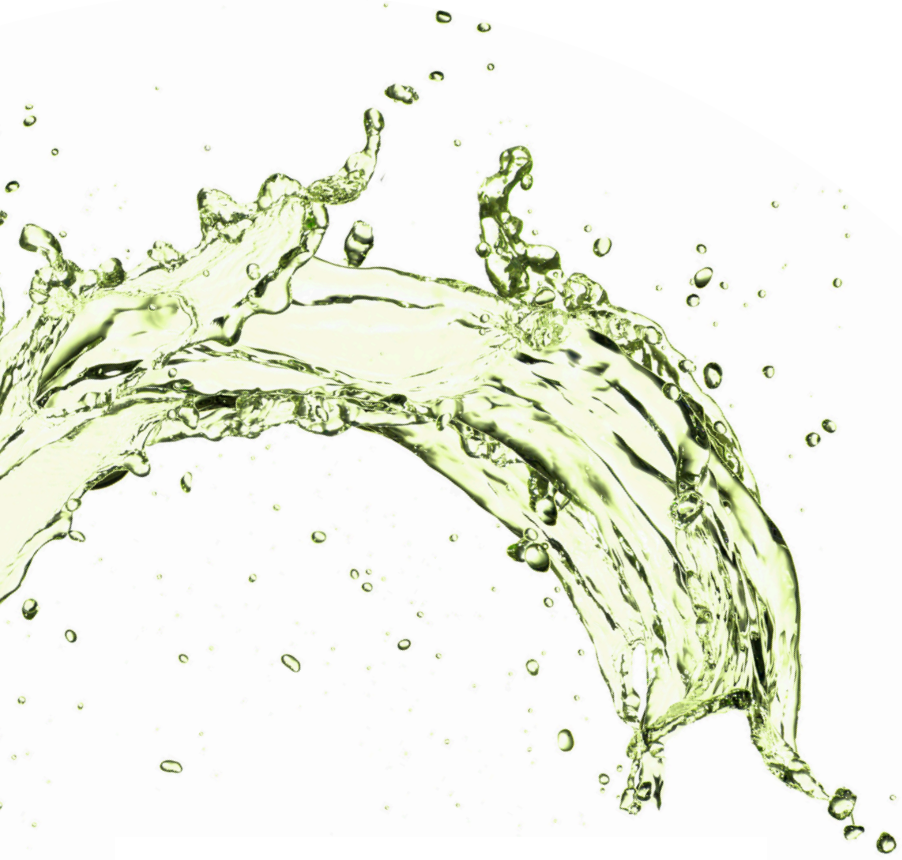
CARBONITE™
HYBRID BACKUP & RECOVERY



RECHTLICHE ASPEKTE DER DATENSICHERUNG

Stand: Oktober 2015

INHALT

EINLEITUNG

Nahezu alle Prozesse in Unternehmen sind heute elektronisch gesteuert. Entsprechend groß ist auch die Menge der dabei anfallenden elektronischen Daten. Gleichzeitig sind diese Daten zu speichern und zu sichern.

Unternehmen haben es in vielen Geschäftsbereichen mit rechtlichen Rahmenbedingungen zu tun, die sie zur revisionssicheren und rechtskonformen Aufbewahrung geschäftlicher Dokumente über viele Jahre hinweg verpflichten. Zur Wahrung der allgemeinen Schutz- und Sorgfaltspflicht verlangt der Gesetzgeber an dieser Stelle den regelmäßigen, geeigneten und lückenlosen Einsatz von Datensicherungsroutinen. Kommen personenbezogene Daten ins Spiel, greifen außerdem die gesetzlichen Vorgaben zum Datenschutz sowie Regelungen für eine sichere Verwahrung und Speicherung von Daten, also zur Datensicherheit.

Die Verantwortung für die Einhaltung von gesetzlichen Bestimmungen und internen Richtlinien liegt bei der Geschäftsführung eines Unternehmens. Hierzu gehört auch die rechtssichere Umsetzung im Bereich der Datensicherung. Ein Unternehmen muss jederzeit plausibel darlegen können, dass es Daten durch eine definierte Backup-Strategie sichert und diese im Verlustfall zeitnah wiederherstellen kann. Ist dies nicht der Fall, können Verantwortliche gegebenenfalls in persönliche Haftung genommen werden. Im Falle erheblicher Pflichtverstöße kann sogar der Versicherungsschutz des Unternehmens und der Mitglieder des Managements gefährdet sein.

Da Datensicherungssysteme neben der Absicherung des Geschäfts gleichzeitig den Bedürfnissen des Datenschutzes genügen müssen, stehen Unternehmen zudem vor der Aufgabe, geeignete Maßnahmen zu ergreifen, die unternehmenskritische und personenbezogene Daten vor Verlust und ungewollter Offenlegung schützen. Laut Bundesdatenschutzgesetz (BDSG) verantworten Unternehmen die Sicherheit personenbezogener Daten, etwa von Mitarbeitern und Kunden (§ 9 BDSG – Technische und organisatorische Maßnahmen). Die Anlage zu § 9 BDSG sieht verschiedene Kontrollmaßnahmen vor. Dabei spielt der Stand der Technik eine entscheidende Rolle. Auf der technischen Seite sind Backup- und Disaster-Recovery-Lösungen in der Praxis häufig tragende Säulen der Umsetzung dieser Anforderungen. Datenverlust und andere Verstöße gegen das BDSG können Informationspflichten auslösen und laut Gesetz mit einem Bußgeld von bis zu 300.000 Euro geahndet werden.

ZU SICHERNDE DATEN UND DOKUMENTE IM UNTERNEHMEN

Grundsätzlich sind alle Daten und Dokumente zu sichern, die gesetzlichen Aufbewahrungspflichten unterliegen oder als Beweismittel in einem Zivilprozess dienen könnten. Beispiele hierfür sind Rechnungen und Lieferscheine, die als Nachweis einer abgeschlossenen Transaktion dienen können. Aber auch andere Unterlagen sind zu sichern. Ärzte oder Rechtsanwälte müssen beispielsweise die ordnungsgemäße Beratung ihrer Patienten und Klienten dokumentieren. So regelt § 10 Abs. 3 der (Muster-Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte (MBO-Ä 1997)), dass ärztliche Aufzeichnungen zehn Jahre lang aufzubewahren sind. All diese Dokumente müssen gesichert und revisionssicher archiviert werden. Lässt sich ein Dokument nachträglich verändern, kann die Beweiskraft der Daten eingeschränkt sein. In diesem Fall würde die Sicherung nicht den geforderten Kriterien genügen.

DIE RECHTLICHEN RAHMEN-BEDINGUNGEN

Gesetzliche Vorschriften wie die des Handelsgesetzbuchs (HGB) über eine ordnungsgemäße, nachvollziehbare und revisionssichere Buchführung bilden den Rahmen für die Pflicht zur Datensicherung im Unternehmen. So regelt es beispielsweise die Aufbewahrungsfristen von kaufmännischen Dokumenten. Nach § 257 Abs. 1 Nr. 2 und 3, Abs. 4 HGB sind empfangene Handelsbriefe und Wiedergaben (Kopien, Durchschriften) abgesandter Handelsbriefe sechs Jahre aufzubewahren. Durch das KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich) wurden insbesondere einige Vorschriften des Handelsgesetzbuches und des Aktiengesetzes präzisiert und erweitert. Die Aufbewahrungsfristen von bestimmten Daten können bis zu zehn Jahre betragen.

Ferner unterliegen in der Bundesrepublik Deutschland alle Dokumente, die sich mit dem Thema Steuern in Verbindung bringen lassen, den „Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff“ (GoBD). Es handelt sich dabei um eine für Behörden verbindliche Verwaltungsanweisung des Bundesfinanzministeriums (BMF), die die Anforderungen der Finanzverwaltung an eine IT-gestützte Buchführung darstellt. Sie hat damit faktisch enorme Auswirkungen auf die Wirtschaft. Die GoBD gelten seit dem 1. Januar 2015. Abgelöst wurden dadurch die GDPdU (Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen), die am 1. Januar 2002 in Kraft traten. Damit wurden seinerzeit Rechtsnormen aus der Abgabenordnung und dem Umsatzsteuergesetz zur digitalen Aufbewahrung von Buchhaltungen, Buchungsbelegen und Rechnungen konkretisiert. Die „Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme“ (GoBS) wurden ebenfalls durch die GoBD abgelöst.

Die GoBD umfassen Regeln zur Aufbewahrung und Archivierung handels- und steuerrechtlich relevanter digitaler Unterlagen und zur Mitwirkung von Steuerpflichtigen bei Betriebsprüfungen. Im Kern geht es darum, dass einem Betriebsprüfer jederzeit lesender Zugriff auf alle digitalen Unterlagen von steuerlicher Bedeutung gewährt werden muss. Dokumente müssen entsprechend so gesichert werden, dass auf die Archive jederzeit zugegriffen werden kann. Zugleich fordern die GoBD sogar, dass Dokumente, die etwa in einem Dokumenten-Management-System abgelegt sind, nicht mehr lediglich in Papierform aufbewahrt werden dürfen, sondern elektronisch zu archivieren sind.

Allerdings dürfte es kein Unternehmen geben, in dem die Regelungen zu 100 Prozent erfüllt sind. Denn beispielsweise gehören zu den steuerlich relevanten digitalen Unterlagen auch alle Mails, die Vorgänge von steuerlicher Bedeutung betreffen. Bei Unterlagen, die im Rahmen einer Betriebsprüfung üblicherweise eine Rolle spielen, sollten sich Unternehmen aber an die strengen Anforderungen der GoBD halten. Letztlich geht es bei der Betrachtung rechtlicher Aspekte der Datensicherung um zwei Fragen: Was kann getan werden und was muss getan werden. Verbleiben die Daten im Unternehmen, können alle Daten gesichert werden, die legal gespeichert wurden.

DER BEGRIFF DER REVISIONSSICHERHEIT

Vielfach genutzt, wird der Begriff der Revisionssicherheit oft mit unterschiedlichen Bedeutungen versehen. Der Gesetzgeber orientiert sich allerdings klar am Verständnis der Revision aus ökonomischer Sicht. Er bezieht sich daher auf aufbewahrungspflichtige Daten und Dokumente des handels- und steuerrechtlichen Bereichs sowie auf deren Archivierung in elektronischen Systemen. In Deutschland muss diese Archivierung, wie bereits erwähnt, den Anforderungen des Handelsgesetzbuches, der Abgabenordnung (AO) und den GoBD (die in Nr. 3.2.5 von Unveränderbarkeit sprechen) sowie weiteren steuerrechtlichen, handelsrechtlichen und gesellschaftsrechtlichen Vorgaben entsprechen.

Revisionssicherheit ist dabei im gesamten Archivierungsprozess einzuhalten. Sie betrifft damit sowohl die Art und Weise der Datenarchivierung als auch die technische Durchführung. Zu diesem Zweck haben Unternehmen also auch für zuverlässige Prozesse, eine ordnungsgemäße Nutzung und den sicheren Betrieb der eingesetzten Lösung zu sorgen. Revisionssichere Systeme kennzeichnen sich hauptsächlich dadurch, dass elektronische Informationen wieder auffindbar, nachvollziehbar, unveränderbar und verfälschungssicher archiviert sind.

In Anlehnung an das HGB lassen sich folgende Kriterien benennen:

- Ordnungsmäßigkeit
- Vollständigkeit
- Sicherheit des Verfahrens
- Schutz vor Verfälschung, Veränderung und Verlust
- Nutzung nur durch Berechtigte
- Einhaltung der Aufbewahrungsfristen
- Dokumentation des Verfahrens
- Nachvollziehbarkeit und Prüfbarkeit

ZERTIFIZIERUNG DER REVISIONSSICHERHEIT

Allgemeingültige Zertifizierungen der Revisionssicherheit gibt es nicht, denn der konkrete Einsatz beim Anwender, seine Verfahren, Informationen und Prozesse sowie der sichere Betrieb sind wesentlicher Bestandteil der Revisionssicherheit. Ob die Revisionssicherheit nach Maßgabe des Gesetzgebers erfüllt ist, ist für jedes Unternehmen im konkreten Einzelfall zu bewerten.

In der Praxis übernehmen in aller Regel Wirtschaftsprüfer die Überprüfung und Zertifizierung von elektronischen Archivsystemen beim Anwender vor Ort. Vom Fachausschuss für Informationstechnologie des Instituts der Wirtschaftsprüfer in Deutschland e.V. (IDW) gibt hierfür eine eigene Vorgabe. Zu finden ist sie in der „Stellungnahme zur Rechnungslegung: Grundsätze ordnungsgemäßer Buchführung bei Einsatz von Informationstechnologie“ (IDW RS FAIT 1).

Aber auch der TÜViT kann die Einhaltung der Revisionssicherheit auf Basis einer Verfahrensdokumentation zertifizieren. Dies geschieht auf der Grundlage der Prüfkriterien für Dokumentenmanagement-Lösungen (PK-DML) des VOI e.V. (Verband Organisations- und Informationssysteme).

RECHTE AN DEN DATEN

In Deutschland können Rechte an Daten unter anderem durch das Urheberrechtsgesetz (UrhG) und andere Gesetze zum Schutz von Immaterialgütern sowie durch Vorschriften des Strafgesetzbuches (StGB) geschützt sein. Sie regeln und beschränken, wie der Urheber, sein Arbeitgeber, eventuelle Auftraggeber und andere Dritte über die Daten verfügen dürfen.

Ein zwingender Zusammenhang zwischen dem Eigentum am Datenträger, auf dem Daten gespeichert werden, und der Verfügungsbefugnis besteht nicht. Hat ein Verfügungsberechtigter die Daten rechtmäßig auf einem Fremddatenträger gespeichert, ist er unverändert Rechteinhaber.

GEEIGNETE SPEICHER- UND SICHERUNGS-VERFAHREN

Eine rechtskonforme Backup-Strategie sollte Datensicherheit mit größtmöglicher Verfügbarkeit und Produktivität verbinden sowie gleichzeitig die besonderen Schutzanforderungen von Daten mit Personenbezug berücksichtigen. Orientierung liefert die „3-2-1-Regel“. Geschäftskritische Daten sollten dreimal existieren und auf zwei verschiedenen Medien gespeichert werden.

ÜBERSICHT RECHTLICHER RAHMENBEDINGUNGEN

Handelsgesetzbuch (HGB)	Nach HGB § 257 Abs. 1 Nr. 2 und 3 HGB sind Geschäftspapiere mit kaufmännischer und steuerlicher Bedeutung sechs Jahre aufzubewahren. §§ 238, 239 HGB schreiben eine nachvollziehbare, revisionssichere Führung der Handelsbücher vor. Weitere Anforderungen an das Kontroll- und Risiko-Managementsystem wurden durch das Gesetz zur Modernisierung des Bilanzrechts (BilMoG) in das HGB eingefügt.
Abgabenordnung (AO)	Nach AO § 147 müssen unter anderem Bücher, Aufzeichnungen, Inventare, Jahresabschlüsse, Lageberichte, die Eröffnungsbilanz und Buchungsbelege zehn Jahre aufbewahrt werden.
Aktiengesetz (AktG), GmbH-Gesetz (GmbHG) sowie sonstige handels- und gesellschaftsrechtliche Gesetze	Durch das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) wurden Aufbewahrungspflichten in die jeweiligen Gesetze eingeführt. Finanz- und steuerrelevante Daten sind derzeit zehn Jahre aufzubewahren. Ein Sicherheitskonzept ist erforderlich.
Bundesdatenschutzgesetz (BDSG)	Enthält Regelungen für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Personenbezogene Daten sind gegen Zerstörung und Verlust zu schützen. § 9 BDSG und die Anlage hierzu schreiben technische und organisatorische Maßnahmen zur Einhaltung des Datenschutzes vor.
Basel II	Unternehmensbezogene Daten von Banken sind zu sichern. Ein hinreichendes Notfallkonzept muss vorhanden sein.
EuroSOX (Abschlussprüfungs-Richtlinie 2006/43/EG)	Planungen für den langfristigen Erhalt des Betriebs sowie ein Notfallkonzept sind erforderlich.
Mindestanforderungen für das Risiko-Management (MaRisk) von Kreditinstituten und Versicherungen	Die BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht) verlangt ein Risikomanagement.
GoBD (Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff)	Konkretisieren die Ordnungsmäßigkeitsanforderungen der Finanzverwaltung an den Einsatz von IT bei der Buchführung und bei sonstigen Aufzeichnungen.
(Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte (MBO-Ä 1997)	Enthält Aufbewahrungspflichten für Patientendaten.

CARBONITE™

HYBRID BACKUP & RECOVERY

www.carbonite.de

CARBONITE GERMANY GMBH
GUTENBERGSTR. 1
85737 ISMANING

TEL: + 49 89 2154 740 0
E-MAIL: SALES@CARBONITE.DE

Stand: Oktober 2015