Compliance Storage Guide

Revisionssichere Archivierung mit «Kendox InfoShare»

Datum	16.09.2019
Version	1.3

Inhaltsverzeichnis

1 Einführung

1.1 Was ist Compliance?

«Compliance» (engl. für Befolgung, Einhaltung, Erfüllung, Konformität u.a.) in dem Sinne, wie es in diesem Dokument verstandenen wird, beschreibt in der Unternehmensführung die **Einhaltung der gesetzlichen, unternehmensinternen und vertraglichen Regelungen** sowie die Dokumentation deren Befolgung im Bereich der IT-Systeme und Anwendungen.

Zu den Compliance-Anforderungen in der Informationstechnologie gehören hauptsächlich Informationssicherheit, Verfügbarkeit, Datenaufbewahrung und Datenschutz.

Unternehmen unterliegen zahlreichen rechtlichen Verpflichtungen, deren Nichteinhaltung zu hohen Geldstrafen und Haftungsverpflichtungen führen kann. EU-Richtlinien, internationale Konventionen, unternehmensinterne Vorgaben und Handelsbräuche fügen weitere Regeln hinzu.

Die Disziplin, diesen Anforderungen zu entsprechen, wird gemeinhin generisch als «Compliance» oder – präziser – als **«Governance, Risk & Compliance (GRC)»** bezeichnet und fasst die drei wichtigsten Handlungsebenen eines Unternehmens für dessen erfolgreiche Führung zusammen: [1]

- Unternehmensführung durch definierte Richtlinien
- Risikomanagement durch definierte Risikoanalysen
- Einhalten interner wie externer Normen für die Bereitstellung und die Verarbeitung von Informationen

1.2 Compliance Storage

Geht es um die langfristige, sichere und integre Speicherung von Daten oder elektronischen Dokumenten auf Datenträgern aller Art, spricht man von **«Compliance Storage»**. Dabei steht der Aspekt der Absicherung der geforderten Eigenschaften durch das Speichersystem resp. dessen Verwaltungs-Software im Vordergrund. Im Weiteren fokussiert der Begriff «Compliance Storage» auf die **unveränderbare Speicherung im Rahmen einer vorgegebenen Aufbewahrungsfrist** im Sinne der elektronischen Archivierung.

Ein weiteres, wesentliches Merkmal von «Compliance Storage Systemen» ist eine Möglichkeit, die **Integrität der gespeicherten Daten** zu überprüfen (also vor allem zu Datenfehler erkennen). Zusätzlich muss die Migration (die Übertragung der Daten und Dokumente auf ein anderes System, andere Datenträger oder eine geänderte Datenorganisation) der gespeicherten Daten unter Aufrechterhaltung der Datenintegrität möglich sein (es muss vor allem die Vollständigkeit und Richtigkeit der Daten sowie deren Verfügbarkeit und Lesbarkeit sichergestellt sein). Dabei hängt der Grad, zu dem dies gewährleistet werden kann, natürlich von den Möglichkeiten der konkret eingesetzten Hardware- und Softwaresysteme ab.

Im Gegensatz zu «Compliance Storage» sind ungesicherte Verfahren zur Speicherung von Daten oder elektronischen Dokumenten (zum Beispiel auf einem herkömmlichen Dateisystem) zu verstehen. Dabei wird weder die Integrität (Unversehrtheit) der gespeicherten Dokumente noch deren Verfügbarkeit (Lesbarkeit) durch systematische Vorkehrungen sichergestellt. Der Beweiswert (vor Gericht) von derart «non-compliant» gespeicherten elektronischen Dokumenten ist dementsprechend gering.

[1] https://de.wikipedia.org/wiki/Governance,_Risk_%26_Compliance, abgerufen am 27. Februar 2019

1.3 Revisionssicherheit

«Revisionssicherheit» (engl. «Auditing Acceptability») ist ein von den Herstellern von elektronischen Archivsystemen eingeführter Begriff (und somit ein Kunstwort), der inzwischen breite Verwendung findet. Der Begriff bezieht sich auf die Archivierung elektronischer Dokumente unter Einhaltung der relevanten gesetzlichen Anforderungen (**gesetzeskonforme Aufbewahrung**) und zugleich von unternehmensinternen Vorgaben oder auch branchenspezifischen sowie spezialgesetzlichen Normen. Der Begriff orientiert sich am Verständnis der Revision aus wirtschaftlicher Sicht und betrifft **aufbewahrungspflichtige und aufbewahrungswürdige Informationen und Dokumente.**

Revisionssicherheit im Zusammenhang mit der elektronischen Archivierung bezieht sich dabei nicht nur auf technische Komponenten, sondern auf die gesamte Lösung und insofern auch auf die damit in Verbindung stehenden Verfahren und Abläufe. In diesem Sinn schließt die Revisionssicherheit demzufolge auch sichere Abläufe, die Organisation des Anwenderunternehmens, die ordnungsgemäße Nutzung, den sicheren Betrieb und den Nachweis in einer Verfahrensdokumentation mit ein.

Das wesentliche Merkmal revisionssicherer Archivsysteme ist aber selbstverständlich, dass die darin enthaltenen Informationen wieder auffindbar, nachvollziehbar, unveränderbar und verfälschungssicher archiviert sind.

1.4 Gesetzeskonforme Aufbewahrung

Die Sicherstellung der gesetzeskonformen Aufbewahrung von Geschäftsdokumenten umfasst im Wesentlichen die folgenden Aufgabenstellungen:

- **Aufbewahrungspflichtige elektronische Dokumente speichern**
  - Aufbewahrung bis zum Ablauf der gesetzlichen Aufbewahrungsfrist
  - Inhaltsgleiche, vollständige und geordnete Wiedergabe
- **Integrität der elektronisch gespeicherten Dokumente durch geeignete technische und organisatorische Verfahren sicherstellen (Unversehrtheit der Information)**
  - Hashwerte, Signaturen
  - Verschlüsselung, spezifische Datenorganisation
  - Kontrollfunktionen und Protokollierung
- **Verfügbarkeit der elektronisch archivierten Dokumente durch technische und organisatorische Verfahren aufrechterhalten (Lesbarkeit der Information)**
  - Lesbarkeit – technische Prozesse und menschliche Interpretation
  - Schutz gegen Veränderung oder Verfälschung
  - Schutz gegen Löschung vor Ende der Aufbewahrungsfrist
- **Beweiswert der Dokumente durch technische und organisatorische Maßnahmen erhalten**
  - Summe der getroffenen technischen und organisatorischen Maßnahmen
  - Dokumentation und Auditierung des Systems und der Verfahren

1.5 Zielsetzung revisionssicherer Archivierung

Revisionssichere, den rechtlichen Anforderungen an die Aufbewahrung von Geschäftsunterlagen entsprechende elektronische Archivsysteme müssen somit

- **den gesetzlichen Anforderungen bei der Aufbewahrungspflicht entsprechen,**
- **Spezialgesetze, Normen, Branchenanforderungen berücksichtigen und**
- **unternehmensinterne Vorgaben und Erfordernisse umsetzen.**

Dokumente müssen dabei **wieder auffindbar** sein; Archivierungsabläufe und –zeitpunkte müssen **nachvollziehbar bzw. nachweisbar** sein und die Datenspeicherung muss **unveränderbar sowie verfälschungssicher** erfolgen.

Dementsprechend lassen sich die folgenden allgemeinen Zielsetzungen für Systeme und Prozesse im Rahmen der Nutzung von «Compliance Storage» festlegen:

- Es wird der Nachweis geführt, **wie das für die elektronische Archivierung eingesetzte technische System als Gesamtes den Anforderungen der einschlägigen gesetzlichen Vorgaben** (insbesondere dem Steuerrecht) entspricht und dies schlüssig dokumentiert. Insbesondere gilt dies für den Bereich der langfristigen Speicherung von elektronischen Rechnungen.
- Es wird sichergestellt, dass die **internen Vorgaben, Verfahren und Einrichtungen des anwendenden Unternehmens nachvollziehbar und nachweislich geeignet** sind, einen sicheren Betrieb und eine geordnete Verwaltung der technischen Systeme zu gewährleisten.
- Zusätzlich wird aufgezeigt, welche **einmaligen Maßnahmen und Prozeduren** allenfalls noch auszuführen sind, um die geforderten Eigenschaften der Gesamtlösung herzustellen und langfristig zu gewährleisten.

2 Relevante Rechtsnormen und Vorgaben

Nachfolgend werden unmittelbar relevante Rechtsnormen und regulatorische Vorgaben in Deutschland, Österreich und der Schweiz angeführt, um in Folge für die Definition von Anforderungen an die gesetzeskonforme Aufbewahrung und die revisionssichere Archivierung als Grundlage zu dienen. Es ist dabei nicht die Intention dieses Dokumentes, alle einschlägigen Rechtsnormen zu diskutieren.

Es wird in diesem Zusammenhang auch auf das durch die VOI Service GmbH ausgestellte Zertifikat hingewiesen, das dem Softwareprodukt «Kendox InfoShare» bescheinigt, gemäß VOI-CERT-Regularien die Anforderungen nach dem Prüfverfahren «PK-DML ready» zu erfüllen und ein revisionssicheres Compliance-Management digitaler Dokumente zu ermöglichen.

2.1 Auswahl relevanter Rechtsgrundlagen

Die im Folgenden genannten gesetzlichen Vorgaben wurden im Zuge der Erstellung dieses Dokumentes detaillierter in Hinblick auf deren Relevanz für die elektronische Dokumentenarchivierung betrachtet:

Deutschland

Grundlage bilden das Handelsgesetzbuch (HGB) sowie die Abgabenordnung (AO), in denen die Anforderungen an die handelsrechtliche und steuerrechtliche Buchführungspflicht formuliert sind:

- HGB §238 Buchführungspflicht
- HGB §239 Führung der Handelsbücher
- HGB §257 Aufbewahrung von Unterlagen und Aufbewahrungsfristen
- AO 1977 §146 Ordnungsvorschriften für die Buchführung und für Aufzeichnungen
- AO 1977 §147 Ordnungsvorschriften für die Aufbewahrung von Unterlagen
- GoBD 14.11.14 (gültig ab 1.1.15)

Die darin enthaltenen Anforderungen sind beim Einsatz von IT-Systemen formuliert in

- den «Grundsätzen ordnungsgemäßer DV-gestützter Buchführungssysteme (GoBS)»,
- den «Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU» und
- den «Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)» (gültig ab 1.1.2015)

Das Bundesministerium der Finanzen, Berlin (BMF) hat hierzu in der Vergangenheit entsprechende Begleitschreiben beigefügt:

- GoBS, Anlage zum BMF-Schreiben vom 7.11.1995, IV A 8 – S 0316 – 52/95, BStBl I 1995, 738
- GDPdU, BMF-Schreiben vom 16.7.2011, IV D 2 – S 0316 – 136/01, BStBl I 2001, 415 geändert durch BMF-Schreiben vom 14.9.202, IV A 4 – S 0316/12/10001, BStBl I 2012, 90

Mit dem BMF-Schreiben vom 14.11.2014 wurden nunmehr neu die sogenannten «Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)» durch das Bundesministerium für Finanzen, Berlin, veröffentlicht.

> GoBD, BMF-Schreiben vom 14.11.2014, GZ: IV A 4 – S 0316/13/10003, DOK: 2014/0353090

Dieses BMF-Schreiben gilt für Veranlagungszeiträume, die nach dem 31.12.2014 beginnen. Es tritt an die Stelle der in diesem Dokument weiter oben erwähnten BMF-Schreiben vom 7.11.1995 und vom 16.7.2001 (und der geänderten Fassung vom 14.9.2012).

Österreich

> Die Bundesabgabenordnung (BAO), insbesondere §§ 131 und 132
> Das Unternehmensgesetzbuch (UGB), §§ 190 und 216
> Das GmbH-Gesetz
> Das Umsatzsteuergesetz (UStG) §§ 11 und 18
> Die 516. Verordnung (e-Rechnungsverordnung), (UStR 2000), Ziffer 11.2.4
> Die Grundsätze ordnungsmäßiger Buchführung (GoB)
> Das Fachgutachten «Die Ordnungsmäßigkeit von EDV-Buchführungen» (KFS/DV1)

Schweiz

> Das schweizerische Obligationenrecht (OR, Artikel 957ff.) über Buchführung, Aufbewahrung und Edition
> Die Verordnung über die Führung und Aufbewahrung der Geschäftsbücher (GeBüV)
> Die «Richtlinien für die Ordnungsmäßigkeit des Rechnungswesens unter steuerlichen Gesichtspunkten sowie über die Aufzeichnung von Geschäftsunterlagen auf Bild- oder Datenträger und deren Aufbewahrung» der eidgenössischen Steuerverwaltung (EStV)
> Das Mehrwertsteuergesetz (MWSTG) sowie die Mehrwertsteuerverordnung (MWSTV) in Verbindung mit der Verordnung des Eidg. Finanzdepartements über elektronisch übermittelte Daten und Informationen (EIDI-V)
> Die Richtlinien der Treuhand Kammer bezüglich der Grundsätze ordnungsmäßiger Buchführung (Revisionshandbuch der Schweiz)
> Das Datenschutzgesetz [DSG] (im Falle der Speicherung personenbezogener Daten)
> Die Datenschutzverordnung (VDSG)

2.2 Datenschutz-Grundverordnung (DS-GVO)

Als gemeinsamer Datenschutzrahmen in der Europäischen Union hat auch die am 25. Mai 2018 in Kraft getretene Datenschutz-Grundverordnung (DS-GVO) eine entsprechende Relevanz für die elektronische Dokumentenarchivierung. Dort werden die Rahmenanforderungen sowohl in Bezug auf die Wahrung der sog. «Betroffenenrechte» (u.a. Auskunftsrecht und Recht auf Löschung bzw. Berichtigung) als auch in Bezug auf die «Verarbeitungssicherheit» beschrieben.

Während sich die «Betroffenenrechte» weitestgehend durch eine anwendungsspezifische Konfiguration der ECM/DMS-Lösung (insbesondere durch Metadaten-Konfiguration und entsprechende Berechtigungskonzepte) sicherstellen lassen, bezieht sich die «Verarbeitungssicherheit» vor allem auf den Betrieb einer ECM/DMS Lösung und dort auf Aspekte wie Belastbarkeit und Verfügbarkeit der ECM/DMS-Lösung, Vertraulichkeit und Integrität der dort verarbeiteten Daten, Wiederherstellbarkeit des Systems inkl. der gespeicherten Daten und Dokumente im Falle eines Teil- oder Totalausfalls etc. Zudem ist explizit auch ein Verfahren gefordert, mit dem regelmässig die sog. «Technischen und Organisatorischen Massnahmen» (kurz: «TOM»), die zur Gewährleistung der Sicherheit der Verarbeitung implementiert sind, zu überprüfen, zu bewerten und deren Wirksamkeit zu evaluieren.

Datenschutzgesetz Schweiz

Im Übrigen müssen sich auch Schweizer Unternehmen an die DS-GVO halten, sofern sie personenbezogene Daten von natürlichen Personen verarbeiten, die sich in der EU befinden, und falls die Verarbeitung beispielsweise dazu dient, diesen Personen Waren oder Dienstleistungen anzubieten. Zudem hat der Bundesrat (der Schweiz) im September 2017 seinen Entwurf für ein totalrevidiertes «Datenschutzgesetz Schweiz» (kurz E-DSG) präsentiert, der sich sehr stark an die DS-GVO anlehnt.

2.3 Feststellungen

Selbstverständlich ist nach den gesetzlichen Vorgaben in Deutschland, Österreich als auch in der Schweiz die elektronische Archivierung von aufbewahrungspflichtigen Unterlagen möglich. Allerdings sind jeweils Anforderungen an die verwendeten Systeme und Verfahren definiert, die entsprechend eingehalten werden müssen. Nachstehend werden stichwortartig wesentliche Erkenntnisse für die praktische Anwendung von elektronischen Archivsystemen zusammengefasst.

Aufbewahrungsfrist

Die archivierten, aufbewahrungspflichtigen Unterlagen müssen bis zum Ablauf der gesetzlichen Aufbewahrungsfrist aufbewahrt werden und dürfen während dieses Zeitraums nicht gelöscht oder verändert werden; es sei denn, es besteht eine Verpflichtung zur vorzeitigen Löschung (z.B. Gerichtsentscheid). In diesem Fall ist die Löschung kontrolliert nach den jeweiligen Vorgaben vorzunehmen.

Integrität und Verfügbarkeit

Wesentliche Anforderungen betreffen die regelmäßige, automatisierte Integritätsprüfung durch das System über die gesamte Aufbewahrungszeit hinweg (sind die gespeicherten Informationen unversehrt und unverändert und entsprechen sie den ursprünglich gespeicherten Daten) sowie die Verfügbarkeit der Dokumente (können die gespeicherten Informationen vom Datenträger innerhalb eines angemessenen Zeitraums übertragen und inhaltsgleich, vollständig und geordnet wiedergegeben werden). Darüber hinaus muss es möglich sein, dass einzelne, entsprechend berechtigte Nutzer des Systems eine ad-hoc Überprüfung der Integrität der Daten und Dokumente durchführen können.

Elektronisch erzeugte Dokumente

Eine Pflicht zur Aufbewahrung in elektronischer Form kann dann angenommen werden, wenn «aufzeichnungs- und aufbewahrungspflichtige Daten, Datensätze, elektronische Dokumente und elektronische Unterlagen im Unternehmen entstanden oder dort eingegangen sind». [2]

Hardware- vs. Software-Verfahren

Die Art der einzusetzenden Hardware- und Software-Systeme wird in den gesetzlichen Vorgaben nicht explizit vorgegeben; es werden vielmehr qualitative Anforderungen definiert, wie nachfolgend exemplarisch aufgezeigt:

> *«Die Sicherstellung der Unveränderbarkeit [der gespeicherten Rechnungen] kann auch durch das Zusammenwirken von systemtechnischen und organisatorischen Maßnahmen gewährleistet werden. Dies erfordert jedoch das Vorliegen eines revisionssicher eingerichteten Archivs (Zusammenwirken von Hardware, Software und Systemadministration), das bereits herstellerseitig keine Eingriffe des Unternehmers bezüglich der Unveränderbarkeit und Unlöschbarkeit der Daten zulässt.»* [3]

Damit sind also Software-definierte Compliance-Storage-Systeme zulässig.

Dokumentation und Protokollierung

Die Führung einer entsprechenden Dokumentation über die eingesetzten Verfahren und Systeme ist hinsichtlich der Rechtsentsprechung des Gesamtsystems relevant (Verfahrensdokumentation). Darüber hinaus sind technische Einrichtungen zu beschreiben und Vorgänge, die Einfluss auf die Konfiguration des Systems, auf die Integrität und die Verfügbarkeit von archivierten Dokumenten haben, in geeigneter Form zu protokollieren.

[2] vgl. BMF-Schreiben vom 14.11.14 zu GoBD, Rz 119; Deutschland

[3] vgl. UStR 2000, Ziff. 11.2.4.1, Rz 1566; Österreich

3 Anforderungen & Maßnahmen

3.1 Primäre Anforderungen

Primäres Erfordernis ist es, den allgemeinen rechtlichen Vorgaben zu entsprechen und die spezifischen Anforderungen an die die elektronische Archivierung von elektronischen Rechnungen und anderen steuerrechtlich relevanten Dokumenten rechtskonform und revisionssicher zu implementieren. [4]

Insbesondere den nachfolgend angeführten Anforderungen muss das elektronische Archivsystem entsprechen:

- **Unversehrtheit des Inhalts: «Integrität»**
  Unversehrtheit, Unveränderbarkeit, Unlöschbarkeit bereits herstellerseitig absichern
- **Lesbarkeit und Wiedergabe: «Verfügbarkeit»**
  Wiederauffinden, Wiederherstellung, inhaltsgleiche, vollständige, geordnete Wiedergabe

3.2 Technische und organisatorische Maßnahmen

Die Unveränderlichkeit von Dokumenten muss mit Hilfe von technischen und organisatorischen Maßnahmen sichergestellt werden («Zusammenwirken von Hardware-, Software- und Systemadministration»). Der Einsatz eines Hardware-Speichersystems, das auf dem Prinzip «einmal beschreibbares Medium» (sog. WORM – «write once, read multiple») oder «firmware-basierender Löschschutz» basiert, schützt dabei a priori noch nicht vor Verfälschungen. [5]

Deshalb muss davon ausgegangen werden, dass in jedem Fall – und zwar unabhängig vom gewählten Compliance Storage System (also auch unabhängig von der Frage, ob es sich um eine reine Hardware-Lösung oder eine Kombination aus geeigneter Hardware und Software handelt) – organisatorische Vorgaben und Regelungen erforderlich sind,

- um den Zugang zum System sowohl physisch (Räumlichkeiten) als auch logisch bzw. system-technisch (Berechtigungen) einzuschränken und zu überwachen,
- die Datensicherung vorzunehmen und zu kontrollieren sowie
- die Wiederherstellung periodisch zu testen.

Auch der Archivierungsprozess selbst muss überwacht werden. Präzisierende Angaben hierzu sind individuell vom bzw. für das anwendenden Unternehmen zu erstellen.

[4] Die aus den einschlägigen Rechtsvorgaben ableitbare Anforderung der Prüfung der «Echtheit der Herkunft» (z.B. von Rechnungen) wird nicht primär mit den Mitteln des elektronischen Archivsystems sichergestellt; dies ist eine Aufgabe der vorgelagerten Fachverfahren (Fachanwendungen), welche die elektronischen Rechnungen generieren.

[5] Beispielsweise durch Datenfehler (Bitfehler), Manipulation von Speicheradressen oder Einträgen in Datenbanken, mit denen der Verweis auf die ursprünglichen Datenelemente (Dokumentendatei, Container-Datei usw.) abgeändert werden könnte.

4 Elektronische Archivierung mit «Kendox InfoShare»

«Kendox InfoShare» ist eine Softwarelösung zur Dokumentenverwaltung, die die Erfassung, Verwaltung, Verteilung und Bereitstellung einer sehr großen Anzahl von elektronischen Dokumenten und anderen Informationen wie z.B. digitalen Akten und Vorgänge sowie strukturierten Datensätzen ermöglicht.

Der **«Kendox InfoShare Server»** benutzt eine **Datenbank**, um Informationen zu elektronischen Dokumenten zu verwalten (Metadaten und Volltext). Die Speicherung von Metadaten in der Datenbank erfolgt nach einem internen (sog. «objekt-relationalen») Verfahren, welches zu einer sehr reduzierten Sicht auf die Daten in der Datenbank führt. Auch für technisches Personal wie beispielsweise Datenbankadministratoren ist es mit üblichen Systemmitteln nahezu unmöglich, Dateninhalte unbefugt zu sichten. Ist die empfohlene Komprimierung (Datenbankkomprimierung) eingeschaltet, ist der «natürliche Sichtschutz» noch größer. Nur die zur Indizierung benutzten Feldinhalte können mit regulären Datenbankmitteln sichtbar gemacht werden.

Wird die **Volltextsuche bzw. –indizierung** eingesetzt, ist zu beachten, dass der gesamte Text eines Dokumentes im Index des Datenbanksystems gespeichert werden muss, was die Sichtbarkeit der Dateninhalte wiederum vergrössert.

In Abhängigkeit der konkreten Implementierung werden die Datenbanken selbst mit Standard-Systemmitteln (Backup-Software) gesichert oder auf verschiedene Standorte repliziert. [6]

Die eigentlichen Dokumenteninhalte (Dokumentendateien) werden auf eines der vom «Kendox InfoShare Server» unterstützten **Speichersysteme** übertragen. «Kendox InfoShare» unterstützt aktuell verschiedene Speichersysteme über unterschiedliche Einbindungsverfahren, angefangen bei einer einfachen Ablage auf Dateisystemen bis hin zu speziellen, von den Speichersystemen bereitgestellten Schnittstellen. Dabei werden die unterschiedlichen, vom jeweiligen Speichersystem zur Verfügung gestellten **«Compliance Storages Features»** genutzt.

Das Schreiben der Datenbanksätze und der Dokumentdaten auf das oder die jeweiligen Speichersysteme erfolgt jeweils unter **Transaktionskontrolle**, wodurch die Datenkonsistenz sichergestellt wird. Die größtmögliche Inkonsistenz wäre das Vorhandensein von Dokumentdaten auf den Speichersystemen während die dazugehörigen Datenbankeinträge fehlen (also quasi ein «orphan object»).

Dokumente werden durch den «Kendox InfoShare Server» von «Kendox InfoShare Clients» [7] zur Ablage entgegengenommen und direkt von der Client-Anwendung zum Zeitpunkt der Ablage mit einer **Prüfsumme** (Hashwert) versehen, die in der Datenbank gespeichert wird. Manipulationen eines derart gespeicherten Hashwertes sind aufgrund der Datenorganisation (vgl. dazu «objekt-relationale Speicherung») sehr schwer und – wenn überhaupt – nur von Spezialisten durchführbar.

Jedem Dokument kann in «Kendox InfoShare» ein sog. **Lebenszyklus-Status** manuell oder automatisiert zugeordnet werden. In der Lebenszyklus-Definition wird unter anderem auch die Aufbewahrungsfrist festgehalten. Der Lebenszyklus-Status wird mit dem jeweiligen Dokumenten-Objekt in der Datenbank gespeichert; eine spätere Änderung der Einstellungen der Lebenszyklus-Definition hat keine Auswirkung auf bereits mit dieser Lebenszyklus-Definition gespeicherten Dokumente.

«Kendox InfoShare» speichert **Versions- und Änderungs-Logs** (sowie wahlweise einen Zugriffs-Log) pro Dokument in der Datenbank. Die Log-Funktion (Versions- und Änderungs-Log) kann nicht deaktiviert werden. Die Log-

[6] Das Anwenderunternehmen bzw. der Anbieter der Cloud-Lösung kann bzw. muss hier seine eigene Datensicherungsstrategie umsetzen.

[7] «Kendox InfoShare Clients» können auf unterschiedliche Technologien bzw. Plattformen implementiert sein: «InfoShare Windows Client» (InfoShare Client-Side Business Objects), «InfoShare Web Client» (RIA Client bzw. HTML5-Client, Implementierung über Web Services bzw. WCF)

Ansicht (pro Dokument) ist immer verfügbar, es sind jedoch allenfalls die Basisdaten (die Informationen zu Vorversionen) nicht verfügbar. [8]

Zusätzlich erlaubt das Modul «Kendox InfoShare Advanced Auditing» eine weitergehende, umfassend **Protokollierung von Systemaktivitäten**, bei der auch administrativen Änderungen (insb. Konfigurationsänderungen), Benutzeraktionen (u.a. gescheiterte Anmeldeversuche) und Dokumentenaktionen (u.a. auch das Anzeigen und Exportieren von Dokumenten) mit detailliert protokolliert werden.

Darüber hinaus generiert der «Kendox InfoShare Server» eine **zentrale Server-Log-Datei**, die durch geeignete Batch-Funktionen regelmäßig (beispielsweise täglich) gesichert und wahlweise wiederum in «Kendox InfoShare» archiviert werden kann. Diese Log-Datei wird vom «Kendox InfoShare Server» während des Betriebs immer wieder mit Schreibrechten (exklusiv) geöffnet und geschlossen. In der Log-Datei des «Kendox InfoShare Servers» werden primär formale Meldungen des Servers (Start, Stopp) sowie allfällige Fehlermeldungen protokolliert.

Zusätzlich werden auch alle **An- und Abmeldevorgänge mit dem administrativen Benutzer** «DCIAdmin» («Kendox InfoShare» Systemadministrator) zwingend und unabhängig von anderen Konfigurationseinstellungen in die Log-Datei geschrieben. Wahlweise können auch beim An- und Abmelden anderer Benutzer Log-Einträge geschrieben werden.

Ergänzend kann «Kendox InfoShare» eine sog. **Statistik-Datenbank** beschreiben, in der die Erstellungs-, Änderungs-, Lösch- und Anzeigevorgänge an Dokumenten inkl. der jeweiligen Metadaten festgehalten werden. Dabei wird durch Konfiguration festgelegt, welche Operationen bzw. «Event Types» (Create, Update, Delete, View) protokolliert werden sollen. [9]

Obligatorische Prüfsummenbildung (Hashwert)

«Kendox InfoShare» erstellt beim Ablegen (Import) eines Dokuments bzw. einer neuen Version eines bestehenden Dokuments einen **SHA-512 Bit Hashwert**. Dieser Hashwert wird immer erzeugt, unabhängig davon, ob zusätzliche Signaturen verwendet werden oder nicht. Im Zusammenspiel mit der Aufbewahrungsfrist, den manipulationssicheren Versions- und Änderungs-Logs sowie den automatischen Mechanismen zur Integritätsprüfung (z.B. Lesen nach Schreiben) wird ein grundlegender, nicht durch Konfigurationseinstellungen, Customizing oder Änderungsprogrammierung beinflussbarer Integritätsschutz ermöglicht (die sog. **«InfoShare Basic Compliance»**).

Objekt-relationales Speicherverfahren

«Kendox InfoShare» nutzt ein sog. «objekt-relationales Speicherverfahren», um Verwaltungsdaten wie Dokumenten- und Versionsstammsätze, Metadaten, Speicherorte, Verknüpfungen zwischen Dokumenten, Annotationen usw. in einer relationalen Datenbank zu speichern (Microsoft SQL Server, Oracle DB). Diese Daten sind außerhalb von «Kendox InfoShare» – wenn überhaupt – nur durch Spezialisten lesbar zu machen, wodurch ein **hoher «Sichtschutz»** gegenüber üblichen Datenbank-Werkzeugen besteht.

[8] Die Versionierung von Dokumenten selbst kann hingegen in «Kendox InfoShare» für Teilbereiche des Systems (sog. «InfoShare Ablagen») im Zusammenwirken mit entsprechenden Berechtigungsdefinitionen deaktiviert werden. Im Rahmen einer effizienten Verwaltung von einfach strukturierten, sehr grossen Datenmengen oder bei der reinen Archivierung von z.B. Belegdaten aus Spezialanwendungen heraus (API-Integration) kann das Abschalten der Versionierung durchaus sinnvoll sein. Für die konventionelle Dokumentenarchivierung (bzw. «Dokumentenmanagement») hingegen sollte die Versionierung nicht ausgeschalten werden.

[9] Hierbei ist zu beachten, dass durch die Statistik-Datenbank je nach Größe und Aktivitätsniveau des «Kendox InfoShare» Systems eine große Datenmenge erzeugt werden kann.

Lebenszyklus (Aufbewahrungsfrist)

«Kendox InfoShare» kann Dokumenten einen sog. **Lebenszyklus-Status** zuweisen, der auch eine Aufbewahrungsfrist umfasst. Ist einem Objekt (z.B. einem Dokument) eine Aufbewahrungsfrist zugewiesen und ist die Einstellung «Löschen verhindern» in der Lebenszyklus-Konfiguration aktiviert, so ist ein Löschen des entsprechenden Objektes nur noch unter Nutzung des Benutzerprofils «DCIAdmin» (Kendox InfoShare Systemadministrators) möglich [10]. Der Lebenszyklus wird dem Dokument fest zugewiesen. Die Informationen werden dabei aus der InfoShare-Konfiguration an das Dokument «übertragen». Somit ist auch sichergestellt, dass spätere Änderungen an der Lebenszyklus-Definition keine Auswirkungen auf Dokumente haben, denen bereits zuvor dieser Lebenszyklus zugewiesen wurde (nur neue Dokumente sind von der geänderten Definition betroffen).

Durch die Zuweisung eines Lebenszyklus-Status mit entsprechender Aufbewahrungsfrist unmittelbar bei der Ablage kann eine sehr sichere Archivierung erreicht werden. Zusätzlich wird die Aufbewahrungsfrist – sofern von den jeweiligen Systemen unterstützt – an die Compliance Storage Sub-Systeme weitergereicht.

Löschen von Dokumenten

Auch wenn über (normale) Berechtigung bzw. Lebenszyklus-Definition das Löschen von Dokumenten verhindert ist, muss es möglich sein, in bestimmten Situationen Dokumente löschen zu können. Hierzu zählen beispielsweise fehlerhafte Batch-Läufe, die große Mengen von irreführenden Daten in das Archiv abgelegt haben oder auch Löschaufträge eines Gerichts. Mit der Benutzer-ID «DCIAdmin» kann ein solches Löschen ausgeführt werden. Hierbei bestehen verschiedene Möglichkeiten (auch in Kombination), um den Löschvorgang selbst transparent und nachvollziehbar zu machen: [11]

- **Löschvorgang in der Statistik-Datenbank aufzeichnen**
  Dadurch werden sämtliche Löschprozesse (aber auch Änderungsprozesse) inkl. diverser Detailinformation in der Datenbank aufgezeichnet. Die Sicherung und Bereinigung dieser Datenbank ist Aufgabe des Anwenderunternehmens bzw. des Betreibers der Cloud Lösung.
  Anmerkung: Das dokumentenbezogene Änderungs-Log, der Bestandteil der Strukturinformation des Dokumentes (und damit Teil des Softwareobjektes «Dokument») ist, wird mit dem Löschen des Dokumentes ebenfalls aus der Datenbank entfernt und kann daher nicht mehr ausgewertet werden. Dagegen bleiben die Einträge in der Statistik-Datenbank auch dann bestehen, wenn ein Dokument gelöscht wird.
- **«Logisches bzw. zweistufiges Löschen» konfigurieren**
  Dabei wird beim Löschen von Dokumenten nicht physisch gelöscht, sondern nur der Sicherheitsbereich geändert. Das betroffene Dokument wird dadurch «unsichtbar». Erst beim zweiten Löschen des Dokuments (das nun durch den neu zugeordneten Sicherheitsbereich für gelöschte Dokumente geschützt ist) wird physisch gelöscht. Ist in dem neu zugeordneten Sicherheitsbereich wiederum ausschließlich «DCIAdmin» zum endgültigen Löschen berechtigt und ist die Verwendung dieser Benutzer-ID im normalen Systembetrieb verunmöglicht, kann somit ein Löschen von Dokumenten in «Kendox InfoShare» nachhaltig verhindert werden. Diese Einstellung gilt übergreifend für das gesamte «Kendox InfoShare» System.

[10] Benutzerprofile, denen der «DCIAdmin» dieses Recht explizit über die Rollendefinition übertragen hat, können die betreffenden Dokumente ebenfalls löschen.

[11] Werden Dokumente in «Kendox InfoShare» gelöscht, bedeutet dies nicht zwingend, dass die Dokumente (Dateien) auch auf dem darunter liegenden Speichersystem gelöscht werden. Ist auf dem Speichersystem (Compliance Storage) ein Löschschutz aktiv (in der Regel über eine Aufbewahrungsfrist), kann «Kendox InfoShare» das betreffende Dokumente aus technischen Gründen nicht löschen (Zugriffsrechte nicht ausreichend).

- **Batch-Läufe aufgrund der «Stapellaufnummer» zurücksetzen**
  Dies löscht alle derart erzeugten Dokumente aus «Kendox InfoShare». Dabei werden die Funktionen «logisches Löschen» und «Aufzeichnen Löschvorgang in Statistik-Datenbank» berücksichtigt, sofern die entsprechenden Einstellungen vorgenommen wurden.

«Advanced Auditing»

Neben den o.g. Mechanismen zur Protokollierung und zum Löschschutz lassen sich mit einem Zusatzmodul noch weitergehende Maßnahmen konfigurieren. Zusätzlich zu den Standard Auditing Funktionen des «Kendox InfoShare Servers» ermöglicht die Server-Erweiterung «Kendox InfoShare Advanced Auditing» eine umfassende Protokollierung von Systemaktivitäten:

- Protokollierung von administrativen Änderungen (Modifikationen an Benutzer-, Gruppen- sowie Berechtigungseinstellungen, Veränderungen von Eigenschaften, Eigenschaftstypen und sog. Importvorlagen)
- Protokollierung von Benutzeraktionen (alle Benutzeranmeldungen und -abmeldungen, Kennwortänderungen, fehlerhafte Anmeldeversuche)
- Protokollierung von Dokumentenaktionen (Erstellen, Ändern, Löschen, Anzeigen, Export etc.)
- Dauerhafter Löschschutz für Dokumente (Dokumente, die mit einem Löschschutz versehen sind, können auch von Benutzern mit administrativen Rechten nicht vor Ablauf des Löschschutzes gelöscht werden)

Aus Gründen der Compliance lassen sich die genannten Protokollierungsebenen nur einmalig und dauerhaft aktivieren. Ist die Protokollierung einmal aktiviert, so lässt sie sich nicht mehr deaktivieren. Insbesondere in sehr sensiblen Umgebungen ermöglichen diese Optionen eine umfassende Möglichkeit der «Auditierung» für das Gesamtsystem.

«Kendox InfoShare»-interne Migration von Dokumenten

«Kendox InfoShare» benutzt sog. «Ablagen» (auch: «InfoShare-Ablagen»), um die physikalische Speicherung zu segmentieren und zu steuern. Dabei können die Ablagen unterschiedlichen Storage Sub-Systeme zugeordnet sein.

Der «Kendox InfoShare Server» verfügt über interne Funktionen, um Dokumente (inkl. aller Vorversionen) zwischen den einzelnen «InfoShare-Ablagen» zu verschieben. Dabei bleiben Prüfsumme (Hashwert) und Aufbewahrungsfrist im «Kendox InfoShare Server» (bzw. genauer in der «Kendox InfoShare» Datenbank) unverändert. Im Verlauf dieser internen «Migration» versucht der «Kendox InfoShare Server» auf der Ziel-Ablage dieselbe Aufbewahrungsfrist an das darunter liegende Speichersystem zu übertragen, wie es in der ursprünglichen Ablage der Fall war. Das bedeutet konkret, dass sich die Aufbewahrungsfrist durch diesen internen Umkopierprozess nicht verlängert – natürlich nur unter der Bedingung, dass das Ziel-Speichersystem die entsprechenden Einstellungen zulässt.

Um die Änderung der «Kendox InfoShare Ablage» bzw. das «Verschieben» nachvollziehbar zu protokollieren, wird im Änderungs-Log der entsprechenden Dokumente ein Eintrag vorgenommen, der neben Datum/Uhrzeit und Benutzer-ID auch die Information enthält, dass das Dokument «verschoben» wurde.

5 Fazit

Die wichtigste Erkenntnis ist, dass der **Einsatz einer zertifizierten 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. Die Einhaltung der gesetzlichen Aufbewahrungsfristen und der Anforderungen für eine regelgerechte Archivierung muss daher sowohl technisch als auch organisatorisch umgesetzt werden.

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.

«Kendox InfoShare» als Software-Lösung zur Dokumentenverwaltung ist bei sachgerechter Anwendung und in Kombination mit entsprechenden technischen und organisatorischen Maßnahmen geeignet, den Anforderung an eine revisionssichere Archivierung gerecht zu werden.

Dies wird unter anderem durch die VOI Service GmbH [12] auf Basis der VOI Prüfkriterien für Dokumentenmanagement-Lösungen (**PK-DML III**) attestiert: [13,14]

Mittels der Softwarelösungen «Kendox InfoShare» lassen sich alle Anforderungen an einen revisionssicheren Einsatz in Unternehmen und öffentlichen Einrichtungen … in Deutschland, Österreich und der Schweiz erfüllen.

«Kendox InfoShare» bietet die technischen Voraussetzungen, um dies zu gewährleisten, die organisatorischen Vorkehrungen muss hingegen das Anwenderunternehmen sicherstellen.

Für die Schweiz hat «Kendox InfoShare» als eine der ersten ECM/DMS-Lösungen überhaupt die Zertifizierung «**GeBüV/MWST konform**» erhalten[15]. In einem aufwändigen und umfassenden Zertifizierungsverfahren wurde die ECM-Lösung durch das «Kompetenzzentrum Records Management» [16] auf Herz und Nieren geprüft. Dabei erfolgte die Prüfung nach anerkannten Prinzipien der Systemprüfung und -zertifizierung. Als Grundlage dienten die Geschäftsbücherverordnung (GeBüV) sowie die Vorgaben der Eidg. Steuerverwaltung (ESTV) zur Mehrwertsteuer. Geprüft wurden alle Aspekte der GeBüV, insbesondere die Anforderungen an die Integrität und den Schutz der Archivdaten.

[12] VOI – Verband Organisations- und Informationssysteme e.V., Heilsbachstr. 25, D-53123 Bonn

[13] Zertifizierungsbericht VCC14008 vom 16.07.2014, VOI Compliance Certificate (VCC)

[14] Für das Audit wurde das gemeinsam von VOI und TÜViT (Nord) erarbeitete Rahmenwerk mit Prüfkriterien für Dokumentenmanagement- und Enterprise Content Management-Lösungen zugrunde gelegt (kurz: «PK-DML», 3. Auflage, 2008). Die Zertifizierungsstelle besteht aus fachkundigen Auditoren aus dem Mitgliederkreis des VOI, die auf Basis standardisierter Prüfungsanforderungen Software, Dienstleistungen und Anwendungen auf die Einhaltung technischer Standards, gesetzlicher Anforderungen und auf Beweissicherheit von Geschäftsprozessen prüfen.

[15] Zertifizierungsbericht 2017-V002 vom 01.02.2017, Kompetenzzentrum Records Management GmbH («KRM»)

[16] Kompetenzzentrum Records Management GmbH, Rotfluhstrasse 91, 8702 Zollikon, www.krm.swiss

Kendox AG

Bahnhof-Strasse 7
CH-9463 Oberriet SG
Schweiz

T +41 (71) 552 34-00

Kendox GmbH

Hohentrüdinger Straße 11
91747 Westheim
Deutschland

T +49 (32) 228 83 70-00

Kendox AG, Niederlassung Österreich

Favoritenstraße 87/2
1100 Wien
Österreich

T +43 (720) 27 34-20

www.kendox.com | info@kendox.com