Juli 2008

Ausgabe #3-08 Deutschland Euro 9,60 ISSN: 1864-8398

4 260122 090006

DOK. magazin

Technologien, Strategien & Services für das digitale Dokument

„Die Zukunft des Dokuments“ Das papierlose Büro

ECM-Compliance, Revisionssicherheit und Rechtssicherheit

Synergien Content Management und Social Software

ECM und Open Source im Unternehmen

Special: E-Billing

Wo bleibt noch Platz für ECM-Integratoren? | Studie E-Mail-Management | Wie Unternehmen Social Software nutzen | Was Knowledgeworker brauchen | Intelligente PDF-Dokumente in Geschäftsprozessen | PDF/A für den Produktzyklus | Watermarking für den Massenmarkt | Low-Scale-Single-Source-Publishing | Online-Storage | Den Speicher im Griff

good source publishing

www.goodsourcepublishing.de

ECM-Compliance: Nachweisbare Revisionssicherheit gleich größere Rechtssicherheit

Compliance, Corporate Governance, Enterprise Content Management, Revisionssicherheit, Risikomanagement, Zertifizierung

„Compliance" bedeutet die Einhaltung von Gesetzen und Richtlinien in Unternehmen – dazu gehören sowohl externe Vorgaben als auch unternehmensinterne Leitlinien. Compliance ist ein wesentlicher Baustein im Rahmen einer ordnungsgemäßen Unternehmensführung, der „Corporate Governance" und damit kein unbekanntes Thema. Im Zuge einer immer stärkeren Nutzung der Informationstechnologie sind Unternehmen angehalten, die mit den neuen Technologien verbundenen Compliance-Regularien einzuhalten – ein Prozess, der das stete Anpassen an entsprechende Vorgaben im Rahmen einer „Information Management Compliance" verlangt. Neben dem technologischen Wandel zwingen einschlägige Vorgaben wie der Sarbanes-Oxley Act, Basel II sowie internationale Rechnungslegungsstandards (IFRS) die Unternehmen dazu.

Rein rechtlich liegt dabei die Verantwortung für die Einhaltung aller Compliance-Anforderungen bei den Vorständen und Geschäftsführungen der Unternehmen; sie haben für die Einführung von Geschäftsprozesskontrollen und interne Steuerungs- und Überwachungssysteme zu sorgen. In diesem Zusammenhang sei auf den Deutschen Governance Kodex (DCGK) in seiner Fassung vom 14.06.2007 verwiesen, in dem die Compliance-relevanten Aufgaben zumindest für Vorstände und Aufsichtsräte von Aktiengesellschaften gesetzlich festgehalten sind. Für die konkrete Einhaltung der Vorgaben allerdings sind alle Mitarbeiter eines Unternehmens verantwortlich. Compliance stellt also stets eine übergreifende unternehmensweite Aufgabe dar.

Im Rahmen des Enterprise Content Managements (ECM) und des Dokumenten-Managements ist ein Unternehmen angehalten, hierfür Kontrollmechanismen einzurichten und eindeutige Informations- und Kommunikationsabläufe zu definieren. Diese „Information Management Policies" dienen dazu, jedem Mitarbeiter, jeder Arbeitsgruppe die jeweiligen Aufgaben für die Einhaltung der ECM-Compliance-Anforderungen darzulegen.

www.consultec.de

Dr. Klaus-Peter Elpel ist einer der drei geschäftsführenden Gesellschafter der **Consultec Dr. Ernst GmbH**. Das herstellerneutrale Beratungsunternehmen ist in den Bereichen Informationsmanagement, Enterprise Content Management, Dokumenten-Management, digitale Archivierung, Workflow sowie Compliance aktiv.

Hierzu gehören Darstellungen der Arbeitsprozesse ebenso wie eindeutige Vorgaben zum Umgang mit Dokumenten und Informationen – und nicht zuletzt die jeweiligen Compliance-Anforderungen selbst. Diese ECM-Compliance-Policies enthalten nicht nur Regularien für den Umgang mit Dokumenten, sondern dienen vielmehr auch der Delegation von Verantwortungen und das Thema Compliance ganz allgemein im Bewusstsein aller Mitarbeiter verankern. Wie das organisatorisch und personell geschieht, ist sicherlich von der Größe des Unternehmens abhängig. So haben einige Großunternehmen hierfür die Stelle eines „Chief Compliance Officers“ (CCO) geschaffen, der für die unternehmensweite Koordination aller Compliance-Aktivitäten verantwortlich zeichnet und die Schnittstelle zur Unternehmensleitung bildet. Als Beispiel sei hier die BASF AG in Ludwigshafen erwähnt: Sie hat als eines der ersten deutschen Unternehmen die Stelle eines CCO geschaffen. Im Zuge der Einführung und Bewusstmachung der hauseigenen Compliance-Vorgaben wurden weltweit Mitarbeiter durch regionale Maßnahmen über die Grundwerte und Leitlinien sowie über das interne Compliance-Programm informiert. Zudem wurde unternehmensweit ein internationales Netzwerk mit lokalen Compliance-Beauftragten aufgebaut. Heute gibt es regelmäßige Trainingsprogramme, bei denen der Compliance-Verhaltenskodex praxisnah auf die alltägliche Arbeit des einzelnen Mitarbeiters bezogen verbreitet wird.

Doch wie erfolgt eine Umsetzung der Compliance-Vorgaben im praktischen Tagesgeschäft, besonders im Rahmen des Enterprise Content Managements? Wie müssen sich Unternehmen aufstellen, wenn es um den konkreten, den Compliance-adäquaten Umgang mit Dokumenten und Informationen geht? Zunächst einmal: IT-Systeme können zwar die Arbeitsprozesse und Compliance-Anforderungen durchaus hilfreich unterstützen; sie allein bieten jedoch auf gar keinen Fall eine Lösung für die Abdeckung der Compliance-Anforderungen.

ECM-Compliance

- zeichnet sich stets durch IT-basierte UND organisatorische Abläufe und Vorgaben aus und
- ist jeweils auf das entsprechende Unternehmen gezielt abzustimmen – auch unter Abwägung dessen, was das Unternehmen bereit ist, an juristischen Restrisiken zu tragen.

Wenn denn Compliance ein wesentlicher Baustein im Rahmen der Corporate Governance ist, so ist das Herstellen von Revisionssicherheit in einem Unternehmen der zentrale Baustein im Rahmen des „Moduls“ ECM-Compliance.

Revisionssicherheit – Basis jeder ECM-Compliance

Revisionssicherheit bezieht sich auf die revisionssichere digitale Speicherung von Dokumenten und Daten in elektronischen Archiven. Die dafür notwendigen Vorgaben ergeben sich in Deutschland aus den Anforderungen des Handelsgesetzbuches (HGB), der Abgabenordnung (AO), der „Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme“ (GoBS) sowie weiteren steuerrechtlichen und handelsrechtlichen Vorgaben. Im europäischen Ausland – etwa in der Schweiz oder in Österreich – existieren ähnliche Regelungen. Nun ist Revisionssicherheit bereits seit langen Jahren ein Thema im ECM-Umfeld. Jedoch hat es in vielen selbst großen Unternehmen immer noch nicht die Aufmerksamkeit erhalten, die ihm gebührt und die nötig wäre, um das Unternehmen und die in der Verantwortung stehende Unternehmensleitung aus juristischer Sicht auch beim Umgang mit Dokumenten möglichst gut abzusichern – und das möglichst über sehr lange Zeiträume hinweg.

Dabei sind insbesondere zwei Szenarien zu beachten, bei denen eine rechtssichere/revisionssichere Aufbewahrung von digitalen

Dokumenten für Unternehmen von besonderer, teilweise gar herausragender Bedeutung sein kann:

- im Rahmen juristischer Verfahren zur (vorsorglichen) Aufbewahrung für Beweiszwecke (beispielsweise bei Schadensersatzklagen) und
- für gesetzliche Dokumentationspflichten (beispielsweise für Betriebsprüfungen der Finanzbehörden).

Solange Dokumente ausschließlich in Papierform vorlagen, brachte die Nachweispflicht prinzipiell keine großen Probleme mit sich – einmal abgesehen davon, dass sich (einzelne) Dokumente womöglich nicht auffinden ließen. Etwa weil sie falsch abgelegt oder irrtümlich vernichtet worden waren oder weil rechtlich „unbrauchbare" Kopien abgelegt wurden. Wenn die entsprechenden Papierdokumente jedoch im Original vorhanden waren, konnte man von einer hohen Beweiskraft dieser Dokumente ausgehen – schließlich gab und gibt es eine hohe, über Jahrhunderte gewachsene Rechtssicherheit bei der Vorlage von Original-Papierunterlagen.
Ganz anders verhält sich dies bei digital gespeicherten Daten und Dokumenten, insbesondere dann, wenn nach einer Digitalisierung die Original-Papierdokumente vernichtet werden (sollen). Dies streben zahlreiche Unternehmen aus Effizienz-/Kostengründen an bzw. haben es bereits umgesetzt. Hierbei ist die aktuelle Rechtssituation rein digitaler Dokumente vielerorts in hohem Maße unklar, und die Beweiskraft vor Gericht stellt häufig genug noch ein gravierendes Problem im Rahmen der freien richterliche Beweiswürdigung (§286 ZPO) dar.

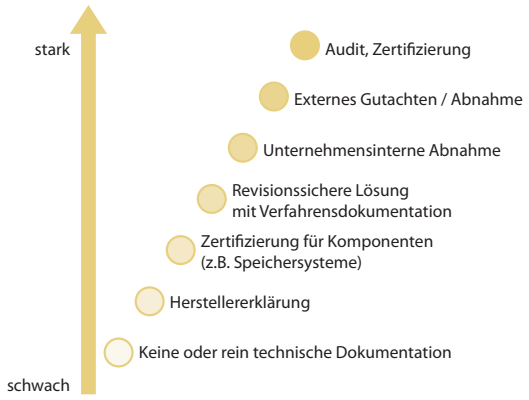
Nun war Revisionssicherheit für so manchen Verantwortlichen lange Zeit gleichbedeutend mit einer langzeitgesicherten IT-basierten Archivierung von Dokumenten, geschützt vor unbefugtem Zugriff sowie Veränderung. Hier kamen bzw. kommen Unterthemen wie „revisionssichere Speichersysteme" oder „Konzeption und Realisierung adäquater Berechtigungskonzepte" zum Tragen. Nur: Dieser Ansatz greift zu kurz, um zur rechtlich geforderten Sicherheit zu gelangen. Um es deutlich zu sagen: Ein elektronisches Archiv allein, das gegen jegliche Veränderbarkeit seiner Dokumente hoch gesichert ist, reicht nicht aus.

Will, oder besser, muss man das eigene Unternehmen im Sinne eines Risikomanagements gegen prinzipiell jede Art von Rechtsangriffen wappnen und möchte die eigene Firma gut aufgestellt wissen, wenn es um eine deutliche Beweiskraft von digital (!) archivierten Dokumenten geht, so muss man Revisionssicherheit als zentralen Baustein einer umfassenden Lösung begreifen. Diese Lösung betrifft die gesamte dokumentenbezogene Prozesskette – vom Posteingang, ob Papier oder digital, über die Vorgangsbearbeitung bis hin zum Versenden, Archivieren und gezielten Vernichten von Dokumenten. Wie können nun die Verantwortlichen in den Unternehmen vorgehen und welche konkreten Maßnahmen müssen vorgenommen werden, um eine Revisionssicherheit zu erlangen, die diese Bezeichnung auch verdient?

Höhere Rechtssicherheit für die Beweiswürdigung von Dokumenten gewinnen

Damit auch digital archivierte Dokumente einer entsprechenden juristischen Beweiswürdigkeit standhalten und so zu einer höheren Rechtssicherheit auf Unternehmensseite führen, sind vier Vorgehensschritte nötig:

1. Zunächst sollte das Unternehmen intern eine Risikoabschätzung vornehmen. Dabei wird ermittelt, welches juristische/kaufmännische Restrisiko noch getragen werden kann, wenn auf den Papier-Nachweis von Originalunterschriften verzichtet und das Gros der Dokumente ausschließlich in



Maßnahmen zum Erlangen einer höheren Rechtssicherheit bei digital archivierten Dokumenten.

digitaler Form archiviert wird – und wenn die (meisten) Papieroriginale nach einer Karenzzeit von wenigen Wochen vernichtet werden. Sodann wird ermittelt, welcher personelle und monetäre Aufwand dafür betrieben werden muss/soll, um das so identifizierte Risiko tragen zu können. Dieser Aufgabenschritt wird in der Regel unter Einbindung der unternehmenseigenen Rechtsabteilung oder externer Berater vorgenommen.

2. Sofern das Risiko und die Aufwände als akzeptabel eingestuft werden, konzipiert und realisiert man eine durchgängig revisionssichere Lösung aller dokumentenbezogenen Prozesse (papierbezogen und digital). Dies kann zu Beginn eines ECM-/DMS-Projektes geschehen oder aber im Nachhinein. Im zweiten Fall werden die vorgefundenen dokumentenbezogenen Teilprozesse unter die Lupe genommen, auf ihre Revisionssicherheit hin überprüft und optimiert. Für diese Aufgabe kann eine externe Beratung, die die Arbeitsprozesse aus unvoreingenommener Sicht bewertet, sinnvoll sein.
3. Die so erreichte oder bereits vorhandene revisionssichere ECM-Lösung wird in einer Verfahrensdokumentation schriftlich dargestellt. Diese wiederum bildet die Basis für eine Abnahme oder gar Zertifizierung der gesamten ECM-Lösung. Die Verfahrensdokumentation enthält eine Darstellung, die sinnvollerweise auf Basis der „Prüfkriterien für Dokumenten-Management-Lösungen“ (PK-DML) des Verbandes für Organisations- und Informationssysteme e.V. (VOI) und des TÜViT erfolgt. Hierzu gehören u. a. die Beschreibung des Einsatzgebietes und der technischen Systemlösung, Maßnahmen zur IT-Sicherheit und Wartung, die Darstellung der dokumentenbezogenen Prozesse sowie des künftig regelhaft anzuwendenden Internen Kontrollsystems (IKS). Das IKS sorgt für die Einhaltung und, im Laufe der Zeit, auch für die fachliche Fortschreibung und Dokumentation der ECM-Gesamtlösung, weshalb das IKS als Qualitätssicherung der Revisionssicherheit zu verstehen ist. Die Erstellung der Verfahrensdokumentation kann prinzipiell auf Basis der PK-DML als Grundgerüst durch unternehmenseigene Mitarbeiter oder externe Berater erfolgen.
4. Schließlich erfolgt die eigentliche Abnahme oder Zertifizierung der Lösung für den dokumentenbezogenen Gesamtprozess.

Die interne Abnahme der ECM-Lösung erfolgt durch unternehmenseigene Abteilungen (beispielsweise die betroffenen Fachabteilungen, die IT-Abteilung, die Rechtsabteilung oder die Revisionsabteilung); bei der Vorbereitung kann ein externer Berater unterstützen. Dieser kann auch die Vorarbeiten und die Koordination für externe Abnahmen übernehmen. Externe Abnahmen erfolgen beispielsweise durch Wirtschaftsprüfungsgesellschaften; Zertifizierungen können beispielsweise durch den TÜViT (Unternehmensgruppe TÜV-NORD) vorgenommen werden.

Abnahmen oder gar Zertifizierungen durch entsprechend autorisierte externe Einrichtungen bieten für rechtliche Auseinandersetzungen, und darum geht es schließlich im Kern, ein deutlich höheres Maß an Rechtssicherheit für die Beweiskraft digitaler Dokumente als etwa rein unternehmensinterne Abnahmen. Hier schließt sich der Kreis: Je dichter das Nachweisverfahren für die Revisionssicherheit, desto rechtlich sicherer schützt sich ein Unternehmen in juristischen Verfahren bzw. verringert daraus resultierende Risiken aufgrund mangelnder Beweisqualität – und deckt damit einen namhaften Teil seiner Compliance-Anforderungen insgesamt ab. ■