SAPERION
Einfach geregelt.

whitepaper

COMPLIANCE

Über das Einhalten von Regeln im Kontext von Schriftgut

EXECUTIVE SUMMARY

Die Herausforderung

Das große Feld der Compliance in allen Facetten zu erfassen, ist bei über 25.000 Regeln, die zudem rasant mehr werden, kaum möglich. Dieses Whitepaper wird daher nach einem kurzen Überblick über das Compliance Management im Detail nur jene Gesetze und Regulierungen konkret ansprechen, bei deren Einhaltung SAPERION-Produkte und -Lösungen unterstützten können.

Konkrete Lösung

Compliance Management kümmert sich zum Einen um die Implementierung einer Firmenkultur zum ethischen wirtschaftlichen Handeln. Dies ist eine eher organisatorische Aufgabe. Zum Anderen werden Maßnahmen ergriffen, die die Risiken durch Nicht-Wissen oder Nicht-Tun minimieren. In diesem Kontext wird auch Software eingesetzt. Die SAPERION ECM Produkte werden weniger zum Management der Risiken eingesetzt als vielmehr zur Vermeidung von Regelverletzungen. Wenngleich der eine oder andere Kunde auch auf Basis von SAPERION ECM ein sogenanntes Governance Risk und Compliance Management System implementiert hat.

Die SAPERION ECM Produkte dienen primär zur Verwaltung elektronischen Schriftguts und zur Steuerung von Geschäftsprozessen in diesem Kontext.

SAPERION ECM ist ein Framework, auf dessen Basis Compliance-unterstützende Anwendungen erstellt werden. Dazu gehört z.B. die Personalakte im Kontext des Datenschutzes genauso wie die Vertragsakte zur Reduzierung von Betrugsfällen, z.B. durch fertige Vertragstextbausteine und Freigaben via Vier-Augen-Prinzip. Ein Internes Kontrollsystem (IKS) hilft, die Prozesse im Allgemeinen und speziell rund um die Rechnungslegung abzusichern. Und was viele bisher kaum im Fokus hatten: Auch Dokumente in den Web-Auftritten sind zum Nachweis der Inhalte besser aufzubewahren.

Die revisionssichere oder besser nach den Grundsätzen ordnungsmäßiger Buchführung (GoB, bald GoBIT) genannte datensichere Archivierung der elektronischen, steuerrelevanten Geschäftsdokumente ist genauso eine Compliance-relevante Anwendung wie die sichere Ablage von Dokumenten bei der Pharma- oder Lebensmittelunternehmen.

Aber auch interne Regularien z.B. für die Freigabe von Dokumenten zum Zwecke der allgemeinen Nutzung im Unternehmen im Sinne eines Qualitätsmanagement-Handbuchs lassen sich mit SAPERION ECM umsetzen.

INHALTSVERZEICHNIS

1	**Compliance im Überblick**	**3**
2	**Compliance-Anwendungen**	**8**
2.1	Records Management	8
2.2	Internes Kontrollsystem (IKS)	9
2.3	E-Mail Lifecycle Management	10
2.4	Web Content Archivierung	12
2.5	Beweiswertsicherung kryptographisch signierter Dokumente	13
3	**Ausgewählte Regularien im Detail**	**16**
3.1	Verschiedene Records Management Standards	16
3.2	Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme	17
3.3	Aufbewahrungsfristen und zu beachtende Regularien des Bundesdatenschutzgesetzes	18
3.4	Was bei der Vernichtung von Papier nach dem Scannen zu beachten ist	18
3.5	Bestimmungen für die Verwaltung von Kreditkartendaten	21
4	**Prüfung der SAPERION ECM Software**	**23**
4.1	Aufgabenstellung	23
4.2	Einige Prüfungsanforderungen im Detail	24
4.3	Das Ergebnis der Prüfung	27
5	**Zusammenfassung**	**28**

Der Autor

Dr. Martin Bartonitz befasst sich seit 1992 mit der Thematik Dokumenten- und Geschäftsprozessmanagement. Seit 2005 ist er verantwortlicher Produktmanager für die Themen Workflow, Signaturen und Eingangspostverarbeitung bei der SAPERION AG.

1 COMPLIANCE IM ÜBERBLICK

Compliance bedeutet, durch Einhalten von Regeln das notwendige Vertrauen in Partnerschaften und damit Verlässlichkeit zu bringen, seien es die UN-Konventionen für die Weltgemeinschaft, die Grundgesetze der Staatsgemeinschaften, das Qualitätsmanagement-Handbuch eines Unternehmens oder die Vereinssatzungen von Sportvereinen.

Nehmen wir die Steuergesetze. Sie sind ein wichtiges Regelwerk zur Aufrechterhaltung gemeinsamer Anstrengungen für unsere Gemeinschaft, wo es kein Kavaliersdelikt sein kann, wenn diese Gelder nicht in sie eingebracht werden. Sie fehlen sonst für das Wohl der Gesellschaft zum Beispiel für die Ausbildung unserer Jugend. Jede Handlung gegen die Regeln schadet der Organisation bzw. der Gemeinschaft, und genauso dem Unternehmen. Der Begriff „ehrbarer Kaufmann“ hat sich zur Zeit der florierenden Hanse entwickelt und ist auch heute noch in Hamburg tief verwurzelt. Ein Wegschauen bei Regelverletzungen hilft nicht, sondern schadet nur und kann bis zur persönlichen Haftung des Unternehmers führen.

Es gilt überall das Sprichwort, auch oder gerade im Wirtschaftsleben: „Ehrlich währt am längsten“. Wem ich nicht mehr vertrauen kann, mit dem mache ich keine Geschäfte mehr. Wer sich also an Regeln hält, wird langfristig einen deutlich günstigeren Geschäftserfolg haben.

Corporate Governance Kodex

Der 2009 in Kraft getretene Deutsche Corporate Governance Kodex hat den Compliance-Gedanken als Standard guter Unternehmensführung definiert: Die Geschäftsleitung hat für die Einhaltung der gesetzlichen Bestimmungen und der unternehmerischen Leitlinien zu sorgen. Ein Geschäftsleitungsorgan, das sich daran nicht hält, verstößt gegen seine Sorgfaltspflichten (§ 43 Abs. 1 GmbHG bzw. § 93 Abs. 1 S. 1 AktG) und handelt womöglich sogar ordnungswidrig (§ 130 OWiG).

Die Einführung eines Compliance-Management-Systems ist vorrangig ein organisatorisches Unterfangen, das von der Geschäftsleitung verantwortet und getragen werden muss, d.h. es gehört zur Corporate Governance[1]. Allein schon weil die geschäftliche Verantwortung in den meisten Fällen nicht delegiert werden kann. Die Geschäftsleitung kann sich durch einen Compliance Manager, bei großen Firmen durch einen Compliance Officer unterstützen lassen. Nach der Formulierung des Mission Statements (Beispiel Bayer AG in 2000: “Wir achten die Gesetze und respektieren die allgemein anerkannten Gebräuche der Länder, in denen wir tätig sind.”) müssen die Mitarbeiter in die relevanten Regeln eingewiesen werden– je nach Branchen und Arbeitsbereichen innerhalb der Organisation unterschiedlich. Die folgende Liste gibt nur einen kleinen Ausschnitt aus dem Wust an Regularien:

[1] Siehe zum Beispiel http://de.wikipedia.org/wiki/Corporate_Governance

Die wichtigsten Gesetze und Regularien im Detail, die von den betreffenden Organisationen beachtet werden müssen:

- in den USA agierende Firmen –SOX
- die Finanzdienstleister in Deutschland –die BaFin, BASEL II, TUG, MiFID, Geldwäschegesetz, Gramm-Leach-Bliley Act oder IFRS
- die Versicherer in Europa –Solvency II (ab voraussichtlich 2012)
- die Automobilhersteller – VDA 6.1, ISO/TS 16949 oder BS 7799 VDA
- die Produzenten von Pharmazeutika – FDA, GMP, GAMP, PharmBetrV, Arzneimittelgesetz
- die Luftfahrt – LuftVG, Zuverlässigkeitsüberprüfung
- die Energieversorger – das Atomgesetz, Beschluss BK6-06-009 der Bundesnetzagentur
- die Abfallentsorger – Abfallverbringungsverordnung, Kreislaufwirtschafts- und Abfallgesetz, Nachweisverordnung.
- das interne IT-Personal ggf. – SAS No 70 Typ 2.
- alle aber speziell die Personalabteilung – das Bundesdatenschutzgesetz (BSDG), Arbeitnehmerüberlassungsgesetz, oder AGG
- der Vertrieb und Einkauf – das Vertragswesen (siehe Schmiergeldaffären)
- die Finanzbuchhaltung – Umsatzsteuergesetz, HGB, AO, GoB und GDPdU (Achtung: E-Mail ist seit 2007 auch ein Handelsbrief und Bedarf der elektronischen Archivierung im Original).

Wie diese bei Weitem unvollständige Liste zeigt, gibt es sehr unterschiedliche Anforderungen an die Überprüfung der Regeleinhaltung, so dass ein jeweils passendes Compliance Management individuell eingerichtet werden muss. Die Fülle an Regularien, in denen sich Unternehmen bewegen müssen, ist inzwischen so angewachsen, dass schon 2-jährige Master-Studiengänge[2] angeboten werden.

Compliance Maturity Model

Es gibt auch schon seit Längerem (2004) ein Compliance Maturity Model (siehe Grafik weiter unten) – verfasst von Gartner, an dem sich ablesen lässt, wie gut eine Firma den Umgang mit dem Compliance Management beherrscht. Für das Management der IT-Compliance ist das CobiT Framework weit verbreitet im Einsatz. CobiT wurde ursprünglich (1993) vom internationalen Verband der IT-Prüfer (Information Systems Audit and Control Association, ISACA) entwickelt.

[2] http://www.duw-berlin.de

Seit 2000 obliegt es dem IT Governance Institute, einer Schwesterorganisation der ISACA, CobiT zu entwickeln und fortzuschreiben. CobiT hat sich von einem Werkzeug für IT-Prüfer (Auditoren) zu einem Werkzeug für die Steuerung der IT aus Unternehmenssicht entwickelt und wird unter anderem auch als Modell zur Sicherstellung der Einhaltung gesetzlicher Anforderungen (Compliance) eingesetzt. Eine Case Study für die Überprüfung einer Firma nach dem CobiT Framework wurde Andrea Pederiva von der ISACA 2003 veröffentlicht.[3]

[3] Pederiva, A. (2003). The COBIT maturity model in vendor evaluation case. *Information Systems Control*, Journal, Vol. 3. pp. 26-29.

Gartner Compliance Maturity Model



Compliance Management in der betrieblichen Praxis

Ein Compliance Manager hat es nach einem Urteil des Bundesgerichtshofs (BGH) in 2009 nicht leicht: Erstmals wurde ein Compliance Officer verurteilt, weil er ihm bekannte Delikte nicht verhindert hat. Das Urteil sorgt für Verunsicherung unter den Aufpassern. Als Konsequenz aus dem Urteil sollten „Chief Compliance Officer in nächster Zeit darauf achten, ihre eigenen Zuständigkeiten, Aufgaben und Befugnisse klar im Arbeitsvertrag und in der Stellenbeschreibung zu definieren", empfiehlt Christian Pelz, Fachanwalt für Strafrecht bei Nörr Stiefenhofer Lutz.

Die Maßnahmen rund um das Compliance Management dürfen aber auch nicht hinderlich sein, oder auch zu teuer. So schreibt trefflich Rechtsanwalt Dr. Peter Mailänder in seinem Fachartikel „Compliance in mittelständischen Unternehmen" in Business & Law Stuttgart 2009: „Das mit Compliance gesteckte Ziel, Rechtsverstöße, Bußgelder, Reputationsschädigungen und Umsatzrückgänge zu vermeiden sowie Haftungsrisiken zu minimieren, darf allerdings nicht zu einer Bürokratisierung und Hemmung des Geschäftsablaufs führen. Compliance-Systeme sind Mittel zum Zweck und unterliegen daher dem **Wirtschaftlichkeitsprinzip und der Zweck-Mittel-Rationalität."**

Nicht nur lästige Pflicht

Einsparpotentiale

Es gibt aber gerade in den Bereichen, in denen Lösungen auf Basis der SAPERION ECM Software zum Einsatz kommen, große Einsparpotentiale, so dass dies Compliance-Anwendungen zu zusätzlichem Nutzen verhilft. Gerade in der Verwaltung von Dokumenten auf elektronischer Basis lassen sich schnell die Investitionen in Monaten wieder amortisieren. Im Folgenden soll nun auf spezielle Compliance-Anwendungen eingegangen werden. Dazu gehören

+ das Verwalten von Dokumenten in Bezug auf Aufbewahrungsrichtlinien,
+ das Interne Kontrollsystem (IKS), wie es z.B. für die Steuerung der Rechnungslegungsprozesse oder von Kontrollaufgabe der Internen IT eingesetzt wird,
+ die E-Mail-Archivierung zur Aufbewahrung geschäftsrelevanter E-Mails inklusive deren Attachments,
+ die Signaturverfahren für elektronische Rechnungen,
+ die Web Content Archivierung zur Beweissicherung von Informationen, die im Rahmen von Web-Auftritten präsentiert werden,
+ die Verwaltung von Personalakten im Hinblick das Bundesdatenschutzgesetz,
+ die Verwaltung von Verträgen zur Reduktion von Kosten aber auch Schutz vor Korruption,
+ die verschlüsselte Speicherung für die Verwaltung von Kreditkartendaten nach PCI-Datensicherheitsstandard (DSS) und
+ die Beweiswertsicherung kryptographisch signierter Dokumente.

2 COMPLIANCE-ANWENDUNGEN

Dieses Kapitel beschreibt unterschiedliche Anwendungsfälle von Schriftgut-zentriertem Compliance Management.

2.1 Records Management

Records Management ist ein Thema, das von zwei Seiten zu betrachten ist. Es gibt auf der einen Seite die so genannten Archivare der öffentlichen Hand, deren Aufgabe es ist, Dokumente der Kommunen, Länder und des Bundes unter den Gesichtspunkten der Historisierung aufzubewahren. Anforderungen daran sehen anders aus als für die Aufbewahrung von Schriftgut, das während des wirtschaftlichen Handelns zwischen Organisationen anfällt. In diesem Dokument sollen letztere besprochen werden, denn erstere haben weniger hohe Anforderungen an den Datenschutz inkl. der Vernichtung.

Die allgemeinsten Regeln legen die Fristen der Aufbewahrung für und Löschvorschriften von Schriftgut fest. So müssen steuerprüfungsrelevante Dokumente in Deutschland in der Regel 10 Jahre aufbewahrt werden. In anderen Ländern können diese Fristen anders gefasst sein.

Es gibt Dokumente wie z.B. im Banken- oder Versicherungssektor, deren Aufbewahrungszeiten erst mit dem Ereignis der Aktenschließung berechnet werden.

Zudem gibt es Dokumente, die nach dem Datenschutzgesetz für nur eine bestimmte Dauer aufbewahrt werden dürfen und anschließend zu löschen sind, wie z.B. eine Abmahnung in der Regel nach 24 Monaten oder Bewerbungsunterlagen nach der Absage an den Bewerber, falls keine Erlaubnis für eine längere Aufbewahrung eingeholt wurde.

Weitergehende Informationen können unserem „Technical Info Records Management“ entnommen werden. In diesem Dokument wird auch die Thematik der Standards für das Records Management behandelt. Es bleibt festzustellen, dass sich der Markt schwer tut, entsprechende Standards wie zum Beispiel MoReq technisch komplett umzusetzen.

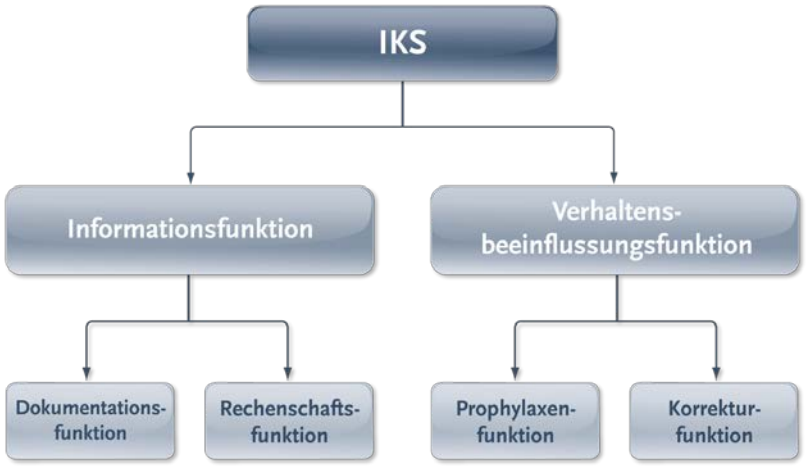
Lösungsansatz

Die SAPERION ECM Compliance Suite bietet die Möglichkeit, für jeden Dokumententyp Aufbewahrungsrichtlinien festzulegen. Unterschieden werden kann zwischen der sogenannten „Fixed Retention“ und „Event-based Retention“. Im ersten Fall wird bei Archivierung direkt die Aufbewahrungszeit gesetzt. Im zweiten Fall wird eine Regel hinterlegt und das Dokument anfangs unbefristet archiviert. Trifft das Ereignis für die Regel ein, z.B. die Akte wird geschlossen, weil der Kredit zurückgezahlt ist, wird die endgültige Aufbewahrungszeit berechnet

und gesetzt. Werden Storage Systeme verwendet, die eigene Retention-Funktionen anbieten, so werden die Parameter an die Systeme weitergereicht. Im Falle von SAN oder NAS Devices verwaltet SAPERION die Funktionen allein.

2.2 Internes Kontrollsystem (IKS)

In Deutschland hat sich ein neuer Begriff im Kontext der Compliance etabliert: das Interne Kontrollsystem, kurz IKS. International wird eher das Akronym GRC für „Governance, Risk, and Compliance“ genutzt. Das IKS besteht aus systematisch gestalteten, organisatorischen Maßnahmen und Kontrollen im Unternehmen zur Einhaltung von Richtlinien und zur Abwehr von Schäden, die durch das eigene Personal oder böswillige Dritte verursacht werden können.



Die Struktur des IKS nach Prof. Thomas Berndt ACA-HSG

Der Vorstand von Aktiengesellschaften, aber auch die Geschäftsführung größerer GmbHs muss ein Risikomanagementsystem nicht nur einrichten, sondern auch umfassend dokumentieren (siehe § 91 Abs. 2 Aktiengesetz). In der unterbliebenen Dokumentation liegt ein wesentlicher Gesetzesverstoß vor und führt in der Regel zur Nichtentlastung des Vorstands. Das Überwachungsorgan hat in seinem Bericht mitzuteilen, in welcher Art und in welchem Umfang die Geschäftsführung der Gesellschaft während des Geschäftsjahres geprüft hat. Dies betrifft die Zahl der Sitzungen, Angaben über die Häufigkeit der Prüfungen, Gegenstand und Methoden der Prüfungen. Bei wirtschaftlichen Schwierigkeiten muss das Überwachungsorgan auch darüber berichten, ob und mit welchem Erfolg es seine Überwachungstätigkeit intensiviert hat. Dies betrifft insbesondere außergewöhnliche Prüfungsmaßnahmen, etwa Anforderungsberichte, Einsicht in Bücher und Dokumente, Beauftragung von Sachverständigen, Entscheidungen über Zustimmungsvorbehalte.

Grundlage eines Internen Kontrollsystems bilden die folgenden vier Prinzipien:

- **Transparenz**: Für Prozesse müssen Sollkonzepte etabliert sein, auf Basis derer Außenstehende beurteilen können, inwieweit Beteiligte konform zu diesem Sollkonzept arbeiten. Gleichzeitig wird dadurch die Erwartungshaltung der Organisationsleitung definiert.
- **Vier Augen:** In einem gut funktionierenden Kontrollsystem bleibt kein wesentlicher Vorgang ohne (Gegen-)Kontrolle
- **Funktionstrennung**: Bestimmte Tätigkeiten innerhalb eines Unternehmensprozesses (z.B. Einkauf verstanden als Prozess von der Bedarfsermittlung bis zum Zahlungsausgang) sind von unterschiedlichen Personen wahrzunehmen: Vollziehende (z.B. Abwicklung von Einkäufen) sind andere als Verbuchende (z.B. Finanzbuchhaltung, Lagerbuchhaltung) oder Verwaltende (z.B. Lagerverwaltung).
- **Mindestinformation:** Mitarbeitern stehen nur diejenigen Informationen zur Verfügung, die sie für ihre Arbeit brauchen. Dies schließt auch die entsprechenden Sicherungsmaßnahmen bei IT-Systemen mit ein.

Die Ziele sichern allen Stakeholdern das Überleben eines Unternehmens (einbezogen auch die Mitarbeiter, die ebenso mitzuwirken haben), seien es die Funktionsfähigkeit und Wirtschaftlichkeit von Geschäftsprozessen, die Zuverlässigkeit von betrieblichen Informationen, die Vermögenssicherung oder Regeleinhaltung in Bezug auf Gesetzgebungen zur Sicherung der Reputation.

Lösungsansatz

Dass die technische Unterstützung der Dokumentationen und Kontrollen von Prüfaufgaben einfach mit einer Tabelle geht, wird auf der Web-Site compliance-net[4] gezeigt. Aber auch einfache Szenarien auf Basis von SAPERION ECM helfen hier. Denn einerseits ist die Dokumentation ein Schwerpunkt des IKS und kann daher gut mit der SAPERION ECM Suite verwaltet werden. Andererseits müssen Kontrollen periodisch über kleine Workflows durchgeführt werden. Dabei helfen die SAPERION ECM Workflow-Funktionen mit dem Audittrail zusätzlich. Weitergehende Information sind in einer Artikelserie[5] auf unserem Blog nachzulesen.

2.3 E-Mail Lifecycle Management

In den letzten Jahren hat die Bedeutung von E-Mails enorm zugenommen. Kein Unternehmen kommt mehr ohne sie aus. Sie wird für die Protokollierung von Absprachen, als Transportmittel für auszutauschende Dokumente in Form von (sig-

[4] http://www.compliance-net.de/node/58
[5] http://www.saperionblog.com/tag/IKS-serie

nierten) Anhängen oder für die schnelle und unkomplizierte Kommunikation verwendet.

Eine E-Mail ist schnell verschickt, jedoch hat die Bereitstellung dieser Kommunikationsform an Komplexität zugenommen. Zeitintensive Administration der E-Mail-Server und -Storages, Separation von relevanten und irrelevanten E-Mails (z.B. Spam) und vor allem der Umgang mit privaten E-Mails zieht einen nicht zu unterschätzenden Aufwand mit sich.

Zudem hat die E-Mail seit dem 01.01.2007 auch rechtlich eine hohe Bedeutung bekommen: Sie ist dem Handelsbrief gleich gestellt worden. Sobald sie relevante Informationen steuerlicher oder geschäftlicher Natur beinhaltet, unterliegt sie einer Frist, in der sie geschützt aufbewahrt und jederzeit im Kontext des Geschäftsfalls verfügbar sein muss. Somit führt an einem durchdachten E-Mail-Management nichts mehr vorbei.

Denn neben der rechtlichen Konformität können zusätzliche Effizienzsteigerungen durch die Einbindung von E-Mails in Geschäftsprozesse und Akten erreicht werden.

Auch die Struktur der Informationssysteme im Unternehmen kann deutlich vereinfacht und der Aufwand der Wartung reduziert werden. Seit einigen Jahren beschäftigen sich IT-Dienstleister und Softwarehäuser intensiv mit dem Thema und bieten unterschiedliche Lösungen, um zumindest bei Compliance-Problematik Abhilfe zu schaffen.

Diese Lösungsansätze differenzieren sich nicht nur anhand von Funktionalität, sondern auch prinzipiell bei der Strategie der Lösung. So unterscheiden sich Strategien z.B. in Hinsicht auf die gesamte IT-Landschaft und die Berücksichtigung von Prozessen und Fremdsystemen.

Problemkind private E-Mail

Demzufolge ist es keine triviale Aufgabe für das Management, eine passende Lösung für das Unternehmen zu finden. Denn E-Mail-Management und gesetzeskonformes Verhalten wird nicht ausschließlich von einer einzigen Software abgedeckt. Eine E-Mail-Management-Strategie betrifft Jeden im Unternehmen und muss in Zusammenarbeit mit dem Betriebsrat abgestimmt und in Form von Prozessen auch außerhalb der IT abgesichert werden, denn der Datenschutz spielt hier eine große Rolle.

E-Mail-Management ist ohne eine durchdachte Bedarfsanalyse langfristig nicht sinnvoll implementierbar. Daher fällt der Unternehmensberatung eine besondere Aufgabe zu. Das Konzept muss auf die Bedürfnisse aller abgestimmt und Problemstellungen adressiert werden, bevor eine Software-Lösung implementiert werden kann.

Lösungsansatz

SAPERION bietet passende Server-basierte Lösungen für Microsoft Exchange und IBM Notes an. Hierbei werden E-Mails, die in bestimmten Ordnern einlaufen, direkt an SAPERION übergeben. In den E-Mail-Systemen verblieben so genannte Stubs. Das sind die E-Mail-Körbe, deren Anhänge nur noch in SAPERION gespeichert sind. Soll ein solcher Anhang geöffnet werden, wird er über SAPERION wieder zur Anzeige gebracht.

Eine weitere Alternative der Archivierung erfolgt in der Verantwortung des Anwenders über eine Integration in Outlook. Hier entscheidet der Anwender selbst, welche E-Mail oder Dokumente wohin archiviert werden sollen, quasi so, wie er es im Falle der Papierakte schon ausführt.

Weitergehende Informationen zum E-Mail-Management sind unseren beiden Whitepapern zum Thema E-Mail-Management für jeweils Exchange und Notes zu entnehmen – veröffentlicht auf unserer Homepage. Best Practice[6]-Artikel sind zudem auf unserem Blog zu finden.

2.4 Web Content Archivierung

Das Internet ist aus unserem Leben nicht mehr wegzudenken, aber dennoch rechtlich auf relativ dünnem Eis stehend. Gemäß der weltweit ersten Studie zu den quantitativen Auswirkungen von Internetaktivitäten sind heute 3,4% des Bruttoinlandproduktes der G8-Staaten direkt auf den Online-Kanal zurückzuführen (McKinsey 2011, Measuring the Net's growth dividend[7]). Ein absolut beachtlicher Wert, der die Landwirtschaft oder auch den Energiesektor bereits in den Schatten stellt und von dem auszugehen ist, dass dessen Anstieg auf absehbare Zeit nicht abreißen wird.

Obwohl für Informationen, die auf öffentlichen Firmen-Websites, e-Shops oder auch innerhalb Intra- und Extranets publiziert sind, grundsätzlich dieselben Aufbewahrungs- und Sorgfaltsrichtlinien gelten wie für „traditionelle" Dokumente oder E-Mails, wurden bisher erst wenige Initiativen im Markt gestartet, die sich auf professioneller Ebene damit auseinandersetzen.

Im ECM-Kontext wurde dies bereits seit geraumer Zeit erkannt (siehe Artikel „Offene Flanke der elektronischen Archivierung: Websites und Webtransaktionen" von Dr. Ulrich Kampffmeyer aus dem Jahr 2003). Dennoch gibt es bisher wenige Lösungen am Markt.

[6] http://www.saperionblog.com/?s=best+practice+E-Mail
[7] https://www.mckinseyquarterly.com/Measuring_the_Nets_growth_dividend_2812

Anforderungen an die Web Content Archivierung

- Die allgemeinen Geschäftsbedingungen, die auf einer Website oder e-Shop veröffentlicht werden, sind verbindlich und sollten hinsichtlich der Sorgfaltspflichten ebenfalls aufbewahrt werden.
- Ebenso ist es hilfreich, nachweisen zu können, was im Impressum zu einem Zeitpunkt stand und welche Haftungsausschlüsse es gab.
- Belege, die bei Bestellungen in e-Shops generiert werden, sollten direkt in das relevante Kundendossier abgelegt werden.
- Aktuelle Websites bieten immer häufiger Multimedia-Inhalte, welche im Kontext einer spezifischen Webpage archiviert werden sollten.
- Aus internen Gründen wie z.B. einer Firmenhistorie könnte auch dies ein wichtiger Punkt für die Aufzeichnung des Web-Auftritts sein.

Lösungsansatz

Die SAPERION AG erkannte Anfang 2011 das schlummernde Potential und fand mit dem Schweizer Softwarehersteller qumram AG einen Partner, mit dem gemeinsam eine Software-Lösung entwickelt wurde, die es Unternehmen und Organisationen erlaubt, Web-Inhalte und -Transaktionen zu archivieren und damit den geltenden regulatorischen Vorschriften und Risikomanagementvorgaben gerecht zu werden. Gesteuert über granulare Konfigurationsmöglichkeiten, werden definierte Datenelemente der Web-Auftritte im SAPERION ECM Archiv revisionssicher aufbewahrt und mittels einer Navigationsoberfläche mit integrierter Suchmöglichkeit wieder gefunden und zur Ansicht gebracht.



Die Lösung „SAPERION ECM Web Content Archive“ gewann – sehr zur Freude aller involvierter Parteien – zur CeBIT 2011 den Innovationspreis-IT in der Kategorie Content Management. Weiterführende Informationen, insbesondere zum Vorgehen der Einrichtung zur Archivierung von Web-Auftritten, sind in einer Artikelserie[8] auf unserem Blog nachzulesen.

2.5 Beweiswertsicherung kryptographisch signierter Dokumente

Ein noch stark in der Diskussion befindliches Thema rund um qualifiziert signierte Dokumente ist ihre Neusignierung, synonym auch Nachsignierung, wie sie laut §6 des Signaturgesetzes (SigG) bei Bedarf anfällt. Grundsätzlich tritt der Bedarf ein, wenn die Bundesnetzagentur (BNetzA) einen der zum Signieren verwendeten Algorithmen ab einem bestimmten Zeitpunkt als schwach einstuft. Welche Dokumente darüber hinaus unter diesen „Bedarf“ fallen, ist nach aktueller Sachlage nicht eindeutig geklärt. Es gibt diesbezüglich bisher keine offiziellen Stellungnahmen, sondern nur Gutachten einzelner Rechtsanwälte. So muss jedes Un-

[8] http://www.saperionblog.com/tag/WCA-serie

ternehmen für sich prüfen, ob ihre Dokumente einen „Bedarf“ haben. Nach reiner Auslegung der Gesetzestexte scheint die Notwendigkeit gegeben, alle Dokumente neu zu signieren, deren Beweiskraft zu erhalten ist; u.a. dann, wenn davon ausgegangen werden muss, dass es zu einem Streitfall kommen könnte. Eine ausführliche Bearbeitung des Sachverhaltes kann in dem Buch „Beweiskräftige elektronische Archivierung – Bieten elektronische Signaturen Rechtssicherheit?“ von Roßnagel und Schmücker nachgelesen werden.

Aufgrund der sehr hohen Anforderungen an die zu verwendenden Komponenten als auch an die Prozesse zur Erstellung der Zertifikate genießen qualifiziert signierte Dokumente den Status der höchsten Beweiskraft. Die Zivilprozessordnung geht bei in dieser Form signierten Dokumenten vom Anscheinsbeweis aus. Dies bedeutet, dass der Richter das Dokument als Beweis anerkennen muss – es sei denn, es bestehen ernstliche Zweifel daran, ob die Erklärung tatsächlich vom Signaturschlüssel-Inhaber abgegeben worden ist (§371a ZPO). Diese hohe Beweiskraft geht verloren, sobald der von der BNetzA genannte Zeitpunkt für die Schwächung eines der beiden verwendeten Algorithmen zum Signieren erreicht wurde.

Aber auch wenn diese hohe Beweiswert fällt, so ist noch immer eine relativ hohe Beweiskraft gegeben, sofern das betreffende Dokument sicher aufbewahrt wurde, wie z.B. in einem elektronischen Archiv. In diesem Fall wird der Richter seine freie Beweiswürdigung durchführen und das Beweismittel anerkennen oder auch nicht.

Anmerkung zu qualifiziert signierten Rechnungen:

> *Der Steuerprüfer verlangt keine Neusignierung. Im Falle der Beweisführung in einem Zivilprozess könnte aber auch das Konzept der Neusignierung relevant sein.*

Weitergehende Informationen können unserem „Technical Info LTANS-konforme Langezeitarchivierung“ entnommen werden. LTANS steht für den Standard “Long-Term Archiving and Notary Service”. Dieser beschreibt u.a. das ERS-Format der beweisenden Reports (ERS = Evidence Record Syntax).

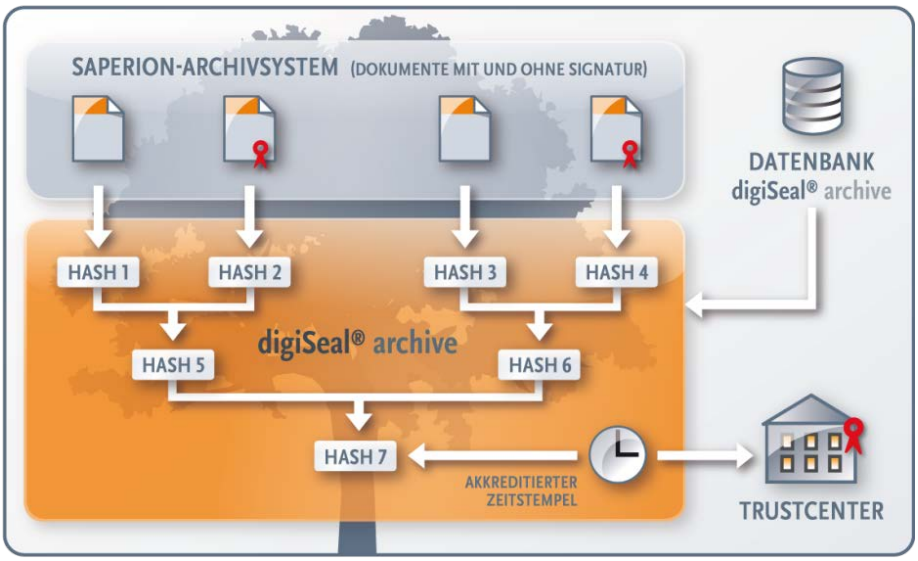
LTANS
Long-Term Archiving and Notary Service

Weitergehende Informationen zum Thema Signaturanwendungen und Verfahren, speziell für den Austausch elektronischer Rechnungen, bietet unser Whitepaper zum Thema Elektronische Signaturen.

Lösungsansatz

Für jene Firmen, die für sich den Bedarf einer Beweiswerterhaltung sehen, können die betreffenden Dokumente zusätzlich mit dem Partnerprodukt digiSeal archive erfasst werden. SAPERION hat das Produkt in die Lösungen so integriert, dass bei Archivierung von Dokumenten nach bestimmten Kriterien zusätzlich ein Hash-Wert berechnet und in einen sogenannten Hash-Baum aufgenommen wird.

Dieser wird typischerweise am Ende des Tages mit einem Zeitstempel signiert, so wie es in der Technischen Richtlinie TR-ESOR (TR-03125) erwähnt wird. Tritt das Ereignis der Algorithmen-Schwächung ein, erfolgt eine automatisierte Neu-signierung.



Hash-Baum-Verfahren und Zeitstempelung

3 AUSGEWÄHLTE REGULARIEN IM DETAIL

In diesem Kapitel gehen wir auf ausgewählte Regularien ein und erläutern, wie diese mit Hilfe von SAPERION konkret unterstützt werden, so dass Ihre Anwendungen auch wirklich „compliant“ werden können. Grundsätzlich ist es aber so, dass der Einsatz von SAPERION ECM Software nicht gleichbedeutend mit der Compliance in Hinsicht auf ein Regelwerk ist – genauso wenig wie die Verwendung eines beliebig anderen ECM-Produkts. Es gilt immer, dass der Gesamtkontext des Betriebs in Hinsicht auf die Regeleinhaltung geprüft werden muss.

3.1 Verschiedene Records Management Standards

ISO 15489

Häufig wird gefragt, ob SAPERION in Bezug auf ein Records Management (Schriftgutverwaltung) ISO 15489 konform ist. Richtig muss die Frage lauten: „Kann ich mit SAPERION mein Records Management ISO 15489 konform betreiben?“. Dieser Standard beschreibt das Organisatorische und nicht die technischen Anforderungen, daher kann hier mit einem klaren „Ja“ geantwortet werden.

MoReq 2010

Anders sieht es mit dem europäischen Standard MoReq 2010 (Model Requirements for the Management of Electronic Records) aus. Der Vorgänger MoReq2 war zu umfangreich, so dass nochmals eine Reduzierung der Anforderungen sowie eine Modularisierung vorgenommen werden mussten. Noch wird an einem Zertifizierungsprogramm gearbeitet, d.h. bisher können Hersteller nur kommunizieren, dass sie konform sind. Das trifft auch für SAPERION zu, sofern das SAPERION ECM System sachgerecht betrieben wird.

DOMEA

In Deutschland war DOMEA (Konzept für Dokumentenmanagement und elektronische Archivierung in der öffentlichen Verwaltung) relevant für Anwendungen auf Bundesebene (Ministerien). Da dieser Standard zu umfangreich war und gerade die Anforderungen der Kommunen deutlich übererfüllte, wird derzeit an einer vereinfachten Version gearbeitet. SAPERION hat hier ebenfalls auf eine explizite Zertifizierung verzichtet, erfüllt aber die Anforderungen der Kommunen. Nach dem DOMEA-Konzept können derzeit keine Systeme mehr zertifiziert werden, da aktuell an dem Folge-Konzept mit der Bezeichnung „Organisationskonzept Elektronische Verwaltungsarbeit“ gearbeitet wird. Sobald die Freigabe des neuen Konzepts erfolgt, wird geprüft, ob wir uns entsprechend zertifizieren lassen wollen.[9]

[9] http://www.verwaltung-innovativ.de/cln_108/nn_684678/DE/Organisation/orgkonzept__everwaltung/orgkonzept__everwaltung__node.html?__nnn=true

DoD 5015.2

Für Nordamerika – besonders in den USA – ist die DoD Directive 5015.*2 (Department of Defense Records Management Program)* relevant. Anfangs war sie vorrangig Pflicht für Anwendungen im militärischen Umfeld, betrifft aber inzwischen den kompletten öffentlichen Bereich in den USA. SAPERION ist hierfür zwar nicht explizit zertifiziert, erfüllt aber die Anforderungen.

3.2 Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme

Die Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (kurz GoBS) sind von der deutschen Finanzverwaltung durch Schreiben des Bundesfinanzministeriums vom 7. November 1995 aufgestellte Regeln zur Buchführung mittels Datenverarbeitungssystemen. Die GoBS stellen eine Erläuterung zum Handelsgesetzbuch und zur Abgabenordnung in Bezug auf die ordnungsmäßige Behandlung elektronischer Dokumente dar.

Umgang mit aufbewahrungspflichtigen Daten und Belegen

In den GoBS wird die Behandlung aufbewahrungspflichtiger Daten und Belege in elektronischen Buchführungssystemen sowie in datensicheren Dokumentenmanagement- und revisionssicheren Archivsystemen geregelt. Die GoBS behandeln dabei auch Verfahrenstechniken wie Scannen und Datenübernahme. Ein wesentlicher Kernpunkt ist dabei das sogenannte „Interne Kontrollsystem“ (kurz IKS), dessen Zweck bereits weiter oben beschrieben ist.

Die GoBS enthalten weiterhin auch die Vorgaben für die Verfahrensdokumentation, die zum Nachweis des ordnungsmäßigen Betriebes des Systems erforderlich ist.

Unmittelbar haben sie nur für steuerliche Buchführung Geltung. Da jedoch zahlreiche – gerade kleine und mittlere Unternehmen (KMU) –eine Einheitsbilanz erstellen, wirken sie sich auch auf die handelsrechtliche Buchführung aus. Denn wenn eine so große Zahl von Kaufleuten diesen Regeln folgt, werden sie zum Handelsbrauch und somit zu handelsrechtlichen Grundsätzen ordnungsmäßiger Buchführung (GoB).

Ist eine Buchführung nicht ordnungsmäßig, so können die Besteuerungsgrundlagen von den Finanzbehörden geschätzt werden. Unrichtige Wiedergabe oder Verschleierung von Jahresabschlüssen wird mit Freiheits- oder Geldstrafen geahndet (§ 331 HGB, §§ 370 f. AO). Im Insolvenzfall ziehen Verstöße gegen die GoB Freiheitsstrafen nach sich (§ 283 Strafgesetzbuch).

3.3 Aufbewahrungsfristen und zu beachtende Regularien des Bundesdatenschutzgesetzes

Datenschutzgesetz

Nach dem Bundesdatenschutzgesetz (BDSG) sind personenbezogene Daten, die für eigene Geschäftszwecke verarbeitet werden, grundsätzlich zu löschen, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist (§ 35 Abs. 2 S. 2 Nr. 3 BDSG). Etwas anderes gilt jedoch, wenn besondere Rechtsvorschriften außerhalb des BDSG die weitere Aufbewahrung der betroffenen Daten vorschreiben (§ 4 Abs. 1 BDSG). Werden personenbezogene Daten für die Verfolgung eigener Geschäftszwecke nicht mehr benötigt und stehen einer Löschung gesetzliche Aufbewahrungspflichten entgegen, so sind die betreffenden Daten zu sperren (§ 35 Abs. 3 Nr. 1 BDSG). Das bedeutet, sie sind mit einer Kennzeichnung zu versehen, um ihre weitere Verarbeitung oder Nutzung einzuschränken (§ 3 Abs. 4 S. 2 Nr. 4 BDSG).

Aufbewahrungsfristen

Die Gesellschaft für Datenschutz und Datensicherung e.V. (GDD) hat eine Checkliste für Allgemeine Aufbewahrungspflichten (HGB und AO) und für Dokumente, die in der Hoheit der Personalabteilungen bewegt werden, veröffentlicht.[10]

3.4 Was bei der Vernichtung von Papier nach dem Scannen zu beachten ist

Da es eine Unmenge unterschiedlichster Typen von Dokumenten gibt, deren Betrachtung hier den Rahmen sprengen würde, werden hier nur die wichtigsten besprochen. Schauen wir uns also an, wie für Handels- und Steuer-relevante Dokumente eine sichere Steuerprüfung sowie eine sichere Beweisführung vor dem Zivilgericht erreicht werden kann.

Handelsrechtliche Regelungen finden sich in § 147 AO und dem etwas enger gefassten § 257 HGB. Zwar beziehen sich diese Vorschriften dem Wortlaut nach zunächst nur auf den Datenzugriff der Finanzverwaltung, aber immer mehr Rechtsvorschriften aus anderen Bereichen verweisen auf sie.

Seit dem 23. Januar 2008 gibt es eine Erweiterung des Katalogs der Finanzverwaltung mit Fragen und Antworten zum Datenzugriffsrecht[11], die sich unter anderem mit der Vernichtung der Originale digitalisierter Belege auseinander setzt. Der Wortlaut ist:

[10] siehe zum Beispiel http://www.lvglth.de/download/mas/Aufbewahrungsfrist2.pdf
[11] siehe http://www.bundesfinanzministerium.de

> *„Werden Unterlagen, die das Unternehmen originär in Papierform erhalten hat, aus betrieblichen Gründen digitalisiert, sind diese in dieser digitalen Form (z.B. in Bildformaten wie PDF oder TIFF) vorzuhalten. Soweit das Verfahren und die Prozesse den GoB/GoBS entsprechen und nicht nach anderen Rechtsvorschriften die Aufbewahrung im Original vorgeschrieben ist, ist auch die anschließende Vernichtung der Originaldokumente zulässig. Die Regelungen zur ordnungsgemäßen Vernichtung nicht mehr benötigter Dokumente und zur Aufbewahrung weiterhin erforderlicher Originaldokumente sind in der Verfahrensdokumentation aufzuführen."*

Sind die Belege digitalisiert und die folgenden durch die Finanzverwaltung geforderten Voraussetzungen erfüllt, dann dürfen die Originale vernichtet werden.

Verfügbarkeit der Belege in digitaler Form

Verfügbarkeit

Sobald die Belege digitalisiert sind, müssen sie in digitaler Form vorgehalten werden. Dafür nennt die Finanzverwaltung beispielhaft zwei Dateiformate, nämlich PDF oder TIFF. Selbstverständlich dürfen auch andere Dateiformate verwendet werden, sofern sie die gesetzlichen Anforderungen an die Manipulationssicherheit erfüllen.

Vorhalten bedeutet: Es ist sicher zu stellen, dass die digitalen Belege „während der Dauer der Aufbewahrungsfrist jederzeit verfügbar sind, unverzüglich lesbar gemacht und maschinell ausgewertet werden können" (§ 147 Abs. 2 Nr. 2 AO).

GoBS-Konformität des Verarbeitungsverfahrens

PK-DML-Zertifikat

GoBS-konforme Gesamtlösung

Die GoBS[12] (Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme) definieren die Anforderungen, die an eine Buchführungssoftware und den Umgang mit ihr gestellt werden, damit die Grundsätze ordnungsmäßiger Buchführung eingehalten sind. Hier sei darauf hingewiesen, dass ein Testat der Konformität eines Produkts, wie dies für SAPERION ECM seitens der KPMG ausgestellt wurde, nicht ausreicht. Da ein Produkt immer in eine Umgebung eingebettet wird, muss die Gesamtlösung GoBS-konform sein. Dies kann sich ein Anwender z.B. durch das Testat nach PL-DML (Prüfkriterien – Dokumentenmanagementlösung des VOI) bestätigen lassen.

GOBS-Konformität der Prozesse

Sichere Verarbeitungsprozesse

Das Verarbeitungsverfahren ist dann GoBS-konform, wenn durch organisatorische Maßnahmen verhindert wird, dass eine Manipulation der Belege durch die verarbeitenden Mitarbeiter erfolgt. Beispielsweise muss es den Angestellten durch technische Maßnahmen verwehrt und durch betriebliche Vereinbarungen unter-

[12] siehe http://www.bundesfinanzministerium.de

sagt sein, Belege durch Bildbearbeitungsprogramme zu verändern. Für die Digitalisierung muss also ein Prozess definiert sein, der durch seine Gestaltung die Manipulation von Belegen verhindert oder zumindest erschwert. Diese Maßnahmen sind in der Verfahrensdokumentation niederzulegen.

Regeln zur Vernichtung der Originale und Einhaltung dieser Regeln

Geregelter Vernichtungsprozess

Das Original eines digitalisierten Belegs ist nicht zwingend zu vernichten. Selbstverständlich darf der Beleg neben der digitalisierten Form auch in Papierform weiterhin aufbewahrt werden. Wenn er allerdings vernichtet werden soll, dann muss dafür ein Prozess nach Datenschutzrichtlinien eingeführt werden.

Was spricht gegen eine Vernichtung?

Die Vorschrift des § 147 AO bezieht sich allein auf die steuer- und handelsrechtliche Aufbewahrungspflichten gegenüber der Finanzverwaltung. Für Dokumente, die als Beweis in einem Zivilprozess dienen könnten, ist eine Vernichtung nicht zu empfehlen. Im Zivilprozess unterliegt eine digitalisierte (und dann ausgedruckte) Rechnung der freien Beweiswürdigung des Richters, § 286 ZPO. Er kann den Ausdruck des digitalisierten Belegs als Beweis anerkennen, muss es aber nicht. Sollte der Richter den Originalbeleg verlangen, so kann man den geforderten Beweis nicht führen, wenn das Original vernichtet wurde. Auch die Vorschrift des § 371 a ZPO, der die Beweiskraft elektronischer Dokumente regelt, hilft hier nicht weiter, da er nicht anwendbar ist – selbst wenn das Dokument durch den Scan-Anwender qualifiziert signiert wurde. In diesem Fall sind nämlich Signaturschlüssel-Inhaber (falls der Beleg nach dem Scannen überhaupt signiert wurde) und Urheber nicht identisch. Es sei denn, das Dokument ist nicht handschriftlich unterschrieben worden und daher keine Urkunde. In den Bereichen, in denen das Sozialgesetzbuch, speziell der § 110d greift, wie z.B. bei den Sozialversicherern und Krankenhäuser, setzt sich das Verfahren von Scannen, Signieren, Vernichten aber inzwischen durch.

Für Verwendungsnachweise sind die Regeln nur teilweise anzuwenden. In Ziff. 6.10. der „Allgemeinen Nebenbestimmungen für Zuwendungen zur Projektförderung“ (ANBest-P) wird auf landesrechtlicher Ebene zwar auf die Vorschriften des HGB und der Grundsätze ordnungsmäßiger Buchführung verwiesen, im europäischen Recht sind allerdings Besonderheiten versteckt. Eine einheitliche Regelung für alle europäischen Ebenen und Projekte existiert nicht. Deshalb sollten aus Vorsichtsgründen immer die Originale aufbewahrt werden – wenn auch in einer vereinfachten Ablage.

Die Faustregel lautet demnach: Risikobetrachtung

Immer dann, wenn die Streitwahrscheinlichkeit und Schadenssumme groß ist, sollte besser ein Original vorgelegt werden. Um Schaden abzuwenden, sollte es besser nicht vernichtet werden. Oder im Umkehrschluss: Wenn kaum Prozesse zu erwarten sind, wie z.B. bei Rechnungsbelegen, und der Streitwert niedrig ist, dann kann digitalisiert und anschließend vernichtet werden. Zusätzlich lässt man sich am besten durch einen Rechtsanwalt bestätigen, was unbedenklich vernichtet werden kann und was nicht. Gegebenenfalls hilft auch eine Klärung mit dem jeweils zuständigen Gericht.

3.5 Bestimmungen für die Verwaltung von Kreditkartendaten

Schutzmaßnahmen für Kreditkartendaten

Der PCI-Datensicherheitsstandard (DSS)[13] wurde entwickelt, um die Datensicherheit von Karteninhabern zu verbessern und die umfassende Akzeptanz einheitlicher Datensicherheitsmaßnahmen auf der ganzen Welt zu vereinfachen. Dieser liefert grundlegende technische und betriebliche Anforderungen zum Schutz von Karteninhaberdaten. Der PCI-DSS gilt für alle Einrichtungen, die an der Verarbeitung von Zahlungskarten beteiligt sind – einschließlich Vertragsunternehmen, EDV-Dienstleistern, abrechnenden Stellen, Kartenemittenten und Dienstleistern – sowie anderen Stellen, die Karteninhaberdaten speichern, verarbeiten oder übertragen. Dies ist entsprechend Version 2.0 vom Oktober 2010 verbindlich. Vielen ist nicht bewusst, dass dieser Standard sie betrifft, daher möge jeder für sich prüfen, ob man vielleicht doch selbst mit Kreditkartendaten arbeitet und die Daten speichert – vielleicht auch nur als Information auf einem eingescannten Dokument.

Schutzmethoden wie Verschlüsselung, Abkürzung, Maskierung und Hashing sind kritische Bestandteile des Schutzes von Karteninhaberdaten, die es einzuhalten gilt. Neben vielen organisatorischen Anforderungen sind im Rahmen der SAPERION-Einführung folgende Punkte zu beachten:

PCI-DSS Anforderungen an eine Sicherung Kartendatenverarbeitung

+ Dokumente mit Karteninhaberdaten müssen verschlüsselt abgelegt werden.
+ Der Zugriff auf kryptographische Schlüssel muss auf einen Kreis von Schlüsselbeauftragten eingeschränkt werden und die Verteilung von und der Zugriff auf Schlüssel muss gesichert sein.
+ Es sind sichere kryptographische Schlüssel zu verwenden. SHA-1 ist ein Beispiel für einen von der Branche getesteten und akzeptierten Hashing-Algorithmus. Zu den branchenweit getesteten und akzeptierten Standards und Algorithmen für die Verschlüsselung gehören zudem AES (128 Bit und höher), TDES (Schlüssel von mindestens doppelter Länge), RSA (1024 Bit und höher), ECC (160 Bit und höher) und ElGamal (1024 Bit und höher); eine einfache Blowfish-Verschlüsselung reicht allerdings nicht aus.

[13] http://de.pcisecuritystandards.org/minisite/en/

- Die Kommunikation zwischen Client und Server muss verschlüsselt sein.
- Das Temp-Verzeichnis des Scan-Clients muss verschlüsselt werden, um einen ungeschützten Zugriff auf temporär lokal gespeicherte Daten zu vermeiden.
- Werden Daten per SFTP mit SAPERION ausgetauscht, so müssen diese in einem verschlüsselten Festplattenbereich zwischengespeichert werden.
- Es muss möglich sein, die kryptographischen Schlüssel zu wechseln. Wird ein serverseitiger Schlüssel für alle Dokumente verwendet und wird dieser gewechselt, bedeutet dies, dass alle bereits verschlüsselten Dokumente entschlüsselt und mit dem neuen Schlüssel verschlüsselt werden müssen.

Diese Anforderungen betreffen also das Gesamtsystem, in das SAPERION ECM eingebettet ist. Die Sicherheitsmaßen sind auch häufig bei Versicherungen und Banken aber auch militärischen Einrichtungen ohne Bezug auf Kreditkartendaten zu finden.

4 PRÜFUNG DER SAPERION ECM SOFTWARE

4.1 Aufgabenstellung

Prüfverfahren

Für die unterschiedlichen Anwendungsfälle gibt es entsprechende Prüfverfahren, die durch autorisierte Dritte durchgeführt werden und damit die Compliance – also die Konformität mit dem zugrundeliegenden Regelwerk – bestätigen bzw. zertifizieren. Zum Beispiel gibt es die Prüfkriterien für Dokumentenmanagementlösungen, kurz PK-DML, die vom VOI in Bezug auf die GoBS-Konformität erstellt wurden und seitens des TÜV per Audit bestätigt werden. Wichtig zu wissen ist, dass ein Teil einer solchen Lösung immer auch das Betriebshandbuch (oder die Verfahrensdokumentation) sein muss, ohne das z.B. ein Wirtschaftsprüfer seine Prüfungen gar nicht erst durchführen darf.

Verfahrensdokumentation

Das Ziel der Prüfung

Mit dem Ziel festzustellen, ob die SAPERION ECM Software bei sachgerechtem Einsatz eine den handels- und steuerrechtlichen Ordnungsmässigkeitskriterien entsprechende Verwendung ermöglicht, hat die SAPERION AG die KPMG AG Wirtschaftsprüfungsgesellschaft mit der entsprechenden Prüfung beauftragt.

Grundlegende Regularien der Prüfung

Rechtliche Grundlagen

Als Maßstab für die Beurteilung der Ordnungsmässigkeit wurden – neben anderen Regelungen – insbesondere die folgenden Gesetze und Richtlinien zu Grunde gelegt:

+ das Handels- und Steuerrecht (§§ 238 ff. HGB sowie §§ 140-148 AO)
+ die Grundsätze ordnungsgemäßer Buchführung (GoB)
+ die „Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme“ (GoBS) sowie
+ die „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen“ (GDPdU).

4.2 Einige Prüfungsanforderungen im Detail

Im Folgenden stellen wir einige ausgewählte Kriterien vor, denen eine Software-Lösung entsprechen muss, um die Prüfung der oben genannten Regularien die Prüfung zu bestehen.

Eine komplette Übersicht der einzelnen Kriterien (inkl. der jeweiligen Prüfergebnisse der KPMG AG) finden Sie im vollständigen Bericht auf der Website der KPMG AG unter dem folgenden Link:

http://www.kpmg.de/bescheinigungen/requestreport.aspx?26009

Vollständigkeit und Zeitnähe der Archivierung

Dokumente müssen möglichst früh und vor allem vollständig in das Archivsystem überführt werden, damit zum Beispiel Manipulationsmöglichkeiten ausgeschlossen werden können.

Unveränderbarkeit der Dokumente

Entgegen der naheliegenden Vermutung, dass archivierte Dokumente nicht verändert werden dürfen, ist diese Anforderung so zu verstehen, dass Änderungen an Dokumenten einerseits als solches nachvollziehbar sind und zum zweiten der ursprüngliche Zustand eines Dokuments erkennbar ist, das heißt, wieder hergestellt werden kann.

Notwendige Protokollierungen

Damit der Archivierungsprozess nachvollziehbar ist, müssen die einzelnen Bearbeitungsvorgänge an den Dokumenten protokolliert werden. Und genauso wichtig. Diese Protokolle müssen zehn Jahre aufbewahrt werden (und sind im Übrigen so zu behandeln wie „normale“ archivierte Dokumente).

Indizierung und Wiederauffindbarkeit

Hier gibt es einige Kriterien, die in direktem Zusammenhang miteinander stehen. Der Index, der zu den einzelnen Dokumenten führt, muss einen gezielten Zugriff auf die Dokumente erlauben (z.B. eine eindeutige Dokumenten-ID). Weiterhin darf er – gewährleistet durch organisatorische Maßnahmen – nicht veränderbar sein (bzw. muss als Änderung als solche erkennbar sein). Zusätzlich müssen – selbstverständlich – entsprechende Werkzeuge verfügbar sein, die die archivierten Dokumente lesbar machen.

Formatierung und Konvertierung

Für den Fall, dass seitens der Archivlösung Modifikationen am Format der abgelegten Daten durchgeführt werden, ist sicherzustellen, dass die ordnungsgemäße Wiedergabe der Daten durch diese Änderungen nicht beeinträchtigt wird. Das gleiche gilt auch für verlustbehaftete Komprimierungsmechanismen, die ebenfalls die Wiedergabe bzw. Wiederlesbarmachung der Informationen nicht einschränken dürfen.

Langfristige Lesbarkeit und Wiederherstellbarkeit

Aufbewahrungspflichtige Unterlagen müssen während der gesamten Dauer der Aufbewahrungsfrist jederzeit verfügbar sein und unverzüglich lesbar gemacht werden können. Diese Forderung ist u.a. durch regelmäßige Integrationsprüfungen durch die Archivlösung sicherzustellen, um so zum Beispiel Defekte an einzelnen Speichermedien zeitnah erkennen zu können.

Datensicherungs- und Wiederanlaufverfahren

Gemäß Handels- und Steuerrecht hat der Aufbewahrungspflichtige Maßnahmen zur Sicherung der Informationen vor Verlust und schädlichen Einwirkungen zu treffen. Dazu ist die Durchführung von Datensicherungsprozeduren erforderlich, die alle wesentlichen Datenbestände berücksichtigen. Implementierte Wiederanlaufverfahren sollen sicherstellen, dass das Datenarchiv im Katastrophenfall zeitnah wiederhergestellt werden kann.

Verfahrensdokumentation

Nach den GoBS müssen aus der Verfahrensdokumentation Inhalt, Aufbau und Ablauf des Verfahrens vollständig ersichtlich sein. Die Verfahrensdokumentation umfasst daher die drei Teile Systemdokumentation, Betriebsdokumentation und Anwenderdokumentation.

In der Verfahrensdokumentation sind insbesondere die folgenden Teile mit aufzunehmen:

- die Beschreibung der sachlogischen Lösung („was“ macht die Lösung überhaupt),
- die Beschreibung der programmtechnischen Lösung („wie“ ist die Lösung implementiert),
- eine Beschreibung, wie die Programmidentität gewahrt wird,
- eine Beschreibung, wie die Integrität von Daten gewahrt wird sowie
- Arbeitsanweisungen für den Anwender.

Neben der inhaltlichen Korrektheit der Verfahrensbeschreibung muss die Dokumentation für einen sachverständigen Dritten verständlich sein. Weiterhin ist sie bei Bedarf regelmäßig zu aktualisieren.

Zusätzlich – obwohl offensichtlich, wird diese Anforderung oft übersehen – unterliegt die Verfahrensdokumentation den gleichen Aufbewahrungspflichten wie die durch das beschriebene Verfahren erfassten, entstandenen oder bearbeiteten buchhaltungspflichtigen Unterlagen.

4.3 Das Ergebnis der Prüfung

Die KPMG AG kommt auf Grund der durchgeführten Prüfungen zu dem Ergebnis, dass die SAPERION ECM Lösung „bei sachgerechter Anwendung eine den deutschen Grundsätzen ordnungsgemäßer Buchführung entsprechende Speicherung und Abfrage von elektronischen Dokumenten ermöglicht".

Der komplette Bericht

Den vollständigen Bericht der KPMG AG inklusive der einzelnen Anforderungen und Prüfungsergebnisse finden Sie auf der Website der KPMG AG unter dem folgenden Link:

http://www.kpmg.de/bescheinigungen/requestreport.aspx?26009

Wie weiter oben bereits erwähnt, bedeutet das aber noch nicht, dass das Unternehmen, das eine SAPERION ECM Lösung einsetzt, automatisch den zugrunde liegenden Regularien gerecht wird. Neben der grundsätzlichen Fähigkeit einer Software-Lösung, den Anforderungen gerecht werden zu können (was der SAPERION ECM Software durch die KPMG Prüfung attestiert wird), sind auch immer auf organisatorischer Seite entsprechende Maßnahmen umzusetzen.

Organisatorische Massnahmen sind mit entscheidend

Dementsprechend weist die KPMG AG ergänzend und klarstellend darauf hin, dass eine „sachgerechte Anwendung der Software" insbesondere die folgenden Maßnahmen beinhalten sollte:

+ Eine zeitnahe Speicherung der zu archivierenden Dokumente auf den endgültigen Archivmedien muss sichergestellt werden.
+ Durch technische und organisatorische Maßnahmen ist sicherzustellen, dass die Dokumente unveränderbar auf dem Archivmedium gesichert sind.
+ Die Indexinformationen sind so einzurichten, dass eine eindeutige Wiederauffindbarkeit gewährleistet ist.
+ Selbstverständlich müssen die Berechtigungen für Administratoren und Benutzer sachgerecht vergeben werden.

Erst wenn beide Bereiche – nämlich die technische Fähigkeit einer ECM Software sowie die individuellen, organisatorischen Maßnahme in einer ganz konkreten Anwendung, u.a. das Vorhandensein einer Verfahrensdokumentation – gegeben sind, ist das Unternehmen bzw. das Szenario, das mit der jeweiligen Anwendung abgedeckt wird, „compliant".

5 ZUSAMMENFASSUNG

Compliance ist ein vielschichtiges Thema, selbst wenn es nur im begrenzten Feld des Schriftguts betrachtet wird. Im Kern geht es um die Vorsorgen, die verantwortende Organisation vor Schäden zu schützen und so für das Überleben zu sorgen. Ein wichtiger Aspekt ist dabei immer die Verhältnismäßigkeit. Es ist jeweils abzuwägen, wie hoch ein Risiko, aber viel mehr wie hoch ein resultierender Schaden bei Eintritt und wie hoch die Wahrscheinlichkeit ist. Sind letztere gering, aber der Aufwand des Schutzes hoch, so könnte das Risiko eingegangen werden und kein Schutz implementiert werden. Bei dieser Betrachtung sollte aber auch der Schaden im Ansehen berücksichtigt werden. Denn hier geht es immer um das Vertrauen, das ein Geschäftspartner berücksichtigen wird.

Ein weiterer wichtiger Aspekt ist, dass der Einsatz einer Software-Lösung allein noch nicht für Compliance sorgen kann. Es gilt immer, dass der Gesamtkontext, in dem die Software betrieben wird, auf die Einhaltung aller zugrundeliegenden Regularien hin überprüft wird. Damit ist auch offensichtlich, dass neben der grundsätzlichen Fähigkeit einer Softwarelösung, den Anforderungen gerecht zu werden, immer auch begleitende organisatorische Massnahmen umzusetzen – und im Rahmen einer Verfahrensdokumentation sauber zu dokumentieren – sind.

Last but not least bleibt anzumerken, dass die Einhaltung von Compliance-Anforderungen natürlich einen entsprechenden Aufwand bedeutet: Zeit für die Umsetzung, finanzielle Investitionen für Hardware, Software und Implementierung und natürlich eine entsprechenden „Durchhalte-Disziplin“.

Allerdings sollte nicht der Fehler gemacht werden und die Einhaltung von Compliance nur als „notwendiges Übel“ betrachtet werden, das vor allem „viel Zeit und Geld kostet“.

Das Gegenteil ist richtig: Die Einhaltung von Compliance-Regeln ist eine grundlegende Voraussetzung für die vertrauensvolle Zusammenarbeit mit Kunden und Lieferanten. Langfristig kann keine Organisation darauf verzichten. Zusätzlich stellt die Umsetzung der Compliance-Richtlinien durchaus auch eine große Chance für Unternehmen dar – interne Prozesse zu kennen, zu dokumentieren, gegebenenfalls zu verbessern und vor allem transparent zu machen. Dies ist mit Sicherheit nicht das Schlechteste, das einem Unternehmen dabei hilft, erfolgreich zu sein, zu bleiben oder zu werden.

Die Angaben in dieser Publikation werden von der SAPERION AG und ihren Konzernunternehmen (zusammen „SAPERION“) bereitgestellt.

Der Inhalt dieser Publikation einschließlich aller Abbildungen, Tabellen und Zeichnungen ist geistiges Eigentum von SAPERION. Alle Rechte vorbehalten. Es ist nicht gestattet, Urheberrechtsvermerke oder Marken zu verändern oder zu entfernen. Weitergabe und Vervielfältigung dieser Publikation oder von Teilen daraus sind, zu welchem Zweck und in welcher Form auch immer, ohne die ausdrückliche schriftliche Genehmigung von SAPERION nicht gestattet.

Alle in dieser Publikation verwendeten Geräte- und Programmnamen bzw. Services von SAPERION sowie die entsprechenden Logos sind Marken oder eingetragene Marken von SAPERION in Deutschland und anderen Ländern weltweit. Einige von SAPERION vertriebenen Software- und/oder Hardwareprodukte können Komponenten umfassen, die Eigentum anderer Hersteller sind. Namen solcher Produkte und Services sowie die damit verbundenen Firmenlogos sind Marken der jeweiligen Unternehmen.

In dieser Publikation enthaltene Informationen können ohne vorherige Ankündigung geändert werden. Die Angaben im Text sind unverbindlich und dienen lediglich zu Informationszwecken. Diese Publikation enthält u. U. bestimmte vorgesehene Strategien, Entwicklungen und Funktionen und ist für SAPERION nicht bindend, eine bestimmte Produktstrategie bzw. -entwicklung einzuschlagen. SAPERION übernimmt keine Verantwortung für Fehler oder Auslassungen in dieser Publikation. SAPERION garantiert nicht die Richtigkeit oder Vollständigkeit der Informationen, Texte, Grafiken, Links oder anderer in dieser Publikation enthaltenen Elemente. Diese Publikation wird ohne jegliche Gewähr, weder ausdrücklich noch stillschweigend, bereitgestellt. Dies gilt u.a., aber nicht ausschließlich, hinsichtlich der Gewährleistung der Marktgängigkeit und der Eignung für einen bestimmten Zweck sowie für die Gewährleistung der Nichtverletzung geltenden Rechts.

SAPERION übernimmt keinerlei Haftung oder Garantie für Schäden jeglicher Art, einschließlich und ohne Einschränkung für direkte, spezielle, indirekte oder Folgeschäden im Zusammenhang mit der Verwendung dieser Publikation. Diese Einschränkung gilt nicht bei Vorsatz oder grober Fahrlässigkeit. Die gesetzliche Haftung bei Personenschäden oder die Produkthaftung bleibt unberührt. Die Informationen, auf die möglicherweise in dieser Publikation über wiedergegebene Links verwiesen wird, unterliegen nicht dem Einfluss von SAPERION, und SAPERION gibt keinerlei Gewährleistungen oder Zusagen über Internetseiten Dritter ab.

SAPERION ist ein Hersteller für Enterprise Content Management und Business Process Management Software.

Oder einfacher: wir stellen Software her, die Ihnen hilft Geld zu sparen, indem Sie Ihre papiergebundenen Vorgänge digitalisieren und damit beschleunigen. Gleichzeitig sorgt unsere Software dafür, dass Ihre Dokumente langfristig und rechtssicher archiviert werden.

Haben wir Ihr Interesse geweckt?

Weitere Informationen finden Sie auf unserer Webseite http://www.saperion.com
Außerdem für Sie verfügbar:

Diesen Code mit dem Mobiltelefon scannen

Compliance einfach geregelt – der Film »

http://www.saperion.com/einfach



Diesen Code mit dem Mobiltelefon scannen

Weitere Informationen zu SAPERION finden Sie unter:

http://www.saperion.com/allgemein/aktuelles/pressemitteilungen/

Diesen Code mit dem Mobiltelefon scannen

Weitere Informationen zu Compliance finden Sie unter:

http://www.saperion.com/unternehmensloesungen/compliance/ueberblick/

Diesen Code mit dem Mobiltelefon scannen

Beiträge zu Compliance in unserem SAPERION Blog finden Sie unter:

http://www.saperionblog.com/tag/compliance/

KONTAKT

SAPERION AG
Steinplatz 2
D-10623 Berlin

Fon: +49 (0)30 600 61-0
Mail: info@saperion.com
www.saperion.com