für welchen Anwendungsfall überhaupt relevant sind

Compliance-Anforderungen sind ein Thema, mit dem sich jedes Unternehmen auseinandersetzen muss, wenn es Bestand im Informationszeitalter haben will.

## **Documentum**

### **Anbieter von Compliance-Lösungen**

Documentum geht das Thema Compliance von verschiedenen Seiten an. Die Kerntechnologie bietet ein extrem hohes Maß an plattformnativer Datensicherheit. Authentifizierung, Zugriffskontrolle und Überprüfungsfunktionen gehören zum standardmäßigen Leistungsumfang. Trusted Content Services bietet darüber hinaus Verschlüsselungsfunktionen, während Content Authentication Services neben anderen Merkmalen auch elektronische Signaturen unterstützen.

In enger Zusammenarbeit mit Branchenspezialisten entwickelte Documentum eine Reihe von Lösungen, mit denen sich die Compliance-Kosten senken und Risiko von Verstößen reduzieren lassen.

#### **Documentum Produkte für Compliance Lösungen**

- Business Process Management
- Content Server
- Digital Asset Management
- Documentum Compliance Manager
- eRoom Enterprise
- GXPharma
- Records Manager
- Records Services for Email
- Site Caching Services

Die Documentum Enterprise Compliance-Lösungen zeichnen sich durch eine nie da gewesene Transparenz und eine Fülle an Kontrollmöglichkeiten aus. Gleichzeitig können Unternehmen den gesetzlichen Anforderungen durch kontrollierte Repositories, automatisierte Abläufe, Collaboration, Kommunikation sowie Archivierungs- und Integrationsfunktionen auf effiziente und zuverlässige Art und Weise nachkommen. Durch den zu Grunde liegenden ganzheitlichen Ansatz können gezielt diejenigen Elemente ausgewählt und umgesetzt werden, die den größten unternehmerischen Nutzen bringen.

Documentum bietet Anwenderunternehmen die folgenden Vorteile bei der Erfüllung von Compliance-Vorgaben:

- Mehr Kontrolle und Transparenz – Nutzung eines zentralen Zugriffspunkts für die Verwaltung von Inhalten, Projekten und Prozessen; Verwaltung von Corporate Governance-Prozessen und Zuordnung zu einem internen Kontrollmechanismus; Steigerung von Genauigkeit und Qualität
- Höhere Effizienz und niedrigere Compliance-Kosten – Automatisierung manueller Arbeitsschritte und Rationalisierung von Abläufen; Senkung der Kosten für die Archivierung und Pflege von Content und Records; Nutzung von Teamarbeit für eine optimierte Entscheidungsfindung
- Effizientes Compliance-Management durch einen ganzheitlichen Ansatz – Übergreifende Betrachtung der Compliance-Thematik und Entwicklung eines in sich geschlossenen Verfahrens für die Handhabung der damit verbundenen Sachverhalte

Informationen zu den Documentum Compliance-Produkten und -Lösungen finden Sie unter: <http://www.documentum.de/solutions/compliance/index.htm>

## ***Adressen***

### **PROJECT CONSULT Unternehmensberatung Dr. Ulrich Kampffmeyer GmbH**

Breitenfelder Str. 17  
20251 Hamburg  
Tel.: + 49 (040) 460762 - 20  
Fax: + 49 (040) 460762 - 29

### **Documentum GmbH**

Inselkammerstr. 2  
82008 Unterhaching  
Tel.: +49 (089) 6 66 81-0  
Fax: +49 (089) 6 66 81-1 11

### **EMC Deutschland GmbH**

Am Kronberger Hang 2a  
65824 Schwalbach/Taunus  
Tel.: + 49 (06196) 47 28-0  
Fax: + 49 (06196) 47 28-139

## ***Literaturtipp***

Randolph A. Kahn, ESQ. and Barclay T. Blair: Information Nation, Seven Keys to Information Management Compliance, AIIM, 2004

Dr. Ulrich Kampffmeyer: Regulative Vorgaben beflügeln den Markt für Dokumenten-Technologien, Keynote-Vortrag auf der DMS EXPO 2004, PROJECT CONSULT/Advanstar, 2004

## ***Links zu weiterführenden Informationen***

Basel II	<a href="http://www.basel-ii.info">http://www.basel-ii.info</a>
BSI GSHB	<a href="http://www.bsi.de">http://www.bsi.de</a>
EMC ILM-Info	<a href="http://www.ilm-info.de">http://www.ilm-info.de</a>
EU Recht	<a href="http://europa.eu.int/eur-lex/de">http://europa.eu.int/eur-lex/de</a>
Forum Elektronische Steuerprüfung	<a href="http://www.elektronische-steuerpruefung.de">http://www.elektronische-steuerpruefung.de</a>
GDPdU	<a href="http://www.bundesfinanzministerium.de">http://www.bundesfinanzministerium.de</a>
GDPDU-Portal	<a href="http://www.gdpdu-portal.com">http://www.gdpdu-portal.com</a>
GOBS Verordnungstext	<a href="http://www.bundesfinanzministerium.de">http://www.bundesfinanzministerium.de</a>
PROJECT CONSULT	<a href="http://www.project-consult.com">http://www.project-consult.com</a>
SOA-Forum	<a href="http://www.sarbanes-oxley-forum.com/">http://www.sarbanes-oxley-forum.com/</a>