

IT-Compliance im Unternehmen

RA Dr. Lars Lensdorf
RA Udo Steger
Heymann & Partner Rechtsanwälte

Vortrag am 15.09.2006

1. Zum Begriff „IT-Compliance“
2. Rechtliche Grundlagen
3. Ausgewählte IT-Compliance Anforderungen
 - Datenschutz und Datensicherheit
 - Arbeitsrecht
 - Unternehmensorganisation
 - Buchhaltung, Rechnungslegung, Prüfung
 - Sektorspezifisch: Banken und Finanzdienstleister
4. Adressaten von IT-Compliance Anforderungen
5. Drohende Sanktionen, Haftungsrisiken
6. Gewährleistung von IT-Compliance
 - insbes. Gewährleistung von IT-Compliance durch Dritte
7. Fazit und Ausblick

1. Zum Begriff „IT-Compliance“

2. Rechtliche Grundlagen

3. Ausgewählte IT-Compliance Anforderungen

- Datenschutz und Datensicherheit
- Arbeitsrecht
- Unternehmensorganisation
- Buchhaltung, Rechnungslegung, Prüfung
- Sektorspezifisch: Banken und Finanzdienstleister

4. Adressaten von IT-Compliance Anforderungen

5. Drohende Sanktionen, Haftungsrisiken

6. Gewährleistung von IT-Compliance

- insbes. Gewährleistung von IT-Compliance durch Dritte

7. Fazit und Ausblick

- Compliance = „*Befolgung*“
 - meint die Einhaltung von Gesetzen, Richtlinien und anderen Verhaltensmaßregeln im Unternehmensalltag
 - Einrichtung von Kontroll- und Steuerungsprozessen
 - Dokumentation solcher Prozesse
 - Ziel ist das „vollständig regelkonforme Unternehmen“
- Compliance als Element der „*Corporate Governance*“:
 - Präambel des Deutschen Corporate Governance Kodex (DCGK):
 - Wahrung von Entscheidungsfähigkeit und Effizienz auf der obersten Unternehmensebene,
 - Transparenz hinsichtlich der Entwicklung und Risiken
 - ausgewogenes Verhältnis von Führung und Kontrolle im Unternehmen

- IT-Compliance = Regelkonforme IT-Systeme
 - im Unternehmen eingesetzte IT-Systeme müssen den für Einrichtung und Betrieb solcher Systeme geltenden Gesetzen, Richtlinien und anderen Verhaltensmaßregeln genügen
- IT-Compliance = Compliance mit Hilfe von IT-Systemen
 - Viele Unternehmensfunktionen, für die Compliance-Anforderungen gelten, werden mit IT-Systemen abgebildet (z.B. Buchhaltung)
 - Compliance betrifft deshalb unmittelbar auch Einrichtung und den Betrieb von IT-Systemen, die jeweils „regelkonform“ sein müssen
 - Zunahme von Compliance-Anforderungen wie Unverfälschbarkeit und Revisionssicherheit von elektronischen Dokumenten
 - z.B. elektronische Rechnung, elektronische Buchführung und Buchprüfung
- Folge: Compliance ist heutzutage ohne IT-Compliance nicht mehr zu gewährleisten

1. Zum Begriff „IT-Compliance“

2. Rechtliche Grundlagen

3. Ausgewählte IT-Compliance Anforderungen

- Datenschutz und Datensicherheit
- Arbeitsrecht
- Unternehmensorganisation
- Buchhaltung, Rechnungslegung, Prüfung
- Sektorspezifisch: Banken und Finanzdienstleister

4. Adressaten von IT-Compliance Anforderungen

5. Drohende Sanktionen, Haftungsrisiken

6. Gewährleistung von IT-Compliance

- insbes. Gewährleistung von IT-Compliance durch Dritte

7. Fazit und Ausblick

- Gesetzliche Anforderungen
 - Gesetze, Verordnungen = direkt normiert, abstrakt-generell
 - z.B. § 91 Abs. 2 AktG, § 9 BDSG mit Anlage
 - nicht dispositiv, können bei Nichtbeachtung behördlich/gerichtlich zwangsweise durchgesetzt werden
 - Aber: enthalten nur selten konkrete Vorschriften zur Umsetzung
- Verwaltungsvorschriften, Verwaltungshandeln
 - Ministerialerlasse, Verfügungen, Richtlinien oder Anordnungen
 - ergehen innerhalb der Verwaltung zur internen Organisation, grundsätzlich keine Außenwirkung
 - legen Gesetze aus bzw. konkretisieren diese und/oder geben Rechtsauffassung der Verwaltung zu bestimmten Fragen wieder
 - z.B. IT-Richtlinie des BMI = Regelung des internen Einsatzes von IT durch die Bundesverwaltung

- Sonderfall: Aufsicht im Banken- und Finanzdienstleistungssektor durch die BaFin
 - KWG (ähnlich: WpHG) enthält gesetzliche Generalklauseln, die mittelbar auch IT-spezifische Organisationspflichten für die erfassten Institute begründen.
 - BaFin konkretisiert diese in Form behördlicher Rundschreiben, Verlautbarungen bzw. Richtlinien
 - z.B. Rs. 11/2001 („Outsourcing-Rundschreiben“)
 - z.B. Rs. 18/2005 („Mindestanforderungen an das Risikomanagement“, MaRisk)
 - formell haben diese keine Außenwirkung, da i.d.R. nicht in Form eines VA, Allgemeinverfügung etc. ergehend
 - Aber: BaFin misst Institute an diesen Anforderungen und KWG räumt BaFin weitgehende Anordnungs-, Kontroll- und Prüfungsbefugnisse ein,
 - z.B. §§ 6, 34, 36 KWG.
 - Folge: Faktischer Zwang zur Umsetzung.

- Richtlinien und Standards

- haben keinen Rechtscharakter, sind nicht unmittelbar durchsetzbar
- im IT-Bereich i.d.R. keine „technische Gesetzgebung“ in dem Sinne, dass bestimmte Verfahren und Einrichtungen konkret beschrieben und vorgeschrieben sind
 - anders z.B. im Bereich der Normung oder Bauordnungsrecht/Baurecht
- Beachtung von Standards kann in Streitfällen als Interpretationshilfe herangezogen werden (z.B. „marktübliches Format“)
- liefern wichtige Hinweise für die praktische Umsetzung von IT-Compliance Anforderungen
- Zertifizierungen können den Nachweis eigener (Sorgfalts-)Pflichterfüllung erleichtern
 - z.B. „Sorgfalt eines ordentlichen Kaufmanns“ (§ 347 Abs. 1 HGB)
 - z.B. „Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters“ (§ 93 Abs. 1 AktG)

- Sonderfall: öffentliche Vergabeverfahren
 - § 7/7a VOL/A: Nachweis der Fachkunde, Leistungsfähigkeit und Zuverlässigkeit
 - IT-Standards und entsprechende Zertifizierungen werden immer öfter als Wertungskriterien und Vertragsbestandteile verwendet
 - Sie haben dadurch (zumindest für die Bieter) faktisch Bindungswirkung
 - z.B. „IT-Grundschutzhandbuch“ (GSHB), „IT Infrastructure Library“ (ITIL).
- Gesetzliche und vertragliche Obliegenheiten
 - nicht selbständig einklagbar, sondern bloße Verhaltensnormen, die bei Nichtbeachtung zum Rechtsverlust führen können.
 - insbesondere im Versicherungsvertragrecht/ VVG
 - z.B. Pflicht, bedeutende Umstände anzuzeigen, § 16 VVG
 - z.B. Pflicht, keine Gefahrerhöhung nach Vertragsschluss vorzunehmen oder dies zuzulassen, Anzeigepflicht § 23 VVG

1. Zum Begriff „IT-Compliance“
2. Rechtliche Grundlagen
- 3. Ausgewählte IT-Compliance Anforderungen**
 - **Datenschutz und Datensicherheit**
 - **Arbeitsrecht**
 - **Unternehmensorganisation**
 - **Buchhaltung, Rechnungslegung, Prüfung**
 - **Sektorspezifisch: Banken und Finanzdienstleister**
4. Adressaten von IT-Compliance Anforderungen
5. Drohende Sanktionen, Haftungsrisiken
6. Gewährleistung von IT-Compliance
 - insbes. Gewährleistung von IT-Compliance durch Dritte
7. Fazit und Ausblick

3.1 Datenschutz und Datensicherheit

- BDSG

3.2 Arbeitsrecht

- BetrVG, Arbeitsschutzvorschriften

3.3 Unternehmensorganisation

- KonTraG, DCGK, UMAG, Basel II

3.4 Buchhaltung, Rechnungslegung, Prüfung

- HGB, GoB, GoBS, GDPdU
- IFRS, Sarbanes Oxley Act

3.5 Sektorspezifisch: Banken und Finanzdienstleister

- § 25 a Abs. 2 KWG und RS'en 11/2001, 18/2005 (MaRisk)

- BDSG

- Querschnittsnorm, daneben sektorspezifische Datenschutznormen:
 - z.B. Telekommunikation, §§ 91 ff. TKG, Sozialdatenschutz, § 67 ff. SGB X
- weite Definition in § 3 Abs. 1 BDSG zu personenbezogene Daten („bestimmbare natürliche Person“)
- § 4 Abs. 1 BDSG: Erhebung, Verarbeitung, Nutzung von Daten nur mit Einwilligung des Betroffenen
- Umsetzung der Anforderungen des BDSG erfordert Dokumentationsprozesse, Berücksichtigung bei Gestaltung von Vertragsunterlagen, AGB, Webseiten, etc.

- § 11 BDSG: Auftragsdatenverarbeitung

- Einwilligung zur „echten“ Übermittlung selten praktikabel einholbar
- daher i.d.R. Vereinbarung einer Auftragsdatenverarbeitung = Vereinbarung zwischen auslagerndem Unternehmen („Herr der Daten“) und Dienstleister („Auftragsdatenverarbeiter“)

- § 11 BDSG: Auftragsdatenverarbeitung
 - möglichst genaue Vorgaben für die Verarbeitung der Daten und die technisch-organisatorische Maßnahmen. Wiedergabe der Anlage zu § 9 BDSG reicht nicht, um § 11 BDSG zu genügen!
 - Überwachung durch DSB, Prüfaufgabe des WP
- § 9 BDSG i.V.m. der zugehörigen Anlage
 - enthält allgemeine, technisch-organisatorische Anforderungen zum Schutz von personenbezogenen Daten
 - Konzepte sind insbesondere im Hinblick auf Datensicherheit auch allgemein gültig (“good practice“)
 - z.B. Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags- und Verfügbarkeitskontrolle
 - dadurch wichtige gesetzgeberische Vorgabe für die Bestimmung einer „angemessenen“ Einrichtung von IT-Systemen
- IT-Compliance: Konzepte in der Anlage zu § 9 BDSG müssen konkret umgesetzt werden, z.B. durch Datensicherheitskonzept

- Betriebsverfassungsgesetz (BetrVG)
 - enthält eine Vielzahl von Rechten des BR, die an technische Einrichtungen, Arbeitsabläufe, etc. anknüpfen und so auch IT-Systeme erfassen. Beispiele:
 - **§ 80 Abs. 1 Nr. 1 BetrVG:** Recht des BR, die Einhaltung von zugunsten des Arbeitnehmers geltenden Rechtsvorschriften zu überwachen (z.B. BDSG)
 - **§§ 80 Abs. 2, 111 BetrVG:** Auskunfts- und Informationsanspruch bzgl. aller betrieblichen Vorgänge, erfasst z.B. Einrichtung und Betrieb von IT-Systemen
 - **§ 87 I Nr. 6 BetrVG:** Mitbestimmungsrecht des BR bei der Einführung und Anwendung von technischen Einrichtungen, die dazu geeignet sind, das Verhalten oder die Leistung der Mitarbeiter zu überwachen
- IT-Compliance: IT-Systeme müssen so eingeführt und betrieben werden, dass in die Rechte des BR nicht eingegriffen wird

- Arbeitsschutzvorschriften
 - insbesondere: „Verordnung über Sicherheit und Gesundheitsschutz bei der Arbeit an Bildschirmgeräten“ (Bildschirmarbeitsschutzverordnung, BildscharbV)
 - regelt bestimmte Mindestanforderungen wie niedrige Strahlung der Geräte, regelmäßige Pausen, Augenuntersuchungen, Reflexions- und blendungsfreier Bildschirm
 - Als Bildschirmarbeitsplätze gelten dabei praktisch alle mit einem PC ausgestattete Arbeitsplätze, ebenso aber z.B. Arbeitsplätze mit Terminals oder ähnlichen Einrichtungen
- IT-Compliance (im weiteren Sinn): die eingesetzten IT-Systeme müssen den Arbeitsschutzvorschriften entsprechen

- Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)
 - **§ 91 Abs. 2 AktG**: Pflicht der Unternehmensleitung, „geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden“
 - Querschnittsnorm, die allgemein die Pflichten einer Geschäftsleitung spezifiziert
 - ist nach allg. Ansicht jedenfalls sinngemäß auf GmbHen anwendbar
 - über Ausstrahlungswirkung auch auf andere Gesellschaftsformen.
 - Unternehmensleitung muss prüfen, ob ein mangelhaftes IT-System dem Unternehmen erhebliche wirtschaftliche Schäden zufügen kann - Identifizierung „Unternehmenskritischer Systeme“
 - typischerweise: F&A-Systeme, ERP, Logistik, u.U.: Webserver
- IT-Compliance: Unternehmensleitung muss ggfs. Absicherung durch angemessene Vorkehrungen veranlassen, z.B. BKM

- Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)
 - Aufstellung von Regelungen/Geschäftsprozessen z.B. für
 - externe/interne Zugriffe auf Daten, Umgang mit Insiderinformationen
 - Datensicherung, Datenaufbewahrung (*data retention*)
 - Kontinuitätsmanagement/Notfallplanung(*business continuity*)
 - **§ 317 Abs. 4 HGB**: Abschlussprüfer hat das Vorhandensein eines geeigneten Überwachungssystems zu prüfen, sowie den Inhalt dieses Systems und seine Aussagekraft zu beurteilen
 - **§§ 298, 315 HGB**: Pflicht zur Erfassung von Risiken sowie ausgewogene und umfassende Darstellung aller Risiken als Teil des Konzernlageberichts
- IT-Compliance: Nicht (genügende) Beachtung des § 91 Abs. 2 AktG indiziert Pflichtverletzung der Unternehmensleitung

- Ziff. 3.4 Deutschen Corporate Governance Kodex (DCGK)
 - Vorstand muss den Aufsichtsrat über alle für das Unternehmen relevanten Fragen [...] der Geschäftsentwicklung, der Risikolage und des Risikomanagements informieren.
 - § 161 AktG: jährliche Entsprechenserklärung bzgl. der Befolgung des DCGK muss abgegeben werden
- Gesetz zur Unternehmensintegrität und Modernisierung des Anfechtungsrechts (UMAG)
 - erleichtert Durchsetzung von Schadensersatzansprüchen der Gesellschaft gegen Vorstände und Aufsichtsräte
 - § 93 Abs. 1 S. 2 AktG: „Grundlage angemessener Information“
 - Beweislast obliegt dabei Organmitgliedern, die persönlich für die Compliance des Unternehmens einstehen und sie auch nachzuweisen haben (§ 93 Abs. 2 AktG)
- IT-Compliance: IT-Systeme müssen „angemessene“ Informationen liefern, sollten ggfs. Entlastungsnachweis führen können

- **Basel II**
 - „Rating“: zentrales Entscheidungskriterium, ob ein Unternehmen und, wenn ja, zu welchen Konditionen Kredite bekommt
 - Folge: erhöhtes Informationsbedürfnis der Bank ist zu bedienen
 - Unternehmen muss IT-Systeme so einrichten, dass diese die geforderten Informationen bereitstellen können
 - Ermittlung der im Unternehmen vorhandenen Risiken unter dem Gesichtspunkt des sich daraus ergebenden Schuldnerausfallrisikos
 - Erforderlich: geeignetes Berichtswesens/Management Information System (MIS), das frühzeitig Handlungsbedarf erkennen lässt, Eingriffsgrenzen vorsieht
 - Sicherheit der unternehmensbezogenen Daten ist zu gewährleisten. Wurde ausreichende Notfallvorsorge getroffen?
- **IT-Compliance**: „ratingoptimale“ Einrichtung der IT-Systeme und Unternehmensprozesse

- HGB, GoB, GoBS, GDPdU
 - immer mehr Informationen und Dokumente entstehen nur noch in digitaler Form und sind nicht mehr für eine Präsentation in Papierform ausgelegt
 - z.B. elektronische Rechnungen, automatisch erzeugte Massendrucke
 - Datensätze, die durch beschreibende Meta-Daten und Formatinformationen erst zum „Dokument“ werden
 - Buchführungsdaten müssen verbindlich und Gegenstand der Buch- und Steuerprüfung sein können. Aber: elektronisch gespeicherte Daten sind i.d.R. leicht änderbar
- Grundsätze ordnungsmäßiger Buchführung (GoB)
 - **§§ 239, 257 HGB:** regeln die grundsätzlichen Voraussetzungen für die Archivierung von kaufmännischen Dokumenten, unabhängig von der Form
 - **§ 238 Abs. 1 HGB:** elektronische Aufzeichnungsführung muss den GoB genügen

- Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS):
 - von der Finanzverwaltung aufgestellte Regeln zur Buchführung mittels Datenverarbeitungssystemen, Präzisierung der GoB
 - z.B. Behandlung aufbewahrungspflichtiger Daten und Belege in elektronischen Buchführungssystemen
- Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)
 - ergeben sich insbesondere aus § 147 Abs. 6 und § 146 Abs. 5 AO
 - Finanzamt muss auf elektronischem Weg Einsicht in die EDV-Buchführung nehmen können
 - definieren u.a. wie die Außenprüfung des Finanzamts bei einem Betrieb mit EDV-Buchhaltung durchzuführen ist, Anforderungen an Unternehmenssoftware, Schnittstelle zur Prüfungssoftware
- IT-Compliance: IT-Systeme müssen geeignete Schnittstellen haben und vom FA geforderte Daten vorhalten/aufbereiten

- International Financial Reporting Standards (IFRS)
 - internationale Rechnungslegungsvorschriften, umfassen u.a.
 - Standards des International Accounting Standards Board (IASB)
 - International Accounting Standards (IAS) des International Accounting Standards Committee
 - Interpretationen des International Financial Reporting Standards Interpretations Committee (IFRIC) bzw. des ehem. Standing Interpretation Committee (SIC)
 - gelten als nationales Recht in allen EU-Mitgliedsstaaten. Ziel ist die Transparenz und Vergleichbarkeit von Konzernabschlüssen auch über Ländergrenzen hinweg
 - Folge: angepasste F&A-Systeme müssen historische Daten wie Zeitwerte, Leistungen an Arbeitnehmer, Segmentinformationen (IAS 14) berücksichtigen
 - Problem: Anpassung Altsysteme vs. Aufbewahrungspflichten
- IT-Compliance: Anpassung von HGB F&A-Systemen; Fähigkeit, die relativ häufigen Änderungen der IFRS zeitnah abzubilden

- Sarbanes Oxley Act (SOX)
 - Reaktion des US-amerikanischen Gesetzgebers auf spektakuläre Unternehmenszusammenbrüche (Enron, Worldcom). SOX gilt seit Ende 2004 für alle Unternehmen, die an US-Börsen notiert sind
 - betrifft damit auch deren deutsche Tochtergesellschaften und deren Dienstleister, die zukünftig verstärkt auf Einhaltung der SOX Anforderungen geprüft werden
 - SOX regelt vor allem Prüfung der Unternehmensfinanzen, sowie die Pflicht, ein Kontrollsystem für Finanzdaten zu unterhalten
 - begründet indirekt Anforderungen an IT-Systeme, da praktisch alle Finanzdaten heutzutage elektronisch verarbeitet werden
 - insbes. Section 404: Dokumentation und Bewertung von Kontrollmechanismen, die üblicherweise mit Hilfe von IT-Systemen implementiert werden
- IT-Compliance: Anpassung der IT-Systeme und Geschäftsprozesse der betroffenen Unternehmen und Dienstleister

- § 25a KWG (ähnlich: § 33 Abs. 2 WpHG)
 - Regelungen zur Steuerung und Überwachung von Risiken, um die Ordnungsmäßigkeit der Bankgeschäfte und Geschäftsorganisation zu gewährleisten.
 - Abs. 1 Nr. 2: Institute müssen über “angemessene Sicherheitsvorkehrungen für den Einsatz der elektronischen Datenverarbeitung“ verfügen
 - Abs. 2: Regelungen zur Auslagerung von Bereichen auf ein anderes Unternehmen
 - Ziele: Sicherung des bankaufsichtlichen Zugriffs
 - letztlich Absicherung der Aufgabenerfüllung der BaFin: Einlagensicherung
 - Ob und Wie der Einhaltung ist Prüfaufgabe (§ 29 Abs. 1, 2 KWG)
 - § 25a Abs. 1 und 2 KW in zwei Bafin-Rundschreiben konkretisiert:
 - „Auslagerung von Bereichen auf ein anderes Unternehmen gemäß § 25a Abs. 2 KWG“, Rundschreiben 11/2001 v. 6.12.2001 („Outsourcing-Rundschreiben“)
 - „Mindestanforderungen an das Risikomanagement“ („MaRisk“), Rundschreiben 18/2005 v. 20.12.2005
- IT-Compliance: Verträge müssen den RSen genügen. Beachte Anzeigepflicht. Vertragsmanagement bzgl. Subunternehmern

1. Zum Begriff „IT-Compliance“
2. Rechtliche Grundlagen
3. Ausgewählte IT-Compliance Anforderungen
 - Datenschutz und Datensicherheit
 - Arbeitsrecht
 - Unternehmensorganisation
 - Buchhaltung, Rechnungslegung, Prüfung
 - Sektorspezifisch: Banken und Finanzdienstleister
- 4. Adressaten von IT-Compliance Anforderungen**
5. Drohende Sanktionen, Haftungsrisiken
6. Gewährleistung von IT-Compliance
 - insbes. Gewährleistung von IT-Compliance durch Dritte
7. Fazit und Ausblick

- Primär: Unternehmensleitung
 - Grundsatz: Compliance ist wesentliche, nicht delegierbare Aufgabe der Unternehmensleitung
 - insbes. Vorstand, Geschäftsführer, auch wenn tatsächliche Umsetzung durch Mitarbeiter oder Dritte erfolgt
- IT-Compliance: Unternehmensleitung muss sich angemessen mit (IT-)Compliance Anforderungen befassen
- Unternehmensaufsicht
 - insbesondere: Aufsichtsrat, der die dem Vorstand obliegende Geschäftsführung zu überwachen hat, § 111 Abs. 1 AktG
 - Aufsichtsrat der GmbH i.d.R nur, wenn im Anwendungsbereich des MitbestG
 - Tendenz des Gesetzgebers, Rechte und Pflichten zu erweitern
 - (TransPuG, DCGK)
- IT-Compliance: Überwachung, soweit Unternehmensleitung ebenfalls zur Gewährleistung von IT-Compliance verpflichtet ist

- Unternehmensmitarbeiter
 - IT-Compliance als Teil arbeitsvertraglicher Pflichten insbesondere: von leitenden Mitarbeitern
 - z.B. CIO, soweit nicht ohnehin im Vorstand, Administratoren, Revisoren, DSB
 - Zunehmend: Whistleblowing-Problematik, z.B. durch SOX
- IT-Compliance: Weisungen des Arbeitgebers dokumentieren
- Aufsichtsbehörden
 - kontrollieren die Einhaltung des öffentlichen Ordnungsrahmens, z.B. BaFin, DSB samt Behördenunterbau, DS-Aufsicht (§ 38 BDSG)
 - aufgrund der häufigen Verwendung von unbestimmten Rechtsbegriffen in Generalklauseln können sich andere Aufsichtsbehörden zuständig fühlen
 - z.B. § 35 GewO („Unzuverlässigkeit“) => Gewerbeaufsichtsbehörde
- IT-Compliance: Beobachtung (und Beachtung!) der von den Aufsichtsbehörden allgemein ergriffenen Aufsichtsmaßnahmen

- Externe (IT-)Dienstleister
 - viele IT-Compliance Anforderungen adressieren explizit den Fall, dass ein Dritter eingesetzt wird. Häufig steigt dadurch Anzahl und Komplexität der Anforderungen
 - Dienstleister sollte vertraglich zur Wahrung der einschlägigen IT-Compliance Anforderungen verpflichtet werden
 - Häufiger Konflikt: wer beobachtet Änderungen der Compliance Anforderungen und sorgt für erforderliche Anpassungen der Leistungen? Unternehmen ist letztlich der Verpflichtete, Dienstleister hat i.d.R. die bessere Sachkunde
 - Dienstleister muss zur Einhaltung besonderer gesetzlicher Anforderungen verpflichtet werden
 - z.B. Bankenaufsichtsrecht
 - Unternehmen behält Auswahl- und Überwachungspflichten
 - z.B. § 11 BDSG, RS 11/2001: sorgfältige Auswahl/Überwachung des AN
 - Subunternehmer
- IT-Compliance: Unternehmen kann Kontrolle und Steuerung des Dienstleisters i.d.R. nicht delegieren, behält Letztverantwortung

1. Zum Begriff „IT-Compliance“
2. Rechtliche Grundlagen
3. Ausgewählte IT-Compliance Anforderungen
 - Datenschutz und Datensicherheit
 - Arbeitsrecht
 - Unternehmensorganisation
 - Buchhaltung, Rechnungslegung, Prüfung
 - Sektorspezifisch: Banken und Finanzdienstleister
4. Adressaten von IT-Compliance Anforderungen
- 5. Drohende Sanktionen, Haftungsrisiken**
6. Gewährleistung von IT-Compliance
 - insbes. Gewährleistung von IT-Compliance durch Dritte
7. Fazit und Ausblick

- Strafrechtliche Folgen:

- „IT-bezogene“ Straftatbestände im StGB:

- Ausspähen/Unterdrücken von Daten (§ 202a StGB), Besondere Geheimhaltungspflichten (§ 203 StGB), Datenveränderung (§ 303a StGB)

- weitere Straftatbestände z.B. im BDSG, KWG, AktG, HGB

- praktisch aber trotz einiger Aufsehen erregender Fälle eher selten relevant

- Zivilrechtliche Folgen:

- Haftung des Unternehmens

- insbesondere für Erfüllungsgehilfen/Subunternehmer
- aus Organisationsverschulden, auch: Zurechnung eines Mitverschuldens

- unvorhergesehene Kosten

- z.B. Datenherausgabe bei Vertragsende, höhere Refinanzierungskosten

- Haftung der Unternehmensleitung

- bei Pflichtverletzung, z.B. §§ 93 Abs. 2, 116 Abs. 1 AktG

- Haftung von Arbeitnehmern

- Ansprüche des AG bei Pflichtverletzung, fristlose Kündigung

- Öffentlich-rechtliche Sanktionen
 - Haftung nach BDSG
 - Gewerberechtliche Unzuverlässigkeit
 - z.B. Androhung der Gewerbeuntersagung wegen Unzuverlässigkeit
 - Bankaufsichtliche Maßnahmen
 - z.B. § 6 Abs. 3 KWG: Anordnungsbefugnis der BaFin
 - Ausschluss von der Vergabe öffentlicher Aufträge
- Verlust von Versicherungsschutz
 - Verstoß gegen Obliegenheiten kann Verlust des Versicherungsschutzes zur Folge haben
 - Verstoß gegen die Pflicht, den Versicherer über alle bekannte Umstände (lies: die bekannt sein *müssen*), die für den Versicherer von Bedeutung sind, zu informieren.
- IT-Compliance: Sanktionen i.d.R. auch bei Fahrlässigkeit.
Bei Bösgläubigkeit: oft Annahme vorsätzlichen Unterlassens

1. Zum Begriff „IT-Compliance“
3. Rechtliche Grundlagen
3. Ausgewählte IT-Compliance Anforderungen
 - Datenschutz und Datensicherheit
 - Arbeitsrecht
 - Unternehmensorganisation
 - Buchhaltung, Rechnungslegung, Prüfung
 - Sektorspezifisch: Banken und Finanzdienstleister
4. Adressaten von IT-Compliance Anforderungen
5. Drohende Sanktionen, Haftungsrisiken
- 6. Gewährleistung von IT-Compliance**
 - insbes. Gewährleistung von IT-Compliance durch Dritte**
7. Fazit und Ausblick

- Allgemeines:
 - Compliance-Anforderungen sind nicht nur zu erfüllen und die entsprechenden Prozesse zu implementieren, sondern die Erfüllung muss ihrerseits dokumentiert und nachgewiesen werden
 - „Aufklärung“: Unternehmen sollte festlegen, wer konkret für die Ermittlung und Beobachtung der einschlägigen IT-Compliance Anforderungen verantwortlich ist
 - zu beobachten: Einrichtung eines Corporate Compliance Officers (COO)
 - IT-Compliance Anforderungen und IT-Systeme ändern sich ständig, das Unternehmen muss deshalb intern und in Verträgen Änderungsverfahren vorsehen
 - IT-Compliance ist ein Zustand, kein Ziel. Deshalb ist IT-Compliance nur im Wege eines kontinuierlichen Prozesses zu erreichen:
 - Teil des Arbeitsalltags der Adressaten, Teil der Abläufe im Unternehmen
 - Ausgestaltung nach Art und Umfang angemessen im Hinblick auf den Unternehmensgegenstand sowie die Kritikalität und typisches Betriebsrisiko der IT-Systeme

- Bedeutung von Standards

- können bei Umsetzung einzelner Anforderungen hilfreich sein
- sind häufig unter Beteiligung von Praktikern bzw. der jeweiligen Interessengruppen geschrieben, oft mit Handlungsempfehlungen
 - z.B. IT-Organisation = COBIT, ITIL
 - IT-Sicherheit = BS 7799/DIN 17799
 - Business Continuity: PAS 56/BS 25999-1 (2006), 25999-2 (2007)
- Beachtung von Prüfungsstandards (PS) des Institutes der Wirtschaftsprüfung (IDW),
 - z.B. IDW PS-330

- Zertifizierungen

- kein „Beweis“ für IT-Compliance, aber im konkreten Fall Indikator für das Maß der Pflichterfüllung => Erschwerung des Beweises
- sind oft nur stichtagsbezogen, unterschiedliche Schwerpunkte
- erlauben oft keine historische Betrachtung

- Kritisch : Gestaltung des Vertrags mit Dienstleistern
 - klare, umfassende vertragliche Regelung
 - dabei RS 11/2001 und MaRisk nützlich auch für Nicht-KWG Unternehmen
 - Ermittlung und Umsetzung der IT-Compliance Anforderungen
 - häufig umstritten, da zwar Aufgabe der Unternehmensleitung, andererseits Wissensvorsprung des Dienstleisters
 - Wer trägt Risiko der Änderungen von geänderten oder neuen rechtlichen Rahmenbedingungen?
 - u.U. „directed change“: Zwang zur Umsetzung geänderter Compliance-Anforderungen, diskutiert wird nur „Wie“ der Umsetzung/Vergütung, nicht „Ob“
 - Leistungsbeschreibung/Änderungsverfahren
 - Aber: Was ist neu, was Teil des vertraglich vereinbarten Leistungsumfangs?
 - Business continuity bei *Force Majeure* Situationen
 - Anpassung bestehender Konzepte bei Einsatz eines Dienstleisters
- Nach dem Vertragsschluss: Vertragsmanagement
 - Steuerung, Überwachung, Prüfung des Dienstleisters

1. Zum Begriff „IT-Compliance“
2. Rechtliche Grundlagen
3. Ausgewählte IT-Compliance Anforderungen
 - Datenschutz und Datensicherheit
 - Arbeitsrecht
 - Unternehmensorganisation
 - Buchhaltung, Rechnungslegung, Prüfung
 - Sektorspezifisch: Banken und Finanzdienstleister
4. Adressaten von IT-Compliance Anforderungen
5. Drohende Sanktionen, Haftungsrisiken
6. Gewährleistung von IT-Compliance
 - insbes. Gewährleistung von IT-Compliance durch Dritte

7. Fazit und Ausblick

- Fazit:

- Jede Unternehmensleitung muss sich aufgrund der drohenden juristischen und ökonomischen Nachteile mit Fragen der IT-Compliance befassen
- Es gehört zu den ständigen Aufgaben der Unternehmensleitung, die aus den IT-Systemen erwachsenden Risiken für das Unternehmen realistisch einschätzen und die notwendigen Prozesse sowie Kontroll- bzw. Überwachungssysteme einzuführen
- IT-Compliance bedarf einer kontinuierlichen, engen Zusammenarbeit aller technischen und rechtlichen Einheiten des Unternehmens, um eine möglichst umfassende Abdeckung des rechtlich Erforderlichen durch das technisch Machbare zu gewährleisten

- Zunehmende Anzahl von Kooperationen mit Dritten
 - Aufrechterhaltung der (IT-) Compliance erfordert geeignete Steuerungs-/Kontrollprozesse
 - insbes. bei Outsourcing, BPO, JV, *post-merger* Projekten
 - IT-Systeme tragen in immer mehr Fällen die Hauptlast der Umsetzung von Compliance-Anforderungen
 - ein Lösungsansatz z.B. (Re-)Zentralisierungsansätze wie SaaS

- Zunehmende Bedeutung von (IT-)Standards
 - erlauben eine systematische Vorgehensweise und können helfen, mehrere IT-Compliance Anforderungen gleichzeitig abzudecken
 - z.B. im Bereich IT: COBIT, ITIL. Aber: Hilfsmittel, kein Allheilmittel!
 - Einführung von IT-Standards führt zur Konfektionierung von IT-Systemen und damit mittelbar zur Umsetzung von IT-Compliance Anforderungen in berechenbarer Qualität
 - Kunde kann von Dienstleistern mehr (ökonomische) Verantwortung für IT-Compliance einfordern

- Zunehmende Bedeutung von IT-Sicherheit
 - Schutz elektronischer Werte fordert von der Unternehmensleitung in Zukunft eine verstärkte Beschäftigung mit der IT-Sicherheit
- Verstärkte Inanspruchnahme der Unternehmensleitung
 - Immer mehr Haftungstatbestände, Klagemöglichkeiten verbessert.
 - auch deshalb immer wichtiger: D&O Versicherung
 - Aufgabe IT-Compliance kann nicht allein von Rechtsabteilung bewältigt werden
 - Corporate Compliance Officer und CIO zukünftig Mitglied der Geschäftsleitung?
- Zunehmende Regelungs- und Regulierungsdichte
 - Nationale Regelungen haben weltweit Auswirkungen, z.B. SOX
 - zunehmende Zahl öffentlicher Konsultationsverfahren erlauben Beteiligung/zeitnahe Umsetzung, z.B. Banken-/Finanzsektor
 - CEBS CP02 revised (2006), BaFin: Integrierung RS 11/2001 in die MaRisk (2007?), Markets in Financial Instruments Directive (MiFid) (2006/2007)

Fragen

Kontakt:

RA Dr. Lars Lensdorf, RA Udo Steger
Heymann & Partner Rechtsanwälte
Taunusanlage 1, 60329 Frankfurt am Main
Tel. 069-768063-0
www.heylaw.de