

# Compliance auf einen Blick

Relevante, nationale Gesetze, europäische Richtlinien und globale Vorschriften

Gesetzliche Richtlinie	Inhaltliche Bedeutung	Gültigkeit für Branche	Bereich	Inkrafttreten	Konsequenzen für die IT
<b>HGB</b>					
<b>Handelsgesetzbuch</b>	Das Handelsgesetzbuch (HGB) ist ein Hauptbestandteil des Handelsrechts in Deutschland. Es regelt die Rechtsverhältnisse der Kaufleute und wird daher auch als „Sonderprivatrecht“ bezeichnet.	Alle Branchen	Deutschland	Seit 1. Januar 1898	§239 und §257 HGB regeln die grundsätzlichen Voraussetzungen für die Archivierung von kaufmännischen Dokumenten. § 239 definiert die Kriterien für die revisionssichere elektronische Archivierung.
<b>KonTraG</b>					
<b>Gesetz zur Kontrolle und Transparenz im Unternehmensbereich</b>	Das KonTraG erweitert die Haftung von Vorstand, Aufsichtsrat und Wirtschaftsprüfer in Unternehmen. Kern des Gesetzes ist eine Vorschrift, die Unternehmensleitungen dazu zwingt, ein unternehmensweites Frühwarnsystem für Risiken (Risikomanagementsystem) einzuführen sowie im Jahresbericht Aussagen zur Risiken und Risikostruktur zu publizieren. Das KonTraG betrifft dabei nicht ausschließlich Aktiengesellschaften. Auch die Rechtsformen der KGaA (Kommanditgesellschaft auf Aktien) und teilweise der GmbH (insbesondere wenn dort ein mitbestimmter oder fakultativer Aufsichtsrat existiert) sind betroffen. Dagegen ist die so genannte „kleine AG“ weitgehend von der Einhaltung der durch das KonTraG neu eingeführten Vorschriften befreit.	Alle Branchen	Deutschland	Seit 1. Mai 1998	Im Gegensatz zum amerikanischen Sarbanes-Oxley Act gibt es beim deutschen Pendant keine Mindestanforderungen. Es werden lediglich erweiterte Pflichten der Unternehmensleitung bzgl. Des Risikomanagements und der Risikosteuerung definiert. Die IT ist für die Absicherung der IT-Infrastruktur für die Audits und Nachweispflichten über Berechtigungen verantwortlich. Hierzu gehört auch die sachgerechte Archivierung dieser Daten.
<b>GdPDU</b>					
<b>Grundsätze ordnungsgemäßer Datenzugriff und zur Prüfbarkeit digitaler Unterlagen</b>	Auf die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen beruft sich ein Finanzbeamter, wenn er bei Betriebsprüfungen auf die Computersysteme von Unternehmen zugreift. Unternehmen müssen hierbei steuerrelevante Daten - also auch umstrukturierte Daten wie E-Mails - in auswertbarer Form zur Verfügung stellen.	Alle Branchen	Deutschland	Änderung 1. Januar 2002	Durch die Archivierung muss gewährleistet sein, dass die steuerrelevanten Daten bzw. alle Kosten- oder Ertragsrelevanten Unterlagen eines Unternehmens in auswertbarer Form für eine Außenprüfung des Finanzamts zur Verfügung stehen.
<b>GoBS</b>					
<b>Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme</b>	Die GoBS regelt die Behandlung aufbewahrungspflichtiger Daten und Dokumente in elektronischen Buchführungs- sowie in revisionssicheren Archivierungssysteme.	Alle Branchen	Deutschland	Ursprüngliche Fassung 7. November 1995	Die Archivierung nach GoBS hat so zu erfolgen, dass Änderungen nicht mehr möglich sind, die Art der Ablage nachvollziehbar ist sowie die Informationen jederzeit verfügbar und unverzüglich für autorisierte Personen lesbar sind.
<b>Basel II</b>					
	Basel II schreibt internationalen Geldinstituten die Schaffung eines risikobewussteren Kapitalrahmens vor. Der Schwerpunkt liegt auf einem eigenen internen Kontrollsystemen, dem bankaufsichtlichen Überprüfungsprozess und der Marktdisziplin. Dies führt zu einem Rating von Kreditnehmern nach Kriterien wie Eigenkapital und Risikoeinschätzung. Die damit verbundene Benachteiligung des kapitaischwächeren Mittelstands sollte durch eine Zusatzvereinbarung wieder ausgeglichen werden.	Alle Branchen - Banken	Alle Mitgliedsstaaten der Europäischen Union (die USA will nach derzeitigem Stand die Regelungen ab 1. Januar 2009 schrittweise einführen).	Seit 1. Januar 2007	Aus den Eigenkapitalrichtlinien leiten sich für die Archivierung im Wesentlichen die Forderung ab, Daten über die Unternehmensprozesse zur Kontrolle und dem Management von Risiken und Anlagewerten eines Unternehmens zu sichern.
<b>Sarbane-Oxly-Act (SOX)</b>					
	US-Gesetz zur Verbesserung der Unternehmensberichterstattung infolge der Bilanzskandale von Unternehmen wie Enron oder Worldcom. Das Gesetz betrifft verschiedene Aspekte der Corporate Governance, Compliance und der Berichterstattungspflichten von Publikumsgesellschaften sowie der damit zusammenhängenden Durchsetzung. Insbesondere legte das Gesetz ein neues aufsichtsrechtliches System für Wirtschaftsprüfungsgesellschaften fest. Diese prüfen Unternehmen, welche von Gesetzes wegen verpflichtet sind, bei der Securities and Exchange Commission (SEC) Abschlüsse und sonstige Berichte einzureichen.	Alle Branchen	Inländische und ausländische Unternehmen, die an US-Börsen (z.B. der NASDAQ) gelistet sind, sowie für deren Tochterunternehmen.	SOX trat im Juli 2002 in Kraft (für an US-Börsen gelistete ausländische Unternehmen : seit 15. Juli 2006).	SOX verlangt die korrekte Archivierung von betriebsrelevanten Informationen (sowohl von strukturierten als auch unstrukturierten Daten wie E-Mails, Präsentationen, Ton- und Bilddaten) bis vier Jahre nach Prüfungsende.
<b>EU - Datenschutzrichtlinie</b>					
	Die EU-Datenschutzrichtlinie 95/46/EG des Europäischen Parlaments und des Rates gilt dem Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EU DPD). Natürliche Personen haben das Recht auf Zugang zu den Daten und ihre Berichtigung.	Alle Branchen	EU und alle einheiten, die mit der EU Handel treiben oder geschäftsmäßig tätig sind.	Seit 1995	Personen, Behörden, Unternehmen, Geschäftsstellen oder anderen für die Verarbeitung personenbezogener Daten verantwortlichen Stellen, müssen die Einhaltung der Schutzprinzipien hinsichtlich der Datenqualität und -Sicherheit ihres Archivs gewährleisten. Zudem haben die Personen, deren Daten Gegenstand von Verarbeitungen sind Recht auf Zugang zu den (Archiv)-Daten.