

<http://www.perspektive-mittelstand.de/Document-Compliance-Management-Sicherer-Dokumentenaustausch-durch-DCM/management-wissen/4026.html>

## Document Compliance Management

### Sicherer Dokumentenaustausch durch DCM

Von Nicole Dietrich, Brainloop AG

**Der Umgang mit vertraulichen digitalen Dokumenten und deren Austausch erfordern eine lückenlose Sicherheit. Document Compliance Management- bzw. DCM-Systeme können eine solche garantieren.**



Zentrale geschäftliche Aktivitäten, bei denen es um viel Geld und manchmal um die Existenz eines Unternehmens geht, beziehen in aller Regel viele Personen ein, die nicht oder nicht direkt dem Unternehmen angehören. Das können Aufsichtsräte oder externe Berater sein, Partner, die an einem Joint Venture interessiert sind und immer öfter staatliche Regulierungsbehörden. Die für diese Geschäftsprozesse relevanten digitalen Dokumente können nicht hinter den Firewall-Systemen des Unternehmens gehalten werden, sondern müssen auf sichere Art unter den berechtigten Personen zirkulieren können. Viele bekannte Sicherheitsmaßnahmen wie Verschlüsselung während des Datentransports und auf den verschiedenen Speichermedien

sowie unternehmensweite Digital-Rights-Management Systeme sind lediglich Teilkomponenten eines umfassenden und ganzheitlich konzipierten Document Compliance Management (DCM), das für die heutige Unternehmensdynamik mit ihrem ausgeprägten »Extranet-Charakter« ausgelegt ist.

#### Hochsicherheitstrakt für vertrauliche digitale Dokumente

DCM-Systeme benötigen auf der Basis einer speziellen IT-Infrastruktur eine Art digitalen Hochsicherheitstrakt, in dem allen Zugangsberechtigten vertrauliche Dokumente gemäß ihrem jeweiligen Rechtstatus zugänglich sind. Dieser Hochsicherheitstrakt für Dokumente muss problemlos über einen Web-Browser durch Endanwender z.B. aus der Vorstands- oder Geschäftsführungsebene bedient werden können.

Das ideale DCM-System deckt den gesamten Lebenszyklus eines Dokuments – vom Anlegen bis zum Löschen – lückenlos ab. Ein Dokument ist folglich auch dann noch unter der Kontrolle des Systems, wenn es am Arbeitsplatz angezeigt, gespeichert oder bearbeitet wird.

Idealer Weise ist ein DCM-System als Software-as-a-Service-Lösung realisiert. Es ist von jedem Arbeitsplatz aus erreichbar und arbeitet ohne das Aufspielen von Client-Software. Die Schlüsselverwaltung ist so organisiert, dass niemand, insbesondere auch nicht das IT-Personal des Unternehmens, Einblick und Zugriff hat. Die Verwaltung eines Generalschlüssels für das Notfallmanagement ist auf mehrere Personen, von denen jeder nur einen Teil dieses Schlüssels besitzt, aufgeteilt. Anwendungsbeispiele für DCM sind u.a.:

- Finanzen: Interne Revision, Quartals- und Jahresberichte, Investor Relations
- Rechtsabteilung: Vertragsmanagement, Patentrecht, Rechtsprüfung
- M&A: Pre-Due Diligence, Due Diligence, Post-Merger Integration
- Einkauf: Ausschreibungen, Lieferantenbeziehungen
- Personalabteilung: Personalakte, Personalentwicklung, Recruitment

## **Die Problemstellung**

Die Arbeitsabläufe bei Behörden und Unternehmen sind heute schon weitgehend durch digitale Infrastrukturen geprägt. Nachrichten und Dokumente sind auf digitalen Speichermedien abgelegt und werden über digitale Netze ausgetauscht. Digitale Dokumente haben Papierdokumente in vielen Bereichen abgelöst. Durch Dokumenten- und Content Management Systeme lassen sich die digitalen Akten in vielfältiger Weise auswerten und mit anderen Dokumenten abgleichen und verknüpfen. Viele der Möglichkeiten, die digitale Dokumente bieten, wären mit Papierakten nicht oder nur mit immensem Zeitaufwand möglich. Durch digitales Dokumentenmanagement und dessen Einbindung in die geschäftlichen Workflows werden indes nicht nur die Verarbeitungsmöglichkeiten erweitert, sondern es werden vor allem auch die Entscheidungsprozesse erheblich beschleunigt.

Ganz gleich, ob es sich um die Vorbereitung von Firmenkäufen, um Abstimmungsprozesse im Vorfeld von Hauptversammlungen oder den Schutz geistigen Eigentums, z. B. von vertraulichen Konstruktionsdaten für Maschinen oder von Rezepturen und Testergebnissen für Pharmaka handelt: Die betreffenden Informationen müssen in Sekundenschnelle zwischen den beteiligten Personen ausgetauscht oder auch gemeinsam bearbeitet werden können. Bei diesen digitalen Abläufen und Kooperationen muss zu jedem Zeitpunkt und an jeder Stelle des Prozesses sicher gestellt sein, dass die Dokumente nur für jeweils berechtigte Personen einsehbar, versendbar, kopierbar oder veränderbar sind. Angesichts der Brisanz der Dokumente dürfen diese für Unbefugte – und das sind in diesem Fall auch die eigenen IT-Systemadministratoren – in unverschlüsselter Form nicht zugänglich sein. Das ist durch entsprechende Verfahren und Kontrollsysteme zu gewährleisten, wobei die diesbezüglichen Regeln die gesetzlich vorgeschriebenen Vorsorge- und Sorgfaltspflichten ebenso umfassen wie branchenspezifische Normen wie etwa die Sicherheitsvorschriften der Kreditkartenherausgeber. Solche Systeme müssen vertrauliche Dokumente von ihrer Entstehung bis zur Archivierung oder Löschung begleiten, ohne dass innerhalb dieses »Lebenszyklus« auch nur die geringste Lücke in den Sicherheitsmaßnahmen auftritt.

Ebenso ist lückenlos zu dokumentieren, wer wann diese Dokumente eingesehen, verschickt oder verändert hat. Ein solcher Anforderungskatalog für den durchgängigen Schutz vertraulicher Dokumente und die komplette und unveränderbare Dokumentation aller Zwischenstände und Zugriffe wird zunehmend unter dem Begriff Document Compliance Management (DCM) diskutiert.

Für ein umfassendes Document Compliance Management bieten bekannte Sicherheitstechniken wie Verschlüsselung der Ablage der Dokumente (Festplatte und Massenspeichersysteme) beziehungsweise der Transportstrecken (E-Mail- und Dateiübertragungstrecken im Internet) keine hinreichende Gewähr. Ebenso sind Digital-Rights-Management-Systeme nur eine (wenn auch sehr wichtige) Teilkomponente eines ganzheitlich angelegten DCM, das allen gesetzlichen und innerbetrieblichen Vorgaben entspricht (Details siehe Abschnitt 5).

Mit anderen Worten: Für ein durchgängiges Document Compliance Management, also den korrekten Umgang mit Dokumenten, die aus unternehmerischen oder gesetzlichen Gründen besonders geschützt werden müssen, ist eine völlig neue Lösungsarchitektur notwendig.

## **Die Anforderungen im Kontext**

Die vernetzten Arbeits- und Geschäftsstrukturen der Gegenwart sind mit dem klassischen statischen

Unternehmensbegriff nicht mehr voll zu erfassen. Unternehmen sind heute in größere Beziehungsgeflechte integriert. Das können Hersteller-Zulieferer-Netzwerke wie beispielsweise in der Automobil- und Luftfahrtindustrie sein oder auch die regelmäßige Interaktion zwischen staatlichen Überwachungsbehörden und Unternehmen, wie sie besonders im Finanz- oder auch im Pharma- und Biotechnologiebereich zu finden ist. »Innen« und »Außen« verschwimmen also zunehmend bei der Organisation unserer Geschäftswelt. So ist schon der Aufsichtsrat einer Aktiengesellschaft sowohl »außen« als auch »innen«, ganz zu schweigen von zeitlich begrenzten Projektteams, die sich bei Fusionsverhandlungen bilden, oder bei partiellen Joint Ventures zwischen Konkurrenten, wie sie etwa bei Automobilbauern vorkommen.

Solche organisatorischen »Extranets« sind in aller Regel zentrale strategische Elemente des Geschäfts. Das heißt, dass gerade an diesen Stellen besonders viele hochbrisante Dokumente ausgetauscht werden müssen. Um hier die vom Gesetzgeber geforderte Sicherheit zu erreichen, taugt der traditionelle Firewall-Ansatz nicht viel. Schließlich sind gerade hier Dokumente und Daten zu sichern, die ständig zwischen den Firewalls der verschiedenen Protagonisten hin und her reisen. Wegsperrern nutzt also wenig, zerstört vielmehr die geschäftlichen Abläufe. Ein adäquater Sicherheitsansatz muss ganz im Gegenteil das »Reisen der Dokumente« zum Ausgangspunkt nehmen und dann die Reiseroute und die zusteigenden Personen absichern und dokumentieren. Die Flugsicherung kann hier als Äquivalent dienen. Sie arbeitet mit diversen Komponenten einer externen Infrastruktur, die eine Verbindung zu den zu sichernden Objekten hat.

Auch für vertrauliche Dokumente können die verschiedenen technischen Komponenten der Verschlüsselungstechnik unter einer integrierenden Applikationsoberfläche zusammengeführt werden, die keine IT-technischen Kenntnisse voraussetzt, sondern vom Endanwender intuitiv bedient werden kann.

### **Ganzheitliche Kontrolle über den gesamten Lebenszyklus eines Dokuments**

Eine Document Compliance Management-Lösung muss also vertrauliche Dokumente sicher schützen, ganz gleich ob sie sich innerhalb oder außerhalb der Unternehmens-Firewall-Systeme befinden. Der Schutz der Dokumente gegen unberechtigtes Lesen oder gegen Verfälschungen darf keine Lücken aufweisen. Bei unvollständigen Lösungen ist z. B. ein Dokument, wenn es erst einmal auf den Client geladen worden ist, in keiner Weise mehr zu schützen.

### **Fehlhandlung verhindern**

Eine DCM-Lösung hat den gesamten Lebenszyklus eines Dokuments im Blick und im Griff. Auf einem gesicherten Server sind alle überhaupt möglichen Zugriffsberechtigten und ihre jeweiligen Rechte gespeichert. Diese Festlegungen sind allerdings nicht statisch, sondern werden ständig angepasst und durch einen nichttechnischen Administrator, beispielsweise den Projektleiter, umgesetzt.

Wenn beispielsweise bei einem Firmenverkauf, an dem sich mehrere Bieter beteiligen, ein Bieter ausscheidet, dann werden dessen bisherige Zugriffsrechte sofort gelöscht. Durch die zeitnahe Aktivierung oder Zuteilung der jeweiligen Berechtigungen durch den Verwalter der DCM-Lösung ist es zum einen möglich, schnell auf neue Gegebenheiten zu reagieren und zum anderen kann mit einer solchen Lösung ein Dokument auch nach dem Übertragen auf den Arbeitsplatzrechner gesperrt beziehungsweise seine Verwendung zeitlich und funktional begrenzt werden. DCM-Lösungen behalten immer die Kontrolle über ein Dokument, vom ersten Anlegen des Dokuments bis zu dessen Löschung.

### **DCM-System als SaaS-Architektur**

Die Verwaltung der Zugriffe auf die vertraulichen Dokumente wird in einem DCM-System von Nicht-IT-Personen durchgeführt, weil nur sie mit den tatsächlichen Geschäftsanforderungen vertraut sind. Dabei ist es ratsam, bestimmte Änderungen und Maßnahmen an ein Mehraugenbeziehungsweise Funktionstrennungsprinzip zu binden. Die IT-technische Infrastruktur, also zum Beispiel die Datenbank, in der die Authentifizierungsdaten verwaltet werden, ist für diese Administratoren nicht sichtbar und natürlich auch nicht beeinflussbar.

Für die technischen Administratoren sind diese Komponenten wie eine »Black Box«, die sie mit ihren Standardtechniken verwalten ohne in die Innereien schauen zu können. Die Administration der IT-Infrastruktur für ein DCM-System kann und sollte überdies in verschiedene Zuständigkeitsebenen aufgeteilt werden. Aus dem Gesagten ergibt sich, dass für ein DCM-System eine browserbasierte Mietlösung (Software-as-a-Service, SaaS) ideal ist. Es wird dabei keine Client-Software benötigt und die IT-Infrastruktur wird von Spezialisten quasi unsichtbar, aber effizient bereitgestellt und gepflegt. Das Document Compliance Management stellt sich insofern für die Nutzer in der Vorstandsetage oder der Konstruktionsabteilung als eine Anwendung dar, die so wie ein normales Office-Programm zu bedienen ist. Unter dieser leicht zu bedienenden Oberfläche befindet sich die IT-technische Infrastruktur. Das Spektrum reicht hier von durchgängiger Verschlüsselung, die den gesamten Lebenszyklus abdeckt, und einer starken Authentifizierungs-Komponente über eine stringente Transportsicherung, unter anderem für E-Mail oder Dokumentenkennzeichnungsverfahren, wie digitale Wasserzeichen, bis hin zu einer rigorosen Schlüsselverwaltung auf der Basis von digitalen Zertifikaten, die dafür sorgt, dass das System vom Rechenzentrumspersonal bedient werden kann, der Zugriff auf die Inhalte aber konsequent ausgeschlossen wird.

### **Ganzheitliches DCM versus Teillösungen**

Document Compliance Management sollte als ganzheitlicher Prozess geplant und auch als ganzheitlich angelegte integrierte Anwendung ausgerollt und betrieben werden. Eine Delegation von Teilkomponenten an das IT-Personal, wie sie heute weitgehend noch gang und gäbe ist, ist höchst gefährlich, weil sie letztendlich nicht die gesetzlichen Vorgaben zum aktiven Risikomanagement erfüllt. Für deren Einhaltung haftet im Übrigen nicht der IT-Administrator, sondern der Geschäftsführer oder Vorstandsvorsitzende im wahrsten Sinne des Wortes »höchstpersönlich«. Gefährlich ist auch eine bloße Teilabsicherung der Dokumente und des Dokumentenflusses. Dreiviertel-Sicherheit ist in Wahrheit Unsicherheit und Dreiviertel-Compliance« ist rechtlich gesehen »Null-Compliance«.

Oft werden solche halben oder Dreiviertel-Lösungen gar nicht als solche erkannt, weil sie ja durchaus in ihrem Bereich für Sicherheit sorgen. So sind viele der auf dem Markt angebotenen Verschlüsselungslösungen für Festplatten durchaus leistungsfähig und auch einfach zu bedienen, aber sie bieten eben nur Sicherheit in einem Teilbereich. Während bei der Verschlüsselung der Festplatte nur ruhende Dokumente gesichert werden, sind es bei der E-Mail-Verschlüsselung wiederum nur die sich bewegenden Daten.

Und wenn man beides verbindet? Dann ist es immer noch nicht gut genug für ein echtes Document Compliance Management, zum Beispiel weil die Dokumente nach der Auslieferung an den Arbeitsplatz ungeschützt sind. Es bleibt immer noch eine Teillösung, bei der die Zugriffe in ihrer Gesamtheit nicht vollständig registriert werden und bei der oftmals Client-Software notwendig ist. Eine starke Authentifizierung ist nicht möglich oder, wenn doch, macht diese das System dann sehr umständlich. Der Einwand gegen eine solche Lösung besteht also einerseits darin, dass das IT-Personal letztlich die Oberhoheit über die Schlüssel behält, andererseits, dass der Rechner des Endanwenders ungeschützt ist und Dokumente von dort durch Angriff oder Fehlhantierung unkontrolliert entwendet oder verändert werden können. Dieser letzte Einwand trifft auch auf andere Lösungen zu, die Module für Dokumentensicherheit enthalten. Das sind in erster Linie die »Collaboration Suites« und die Dokumentenmanagement-Systeme. Nicht zuletzt ist aber mit solchen

Systemen keine durchgängige interne Kontrolle der Zugriffe und Eingriffe (Audit Trail) möglich oder zumindest nicht so möglich, wie es der Gesetzgeber vorschreibt und im Streitfall auch einfordert.

Können Systeme wie »Enterprise Rights Management« (ERM), wie sie von Microsoft, Adobe und anderen Herstellern implementiert wurden, ein ganzheitliches DCM gewährleisten? Die Antwort ist ein klares Nein. Diese Systeme haben zwar eine durchgängige Dokumenten-Verschlüsselung und sind für die unternehmensweite Verwendung ausgelegt, aber auch bei ihnen bleibt das Schlüsselmanagement in der Hand der IT-Administratoren und es muss Software auf den Client aufgespielt werden. Darüber hinaus enthalten ERM-Systeme keine nennenswerte Applikationslogik. Sie sind deshalb für Endnutzer nur schwer zu bedienen und können aufgrund der Systemarchitektur nur innerhalb des Unternehmens eingesetzt werden.

Ganzheitliche DCM-Systeme gibt es heute nur wenige. Aber auch bei diesen wenigen Systemen muss noch einmal die Spreu vom Weizen getrennt werden. Einige haben nur einen sehr eingeschränkten Funktionsumfang für das Dokumentenmanagement, viele keine durchgängige Verschlüsselung und keine starken Authentifizierungsmechanismen. Auch bieten nur ganz wenige Anbieter sowohl eine SaaS-Variante als auch eine Lizenzvariante an, sodass ein Unternehmen auf Wunsch das DCM-System auch in Eigenverantwortung betreiben kann.

### **Die Eckpunkte eines Document Compliance Management-Systems**

Gerade die brisantesten und wertvollsten Daten und Dokumente lassen sich heute nicht mehr hinter einer Firewall halten, wenn nicht die Schlagkraft eines Unternehmens gestört werden soll. Der Raum, in dem heute Dokumente vor unbefugter Einsichtnahme und Änderung geschützt werden müssen, ist das Extranet. Diese Tatsache ist maßgebend für die Architektur von DCM-Lösungen. Es ist deshalb konsequent, den DCM-Server außerhalb des eigenen Unternehmens in einer Art Hochsicherheitstrakt unterzubringen. Weiterhin gilt:

- Die Nutzer des DCM-Systems dürfen nicht mit IT-Infrastrukturproblemen behelligt werden, sondern sollen das DCM-System als browserbasierte, leicht bedienbare Anwendung erleben.
- Die gesamte Anwendung muss nicht nur absolut angriffssicher gestaltet sein, sondern auch jeden Schritt der Protagonisten lückenlos aufzeichnen, um so allen »Compliance-Forderungen« interner Revisoren und des Gesetzgebers genügen zu können.
- Eine starke Authentifizierung ist unabdingbar für alle, die mit dem DCM-System arbeiten. Durch Einmal-Passwörter, bei denen das Mobiltelefon als Token benutzt wird, lässt sich die Authentifizierung innerhalb des gesamten Extranets flexibel, kostengünstig und hochsicher gestalten.

Enterprise-Rights-Management-Systeme bilden in vielen Punkten die hier beschriebene DCM-Architektur nach. Schwachpunkte sind die Schlüsselverwaltung durch das IT-Personal und die komplizierte Bedienungsstruktur. ERM-Systeme können aber in sinnvoller Weise in eine ganzheitliche DCM-Architektur integriert werden.

<http://www.perspektive-mittelstand.de/Document-Compliance-Management-Sicherer-Dokumentenaustausch-durch-DCM/management-wissen/4026.html>

Über Nicole Dietrich  
Brainloop AG



Nicole Dietrich ist Senior Marketing Director bei der Brainloop AG. Dort ist sie verantwortlich für alle Marketingaktivitäten und die Öffentlichkeitsarbeit. Bereits seit über 15 Jahren befasst sich Frau Dietrich mit dem Dokumenten-Management und Enterprise-Content-Market und hielt verschiedene Marketing Management Positionen bei nord-amerikanischen High Tech Unternehmen. Die Brainloop AG ist führender Anbieter von Lösungen für Document Compliance Management, die den hochsicheren und jederzeit nachvollziehbaren Austausch vertraulicher Dokumente ermöglichen.

Brainloop AG  
Franziskanerstr. 14  
81669 München

☎ +49-89-444699-0

✉ [Email senden](#)

🏠 [Homepage](#)