Information Management Compliance

PROJECT CONSULT Whitepaper

Dr. Ulrich Kampffmeyer

P R O J E C T C O N S U L T

Unternehmensberatung Dr. Ulrich Kampffmeyer GmbH

Hamburg, September 2007

Information Management Compliance

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

Every effort has been made to make this white paper as complete and as accurate as possible, but no warranty or fitness is implied. The authors shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

This work including all parts is protected by copyright. No part of this work covered by the copyright hereon may be reproduced or used in any form or by any means – graphic, electronic or mechanical, including photocopying, recording, translating, taping, or information storage and retrieval systems – without the written permission from the author.

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
Web: www.PROJECT-CONSULT.com

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.

All content is the orginal text of the autor if not otherwise cited. The author must agree to copies or citations before publishing. No part of this work covered by the copyright hereon may be reproduced or used in any form or by any means without citing the author. Specimen copies have to be sent to the author without request even if published partly or cited.

Information Management Compliance

Ein PROJECT CONSULT Whitepaper

A PROJECT CONSULT Whitepaper

Dr. Ulrich Kampffmeyer

Geschäftsführer der PROJECT CONSULT Unternehmensberatung GmbH, Hamburg

Managing Director PROJECT CONSULT Unternehmensberatung GmbH, Germany

Keynote-Präsentation auf der DMS EXPO 2007, 26. September 2007, Köln

Keynote presentation at the DMS EXPO 2007, September 26th, 2007, Cologne, Germany

„Es muss eine Angleichung der elektronischen Welt an die Papierwelt stattfinden. Nur mit einem komplett neuem Rahmenwerk von Gesetzen und Richtlinien können allgemeingültige und gerechte Grundlagen für Information Management Compliance geschaffen werden.“ [1)]

“The electronic world must become equivalent to the paper world. A generally accepted and fair basis for information management compliance requires a completely new legal and regulatory framework.”[1)]

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-Informations-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.

The term “compliance” is confusing for many users. Numerous vendors market their products using the compliance label – the traditional DMS and ECM solution vendors, as well as manufacturers of data storage systems, management information software, and ERP solutions. “Compliance” has become a new market niche. In Germany the term has thus far not gained broad currency, but the legal and regulatory documentation requirements are increasing steadily – one need look no further than the GDPdU or Basel II. Thus, users now find themselves having to decide between specialist island solutions to fulfill specific compliance requirements, or broader-based solutions that include compliance fulfillment in their portfolio.

Das Whitepaper bietet einen Überblick über Hintergründe und notwendige Maßnahmen zur Erfüllung der zunehmenden Compliance-Anforderungen im Umfeld der Informationstechnologie. Die aktuelle Situation im Jahr 2007 wird an Hand einiger, ausgewählter Beispiele dargestellt.

This White Paper gives an overview of the background and and actions needed to fulfill the growing compliance reqirements in IT. It will illustrate the current situation in 2007 using a few selected examples.

[1)] Ulrich Kampffmeyer, Bedeutung von Compliance, Vortrag auf dem SAPERIONcongres 2007, „ECM 2.0“, 2007

[1)] Importance of “Compliance”. Dr. Ulrich Kampffmeyer at the SAPERIONcongress 2007

Compliance und Information Management Compliance

„Alle Gesetze und Regeln der Papierwelt gelten auch in der elektronischen Welt.“[2)]

Was verbirgt sich hinter dem Begriff Compliance?

Zu den häufig, zumindest für deutsche Ohren, schwer verständlichen Begriffen aus dem anglo-amerikanischen Sprachraum muss auch der Begriff „Compliance“ gezählt werden.

Compliance umfasst die Gesamtheit aller zumutbaren Maßnahmen, die das regelkonforme Verhalten eines Unternehmens, seiner Organisationsmitglieder und seiner Mitarbeiter im Hinblick auf alle gesetzlichen Ge- und Verbote begründen.

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.

Im Folgenden wird für den Begriff Compliance nachstehende Übertragung verwendet:

„Übereinstimmung mit und Erfüllung von gesetzlichen und regulativen Vorgaben“[3)]

[2)] Ulrich Kampffmeyer, Dokumenten-Technologien – Wohin geht die Reise. PROJECT CONSULT 2003

[3)] Ursprünglich *“Übereinstimmung mit und Erfüllung von* rechtlichen *und regulativen Vorgaben“*. Ulrich Kampffmeyer, Compliance Whitepaper, Documentum, 2004, S.3.

1 Compliance and Information Management Compliance

“All laws and rules of the paper world also apply to the electronic world.”[2)]

What is behind the term “Compliance”?

“Compliance” is yet another English term that has found its way into international IT parlance.

Compliance refers to the totality of reasonable actions that underpin the compliance of a company, its organizational members, and its employees with all legal requirements.

There have always been compliance reguirements, but after the the ENRON and WorldCom scandals in the US the topic has gained a new, more intense quality. Harsher penalties and new requirements govern the storage of digital business records. In the past there was already legislation; for example, bookkeeping software has always had to meet compliance standards. With the increasing volume and significance of e-mail and e-commerce, the documentation and digital preservation or archiving of business processes have become ever more important.

In the following, “compliance” refers to:

“Agreement with and fulfillment of legal and regulatory requirements” [3)]

[2)] Ulrich Kampffmeyer, Dokumenten-Technologien – Wohin geht die Reise. PROJECT CONSULT 2003

[3)] Previous version: Ulrich Kampffmeyer, Compliance Whitepaper, Documentum, 2004, S.3.

Betrachtet man die einzelnen Begriffe der deutschen Übertragung der Definition von Compliance „Übereinstimmung mit und Erfüllung von gesetzlichen 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 das 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.
- **„Gesetzliche 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“**
  Man unterschiedet zwischen „rechtlich“ und „regulativ“, da es eine Reihe von Vorgaben, die nicht direkt auf Gesetzen basieren wie z.B. Normen, Standards, Codes of Best Practice 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.

Looking at the individual terms in the above definition “Agreement with and fulfillment of legal and regulatory requirements,” several aspects of compliance stand out.

- **“Agreement”**
  Agreeing with something assumes that there are defined, official, accessible rules to agree with in the first place. These rules do not usually contain technical requirements on implementation. This makes sense, since the rules should not be tied to technologies that may be obsolete in just a few years. Agreement is the static aspect of compliance.
- **“Fulfillment”**
  This implies two things – first, that the requirements have to be implemented in some form, and secondly, that this is a process, not a one-time action. The company or organization must attend to fulfillment on an ongoing basis. Fulfillment usually goes beyond mere technology, to include organizational and management aspects.
  Fulfillment is the dynamic aspect of compliance.
- **“Legal requirements”**
  These are laws or bureaucratic regulations that require specific organizations or persons to obey the rules. It is not possible to get around fulfilling these; the only room to maneuver is in interpretation, scope, and mode of implementation.
- **“Regulatory requirements”**
  Legal and regulatory requirements are distinct from one another, as there are numerous requirements that do not have force of law, such as standards, codes of best practice, etc. In many cases, legal requirements for a given instance have consequences and implications for other instances. These are demarcated as regulatory requirements.

Unterschiedliche Auswirkungen

Grundsätzlich gelten alle gesetzlichen, rechtlichen und regulativen Vorgaben auch in der elektronischen Welt. Häufig sind die Anforderungen der DV-Welt jedoch noch nicht oder nicht direkt enthalten und müssen daher adäquat abgeleitet werden.

- **„Direkte Betroffenheit“**
  Dies betrifft besonders Gesetze und gesetzesgleiche Verordnungen, die in jedem Fall eingehalten werden müssen. Hier kann man lediglich den Umfang und die Ausprägung interpretieren. Neben generell gültigen Vorgaben treten besondere, die auf die Branche oder Geschäftstätigkeit bezogen sind.
- **„Indirekte Betroffenheit“**
  Hier beginnt die große Grauzone, wo es darum geht, zunächst die für das Unternehmen oder die Organisation zutreffenden Regelungen zu ermitteln und zu bewerten. So betrifft beispielsweise Basel II[x)] nicht nur die Banken, sondern jedes kreditnehmende Unternehmen, da die Dokumentations- und Transparenzauflagen an die Kunden weitergegeben werden.

Für direkte und indirekte Auswirkungen gibt es zahlreiche Compliance-Regeln, die sowohl die herkömmliche Papierdokumentation wie auch die eingesetzte EDV betreffen.

Der bindende Charakter einer Vorgabe kann also sehr unterschiedlich sein. Nicht zuletzt Steckdosen, Lebensmittel, Flugzeuge, elektrische Geräte, Medikamente, Kindergärten, Bildschirme usw. müssen auch bestimmte Compliance-Anforderungen erfüllen, die sich beispielsweise in Prüfsiegeln niederschlagen.

Ein Abgleich der unterschiedlichen Anforderungen und Ausprägungen mit dem, was heute unter dem Schlagwort „Compliance“ bei informationstechnologischen Lösungen verstanden wird, zeigt aber große Unterschiede. Daher wird im Folgenden konkreter im Sinne von „IMC“, „Information Management Compliance“, gesprochen.

Different consequences

In principle, all legal and regulatory requirements apply to the digital world just as they do to the paper world. Often, however, the requirements are not phrased specifically for IT applications, and these must therefore be derived.

- **“Direct consequences”**
  Certain laws and requirements with the force of law must be complied with under all circumstances. There is room for interpretation only in terms of scope and extent. In addition to generally applicable laws, there are laws that refer to specific industries or activities.
- **“Indirect consequences”**
  The uncertainty begins with determining and assessing the rules that apply to a company or organization. For example, Basel II[x)] applies not only to banks, but to any organization that borrows money, since the documentation and transparency rules are propagated through from lender to borrower.

There are numerous compliance rules with direct and indirect consequences, that apply to both conventional paper documentation and to IT.

Exactly how binding a requirement is can therefore differ greatly. Electrical sockets, food, aircraft, electrical devices, medications, kindergartens, video screens etc. must meet certain compliance rules that find expression in test seals, for example.

A comparison of the requirements and their general meaning, with what is understood by the term “compliance” specifically for IT solutions, shows significant differences. Therefore, in the following we will discuss compliance in the specific sense of IMC, Information Management Compliance.

Aktuelle Situation und wichtige Regularien

„Der elektronische Geschäftsverkehr wird zum Regelfall. Gleichbehandlung ist nur möglich, wenn für alle Beeiligten die selben Transparenzpflichten gelten. Compliance muss daher für alle und unabhängig von der Form der Geschäfts- oder Verwaltungstätigkeit gleichermaßen gültig sein.“[4)]

Compliance-Anforderungen gibt es überall. Sie machen vor Landesgrenzen nicht halt. Sie betreffen Organisationen ebenso wie Individuen. In einer globalisierten Gesellschaft stellt sich zunehmend das Problem, dass jedes Land immer noch eigene Gesetze und Regularien für Geschäfte, Prozesse und Transaktionen hat, die längst harmonisiert sein sollten. Internationalen „Gesetzen“ und Regeln kommt daher eine immer wichtige Rolle zu, da herkömmliche Grenzen im Internet keien Bedeutung mehr haben.

International

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.

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. [5)]

Basel II hat eine Vielzahl von Auflagen für die Dokumentation nach sich gezogen, die in einer elektronischen Welt nur mit Informationsmanagementlösungen vollzogen werden können.

[4)] Ulrich Kampffmeyer, Marcus Evans Conference „Content Management – The driving factor for successful eBusiness”, Berlin, 2001

[5)] Wirtschaftswiki, Definition Basel II, 2005

2 Current situation and important regulations

“Digital business transactions will become the rule. Equal treatment is possible only when the same transparency rules apply to everybody. Therefore, compliance must have the same validity for all, regardless of the form taken by a business or administrative activity.” [4)]

Compliance requirements are everywhere, and do not stop at national borders. They affect organizations and individuals alike. In a globalized society, problems are increasingly caused by the fact each country has its own laws and regulations for businesses, processes, and transactions, which should have been harmonized long ago. International “laws” and rules are therefore more and more important, since traditional borders have no meaning in the Internet.

International

Basel II is a good example of direct and indirect consequences of legislation. Financial service providers must retain more own capital as the borrower’s risk increases. Although this legislation concerning credit and documentation was intended only for banks, Basel II has substantial effects on all companies.

Basel II refers to the reformation of own capital requirements for banks and credit institutes.

The objective of Basel II was to increase the stability of the international finance system. The idea is to evaluate risks in the credit business better, and bring lender capital overage more into line with risk. [5)]

Basel II brought with it a great number of rules for documentation, which in a digital world can only by followed using information management solutions.

[4)] Ulrich Kampffmeyer, Marcus Evans Conference „Content Management – The driving factor for successful eBusiness”, Berlin, 2001

[5)] Wirtschaftswiki (German), Definition of the term „Basel II“, 2005

USA

In den USA gab es schon sehr lange Compliance-Anforderungen an Softwaresysteme und die Dokumentation von Geschäftsprozessen.

Am bekanntesten und am engsten mit dem Begriff Compliance ist jedoch der Sarbanes Oxley Act verknüpft.

Sarbanes-Oxley-Act

Durch die Skandale um ENRON, WorldCom und einige andere Unternehmen 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 hat.

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 und 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. [6)]

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.

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.

[6)] USA, SOA Sarbanes-Oxley Act of 2002 (häufig auch als SOX abgekürzt)

USA

In the US there have long been compliance requirements for software systems and business process documentation.

The most well-known of these, and most closely associated with the term compliance, is the Sarbanes Oxley Act.

Sarbanes Oxley Act

The scandals surrounding ENRON, WorldCom and other companies brought compliance into the center of public attention. The cause was "edited" audits by auditors and the companies' own reporting. In the process of uncovering all this, e-mail was found to be one possible source of proof of illegal actions. In 2002 this led to the Sarbanes-Oxley Act, abbreviated as SOA or SOX. In accordance with common US practice it was named after the leaders of the commission that drafted the law.

The law applies to all companies listed on the New York Stock Exchange.

SOA is intended to improve the transparency and auditability of companies' dealings in audits by the SEC, the Securities und Exchange Commission.

Among other things, it requires that companies maintain an internal monitoring system for accounting, that they evaluate the effectiveness of their systems, and that they certify quarterly and annual reports. [6)]

In the US, SOA is important especially because of Section 802, which mandates severe penalties of up to 20 years imprisonment for the destruction or alteration of documentation that is required to be kept unaltered.

Auditors in particular now attach great importance to compliance, since the scandals caused the disappearance of formerly large, well-regarded auditing firms like Andersen.

[6)] SOA Sarbanes-Oxley Act of 2002

e-Discovery

Die in den USA am 1. Dezember 2006 in Kraft getretenen Änderungen der FRCP Federal Rules of Civil Procedure[7)] können als signifikanter Wendepunkt von den herkömmlichen papierbasierten hin zu elektronischen Beweisführungsregeln gesehen werden. Die wachsende Bedeutung von elektronisch gespeicherten Daten wurde somit auch durch den obersten Gerichtshof unterstrichen.

Electronic discovery, auch e-discovery oder eDiscovery, bezieht sich dabei auf jeden Prozess bei dem elektronische Daten abgefragt, gefunden, gesichert und gesucht werden, mit dem Ziel, sie bei einem Gerichtsverfahren zu verwenden. Dabei können sämtliche Daten, wie z.B. Texte, Bilder, Datenbanken, Audio-Dateien, Animationen, Webseiten und Programme als Beweis dienen. Die wertvollsten Quellen für strafrechtliche oder zivile Gerichtsverfahren stellen aber oft E-Mails dar.

Nachdem mit Sarbanes-Oxley bereits die elektronische Information vor Gericht aufgewertet worden war schafft eDiscovery nun die rechtliche Grundlage für die Anerkennung elektronsicher Informationen in Gerichtsverfahren. Alle Formen von elektronischen Informationen, nicht nur als Record definierte Dokumente, können als Beweismittel vorgebracht werden. Anders als in Europa und besonders in Deutschland spielt die elektronische Signatur dabei keine Rolle. Bei der Ermittlung gilt das als gültig, was von den ermittelnden Behörden vorgefunden wurde. Bei der Beweissicherung galten bisher nur Papierdokumente als sicherer Nachweis. Durch die Möglichkeiten der elektronischen Recherche dürfte sich dies ändern.

eDiscovery wird nicht nur die sichere, unveränderbare Speicherung von Informationen fördern sondern mehr noch den Schutz des Zugriffs und andere Sicherheitsaspekte. Policies zur kontrollierten Entsorgung von Information werden dabei zunehmend wichtiger.

Es sind aber nicht allein SOA und FRCP, die den Druck in bezug auf umfassende Dokumentationsanforderungen im Umfeld der Steuerprüfung und Steuerfahndung erhöht haben.

Aus den CFR Code of Federal Regulations[8)] lassen sich inzwischen eine Vielzahl weiterer Anforderungen für spezielle Branchen und Geschäftstätigkeiten ableiten.

7) United States Supreme Court, Federal Rules of Civil Procedure, Bundesrichtlinie für zivilrechtliche Verfahren, 2006

8) National Archives and Records Administration, Code of Federal Regulations. Bundesgrundsätze für Archive

e-discovery

The changes to the FRCP or Federal Rules of Civil Procedure[7)] that came into force on December 1, 2006 are a significant turning point in the change of focus from conventional paper-based to digital evidence. The Supreme Court underlined the growing importance of digitally preserved information.

Electronic discovery, also termed e-discovery oder eDiscovery, refers to any process in which electronic data is referenced, found, saved, or searched, with the objective of using it in court. Any data can serve as evidence, including text, images, databases, audio files, animations, websites, and software. But frequently, e-mail is the most important source of evidence in criminal and civil cases.

After Sarbanes-Oxley had already boosted the importance of digital information in a court of law, eDiscovery created the legal basis for recognizing digital information in court. All forms of digital information, not just documents defined as records, are admissible as evidence. Unlike in Europe and Germany in particular, the presence or absence of an electronic signature is of no consequence. The only thing that matters is what the investigators uncover. Formerly, only paper documents were considered to be firm proof. The possibilities opened up by electronic research will now change this.

eDiscovery will not only promote the secure, edit-proof archiving or preservation of information, but also access protection and other security aspects. Policies for the controlled disposal of information will grow in importance.

But it is not just SOA and FRCP that have increased the pressure on documentation in the context of tax audits.

Many other requirements for specific industries and business activities can now be derived from the CFR or Code of Federal Regulations[8)].

7) United States Supreme Court, Federal Rules of Civil Procedure, 2006

8) National Archives and Records Administration, Code of Federal Regulations.

Ein Beispiel ist der CFR 17[9], § 240, mit harten Regularien für Börsenmakler. Die Regeln der US-Börsenaufsicht für Aktien-Broker SEC 17A-3[10] und SEC 17A-4 definieren exakt, welche Aufzeichnungen und Belege bei einer Transaktion aufgehoben und auf welchem Medium sie gespeichert werden müssen.

Ähnliche Regeln für die Finanzwelt hat die National Association of Securities Dealers (NASD)[11] entwickelt. NASD 3010 und NASD 3110 beispielsweise verlangen, dass Broker und Händler externe Transaktionen von registrierten Stellvertretern überwachen.

Eine besondere Bedeutung hat zu dem der Patriot Act[12], der weitgehenden Zugriff auf alle Informationen ermöglicht und eine transparente Informationsbereitstellung fordert.

In anderen Bereichen gibt es ebenfalls rechtliche und regulative Vorgaben wie z.B. HIPAA[13] im Krankenhaus- als auch im Versicherungsbereich, den Tread Act[14] mit umfangreichen Anforderungen zur Produkt-, Qualitäts- und Herstellungsdokumentation oder Regularien der EPA, Environmental Protection Agency [15].

Viele dieser Regelwerke beziehen sich auf die neu gefassten FSG, Federal Sentencing Guidelines[16] von 2002, so dass Verstöße mit erheblichen Strafen belegt werden können.

Gesetze und Regularien in den USA haben auch Auswirkungen auf Unternehmen im Ausland, wenn sie Tochtergesellschaften oder Muttergesellschaften amerikanischer Unternehmen sind, oder bestimmte Geschäfte in den USA abwickeln.

For example, CFR 17[9], sec. 240 strictly regulates stockbrokers. SEC 17A-3[10] and SEC 17A-4 regulations for stockbrokers define exactly what notes and documents must be retained for a transaction, and what medium they must be stored on.

The National Association of Securities Dealers (NASD)[11] has developed similar rules for the financial business. For example, NASD 3010 and NASD 3110 require that brokers and dealers monitor external transactions via registered representatives.

Of special significance is the Patriot Act[12], which allows far-reaching access to all information, and requires transparent information provision.

There are also legal and regulatory requirements in other areas as well, for example HIPAA[13] for hospitals and insurers, the Tread Act[14] with comprehensive requirements concerning product, quality, and manufacturing documentation, and the regulations of the EPA, the Environmental Protection Agency [15].

Many of these regulations cite the new FSG, the Federal Sentencing Guidelines[16] of 2002, meaning that infractions can be punished with severity.

Laws and regulations in the US affect companies in other countries, if they are subsidiaries of US companies or themselves maintain US subsidiaries, or do certain types of business in the US.

[9] Compliance Whitepaper, Documentum 2004, S.4

[10] Securities and Exchange Commission, Books and Records Requirements for Brokers and Dealers Under the Securities Exchange Act of 1934, 2003

[11] National Association of Securities Dealers, NASD 3010 und NASD 3110

[12] U.S. Department of Justice , The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, 2001 (Patriot Act)

[13] United States Department of Health & Human Services, Office for Civil Rights, Health Insurance Portability and Accountability Act, 2003

[14] National Highway Traffic Safety Administration , Transportation Recall Enhancement, Accountability and Documentation Act , 2000

[15] U.S. Environmental Protection Agency

[16] United States Sentencing Commission, Federal Sentencing Guidelines, 2007 (Rechtsprechungsrichtlinie)

[9] Compliance Whitepaper, Documentum 2004, S.4

[10] Securities and Exchange Commission, Books and Records Requirements for Brokers and Dealers Under the Securities Exchange Act of 1934, 2003

[11] National Association of Securities Dealers, NASD 3010 und NASD 3110

[12] U.S. Department of Justice , The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, 2001

[13] United States Department of Health & Human Services, Office for Civil Rights, Health Insurance Portability and Accountability Act, 2003

[14] National Highway Traffic Safety Administration , Transportation Recall Enhancement, Accountability and Documentation Act , 2000

[15] U.S. Environmental Protection Agency

[16] United States Sentencing Commission, Federal Sentencing Guidelines, 2007

Europa

Auf europäischer Ebene werden durch die Europäische Kommission zahlreiche Richtlinien entwickelt, die von den Mitgliedstaaten in nationales Recht überführt werden müssen. Bereits durch die Richtlinien zum E-Commerce und zur elektronischen Signatur sind eine Reihe von Anforderungen für Compliance entstanden. Der elektronische Geschäftsverkehr und die Umstellung der öffentlichen Verwaltung auf elektronisch unterstützte Verfahren wird weitere Compliance-Anforderungen nach sich ziehen.

Beispiele für europäische Richtlinien mit Gesetzescharakter, die Bedeutung für die Rechtskraft elektronischer Dokumente besitzen und Dokumentationspflichten nach sich ziehen, sind z.B.:

- **„E-Commerce“**
  E-Commerce-Richtlinie[17)], die genau festgelegt, was im elektronischen Geschäftsverkehr erlaubt und verboten ist. Hierzu gehören auch Nachweis- und Dokumentationspflichten.
- **„E-Signatur“**
  Europäische Richtlinie zur elektronischen Signatur[18)]. Der Einsatz der elektronischen Signatur ersetzt unter bestimmten Voraussetzungen das Papier. Die elektronische Signatur ist daher Bestandteil zahlreicher Compliance-Regelungen.

Zahlreiche andere Richtlinien der Europäischen Kommission haben ebenfalls Compliance- und Dokumentationspflichten nach sich gezogen. Die größte Wirkung entwickelt jedoch zur Zeit die sogenannte 8. Direktive.

8. EU-Richtlinie

Die 8. Direktive setzt Standard für Bilanzierungsrichtlinien von börsennotierten Unternehmen.

Am 07. Juli 2006 ist die 8. EU-Richtlinie[19)] („Euro SOX“) in Kraft getreten, die für alle europäischen Kapitalgesellschaften ähnliche Auswirkungen haben wird wie Sarbanes-Oxley Act (SOX) in USA. Spätestens bis Juli 2008 muss die 8. EU-Richtlinie in nationales Recht umgewandelt sein. Damit greifen EU-weit unter anderem verschärfte Regeln in Bezug auf die Dokumentation der Geschäftsprozesse und –transaktionen sowie der verwendeten IT- und TK-Infrastruktur eines Unternehmens.

[17)] EU-Parlament, Richtlinie 2000/31/EG, 2000
[18)] EU-Parlament und Rat, Richtlinie 1999/93/EG, 2000
[19)] EU-Parlament und Rat, Richtlinie 2006/43/ EG, 2006

Europe

At the European level, the European Commission develops many guidelines which the Member States must translate into national law. The guidelines on e-commerce and electronic signature have already led to a number of compliance requirements. Electronic business transactions and the switch by public administration to electronically supported processes will give rise to further compliance requirements.

Some European guidelines have legal character and affect the legal validity of digital documents, as well as documentation responsibilities. Examples are:

- **“E-Commerce”**
  E-commerce guideline[17)] which specifies what is permitted and prohibited in digital business transactions. Includes proof and documentation responsibilities.
- **“E-Signature”**
  European guideline on electronic signatures[18)], which replace paper signatures under certain conditions. The e-signature is therefore included in numerous compliance rules and regulations.

Many other guidelines of the European Commission have also given rise to compliance and documentation requirements. However, the so-called 8th Directive currently has the greatest effect.

8th EU Directive

The 8th Directive sets the standard for the financial accounting of stock-exchange listed companies.

On July 7, 2006 the 8th EU Directive[19)] (“Euro-SOX”) came into force. For European corporations it will have similar effects to Sarbanes-Oxley (SOX) in the US, and must be translated into national law by July 2008 at the latest. With it, throughout the EU there will be more stringent rules on documentation of business processes and transactions, and of corporate IT and communication infrastructures.

[17)] European Parliament, Directive 2000/31/EG, 2000
[18)] European Parliament and Assembly, Directive 1999/93/EG, 2000
[19)] European Parliament and Assembly, Directive 2006/43/ EG, 2006

Deutschland

In Deutschland wird der Begriff „Compliance“ zwar noch selten verwendet, doch die Anforderungen gibt es schon längst. Auch in Deutschland werden die Gesetze, wie BGB[20], ZPO[21] oder HGB[22], immer mehr den Anforderungen der Informationsgesellschaft angepasst sowie Richtlinien der Europäischen Kommision in nationales Recht übertragen.

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.

Aktuelle Beispiele sind das EHUG und die Erweiterung des Anwendungsbereiches der GDPdU durch aktuelle Gerichtsurteile. In eine ähnliche Kerbe wie die GDPdU schlägt auch das Gesetz zu den Dokumentationspflichten bei Verrechnungspreisen. die Gewinnabgrenzungsaufzeichnungsverordnung (GAUFZ)[23], die anders als die GDPdU bereits direkt strafbewehrt ist.

EHUG und E-Mail-Management

Das bundesweite Elektronische Handels- und Genossenschaftsregister (EHUG)[24], welches am 1. Januar 2007 in Kraft getreten ist, stellt eine digitale Version des Handelsregisters dar. Kapitalgesellschaften sind verpflichtet, ihre Abschlüsse beim elektronischen Bundesanzeiger einzureichen. Verstöße gegen die Offenlegungspflicht werden mit bis zu 25.000 Euro von den Verwaltungsbehörden, welche vom elektronischen Bundesanzeiger informiert werden, geahndet.

[20] BGB Bürgerliches Gesetzbuch, §§ 126, 127
[21] ZPO Zivilprozessordnung, §§ 292a, 286, 130, 371
[22] HGB Handelsgesetzbuch, §§ 239, 257
[23] GAUFZ Gewinnabgrenzungsaufzeichnungsverordnung
[24] EHUG Elektronisches Handels- und Genossenschaftsregister

Germany

In the Germany the term “compliance” is still seldom used, but the requirements have been in place for a while. Laws such as BGB[20], ZPO[21] or HGB[22] are more and more conformant with the requirements of the information age, and EU guidelines are being implemented in national legislation.

In this context the electronic signature is gaining importance, and is now required by almost all recent legislation. Thus, for example with digital invoices payers are allowed pretax deduction only with e-signed invoices. Since the e-invoice constitutes the original, it must be stored electronically. Here, new laws and regulations interact, and the signature law and changes to the BGB (German Civil Code) and ZPO (German Code of Civil Procedure) mandating the electronic signature are reflected in trade and tax law.

Current examples are the EHUG and the extension of the application area of the GDPdU (German Data Access and Digital Signature Authentication Law) by recent court decisions. The GAUFZ [23] is in a similar vein, but unlike the GDPdU it is enforced by criminal penalties.

“EHUG” and E-Mail Management

The national electronic commercial and company registry (EHUG)[24], which came into force January 1, 2007, is a digital version of the commercial registry. Corporations are required to submit their accounts to the electronic Federal Bulletin. Failure to comply is punishable by a fine of up to 25,000 Euros by the government administrative offices who draw their information from the electronic bulletin.

[20] BGB, German Civil Code §§ 126, 127
[21] ZPO, German Code of Civil Procedure §§ 292a, 286, 130, 371
[22] HGB, German Commercial Law §§ 239, 257
[23] GAUFZ, German Regulation on Recording Profit Accruals
[24] EHUG, German Electronic Commercial and Company Registry

Das EHUG hat eine Reihe von Änderungen auch in anderen Gesetzen wie z.B. für GmbHs und AGs nach sich gezogen. Eine regelung betrifft die Angabe der kompletten Firmierungs- und Verantwortungsangaben in der Signatur von E-Mails. Was längst schon galt wird hierdurch jetzt jedem deutlich gemacht: E-Mails sind Geschäftsbriefe und sind dementsprechend aufzubewahren.

Dies hat ein wahren Boom bei der E-Mail-Archivierung ausgelöst. Dabei wird häufig übersehen, dass E-Mails in einen Geschäftszusammenhang gehören und nicht isoliert archiviert werden sollten. Sie müssen zusammen mit anderen Dokumenten in Kunden-, Sach-, Projekt- oder anderen Akten gemeinsam verwaltet werden, damit die Vollständigkeit und Nachvollziehbarkeit des Geschäftsganges gewährleistet ist.

Da jeder Mitarbeiter im Unternehmen Empfänger wie Versender von geschäftsrelevanten E-Mails sein kann, ist jedwede technische Lösung durch organisatorische Maßnahmen zu unterfüttern.

GDPDU: aktuelle Urteile

Nach den Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)[25)] sind alle steuerlich relevanten Daten auswertbar über den zeitraum der Aufbewahrungsfristen nach HGB auswertbar aufzubewahren und für Prüfungen zugänglich zu machen.

Die GDPdU 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. 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.

[25)] GDPdU Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen, 2001

The EHUG has caused a series of modifications to other laws relevant for registered companies and their responsible managers. One rule concerns the naming of complete company and responsibility information in e-mail signatures. This codifies what everybody already knew – that e-mails are business correspondence, and must be archived as such.

This has launched a boom in e-mail archiving, but implementers often overlook the fact that e-mails belong in a business context, and should not be archived in isolation. They need to be preserved together with other documents by customer, matter, project, or associated files, so that the completeness and auditability of the business procedure is assured.

Since any employee in a company can be sender or recipient of relevant e-mails, any and all technology solutions must be underpinned by organizational measures.

"GDPDU": Current verdicts

According to the German Data Access and Digital Signature Authentication law (GDPdU)[25)], all tax-related information must be stored in interpretable form for the perod of time mandated by the Commercial Code, and made available for audits.

The GDPdU is a regulation that is based on canges in the tax change law and commercial code tax regulation, sections 146, 147, and 200. It provides a guideline for tax authorities to use in auditing. Companies must ensure that all tax-relevant data is preserved identifiably, unchanged, and completely, for a period of 10 years. The original data must be complete, correct, and interpretable, either in their origination systems or in digital archives. Documents and e-mails play an increasingly important role for the GDPdU, alongside ERP and bookkeeping systems.

[25)] GDPdU Data Access and Digital Signature Authentication law, 2001

Bereits in einer Reihe von Verfahren vor Finanzgerichten war die Auslegung der GDPdU ein Thema. Während frühere Urteile der Finanzgerichte Rheinland-Pfalz und Hamburg aus dem Jahr 2006 das Recht auf Datenzugriff noch an vielen Stellen eingeschränkt und damit den Steuerpflichtigen unterstützt haben, weisen die Urteile der Düsseldorfer Fi-nanzrichter nun in eine andere Richtung. Beide Entscheidungen vom 5. Februar 2007 beschäftigen sich im Kern mit der Reichweite des Datenzugriffs, also mit dem Umfang, welcher einer digitalen Betriebsprüfung zu Grunde zu legen ist und interpretieren diesen in einer Art, welche über das bisherige Verständnis von Literatur und Verwaltung hinausgeht. Dazu haben die Richter teilweise eigenständige Definition von GDPdU-Begrifflichkeiten vorgenommen und damit neue Diskussionspunkte eröffnet.

Steuerrelevanz versus Steuerauswirkung:
Die Finanzbehörde darf im Rahmen des steuerlichen Datenzugriffs auch auf solche Konten der handelsrechtlichen Finanzbuchhaltung zugreifen, auf denen steuerlich nicht abzugsfähige Betriebsausgaben verbucht werden. Auf der Grundlage des § 147 Abs. 1 i. V. m. Abs. 6 AO darf die Finanzverwaltung für Zwecke der steuerlichen Außenprüfung ausschließlich auf Daten zugreifen, die für die Besteuerung von Bedeutung sind. Die vom Datenzugriff betroffenen Unternehmen sind deshalb seit jeher darauf bedacht, das digitale Suchfeld des Betriebsprüfers auf solche Datenbestände zu begrenzen, die vom Sinn und Zweck des Rechts auf Datenzugriff gedeckt sind. Das Finanzgericht Düsseldorf gab der Auffassung des Finanzamts Recht und sah keine ernstlichen Zweifel an der Rechtmäßigkeit des Datenzugriffs auf die ursprünglich gesperrten Konten. Bei den fraglichen digitalen Kontoaufzeichnungen handele es sich um „Bücher“ i.S.d. § 147 Abs. 1 Nr. 1 AO, die – anknüpfend an das Handelsrecht – die Funktion erfüllen, für einen Kaufmann seine Handelsgeschäfte und die Lage seines Unternehmens zu dokumentieren. Die im Rahmen der GDPdU geforderte steuerliche Relevanz kann nicht mit der vom betroffenen Unternehmen angeführten steuerlichen Auswirkung gleichgesetzt werden. Dabei habe sich die eigentliche Steuerrelevanz stets auch daran zu orientieren, inwieweit die in Frage kommenden Unterlagen einen Bezug zur Buchführung aufwiesen und mithin zu deren Verständnis erforderlich seien. [26)]

[26)] PROJECT CONSULT, Newsletter 20070720, 2007

Interpretation of GDPdU has already been a topic of debate in a number of Finance Court cases. While 2006 verdicts of the Finance Courts of the states of Rhineland-Palatinate and Hamburg limited the right to data access at many points and thus supported the taxpayer, the verdicts of the Düsseldorf Finance Court go in a different direction. Both verdicts of February 5, 2007 ultimately involve the scope of data access, i.e. how far a digital audit can go, and interpret this in a way that goes beyond the previous interpretation of the literature and official usage. In doing this, the judges made some individual definitions of GDPdU terminology, thereby opening up new points for discussion.

Tax-relevance vs. tax effect:
Tax authorities can, within the framework of tax data access, access accounts of commercial-law bookkeeping that record non-tax-deductible business expenses. Per Sec. 147 para. 1 through 6 of the Tax Procedure Act (AO), tax authorities may, for the purposes of tax auditing, access only such data as is relevant to tax assessment. Companies affected by data access have therefore always tried to limit the digital search scope of auditors to data records to which this right to data access applies. The Düsseldorf Finance Court supported the view of the tax office, and had no serious doubts as to the legality of data access to such formerly closed accounts. The digital account entries in question were “books” in the sense of Sec. 147 para. 1 no. 1 of the Tax Procedure Act, which – based on commercial law – fulfill the function of documenting a businessperson’s commercial business and the position of his company. The tax relevance required by GDPdU cannot be made equivalent to the tax consequence, as claimed by the company involved in the case. Further, the own tax relevance is always based on the extent to which the documents in question are relevant to the accounts and therefore to understanding them.[26)]

[26)] PROJECT CONSULT, Newsletter 20070720, 2007

GDPdU-Begrifflichkeiten neu definiert:
Werden Eingangsbelege beim Steuerpflichtigen gescannt, gespeichert und die Originale anschließend vernichtet, so erstreckt sich das Zugriffsrecht im Rahmen der elektronischen Steuerprüfung auch auf derart erzeugte Datenbestände. Der Steuerpflichtige muss diese Datenbestände so organisieren, dass bei einer zulässigen Einsichtnahme keine geschützten Bereiche des Unternehmens tangiert werden. Der EDV-Zugriff der Finanzverwaltung bezieht sich grundsätzlich auf solche Datenbestände, die originär bereits in elektronischer Form vorliegen. Dies schließt eine Verpflichtung zum Einscannen oder Digitalisieren von Papierdokumenten aus. In Bezug auf den viel diskutierten Umfang einer digitalen Betriebsprüfung stellt sich jedoch vermehrt die Frage, inwieweit digitalisierte Eingangsbelege, deren Papieroriginal vernichtet wurde, dem Betriebsprüfer auch in digitaler Form zur Verfügung zu stellen sind. Das Finanzgericht Düsseldorf gestand dem Finanzamt das Recht zu, auf die fraglichen Belege aus dem System des Unternehmens heraus zuzugreifen und diese am Bildschirm einzusehen. Die Rechtsgrundlage hierfür ergibt sich nach Auffassung der Richter bereits aus § 147 Abs. 6 Satz 1 AO. [27)]

Während die bisherige Rechtsprechung eher in Richtung Unternehmensseite tendierte, verschaffen die beiden nun vorliegenden vorläufigen Entscheidungen aus Düsseldorf der Finanzverwaltung einen deutlichen Rückenwind. Die Unternehmen sollten insbesondere das Urteil betreffend die digitalisierten Originalbelege in ihre künftige GDPdU-Strategie einbeziehen und einen adäquaten Datenzugriff nebst Trennung in steuerlich relevante und irrelevante Unterlagen einplanen. Was man in diesem Zusammenhang nicht vergessen sollte, ist das derzeit häufig bemühte Thema der Verfahrensdokumentation. In dem Maße, wie der Außenprüfer selbst solche Systeme für den Z1- und Z2-Zugriff benutzt, wird der Nachweis von ordnungsgemäßer Verarbeitung, Nutzung und Betrieb immer wichtiger.

[27)] PROJECT CONSULT, Newsletter 20070720, 2007

GDPdU terms redefined:
If the taxpayer scans and stores incoming records and then destroys the originals, the right to access as part of electronic tax audit extends to the records thus generated. The taypayer must organize these records in such a way that allowable access does not touch protected areas of the company. The IT access of the tax office is solely for records that were originally in digital form. This means that taypayers are not obliged to scan or digitize paper documents. With regard to the widely discussed scope of digital tax audit, there is increasingly the question of to what extent digitized incoming records, whose paper originals were destroyed, should be made available to auditors in digital form as well. The Düsseldorf Finance Court gave the tax office the right to gain access to the documents in question from the companies' systems, and display them on-screen. The legal basis for this is provided, in the opinion of the court, by Sec. 147 para. 6 sentence 1 of the Tax Procedure Act. [27)]

While previous verdicts tended to side with business, these provisional verdicts by the Düsseldorf Finance Court give the tax office significant backup. Companies should pay special attention to the verdict on digitized originals in their future GDPdU strategies, and ensure good data access plus separation into tax-relevant and irrelevant documents. In this context, process documentation should not be forgotten. To the extent that outside auditors themselves use such systems for direct and indirect access, evidence of proper processing, use, and operation will become ever more important.

[27)] PROJECT CONSULT, Newsletter 20070720, 2007

Verfahrensdokumentation nach GoBS

Die Anforderungen an eine Verfahrensdokumentation sind in den Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme (GoBS)[28)] niedergelegt. Die GoBS selbst leiten sich aus dem Handelsgesetzbuch[29)] und der Abgabenordnung[30)] ab. Sie stellen quasi eine Übertragung der Anforderungen, die ursprünglich für eine papiergebundene Dokumentation gedacht waren, in die elektronische Welt dar.

In den GoBS wird die Behandlung aufbewahrungspflichtiger Daten und Belege in elektronischen Buchführungssystemen sowie in revisionssicheren Dokumentenmanagement- und Archivsystemen geregelt. Die GoBS behandeln dabei auch Verfahrenstechniken wie Scannen und Datenübernahme. Ein wesentlicher Kernpunkt ist das so genannte Interne Kontrollsystem (IKS). Die Verfahrensdokumentation muss alle Angaben zum Nachweis des ordnungsmäßigen Betriebes des Systemes beinhalten. Aus HGB, AO und GoBS leiten sich auch die grundsätzlichen Anforderungen an die Dokumentation und Aufbewahrung ab:

- Ordnungsmäßigkeit
- Vollständigkeit
- Sicherheit des Gesamtverfahrens
- Schutz vor Veränderung und Verfälschung
- Sicherung vor Verlust
- Nutzung nur durch Berechtigte
- Einhaltung der Aufbewahrungsfristen
- Dokumentation des Verfahrens
- Nachvollziehbarkeit
- Prüfbarkeit [31)]

Dokumentationspflichten ergeben sich jedoch nicht nur für den handelsrechtlichen und steuerrechtlichen Bereich sondern gelten auch alle anderen Anwendungsgebiete, die gesetzlich oder regulativ betroffen sind. Die oben aufgeführten Grundsätze aus dem Handelsrecht gelten so im Prinzip für alle Compliance-relevanten Anforderungen.

[28)] GoBS Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme, 1995

[29)] HGB Handelsgesetzbuch, §§ 239, 257

[30)] AO Abgabenordnung, §§ 146, 147, 200

[31)] PROJECT CONSULT, Artikel “Verfahrensdokumentation leicht gemacht”, 2001

„GoBS Verfahrensdokumentation“

Requirements for process documentation are laid down in GoBS (Basic Regulations for DP-supported Accounting Systems) [28)], which are derived from the German Commercial Code[29)] and Tax Procedure Act[30)]. They represent a kind of translation to the digital world of the requirements for paper-based documentation.

The GoBS regulates the treatment in electronic accounting systems of custodyworthy data and documents, and deals with process technologies such as scanning and data transfer. A core point is the Internal Control System (ICS). Process documentation must contain all information needed to demonstrate the proper operation of the system. From the German Commercial Code, the Tax Procedure Act, and the GoBS are derived the basic requirements for documentation and preservation:

- Proper procecure
- Completeness
- Security of the overall process
- Protection from editing and falsification
- Protection from loss
- Use only by authorized persons
- Mandated retention periods
- Documentation of the process
- Traceability
- Auditability [31)]

Documentation is mandatory not just for commercial law and tax-related matters, but for all other areas touched on by legislation and regulations. The principles given above from commercial law thus essentially apply to all compliance requirements.

[28)] GoBS, Basic Regulations for DP-supported Accounting Systems, part of the German commercial laws, 1995

[29)] HGB, German Commercial Law §§ 239, 257

[30)] AO Tax Procedure Act, §§ 146, 147, 200

[31)] PROJECT CONSULT, article “Verfahrensdokumentation leicht gemacht”, 2001

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.

Im Jahr 2007 wurde das UGB Unternehmensgesetzbuch[32)] in Kraft gesetzt, dass das bisherige österreichische HGB Handelsgesetzbuch ablöst. Aus dem neuen UGB ergeben sich zahlreiche Informations- und Dokumentationspflichten Unter der Überschrift „Geschäftspapiere und Bestellscheine“ werden die Mindestangaben festgelegt, die für Geschäftsbriefe und ähnliche Dokumente gelten. Es müssen die Firma, die Rechtsform und der Sitz sowie auch Firmenbuchnummer und –Gericht angegeben werden. Die neuen Bestimmungen gelten nicht mehr nur für Geschäftspapiere und Bestellscheine, sondern in Ergänzung zu den Bestimmungen des MedG[33)] auch für E-Mails und Webseiten.

[32)] UGB Unternehmensgesetzbuch, 2007

[33)] MedG Mediengesetz, 2005

Austria and Switzerland

The situation in Austria does not differ greatly from that in Germany. The differences are only in details. This is due to the fact that the basic compliance requirements are based on the same European guidelines. Like in Germany, in Austria the electronic signature is legally binding, and commercial and tax law provisions are similar to those in Germany in matters such as digital information storage completeness, identical nature of content, orderliness, and faithfulness to the original. While it may seem that in Austria data for tax audits need only be held in list form, the same requirements apply in terms of interpretability of data. To prevent VAT fraud, essentially the same rules apply to digital invoices as in Germany.

In 2007 the new Business Code[32)] came into force, replacing the former Austrian Commercial Code. The Business Code contains numerous requirements concerning information and documentation. The header “Geschäftspapiere und Bestellscheine“ (Business Documents and Order Forms) lays down the minimum information required for business letters and similar documents – company, legal form, office location, registry number and legal domicile. The new rules apply not just to business documents and order forms, but also to e-mails and websites, supplementing the rules laid down in the Media Law[33)].

[32)] UGB Business Code, 2007

[33)] MedG Media Law, 2005

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.

Ein wesentliches Dokument ist die GeBüV[34)], Geschäftsbücherverordnung bzw. die Verordnung über die Führung und Aufbewahrung der Geschäftsbücher.

- Die GeBüV legt fest, wie die Geschäftsunterlagen geführt und aufbewahrt werden müssen
- Die GeBüV beinhaltet die Grundsätze der ordnungsgemässen Buchführung sowie die Grundsätze der ordnungsgemässen Datenverarbeitung bei elektronisch oder in vergleichbarer Weise geführten Büchern
- Die GeBüV hält die Anforderungen an Integrität, zulässige unveränderbare Speichermedien und andere Spezfikationen mit Compliance-Relevanz fest

Weitere Gesetze regeln sehr dediziert und mit Hinweisen auf geeignete Speichertechnologien und elektronische Signatur die Dokumentations- und Aufbewahrugnspflichten auch außerhalb des Handelsrechtes.

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.

Switzerland, while not in the EU, has also aligned its laws and regulations with the EU step by step. This is evident in the Code of Obligations in the rules for accounting, OR Art. 957ff, which regulate the retention of business correspondence, accounts, and accounting records in digital form.

The GeBüV[34)], the law governing the maintenance and retention of accounts, is a key document.

- The GeBüV mandates which business documents must be kept and retained.
- The GeBüV contains the principles of orderly accounting and data processing of digital or similarly kept accounts.
- The GeBüV contains requirements concerning data integrity, permissible edit-proof storage media, and other coompliance-relevant specifications.

Other dedicated laws regulate documentation custodyworthiness and retention periods, and refer to suitable storage technologies and to electronic signatures, including outside the context of commercial law.

As the European Union member states become more tightly integrated, the growth of cross-border business and electronic services over the Internet makes a uniform legal space indispensable, particularly as concerns commercial and tax law. Accordingly, the resulting compliance requirements are becoming ever more similar across Europe.

[34)] Verordnung über die Führung und Aufbewahrung der Geschäftsbücher (GeBüV Geschäftsbücherverordnung)

[34)] GeBüV law governing the maintenance and retention of accounts

Branchenspezifische Regularien

Neben den Richtlinien, die für alle Unternehmen, Organisationen, Behörden und Personen gleichmaßen gelten, gibt es zahlreiche spezielle Regelungen für bestimmte Branchen, die öffentliche Verwaltung und Geschäftstätigkeitsgebiete. Hierbei gibt es internationale wie auch nationale Regelungen.

So ist die FDA Food and Drug Administration[35)] aus den USA, mit ihren bindenden Regularien für die Herstellung von Lebensmitteln, Pharmazeutika und Medikamenten auch über die Grenzen der Vereinigten Staaten zu beachten. Bei der Beantragung eines neuen Medikamentes, mit Vorlage von allen Testnachweisen und Produktionsverfahren, hat sich die Anschaffung eines Dokumentenmanagementsystems meistens bereits gelohnt. die FDA-Kriterien, auch abgekürzt unter FDA Part 11[36)] bekannt. Um Herstellungsmethoden zu standardisieren hat die FDA ein Regelwerk mit der Bezeichnung CGMP[37)] herausgebracht. 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. Auf europäische Ebene sind die entsprechenden Regualarien als GxP[38)] mit den Teilen GSP und GMP[39)] einzuhalten.

Den Gesundheitssektor in den USA reguliert HIPAA[40)]. Das Ziel von HiPAA ist die Vordergrund steht die Reformierung der Gesundheitspflege-Industrie. Die Gesetzgebung strebt nach größerer Wirtschaftlichkeit, Verringerung von Schreibarbeiten und einfacher Identifizierung und Weiterverfolgung von Betrug durch die Auferlegung von unterschiedlichen Normen und Sicherheitsmaßnahmen gegen den Missbrauch von gesundheitsbezogenen Angaben des Bürgers. HIPAA beinhaltet so zahlreiche Dokumentations- und Vertraulichkeitsanforderungen.

Industry-Specific Regulations

In addition to guidelines that apply equally to all companies, organizations, authorities, and persons, there are numerous special regulations for individual industries, government administration, and business areas. These can be national as well as international.

Thus, the US Food and Drug Administration[35)] (FDA), with its binding regulations concerning pharmaceuticals and medications, has effects beyond the borders of the United States. A document management system usually pays for itself just in applying for a permit for a new medication, for providing all documentation on tests and production processes to FDA criteria, abbreviated as FDA Part 11[36)]. To standardize manufacturing methods, the FDA has brought out a regulation called CGMP[37)]. One of the FDA's basic requirements is that digital records be equivalent to paper records, and that electronic signatures have the same significance and uniqueness as handwritten signatures. The corresponding regulations at the European level are GxP[38)] with the GSP and GMP[39)] sections.

In the US, the HIPAA[40)] regulates the health industry. HIPAA's primary goal is health industry reform, and legislation aims at greater economy, reduction in paperwork, and simpler identification and tracing of fraud by mandating standards and safety measures to combat the misuse of citizens' health information. Thus, HIPAA contains numerous documentation and confidentiality requirements.

35) U.S. Food and Drug Administration

36) U.S. Food and Drug Administration, Federal Register Part II, 21 CFR Part 11; allgemein als "FDA-Richtlinie" bekannt

37) U.S. Food and Drug Administration , Current Good Manufacturing Practices

38) Zusammenstellung der "guten Arbeitspraxis" für die Pharmabranche mit GLP, GSP, GMP

39) "Good Storage Practice" und "Good Manufacturing Practice"

40) United States Department of Health & Human Services, Office for Civil Rights, Health Insurance Portability and Accountability Act

35) U.S. Food and Drug Administration

36) U.S. Food and Drug Administration, Federal Register Part II, 21 CFR Part 11

37) U.S. Food and Drug Administration , Current Good Manufacturing Practices

38) Compilation of "Good practices" containing GLP, GSP, GMP

39) "Good Storage Practice" and "Good Manufacturing Practice"

40) United States Department of Health & Human Services, Office for Civil Rights, Health Insurance Portability and Ac-countability Act

Aus den USA kommt auch der defacto Standard für das Records Management: DoD 5015.2[41)] im militärischen Umfeld. Der Standard des Department of Defense definiert die grundsätzlichen Anforderungen an Dokumenten-Management und Records-Management-Systeme. Die Einhaltung der Standards ist für alle Hersteller erforderlich, die für die Bundesverwaltung in den USA im militärischen und angrenzenden Bereich anbieten wollen.

Ein Beispiel für einen detaillierten Standard für den Einsatz elektronischer Vorgangsbearbeittungssysteme ist das deutsche DOMEA-Konzept[42)] DOMEA beschreibt die Anforderungen an das Dokumentenmanagement und elektronische Archivierung in der öffentlichen Verwaltung und ermöglicht auch die Prüfung und Zertifizierung von etsprechenden Produkten. DOMEA-Compliance ist bei vielen Ausschreibungen eine Anforderung. Wesentliches Ziel des DOMEA-Konzeptes ist die Einführung der elektronischen Akte. Da für diese die gleichen Gesetze, Geschäftsordnungen, Richtlinien und Vorschriften wie für Papierakten gelten, müssen behördliche Geschäftsprozesse, Vorgangsbearbeitung und Archivierung vollständig in konforme IT-Prozesse überführt werden. Das DOMEA-Konzept liefert dafür Richtlinien, ist aber trotz seiner weiten Verbreitung und der Möglichkeit der Zertifizierung kein genormter Standard.

The de-facto standard for records management comes from the US, DOD 5015.2[41)] for military contexts. This Department of Defense standard defines the basic requirements for document and records management systems. This standard must be adhered to by all manufacturers hoping to sell to the US government in military and quasi-military areas.

The German DOMEA concept[42)] is a good example of a detailed standard for digital process management systems. DOMEA discribes the requirements for document management and electronic archiving in public administration, and permits the testing and certification of products in this area. DOMEA compliance is a requirement in many RFPs. The fundamental objective of DOMEA is the introduction of the virtual folder. Since the same laws, business regulations, guidelines, and requirements exist for these as for paper folders, official processes, procedures, and archiving must be transferred to fully conformant IT processes. The DOMEA concept supplies guidelines for this, but despite its widespread use and certificability, it is not an official standard.

[41)] Department of Defense, Electronic records management software applications design criteria standard, 2007, allgemein als DoD 5015.2 bekannt

[42)] DOMEA Dokumenten-Management und elektronische Archivierung. Aktuell DOMEA Version 2

[41)] Department of Defense, Electronic records management software applications design criteria standard, 2007, generically referred to as DoD 5015.2

[42)] DOMEA document management and electronic archiving. Current Version is DOMEA Version 2

Corporate Governance

„Information Management Compliance darf nicht isoliert betrachtet werden. Compliance muss Bestandteil der Corporate Governance des Unternehmens und ständiger Begleiter aller Prozesse werden.“ [43)]

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.

Corporate Governance beinhaltet die rechtlichen und institutionellen Rahmenbedingungen, die mittelbar oder unmittelbar Einfluss auf die Führungsentscheidungen eines Unternehmens und somit auf den Unternehmenserfolg haben.

Der Ursprung für Corporate Governance liegt bereits in den 30er Jahren, als man sich verstärkt Gedanken über die Rechte der Aktionäre machte.

Corporate Governance Richtlinien

- International wurden Corporate Governance durch die OECD in Gestalt der „Principles of Corporate Governance“ 1984 verankert und 2004 aktualisier.t[44)]
- Die Europäische Kommission hat im Jahr 2004 ein European Corporate Governance Forum[45)] als Beratungsgremium eingerichtet, ohne jedoch bisher eine verbindliche Richtlinie herauszugeben.
- In Deutschland hat das Bundesministerium der Justiz im Jahr 2002 den Corporate-Governance-Kodex veröffentlicht. Dieser hat Auswirkungen auf die Unternahmensgesetze KonTraG und UMAG sowie auf das Handels- und Steuerrecht und auf den Verbraucherschutz. [46)]

[43)] Ulrich Kampffmeyer, IMC Information Management Compliance Policies und ihre Umsetzung. 2006

[44)] OECD Principles of Corporate Governance, 2004

[45)] Europäische Kommission, European Corporate Governance Forum, 2004

[46)] DCGK Deutscher Corporate Governance Kodex, 2002

3

Corporate Governance

“Information Management Compliance cannot be seen in isolation. Compliance must become part of Corporate Governance and an integral part of all processes.” [43)]

Behind terms like corporate governance, enterprise information policy or records management policy, and projects for the implementation of such policies, are many approaches to meeting compliance requirements.

Corporate governance covers the legal and institutional framework, which have proximate or immediate influence on management decisions and thus company success.

The origins of corporate governance in this sense lie in the 30s, with the goal of strengthening shareholders’ rights.

Corporate Governance Guidelines

- Internationally, corporate governance principles were laid down in 1984 by the OECD in the form of “Principles of Corporate Governance,” and updated in 2004.[44)]
- In 2004 the European Commission created a European Corporate Governance Forum[45)] as an advisory body, which however has not resulted in a binding guideline as yet.
- In Germany, the Federal Justice Ministry published the Corporate Governance Code in 2002. This has consequences for the corporate laws KonTraG and UMAG, as well as commercal and tax law, and consumer protection.[46)]

[43)] Ulrich Kampffmeyer, IMC Information Management Compliance Policies und ihre Umsetzung. 2006

[44)] OECD Principles of Corporate Governance, 2004

[45)] European Commission, European Corporate Governance Forum, 2004

[46)] DCGK German Corporate Governance Code, 2002

- In Österreich gibt es den ÖCGK Österreichischen Corporate Governance Kodex, der im Jahr 2002 veröffentlicht wurde und sich an den internationalen Vorgaben orientiert.
- In der Schweiz gibt es nur einen freiwilligen Swiss Code of Best Practice aus dem Jahr 2002.

Compliance und Information Management Compliance müssen in der Corporate Governance verankert sein. Corporate Governance und Compliance müssen auch die Umsetzung von Prozessen und die Aufbewahrung von Dokumenten berücksichtigen und entsprechende Vorgaben für die IT-Strategie machen und deren Umsetzung überprüfen.

- In Austria there is the ÖCGK, the Austrian Corporate Governance Code, published in 2002. This follows international precedents.
- In Switzerland there is only a volutary Swiss Code of Best Practice from 2002.

Compliance and information management compliance must be anchored in corporate governance. Corporate governance and compliance must take into account the implementation of processes and retention of documents, create requirements for IT strategies, and monitor their implementation.

Risiko-Management

Würde man alle nur denkbaren und eine spezifische Situation betreffenden Compliance-Anforderungen im Unternehmen vollständig umsetzen und durch technische Systeme unterstützen wollen, käme die Geschäftstätigkeit zum Erliegen. Risiko-Management ist daher ein wichtiger Bestandteil von Corporate Governance und Information Management Compliance.

Die Risiken müssen erhoben, aufbereitet und bewertet werden. Maßnahmen zur Vermeidung der Risiken und zur Einhaltung der relevanten Compliance-Anforderungen sind zu treffen. Dabei obliegt es der Geschäftsführung bzw. dem Vorstand eines Unternehmens die Verantwortung für den Umfang der Maßnahmen und deren Einhaltung zu übernehmen. Entsprechend Corporate Governance und Unternehmensgesetzen ist dies auch genau die Aufgabe der für die Geschäftstätigkeit verantwortlichen Personen und Gremien. Diese Verantwortung schließt heute bei Aktiengesellschaften auch den Aufsichtsrat ein.

In Bezug auf eine Information Management Policy sind dabei nicht nur die technischen Risiken zu betrachten sondern auch diejenigen Risiken, die sich aus der Nutzung und dem Betrieb der Systeme, den Prozessen und aus dem Ausbildungsstand der Mitarbeiter ergeben.

Risk Management

A company that tried to account for all imaginable compliance requirements in a specific situation, and support it with technical systems, would come to a standstill. Risk management is therefore an important element in corporate governance und information management compliance.

Risks must be assessed and evaluated, and action taken to prevent them and meet relevant compliance requirements. Management must take responsibility for the extent of action planned and taken. According to corporate governance and business law, this is the job of the people and committees responsible for a business. This includes the supervisory board of joint stock corporations.

In terms of an information management policy, not just the technological risks must be taken into consideration, but also the risks arising from the use and operation of the systems, the processes, and the training levels of employees.

- Zu den technischen Risiken gehören die Verfügbarkeit der Systeme, der Schutz vor unberechtigter Nutzung oder Löschung von Daten, Wiederanlauf und Recovery, Richtigkeit der Daten, Backup und Katastrophenschutz, Zugang, Konsistenz und Integrität der Datenbestände, Kompatibilität der eingesetzten Softwarestände, Virenschutz, Transaktionssicherheit, Ausfallsicherheit und Systemauslegung, Datenschutz und Datensicherheit sowie die fehlerfreie Ablauffähigkeit der Softwaresysteme.
- Zu den organisatorischen Risiken zählen Berechtigungsstrukturen, Ausbildungstände der Mitarbeiter, Betreuung der Systeme und Mitarbeiter, durchgängige Prozesse, Zuständigkeiten und Verantwortlichkeiten, korrekte und aktuelle Arbeitsanweisungen, fehlendes Bewusstsein für den Wert von Information und andere aufbauorganisations-, prozess- und personenbezogene Kriterien.

Eine Information Management Compliance Policy muss allen Faktoren der Informationsentstehung, -verarbeitung, -verwaltung, -nutzung und -speicherung berücksichtigen und in die Corporate Governance Richtlien des Unternehmens nahtlos integrieren.

- Technological risks include system availability, protection from unauthorized use or deletion of data, restarting and recovery, correctness of data, backup and catastrophe protection, access, consistency and integrity of data, software compatibility, virus protection, transaction security, protection from downtime, system design, data protection, data security, and the fault-free running of software.
- Organizational risks include authorization structures, employee training levels, system and employee support, consistent processes, responsibilities, correct and updated work instructions, understanding of the value of information, and other organizational, procedural, and person-related criteria.

An information management compliance policy must consider all factors in information origin, processing, administration, use, and storage, and integrate them seamlessly into the company's corporate governance guidelines.

Information Management Compliance Policy

„Policies und Richtlinien haben nur dann einen Nutzen, wenn sie nachgehalten und befolgt werden. Elektronische Systeme können hierbei effektiv unterstützen und die Nachvollziehbarkeit von Geschäftsgängen besser dokumentieren als dies je ein Mensch könnte.“ [47)]

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. **Policy**
   Grundregeln und Verhaltensweisen für den Umgang mit Prozessen und Informationen, die sich in der Information Management Compliance Policy 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.

[47)] Ulrich Kampffmeyer, “Rechtsänderungen im IT-Umfeld – Anforderungen an elektronische Archivsysteme“, EURO-FORUM, 2002

4

Information Management Compliance Policy

“Policies and guidelines are useful only when they are followed. Electronic systems can be an effective aid here, and document the auditability of business processes better than any person ever could.” [47)]

An information management compliance policy provides the basis for planning, implementing, and maintaining information compliance management. The policy should comprise four key points:

1. **Policy**
   The information management compliance policy contains basic rules for processes and information handling. It allocates responsibility, and makes company management aware of the importance of compliance. Company management is responsible not just for abiding by the rules, but also for setting a good example in the company as a whole.
2. **Delegation**
   The assignment of responsibility and appropriate training at operational levels should make all involved aware of the importance of compliance rules. This finds expression in work processes, workplace descriptions, contracts, and work instructions. Compliance must be consistently implemented at all levels of an organization, as appropriate for the job description and area of responsibility of each employee.

[47)] Ulrich Kampffmeyer, “Rechtsänderungen im IT-Umfeld – Anforderungen an elektronische Archivsysteme“, EURO-FORUM, 2002

3. **Nachhaltung**
   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 integre Verfügbarkeit von Information ein hoher qualitativer Nutzen gegeben, der sich auch betriebswirtschaftlich auszahlt.

3. **Follow-through**
   Adherence to the rules must be monitored regularly. This includes quality assurance programs as well as audits, focusing on continuous improvement of processes and tracing documentation on the actions taken.

4. **Secure systems**
   IT systems must have sufficient functionality, security, and availability, and ensure auditability. Compliance is not just limited to application functionality and document management, but comprises the entire operation of a solutuion.

Although compliance has much to do with documents and documentation, it is important to always think in terms of processes. The main problem in compliance is that actions start out costing too much money and organizational effort, without generating any additional revenue. Therefore compliance is usually not popular with management. But when a company is well structured and organized, the resulting transparency, auditability, and integral availability of information gives benefits that pay in day-to-day business.

Aspekte der Information Management Compliance

Bei der Erstellung einer Richtlinie sind folgende Aspekte zu berücksichtigen:

- Compliance ist vorrangig ein organisatorischer Prozess. Systeme dienen zur Unterstützung des Prozesses. Sie sind nicht in sich „compliant“. Zertifikate der Ordnungsmäßigkeit und Compliance-Einhaltung beziehen sich auf das indviduelle Unternehmen und den Einsatz der Lösungen, nicht auf Produkte.
- Moderne Software kann alle notwendigen Informationen über die Systeme und Komponenten sowie deren Nutzung selbst aufzeichnen. Die Zukunft liegt in selbstdokumentierenden Systemen, die den Menschen von der Dokumentation, Überprüfung und Nachhaltung entlasten. Die Aufzeichnung und Auswertung kann im Widerspruch zu Anforderungen des Datenschutzes stehen.
- Compliance ist nicht punktuell und nicht statisch. Compliance muss kontinuierlich über alle Ebenen, alle Mitarbeiter, alle Prozesse und alle Systeme des Unternehmens gelebt werden.
- Compliance darf nicht nur als lästige, die Geschäftstätigkeit behindernde Aufgabe betrachtet werden. Compliance vermeidet nicht nur Risiken sondern schafft Transparenz im Unternehmen, erlaubt die Erkennung von Potentialen und die Verbesserung der Organisation und Prozesse. Compliance kann so auch zur Wertsteigerung und Wertschöpfung eingesetzt werden.
- Systeme nur zur Erfüllung der Compliance-Anforderungen einzuführen ist unwirtschaftlich. Systeme müssen die Compliance-Anforderungen so quasi nebenbei mit erfüllen.
- Neben die sichtbare Welt der Geschäftsprozesse treten Compliance-Prozesse in den Systemen selbst. Workflow, Business Process Management und Protokollierung im Rahmen des Records Management liefern notwendige Informationen.
- Compliance ist kein Projekt. Compliance kann im Rahmen eines Projektes initiiert und eingeführt werden, ist jedoch ein kontinuierlicher Prozess.

Aspects of Information Management Compliance

When drawing up a guideline, the following aspects must be born inmind:

- Compliance is primarily an organizational process. Systems merely support the process, but are not in and of themselves compliant. Certificates of proper procedure and compliance refer to individual companies and the way they use IT solutions, not to the solutions themselves.
- Modern software can record all necessary information on systems and components, and their use. The future lies with self-documenting systems that relieve people of the burden of documentation, checking, and follow-through. Recording and evaluating this information can contravene data protection, however.
- Compliance is neither one-time nor static. Compliance must be continuously lived at all levels, by all employees, and in all processes and systems of a company.
- Compliance must not be seen as an annoying task that gets in the way of business. Not only does compliance help prevent risk, it also creates transparency in a company, helps make potential visible, and promotes the improvement of organization and processes. Thus, compliance can promote value addition and growth.
- It is uneconomical to implement systems solely for the purpose of meeting compliance requirements. Systems should meet these requirements “automatically” on the side.
- Alongside the visible world of business processes, compliance processes enter into systems themselves. Workflow, business process management, and logging as part of records management supply information that is needed for many purposes.
- Compliance is not a project. Compliance can be initiated and implemented within the framework of a project, but it is an onging process.

- Der Mensch ist bequem und damit das größte Hindernis für Compliance. Information Management Compliance muss vorausschauend und aktiv gelebt werden. Die Bedeutung von Compliance wird auf Entscheiderebene immer noch unterschätzt.
- Compliance ist unumgänglich. IT-Compliance sorgt für Transparenz in der virtuellen Welt der Systeme. Ohne IT-Compliance ist eine rechtliche Gleichberechtigung elektronischer und papiergebundener Information nicht möglich.
- Eine Information Management Compliance Policy regelt den Umgang mit Information. Wird sie nicht umgesetzt und ständig nachgehalten, ist sie wertlos. Ohne sie fehlt der Maßstab um Risiken, den Wert von Information und die Abhängigkeit von Information zu erkennen.

- People are lazy and therefore the greatest hindrance to compliance. Information management compliance must be practiced proactively and predictively. Many decision-makers still underestimate the importance of compliance.
- Compliance is indispensable. IT compliance creates transparency in the virtual world of systems. Without IT compliance, the legal equivalence of paper-based and digital information is not possible.
- An information management compliance policy controls the use of information. If it is not implemented and constantly followed though on, it is valueless. Without it, there is no benchmark for recognizing risks, the value of information, and information dependencies.

5 Compliance und Records Management

„Immer mehr Information entsteht elektronisch. Der Ausdruck dieser Information auf Papier ist nur noch eine mögliche Form der Repräsentation. Das elektronische Dokument wird selbst zum Original.“ [48)]

Um alle Informationen in einem Unternehmen, einer Behörde oder einer Organisation effektiv verwalten zu können, ist der Einsatz von 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.

[48)] Ulrich Kampffmeyer, „Paradigmenwechsel im Dokumenten-Management“, DMS EXPO, 1998

5 Compliance and Records Management

“More and more information is created digitalally. Printingg this information out on paper is just one possible form of representation. The electronic document itself is now the original.” [48)]

Records management (often called ERM, Electronic Records Management, or EDRM, Electronic Document and Records Management) is necessary for the efficient administration of all of the information in a company, government office, or organization. Records management goes beyond digital preservation:

- Records management systems have references to information on paper, in folders, or on microfilm. This allows complete control of “mixed” processes that require parallel activities on different media.
- Records management systems have electronic filing plans and thesauri which enable a structured, comprehensible, and clear ordering of information. They support multiple filing iterations based on different topic criteria and the management of different versions and statuses of the filing structure.

This makes records management a basic component for the imaging of virtual digital folders and for digital processing of information subject to compliance regulations.

[48)] Ulrich Kampffmeyer, „Paradigmenwechsel im Dokumenten-Management“, DMS EXPO, 1998

Records Management nach ISO 15489

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.

Die Norm definiert „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 regulativer Vorgaben vollständig, richtig, authentisch, beweiskräftig und nachvollziehbar dokumentieren“.[49)]

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 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 Norm 15489 beschreibt in Teil 2 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 transparent, geordnet und nachvollziehbar zu verwalten. Professionelles Records-Management ist damit eine Grundvoraussetzung zur Erfüllung von Compliance-Vorgaben.

[49)] ISO, ISO Norm 15489 Records Management, 2001 (Schriftgutverwaltung)

Records Management per ISO 15489

ISO 15489 Records Management presents management guidelines for company policy and procedure for record management, and is a guide for implementing records management systems.

As defined by the standard records management is the „Field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records”.[49)]

The basic principles of record management are contained in numerous national regulations for public administration and archiving, as well as in an international standard. ISO 15489 Part 1 helps to:

- Define which documents must be generated and what information included in these documents, and what level of exactitude is necessary.
- Decide on the form and structure in which documents should be generated and captured.
- Define the requirements for retrieval and use of documents, and how long they need to be archived for, in order to meet these requirements.
- Define how documents should be organized in order to best support their efficient use.

ISO 15489 Part 2 lays out the steps for implementation, from the initial analysis and indentification of the requirements, to the implementation of a records management system and company policies surrounding it.

While the ISO standard does not contain specific criteria for the technical testability of systems, it is nevertheless a valuable guide for administering company information in a transparent, organized, auditable fashion. Professional records management is thus a basic tool for meeting compliance requirements.

[49)] ISO, ISO Standard 15489 Records Management, 2001

MoReq Model Requirements

MoReq[50] ist die wichtigste Spezifikation für elektronisches Dokumenten- und Records-Management in Europa. Die Abkürzung MoReq steht für „Model Requirements for the Management of Electronic Records“. MoReq wurde im Auftrag der Europäischen Kommission[51] durch das DLM-Forum[52] erarbeitet. Die Vorteile von MoReq liegen darin, dass Anbieter ihre Produkte zukünftig nur noch auf einen europäischen Standard ausrichten müssen, und nicht mehr für jedes Land einen eigenen Standard in der Implementierung zu berücksichtigen haben.

MoReq in der ersten Version (MoReq1) wurde bereits von zahlreichen nationalen Standards als maßstab genutzt, so z.B. TNA in England, Noark in Norwegen oder Remano in den Niederlanden. MoReq beschränkt sich jedoch nicht nur auf die öffentliche Verwaltung oder Nationalarchive sondern ist ein offener Standard, der auch in der freien Wirtschaft zum Einsatz kommt. MoReq1 wurde inzwischen in 10 Sprachen übersetzt und konnte sich als europäische Alternative zum amerkanischen DoD 5015.2 Standard etablieren. Da MoReq1 bereits 2001 entstanden ist, wurde von der Europäischen Kommission zusammen mit dem DLM Forum eine Aktualisierung und Erweiterung vereinbart.

Wesentliche Neuheiten in MoReq2[53] sind:

- **Fexiblere Struktur**
  Berücksichtigung nationaler Anforderungen, Erweiterung des Funktionenkataloges, Definition optionaler Komponenten für unterschiedliche Umgebungen und Anforderungen
- **Erweitertes Basismoduls**
  Zugriffsverwaltung, Aufbewahrungsfirsten und Vernichtung, Export, Übertragung und Dokumentenaustausch, langfristige Bewahrung, konkretere Fassung und Beschreibung der Metadaten
- **Optionale Module**
  Content-Management, Hybridsysteme, Workflow und Vorgangs-/Fallbearbeitung, E-Mail-Management, Dokumentenmanagement und Collaboration, Kryptographie, Verschlüsselung, Wasserzeichen, Digital Rights Management, Interoperabilität und Offenheit sowie dezentrale Systeme

[50] Archiv der Europäischen Kommission, Model Requirements for the Management of Electronic Documents and Records, 2001

[51] IDA Interchange of Data between Administrations, Katalog gemeinsamer Werkzeuge und Techniken

[52] DLM Network EEIG, DLM-Forum

[53] Ulrich Kampffmeyer; Sarah Risse, Artikel „MoReq Update“

MoReq Model Requirements

MoReq[50] is the most important European specification for electronic document and records management. The abbreviation MoReq stands for “Model Requirements for the Management of Electronic Records.” MoReq was put together by the DLM Forum[52] at the reqest of the European Commission[51]. Its advantage is that vendors need in future orient their products to just one European standard, instead of different implementation standards for each country.

The first iteration of MoReq (MoReq1) was used as a benchmark for many national standards, such as TNA in England, Noark in Norway, and Remano in the Netherlands. MoReq is not limited just to pubic administration or national archives, but is an open standard that has application in the private sector. MoReq1 has been translated into 10 languages, and may establish itself as the European alternative to the American DoD 5015.2 standard. Since MoReq1 came out in 2001, the European Commission and the DLM Forum have agreed on an updated and expanded version.

The main innovations in MoReq2[53] are:

- **More flexible structure**
  Consideration of individual national requirements, expanded function catalog, definition of optional components for different environments and needs
- **Expanded basic module**
  Access management, retention periods and destruction, export, transfer, and document exchange, long-term storage, more specific description of metadata
- **Optional modules**
  Content management, hybrid systems, workflow and process/case handling, e-mail management, document management and collaboration, cryptography, encoding, watermarks, digital rights management, interoperabiliy and openness, decentral systems

[50] Archive of the European Commission, Model Requirements for the Management of Electronic Documents and Records, 2001

[51] IDA Interchange of Data between Administrations, Catalogue of Common Tools and Techniques

[52] DLM Network EEIG, DLM-Forum

[53] Ulrich Kampffmeyer; Sarah Risse, „MoReq Update“

- **MoReq Compliance Test**
  Beurteilung von Produkten, Entwicklung von standardisierten Testskripten, Unterstützung einheitlicher MoReq-Compliance-Evaluierungen durch Tests als Vorlage für ein Zertifizierungsverfahren

Ende des Jahres 2007 wird die neue Version MoReq2 und das dazugehörige Test- und Zertifizierungsverfahren für Records Management Produkte fertig gestellt[54].

Übergreifende Ansätze

Vielfach wird Records Management wie die althergebrachte Archivverwaltung als eigenständige Lösung betrachtet. Bedeutsamer wird aber unter Compliance-Gesichtspunkten die Integration in die IT-Landschaft als Infrastruktur, die alle Komponenten berücksichtigt und die Durchgängigkeit der Dokumentation über alle Prozesse, Datenquellen und Anwendungen sicherstellt. Records Management ist daher eine wichtige Komponente in Konzepten wie ECM Enterprise Content Management, ILM Information Lifecycle Management und elektronischer Archivierung.

ECM Enterprise Content Management

"Enterprise Content Management sind die Technologien zur Erfassung, Verwaltung, Bereitstellung, Speicherung und Langzeitarchivierung von elektronischen Inhalten und Dokumenten zur Unterstützung der Geschäftsprozesse im Unternehmen."[55]

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.

54) Der MoReq2 Standard wird im Auftrag der Europäischen Kommission vond er Firma SERCO erstellt. MoReq-Information in Deutsch, www.moreq2.de, in Englisch www.moreq2.eu.

55) AIIM Association for Information and Image Management International, 2005

- **MoReq Compliance Test**
  Evaluation of products, development of standardized test scripts, support of uniform MoReq compliance evaluations through tests as a basis for a certification process

At the end of 2007, the new MoReq2 and its associated test and certification procedures will be made available for records management products. [54]

Comprehensive Approaches

Often, records management, like traditional archive administration, is seen as a discrete solution. But in terms of compliance, it is more important to integrate it into the IT landscape as an infrastructure which takes into account all components and ensures the consistency of documentation of all processes, data sources, and applications. Records management is thus an important component in ECM (Enterprise Content Management), ILM (Information Lifecycle Management) and digital preservation.

ECM Enterprise Content Management

"Enterprise Content Management is the Technologies used to Capture, Manage, Store, Preserve, and Deliver Content and Documents related to Organizational Processes." [55]

ECM comprises conventional document-riented information technologies such as scanning, document management, knowledge management, workflow, archiving etc., and integrates the host and client server world with web content management, portal, and other internet technologies.

54) The MoReq2 standards ist authored by the company SERCO, who was contracted by the European Commission. Detailed information www.moreq2.eu.

55) AIIM Association for Information and Image Management International, 2005

Die Komponente Verwaltung sowie Verarbeitung von Information beinhaltet Document Management, Records Management, Business Process Management/ Workflow, Web Content Management und Collaboration. [56)]

Ein wesentliches Ziel von Enterprise Content Management ist die Sicherstellung der Einhaltung von Compliance-Anforderungen. Komponenten wie elektronische Archivierung, virtuelle Akten, Records Management und Process Management sind hierfür die entsprechenden Bestandteile.

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.

Information wird mit der Geschäftstätigkeit durch Prozess-Management und Serviceleistungen in Zusammenhang mit Anwendungen, Metadaten, anderen Informationen und Daten koordiniert.“ [57)]

Die Compliance-Anforderungen in den USA führten auch zu neuen Trends wie ILM Information Lifecycle Management. Getrieben von Hardware- und Speichersoftwareanbietern zielten diese Lösungen besonders auf die Erfüllung von Compliance-Anforderungen wie SOX. Daher ist auch E-Mail-Archivierung eine Komponente, die häufig unter der Flagge ILM angeboten wird. Kern ist dabei, dass Speichersysteme um immer mehr Softwarekomponenten ergänzt werden und in die traditionellen Bereiche von Records Management, Archivierung und Dokumentenmanagement vordringen.

ILM setzt auf herkömmlichen HSM Hierarchischem Speichermanagement auf und ergänzt dieses um Regeln, Prozesse und nur einmal beschreibbare Speichersysteme.

[56)] AIIM international 2003

[57)] The Storage Networking Industry Association (SNIA), ILM definition, 2004

The information administration and processing components include document management, records management, business process management/workflow, web content management, and collaboration. [56)]

One of the key objectives of enterprise content management is to ensure adherence to compliance requirements. Components such as digital preservation, virtual folders, records management, and process management are examples of this.

ILM Information Lifecycle Management

“Information Lifecycle Management is compromised of the policies, processes, practices and tools used to align the business value of information with the most appropriate and cost effective IT infrastructure from the time information is conceived through its final disposition.

Information is aligned with business processes through management processes and service levels associated with applications, metadata, information and data” [57)]

The compliance requirements in the US are leading to new trends, such as ILM or Information Lifecycle Management. Driven by storage hardware and software vendors, these solutions are targeted specifically at compliance regulations such as SOX. Therefore they include e-mail archiving as a component that often goes under the name ILM. The take-home is that storage systems are being supplemented with more and more software components and pushing into the traditional preserves of records management, archiving and document management.

ILM sits on top of traditional hierarchical storage management (HSM) and adds to it rules, processes, and write-once storage systems.

[56)] AIIM international 2003

[57)] The Storage Networking Industry Association (SNIA), ILM definition, 2004

Elektronische Archivierung und Speichersysteme

"Elektronische Archive sind das Gedächtnis der Informationsgesellschaft"[58)]

Elektronische Archivierung steht für die unveränderbare, langzeitige Aufbewahrung elektronischer Information. Für die elektronische Archivierung werden in der Regel spezielle Archivsysteme eingesetzt. Der Begriff Elektronische Archivierung fasst unterschiedliche Komponenten zusammen, die im angloamerikanischen Sprachgebrauch separat als „Records Management", „Storage" und „Preservation" bezeichnet werden. [59)]

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 langzeitig unverändert und sicher aufbewahrt werden müssen. Man unterscheidet in Deutschland die Begriffe Langzeitarchivierung und Revisionssichere Archivierung:

- Unter elektronischer Langzeitarchivierung versteht man Archivsysteme, die Daten und Dokumente über einen Zeitraum von mindestens 10 Jahren verfügbar halten.
- 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. [60)]

Elektronische Archivsysteme stellen für die gespeicherten Dokumente, dazugehörige Daten und Protokolle der Transaktionen die sichere Ablage dar, die die Nachvollziehbarkeit, Unveränderbarkeit und Vollständigkeit gewährleistet.

[58)] Erki Liikanen, EU-Kommissar, DLM Forum 1999

[59)] Verband Organisations- und Informationssysteme e. V. (VOI), Grundsätze der elektronsiche Archivierung, 1997

[60)] Dr. Ulrich Kampffmeyer, PROJECT CONSULT, 1996

Digital Preservation and Storage Systems

"Electronic Archives are the Memory of the Information Society"[58)]

Digital preservation refers to the unalterable, long-term storage of electronic information. As a rule special archiving systems are used for digital preservation. The term digital preservation encompasses different components, which in common parlance are separately designated as "records management," "storage," and "preservation." [59)]

The objective of a digital preservation system is to keep information secure, regardless of source, originator, or subsequent use, and make it available with database support upon request. Preservation systems are therefore services which are available to all users who generate information that needs to be retained long-term and securely. In Germany, a distinction is made between long-term archiving and auditable archiving:

- Long-term digital preservation is used to denote archive systems that keep data and documents available for at least ten years.
- Auditable digital preservation is used to denote archive systems which meet the requirements of Commercial Code § 239, Tax Procedure Act §147 and GoBS in terms of keeping data and documents secure, unaltered, complete, orderly, reproducible without loss, and searchable with database support. [60)]

Digital preservation systems are a secure archive for documents, their data, and transaction records, ensuring their auditability, unalterability, and completeness.

[58)] Erki Liikanen, EU- commissioner, DLM Forum 1999

[59)] Verband Organisations- und Informationssysteme e. V. (VOI), Grundsätze der elektronsiche Archivierung, 1997

[60)] Dr. Ulrich Kampffmeyer, PROJECT CONSULT, 1996

Speichertechnologien für die elektronische 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.

Für die unveränderbare Langzeitarchivierung wurden Speichertechnologien geschaffen, die nur das einmalige Beschreiben erlauben. Dieses Verfahren nennt man WORM: „Write Once, Read Many“[61)]. 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[62)]: nur einmal selbst beschreibbare Compact Disk Medien
- DVD-WORM[63)]: ähnlich wie die CD wird bei der DVD die Speicheroberfläche irreversibel im Medium verändert.
- 5¼“ WORM als UDO[64)] oder PDD[65)]
  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.

Für die Verwaltung und Nutzung dieser 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.

[61)] WORM, Write Once, Read Many
[62)] CD-WORM, Compact Disc - Write Once, Read Many
[63)] DVD-WORM, DVD - Write Once, Read Many
[64)] UDO, Ultra Density Optical, ISO/IEC 17345
[65)] PDD, Professional Disc for Data

Storage Technologies for Electronic Archiving

Systems for the safe storage of data and documents are an essential part of any preservation or compliance solution. Storage systems today consist of administration and control software, as well as the actual storage media per se.

Edit-proof long-term archiving requires storage technologies that allow writing just once. These are called WORM (Write Once Read Many)[61)]. Orginally the term was used only for digital-optical storage media such as CDs. The physical properties of the media themselves inherently prevent alteration of the data stored on them and have a much longer lifetime that the older magnetic storage media. Today, this category includes the following types of media:

- CD-WORM[62)]: Compact discs that allow recording (writing) just once
- DVD-WORM[63)]: Like with CDs, the DVD surface is irreversibly altered during recording.
- 5¼“ WORM as UDO[64)] or PDD[65)]
  These media and drives are traditional technologies designed especially for digital preservation. The discs are protected by a sleeve and thus less exposed to outside influences than CDs and DVDs, which were developed for the consumer market.

So-called jukeboxes, or automatic disc changers, are normally used to manage these media. Jukeboxes are driven by software and provide the desired data on demand. The software usually also enables administration of media outside the jukebox which must be manually accessed when needed.

[61)] WORM, Write Once, Read Many
[62)] CD-WORM, Compact Disc - Write Once, Read Many
[63)] DVD-WORM, DVD - Write Once, Read Many
[64)] UDO, Ultra Density Optical, ISO/IEC 17345
[65)] PDD, Professional Disc for Data

Neben die klassischen Archivspeicher, die auf rotierenden, digital-optischen Wechselmedien basieren, treten inzwischen zwei weitere Technologien:

- WORM-HD[66]: RAID-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.
- WORM-Tape[67]: 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 für größere Unternehmen und Verwaltungen mit Rechenzentren und als Komponenten in einer Speicherhierarchie stellen Festplatten- oder WORM-Tape-Archive eine Option dar, da sie sich einfach in den laufenden Betrieb und vorhandene Infrastrukturen integrieren lassen.

Generell gilt aber für alle Speichermedien:

- Ein Medium allein und Medien nur einen Typs sind nie genug
- Die Sicherheit von Hard- und Software allein ist nicht ausreichend – der gesamte Betrieb, die Nutzung und die Verfahren müssen sicher sein
- Die regelmäßige Prüfung der Lesbarkeit und Verarbeitungsfähigkeit vermeidet Risiken und Verluste
- Bereits bei der Erstinstallation eines elektronischen Archives ist die Migration mit einzuplanen

[66] WORM-HD, Write Once, Read Many – Hard Disc
[67] WORM-Tape, Write Once, Read Many - Tape

In addition to the classic digital-optical preservation based on removable discs, there are two further technlogies

- WORM-HD[66]: RAID hard drives using special software to provide the same characteristics as conventional WORM media. Encoding during recording and special address allocation prevent overwriting or alteration of the data on the drive, once it has been recorded.
- WORM-tape[67]: Magnetic tape, again with characteristics that provide the functions of conventional WORM media. Special tape, protected cassettes, and specially designed drives prevent overwriting and editing.

WORM-HD and WORM-tape are viable alternatives for large computing centers in particular, since they are simple to integrate into the exsting infrastructure.

A few principles apply to all storage technologies:

- One medium alone, or media of just one type, is never enough.
- Hard- and software security alone is not enough – the entire operation, usage, and process must be secure.
- Regular inspection of readability and processability prevents risks and losses.
- Migration should be planned for right from the initial installation of any digital archive.

[66] WORM-HD, Write Once, Read Many – Hard Disc
[67] WORM-Tape, Write Once, Read Many - Tape

10 Compliance-Merksätze

6

10 Compliance Rules

„Wichtigster Grundsatz: Keine Angst vorm Thema Compliance!“[68)]

Als Zusammenfassung eine Reihe von Merksätzen zur Information Management Compliance[69)]:

1. Compliance-Themen gehören auf die Entscheiderebene, 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.

“Most important: Don’t be afraid of compliance!” [68)]

In summary, 10 rules for information management compliance [69)]:

1. Compliance is a C-level matter, and executives are responsible for its implementation and execution.
2. Compliance requirements must be part of any corporate governance strategy.
3. All companies need a guideline for working with information – an information policy that includes compliance requirements and solutions for meeting them.
4. Compliance must be implemented consistently within a company in order to be effectual.
5. Fulfillment of compliance requirements is not a one-time project, but an ongoing process.
6. Compliance requirements must be part of any corporate governance strategy.
7. Information management compliance affects not just software and systems, but the way those systems are used, as well as company processes and organization.
8. Compliance requirements affect not just digital arcives, but all system components in which custodyworthy data, information, and documents are generated, used, and managed.
9. Compliance requirements should be met not only for their own sake, but also as a tool to create more transparency and security within a company, and make it more competitive in an age of information.
10. Compliance is nothing to be afraid of. Instead of shying away from it, companyies should start by examining what compliance requirements are relevant for what application cases.

[68)] Ulrich Kampffmeyer, Vortrag “Compliance“. DMS EXPO 2004

69) Ulrich Kampffmeyer, Compliance. Documentum Whitepaper, 2004

[68)] Ulrich Kampffmeyer, Keynote presentation “Compliance“. DMS EXPO 2004

69) Ulrich Kampffmeyer, Compliance. Documentum Whitepaper, 2004

7 Ausblick

„Lösungen für die Unterstützung von Compliance wie E-Mail-Management und Records Management sind heute die wichtigsten Markttreiber für den Einsatz von Enterprise Content Management.“[70)]

Anbieter von Informations- und Dokumenten-Management-Lösungen wittern, aufgrund der in nahezu allen Staaten wachsenden Compliance-Anforderungen, das große Geschäft. Compliance-Angebote sind bei den meisten ECM Enterprise-Content-Management-Anbietern mittlerweile fester Bestandteil des Produktangebotes.

Compliance-Anforderungen treiben den Markt für Dokumenten-Technologien

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. Das Gleiche gilt für steuerrelevante Daten. Sie separat und nur für den Steuerprüfer aufzubewahren ist unwirtschaftlich. Auch dedizierte Systeme nur für Daten aus dem ERP oder nur für gescannte Dokumente sind aus Compliance-Gesichtspunkten nicht empfehlenswert. Alle Informationen gehören unabhängig von ihrem Format entsprechend ihrem Inhalt und Rechtscharakter in einen Sachzusammenhang.

[70)] Ulrich Kampffmeyer, „Compliance“. Documentum Whitepaper 2004

7 Outlook

“Solutions for supporting compliance, such as e-mail and records management, are today’s leading market drivers for enterprise content management.” [70)]

Information and document management vendors see the growing compliance requirements in almost every country as a great business opportunity. Most enterprise content management vendors offer compliance solutions as a key part of their product offerings.

Compliance is driving the market for document technologies

Of course there are differences in the scope and goals of the software and systems on the market. The larger vendors aim for complete control and documentation of the flow of information, and do not limit themselves to preservation or records management. Other vendors offer dedicated e-mail archiving solutions which brings the risk for users of getting stuck with an isolated compliance solution. E-mails and their attachments should not be stored on an island, but instead archived in their subject context, in virtual client, product, or process folders. Merely archiving e-mails ultimately creates more problems than it solves. The same goes for tax-related data. Preserving this information separately ond only for the auditor is uneconomical. Likewise, dedicated systems just for ERP data or scanned documents cannot be recommended from a compliance point of view. All information, regardless of format, should be preserved in its context, in a way appropriate to its content and legal character.

[70)] Ulrich Kampffmeyer, „Compliance“. Documentum Whitepaper 2004

Ein wesentliches Konzept ist daher die Nutzung einheitlicher Speichersysteme, die unabhängig von Format, Quellsystem oder Erzeuger Informationen recherchierfähig und im Kontext allen Anwendungen zur Verfügung stellen. Aber nicht der Speicherort und seine Verwaltung mit einem Records-Management-System allein ist die Lösung für Compliance. Es gilt die Prozesse selbst zu unterstützen und selbstdokumentierende Systeme zu schaffen, die den Anwender entlasten sowie Vollständikeit und Richtigkeit der Aufzeichnungen sicherstellen.

Lösungen zur Unterstützung von Compliance-Anforderungen sind daher zukünftig eher Infrastruktur denn separate Einzelsysteme.

Der Markt und das Produktangebot reagieren auf diese Anforderung mit der Bereitstellung von Diensten für SOA-Architekturen, ECM Enterprise-Content-Management-Suiten, die alle Aspekte berücksichtigen, und Business-Process-Management-Komponenten, die die prozessualen Aspekte von Compliance abdecken sollen.

Dennoch bleibt bei Information Management Complaince die wichtigste Voraussetzung nicht nur in Systemen denken. Alle Komponenten – Richtlinien, Geschäftsprozesse, Aufbauorganisation, Mitarbeiter – müssen zusammenspielen. Einzellösungen gibt es bei Compliance nicht. Durchgängigkeit und Nachhaltigkeit sind entscheidend.

Systeme können Compliance-Prozesse unterstützen, überwachen und dokumentieren. Sie selbst sind jedoch nur ein Baustein in einem größeren Gesamtprozess.

In dem Maße, wie das Thema Compliance in Wirtschaft und Gesellschaft an Raum gewinnt, müssen alle Softwaresysteme eines Unternehmens oder einer Organsiation Compliance-fähig gemacht werden. Dies geht über spezielle Systeme wie Records Management oder elektronische Archivierung weit hinaus. Der Markt wird auf diese sich verändernde Anforderung reagieren, denn

„Ohne Information Management Compliance kann die Informationsgesellschaft nicht funktionieren.“[71)]

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

[71)] Ulrich Kampffmeyer, Marcus Evans Conference „Content Management – The driving factor for successful eBusiness”, Berlin, 2001

Therefore, the use of uniform storage systems is a key concept. These systems make information searchable and available in the context of all applications, regardless of the format, origination system, or source of the information. Yet the storage location and its administration via a records management system are not compliance solutions in and of themselves. Processes must be supported, and self-documenting systems created, that unburden the user and ensure the completeness and correctness of recorded data.

Therefore, solutions that support compliance will in the future be part of infrastructure, rather than separate systems.

The market and product offerings are reacting to this need by providing services for SOA architectures, ECM suites that cover all aspects, and business process management components that cover the procedural aspects of compliance.

But the most important requisite for information management compliance is to avoid thinking only in terms of technology systems. All components – guidelines, business processes, organizational structures, employees – must work together. There are no single solutions to compliance. Consistency and follow-through are the decisive factors.

Systems can support, monitor, and document compliance processes. But they are just one part of a larger process.

To the extent that compliance gains currency in business and society, all software systems in an organization must be made compliant. This goes far beyond purpose-designed systems like records management or digital preservation. The market will respond to this changing need, because

“The information society cannot function without information management compliance.” [71)]

Compliance is something that every company needs to face, in order to thrive in the information age.

[71)] Ulrich Kampffmeyer, Marcus Evans Conference „Content Management – The driving factor for successful eBusiness”, Berlin, 2001

Literatur

Bibliography

Bundesministerium der Finanzen: *Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)*. BStBl 1995 I S. 738, 1995 (GoBS)

Bundesministerium der Finanzen: *Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)*, BGBl. I S. 1542, 2001 (GDPdU)

Bundesministerium der Justiz: *Abgabenordnung (AO), §§ 146, 147, 200*, BGBl. I S. 3866, ber. 2003 S. 61, 2002 (AO)

Bundesministerium der Justiz: *Bürgerliches Gesetzbuch (BGB) §§ 126, 127*, BGBl. I S. 42, ber. S. 2909 und BGBl. 2003 S. 738, 2002 (BGB)

Bundesministerium der Justiz: *Gesetz über elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister (EHUG)*, BGBl. 2006 Teil I Nr. 52, 2553 ff., 2007 (Unternehmensregister)

Bundesministerium der Justiz: *Gewinnabgrenzungsaufzeichnungsverordnung (GAufzV)*, BGBl. I S. 2296, 2003 (GAufzV)

Bundesministerium der Justiz: *Handelsgesetzbuch (HGB), §§ 239, 257*, (Letzte Änderung) BGBl. I S. 1330, 1379,2007 (HGB)

Bundesministerium der Justiz: *Zivilprozessordnung (ZPO), §§ 292a, 286, 130, 371*, BGBl. I S. 3202, ber. 2006 I S. 431, 2007 I S. 1781, 2005 (ZPO)

Bundesministerium des Innern: *DOMEA-Konzept (Konzept für Dokumenten-Management und elektronische Archivierung in der öffentlichen Verwaltung)*, Fassung 2.1, 2005 (DOMEA)

Bundesministerium für Justiz: Bundesgesetz über besondere zivilrechtliche Vorschriften für Unternehmen (Unternehmensgesetzbuch (UGB)), BGBl. I Nr. 120/2005, 2005 (Handelsrechts-Änderungsgesetz (HaRÄG))

Cornell Law School, Legal Information Institute: *Federal Rules of Civil Procedure (FRCP)*, 2006 (FRCP)

EU-Parlament: *Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt ("Richtlinie über den elektronischen Geschäftsverkehr")*, 2000 (2000/31/EG)

EU-Parlament und Rat: *Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen*, 1999 (1999/93/EG)

EU-Parlament und Rat: *Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen, zur Änderung der Richtlinien 78/660/EWG und 83/349/EWG des Rates und zur Aufhebung der Richtlinie 84/253/EWG des Rates (8. EU-Richtlinie)*, 2006 (2006/43/EG)

Europäische Kommission: *Model Requirements for the Management of Electronic Documents and Records. MoReq Specification*. INSAR Supplement VI, ISBN 92-894-1290-9. 2001

Finra - the Financial Industry Regulatory Authority: *NASD 3010 und NASD 3110*

handelsblatt.com/wirtschaftswiki: *Definition Basel II*, 2005 (Basel_II)

ISO: *DIN ISO 15489-1 (Information and documentation - Records management - Part 1: General)* und *DIN ISO 15489-2 (Information and documentation - Records management - Part 2: Guidelines)*, 2001 (15489-1 und 15489-2)

Kahn, Randolph A.; Blair, Barclay T.: *Information Nation - Seven Keys to Information Management Compliance*. AIIM, 2004

Kampffmeyer, Ulrich: *IMC Information Management Compliance Policies und ihre Umsetzung*. IIR Kongress „IT-Compliance“, 2006

Kampffmeyer, Ulrich: *Corporate Governance*, PROJECT CONSULT Newsletter 20050817, ISSN 1439-0809, 2005 (20050817)

Kampffmeyer, Ulrich: *Dokumenten-Technologien: Wohin geht die Reise?*, PROJECT CONSULT, ISBN 3980675645, 2003.

Kampffmeyer, Ulrich: *Compliance*. Documentum Whitepaper zum Keynote-Vortrag „Regulative Vorgaben beflügeln den Markt für Dokumenten-Technologien“, DMS EXPO 2004, Essen, PROJECT CONSULT/Advanstar, 2004 (Compliance Whitepaper)

Kampffmeyer, Ulrich; Groß, Stefan und Lamm, Martin: *GDPdU: Finanzgerichte weiten das Recht auf Datenzugriff aus*, PROJECT CONSULT Newsletter 20070720, ISSN 1439-0809, 2007

Literatur
Bibliography

Kampffmeyer, Ulrich und Risse, Sarah: *Artikel „MoReq Update - Die Model Requirements für elektronisches Records Management der Europäischen Kommission werden aktualisiert und erweitert“*, 2007 (MoReq-Update)

Kampffmeyer, Ulrich und Rogalla, Jörg: *Grundsätze der elektronischen Archivierung*. VOI-Kompendium Band 3. Verband Organisations- und Informationssysteme e. V (VOI), ISBN 3-932898-03-6, 1997

Kampffmeyer, Ulrich; Henstorf, Karl-Georg; Prochnow, Jan et. al.: *Grundsätze der Verfahrensdokumentationen nach GoBS*. VOI-Kompendium Band 4, Verband Organisations- und Informationssysteme e. V (VOI), ISBN 3-932898-04-4, 1999

Kampffmeyer, Ulrich; Llewellyn, A.: *Are e-documents legal in Europe?*. Document World, Vol. 4 No.3, pp.45-8, 1999

Kampffmeyer, Ulrich: *GDPdU & Elektronische Archivierung*. PROJECT CONSULT Newsletter (Teil 1-4) 20050531, 20050624, 20050720, 20050817, 2005 (GDPdU & Elektronische Archivierung)

National Archives and Records Administration: *Code of Federal Regulations (CFR)*, (CFR)

National Highway Traffic Safety Administration: *Transportation Recall Enhancement, Accountability and Documentation Act (TREAD)*, 2000 (TREAD)

Österreich: *Mediengesetz (MedG)*. BGBl I Nr. 49/2005 und 151/2005, 2005 (MedG)

PROJECT CONSULT: *Recht & Gesetz: Unternehmensgesetzbuch*, PROJECT CONSULT Newsletter 20070529, ISSN 1439-0809, 2007 (20070529)

Sarbanes-Oxley Act of 2002 (SOX). Pub. L. No. 107-204, 116 Stat. 745, 2002 (Sarbanes-Oxley Act)

Securities and Exchange Commission: *Books and Records Requirements for Brokers and Dealers Under the Securities Exchange Act of 1934*, 17 CFR PARTs 240 and 242 [Release No. 34-44992 ; File No. S7-26-98] RIN 3235-AH04, 2003 (SEC: 34-44992)

United States Department of Defense: *DoD 5015.2-STD RMA Design Criteria Standard*, 2007 (DoD 5015.2-STD)

United States Food and Drug Administration, Office of Regulatory Affairs: *Federal Register Part II, 21 CFR Part 11*, 2003 (Draft Guidance for Industry on Part 11)

United States Food and Drug Administration: *21CFR210 (Current good manufacturing practice in manufacturing, processing, packing, or holding of drugs; general) und 21CFR211 (Current good manufacturing practice for finished pharmaceuticals)*, 2006 (21CFR)

United States Department of Health & Human Services, Office for Civil Rights: *Health Insurance Portability and Accountability Act (HIPAA)*, Pub. L. 104-191, 110 Stat. 1936, 1996 (HIPAA)

United States Department of Justice: *The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT ACT) of 2001*. Pub. L. No. 107-56, 115 Stat. 272, 2001 (USA PATRIOT ACT)

United States Sentencing Commission: *Federal Sentencing Guidelines (FSG)*, 2006 (FSG)

Winkler, Maria: *Verordnung über die Führung und Aufbewahrung der Geschäftsbücher – GeBüV*, Vortrag „Rechtliche Aspekte der elektronischen Archivierung“ auf dem Datenschutz-Forum, 2005 (Rechtliche Aspekte der elektronischen Archivierung)

Über den Autor

Dr. Ulrich Kampffmeyer,

Jahrgang 1952, ist Gründer und Geschäftsführer der PROJECT CONSULT Unternehmensberatung GmbH, Hamburg, eine der führenden produkt- und herstellerunabhängigen Beratungsgesellschaften für ECM Enterprise Content Management, BPM Business Process Management, Knowledge Management und andere DRT Document Related Technologies.

Er berät namhafte Kunden aller Branchen im In- und Ausland bei der Konzeption und Einführung von Compliance-, DRT-, ERM- und ECM-Lösungen.

Als Gründer und langjähriger Vorstandsvorsitzender nationaler und internationaler Branchenverbände prägte er wesentlich den deutschen Markt für Dokumenten-Management. Er ist einer der Gründer und Geschäftsführer des DLM-Network EEIG. Ulrich Kampffmeyer ist Mitglied in mehreren internationalen Standardisierungsgremien im Umfeld des Workflow-, Dokumenten- und Records-Management.

Dr. Kampffmeyer ist anerkannter Kongressleiter, Referent und Moderator zu Themen wie elektronische Archivierung, Records-Management, Dokumenten-Management, Workflow, Rechtsfragen, Business Re-Engineering, Wissensmanagement und Projektmanagement. Auf zahlreichen nationalen und internationalen Kongressen und Konferenzen wirkte er als Keynote-Sprecher mit.

About the author

born in 1952, is founder and president of PROJECT CONSULT Unternehmensberatung Dr. Ulrich Kampff¬meyer GmbH, one of the leading independent management consultancies for ECM Enterprise Content Management, BPM Business Process Management, Knowledge Management, and other DRT Document Related Technologies.

He consults clients of all industries in Europe in planning, organization, and implementation of compliance, DRT, ERM and ECM solutions.

As founder and chairman of the boards of trade associations, he formed the German market for document management and is regarded as mentor. He is one of the founders and president of the DLM network EEIG. Ulrich Kampffmeyer is member of several international standarization groups for workflow, document and records management

Dr. Kampffmeyer is an internationally well-known keynote speaker, presenter, and panelist on the subject of archiving, records management, document management, workflow, code of practices, business reengineering, knowledge management, and project management. He took part in many national and international conferences as keynote speaker.

Über PROJECT CONSULT

Die PROJECT CONSULT Unternehmensberatung GmbH mit Sitz in Hamburg wurde am 01.07.1992 gegründet.

PROJECT CONSULT hat sich auf die Beratung im Umfeld von DRT Document Related Technologies wie ECM Enterprise Content Management, Wissensmanagement, Dokumentenmanagement, elektronische Archivierung, Records Management, ILM Information Lifecycle Management und angrenzende Bereiche spezialisiert. Zum Leistungsangebot gehören Strategie, Konzeption, Auswahl, Abnahme und Dokumentation sowie das zugehörige Projektmanagement zur Einführung von komplexen Informationsmanagementsystemen.

PROJECT CONSULT arbeitet branchenübergreifend mit Schwerpunkt im deutschsprachigen Raum. Die Unternehmensberatung ist ausschließlich für Endanwender tätig um eine von Anbietern unbeeinflusste, unabhängige Beratung sicherzustellen.

PROJECT CONSULT setzt auf das KnowHow langjährig im ECM-Markt erfahrener Berater.

PROJECT CONSULT ist in verschiedenen Standardisierungsinitiativen wie z.B. MoReq der Europäischen Kommission, aktiv tätig.

About PROJECT CONSULT

PROJECT CONSULT Unternehmensberatung GmbH, located in Hamburg, was founded in july 1992.

PROJECT CONSULT is specialised on all topics of DRT Document Related Technologies as enterprise content management, knowledge management , document management, electronic archiving, records management, information lifecycle management, compliance and others.
We offer strategy, planning, selection, test and acceptance test, documentation and project management for the implementation of information systems.

PROJECT CONSULT supports all industries in the German speaking countries. The consulting company only serves end users of document technologies. This is to ensure independent and impartial consulting.

PROJECT CONSULT assigns consultants based on their industry qualifications and special knowledge.

PROJECT CONSULT is actively involved in several standardization initiatives as MoReq of the European Commission.

PROJECT CONSULT

Unternehmensberatung Dr.Ulrich Kampffmeyer GmbH

Breitenfelder Straße 17 • 20251 Hamburg

Tel.: + 49 (040) 460762-20 • Fax: + 49 (040) 460762-29

Information Management Compliance

Dr. Ulrich Kampffmeyer
DMS EXPO
Köln, 26.09.2007

PROJECT CONSULT
Unternehmensberatung Dr. Ulrich Kampffmeyer GmbH

PROJECT CONSULT
Unternehmensberatung
Dr. Ulrich Kampffmeyer GmbH
Breitenfelder Straße 17
20251 Hamburg
www.project-consult.com

Agenda

1. Einführung
2. Information Management Compliance
3. Aktuelle Situation: wichtige Regularien und Gesetze
4. Corporate Governance
5. Information Management Compliance Policy
6. Compliance und Records Management
7. Zehn Compliance Merksätze
8. Ausblick

PROJECT CONSULT
Unternehmensberatung
Dr. Ulrich Kampffmeyer GmbH
Breitenfelder Straße 17
20251 Hamburg
www.project-consult.com

Einführung

2.

Compliance und Information Management Compliance

Alle Gesetze und Regeln der Papierwelt gelten auch in der elektronischen Welt.

Was verbirgt sich hinter dem Begriff Compliance?

Übereinstimmung mit und Erfüllung von gesetzlichen und regulativen Vorgaben.

Unterschiedliche Auswirkungen

3.

Aktuelle Situation und wichtige Regularien

International

Zum Beispiel: Basel **II**

USA

Zum Beispiel: Sarbanes Oxley Act

Zum Beispiel: eDiscovery

Tut uns leid, in diesem Vortrag gibt es keine Bilder, ist halt staubtrocken …

Europa

Zum Beispiel: 8. Direktive

Deutschland

Zum Beispiel: EHUG und
E-Mail-Management

Zum Beispiel: GDPDU
Aktuelle Urteile

Zum Beispiel: Verfahrensdokumentation
nach GoBS

Schweiz

Branchenspezifische Regularien

elen? Pharma, Automobile, Kernkraftwerke, öffentliche Verwaltung, Energieversorger, Militär, Chemie, usw.

4.

Corporate Governance

Information Management Compliance
darf nicht isoliert betrachtet werden.
Compliance muss Bestandteil der
Corporate Governance des Unternehmens und
ständiger Begleiter aller Prozesse werden.

Corporate Governance Richtlinien

Risiko Management

5.

Information Management Compliance Policy

1. Policy

Grundregeln und Verhaltensweisen für den Umgang mit Prozessen und Informationen.

2. Delegation:

Zuordnung von Verantwortlichkeiten und entsprechende Ausbildung auf den nachgeordneten Ebenen, die allen Betroffenen die Bedeutung von Compliance-Regeln deutlich macht.

2. Delegation:

Zuordnung von Verantwortlichkeiten und entsprechende Ausbildung auf den nachgeordneten Ebenen, die allen Betroffenen die Bedeutung von Compliance-Regeln deutlich macht.

2. Delegation:

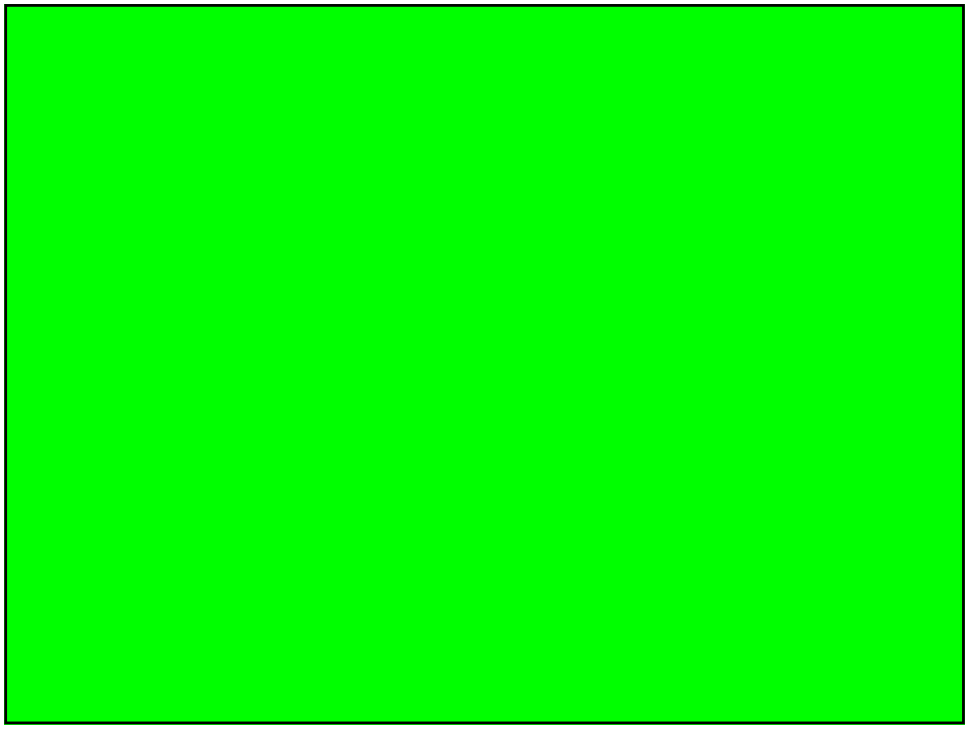
Zuordnung von Verantwortlichkeiten und entsprechende Ausbildung auf den nachgeordneten Ebenen, die allen Betroffenen die Bedeutung von Compliance-Regeln deutlich macht.

2. Dele ation:

Zuordnun von Verantwortlichkeiten und entsprechende Ausbildun auf den nach eordneten Ebenen, die allen Betroffenen die Bedeutun von Compliance-Re eln deutlich macht.

2. Dele ation:

Zuordnun von Verantwortlichkeiten und entsprechende Ausbildun auf den nach eordneten Ebenen, die allen Betroffenen die Bedeutun von Compliance-Re eln deutlich macht.



2. Delegation:

Zuordnung von Verantwortlichkeiten und entsprechende Ausbildung auf den nachgeordneten Ebenen,
die allen Betroffenen die Bedeutung von Compliance-Regeln deutlich macht.

Daran waren wir aber nicht Schuld. Deine Doku

3. Nachhaltung

Die Einhaltung der Regeln muss regelmäßig überprüft werden. Hierzu gehören z.B. Qualitätssicherungsprogramme ebenso wie Audits.

4. Sichere Systeme

Die IT-Systeme müssen den Anforderungen mit ihrer Funktionalität, Sicherheit und Verfügbarkeit genügen und die Nachvollziehbarkeit unterstützen.

Aspekte der
Information Management Compliance

6.

Compliance und Records Management

Immer mehr Information entsteht elektronisch. Der Ausdruck dieser Information auf Papier ist nur noch eine mögliche Form der Repräsentation. Das elektronische Dokument wird selbst zum Original.

Die internationale Norm:

ISO 15489
Records Management

Der europäische Standard:

MoReq
Model Requirements

Übergreifende Ansätze

Enterprise Change Management

Enterprise Content Management

Enterprise Content Management

Enterprise Content Management

Enterprise **Change** Management

!

Information Lifecycle Management

Elektronische Archivierung

… deutscher Prägung. In den USA ist das ja Records Management + Digital Preservation …

Speicher & Speichersubsysteme

7.

Zehn Compliance-Merksätze

1. Compliance-Themen gehören auf die Entscheiderebene, die die Verantwortung für die Einhaltung und Umsetzung der Anforderungen hat.

2. Compliance-Anforderungen sind ein integraler 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 man zunächst im Unternehmen prüfen, welche Regelungen für welchen Anwendungsfall überhaupt relevant sind.

8.

… noch etwas Geduld, der Vortrag ist gleich zu Ende!

Ausblick

Lösungen für die Unterstützung von Compliance wie E-Mail-Management und Records Management sind heute die wichtigsten Markttreiber für den Einsatz von Enterprise Content Management.

Compliance-Anforderungen
durchdringen alle Unternehmensbereiche.

Ohne Information Management Compliance kann
die Informationsgesellschaft nicht funktionieren.

Vielen Dank für Ihre Aufmerksamkeit !

Dr. Ulrich Kampffmeyer
E-Mail: Ulrich.Kampffmeyer@PROJECT-CONSULT.com

Handout zum Vortrag, Newsletter, weiterführende Informationen ...
http://www.PROJECT-CONSULT.com