

# IT-Compliance

Rechtsanwalt Martin Kuhr, LL.M.

13.04.2010

**RESMEDIA**  
Kanzlei für IT- und Medienrecht

## IT-Compliance

- **oder anders:**
  - wollen Sie:
    - Ihren Gewinn behalten?
    - Nicht strafrechtlich belangt werden?

Rechtsanwalt Martin Kuhr, LL.M.

**RESMEDIA**  
Kanzlei für IT- und Medienrecht

## IT-Compliance

- **Wer steht vor Ihnen?**
  - Rechtsanwalt Martin Kuhr, LL.M.  
(Medienrecht)
  - seit 10 Jahren im IT-Recht
  - Datenschutzbeauftragter (IHK)
  - Mannheim

Rechtsanwalt Martin Kuhr, LL.M.

# IT-Compliance

- **Gliederung**
  - Einleitung
  - Begriff IT-Compliance
  - IT-Security
  - Archivierung
  - E-Mail und Internetnutzung
  - Datenschutz

Rechtsanwalt Martin Kuhr, LL.M.

# IT-Compliance

- **Einleitung**

Rechtsanwalt Martin Kuhr, LL.M.

**RESMEDIA**  
Kanzlei für IT- und Medienrecht

# IT-Compliance

- **Einleitung**

- Gesetzgeber:

- von Unternehmen gehen Gefahren aus

- (Gefahren von/durch Sachen/Produkte)

- (Gefahren durch Menschen)

Rechtsanwalt Martin Kuhr, LL.M.

**RESMEDIA**  
Kanzlei für IT- und Medienrecht

# IT-Compliance

- **Einleitung**

- Gesetzgeber:

- Interesse der Allgemeinheit:

- Schaffung + Aufrechterhaltung einer innerbetrieblichen Organisationsform, mit der den Gefahren begegnet werden kann

Rechtsanwalt Martin Kuhr, LL.M.

# IT-Compliance

- **Einleitung**

- **Corporate Compliance**

- dient der Haftungs- und Strafvermeidung für das Unternehmen und seine Organe

- **Ziel:**

- Schadensprävention durch frühzeitige  
Aufdeckung von Rechtsverletzungen

Rechtsanwalt Martin Kuhr, LL.M.

# IT-Compliance

- **Einleitung**
  - **Compliance Systeme sollen klären:**
    - 1. anzuwendenden Normen/Gesetze**  
**über 10.000 Dokumentationspflichten**  
[www.bundesregierung.de/informationspflichten](http://www.bundesregierung.de/informationspflichten)
    - 2. Fragen der Aufbauorganisation**

Rechtsanwalt Martin Kuhr, LL.M.

**RESMEDIA**  
Kanzlei für IT- und Medienrecht

# IT-Compliance

- **Begriff: Compliance**

Rechtsanwalt Martin Kuhr, LL.M.

**RESMEDIA**  
Kanzlei für IT- und Medienrecht

## IT-Compliance

- **Begriff: Compliance**
  - ursprünglich in Medizin:  
Bereitschaft des Patienten, den Weisungen des Arztes zu folgen

## IT-Compliance

- **Begriff: Compliance**
  - angelsächsischer Raum:  
Wirtschaftsrecht  
**Einhaltung, Befolgung,  
Übereinstimmung,  
Einhaltung bestimmter Gebote**

Rechtsanwalt Martin Kuhr, LL.M.

**RESMEDIA**  
Kanzlei für IT- und Medienrecht

## IT-Compliance

- **Begriff: Compliance**
  - **Einhaltung geltenden Rechts**  
eigentlich selbstverständlich
  - USA: 2002 SOX (Sarbanes-Oxley Act)
  - Basel II

## IT-Compliance

- **Begriff: Compliance**
  - D: § 33 WpHG: Organisationspflichten  
§ 13 Wertpapierdienstleistungs-  
Verhaltens- und OrganisationsVO
  - D: Corporate Governance Kodex

## IT-Compliance

- **Begriff: Compliance**

- D: § 91 Abs. 2 AktG:

- „Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein **Überwachungssystem** einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen **früh erkannt** werden“

Rechtsanwalt Martin Kuhr, LL.M.

## IT-Compliance

- D: § 93 Abs. 1 S. 2 AktG:

„Eine Pflichtverletzung liegt nicht vor, wenn das Vorstandsmitglied bei einer unternehmerischen Entscheidung **vernünftigerweise** annehmen durfte, auf der Grundlage angemessener Informationen zum Wohle der Gesellschaft zu handeln“

Rechtsanwalt Martin Kuhr, LL.M.

**RESMEDIA**  
Kanzlei für IT- und Medienrecht

# IT-Compliance

- gilt auch bei GmbH

Rechtsanwalt Martin Kuhr, LL.M.

**RESMEDIA**  
Kanzlei für IT- und Medienrecht

## IT-Compliance

- D: § 130 OWIG:

„Wer als Inhaber eines Betriebs oder Unternehmens vorsätzlich oder fahrlässig die **Aufsichtsmaßnahmen unterlässt**, die erforderlich sind, u in dem Betrieb oder Unternehmen Zuwiderhandlungen gegen Pflichten zu verhindern...“

# IT-Compliance

- **Begriff: IT-Compliance**

Rechtsanwalt Martin Kuhr, LL.M.

**RESMEDIA**  
Kanzlei für IT- und Medienrecht

# IT-Compliance

- **Begriff: IT-Compliance**
  - dient der Einhaltung der gesetzlichen und anderweitig zugesagten Regeln im Bereich der IT.
  - IT-Systeme betreffend

Rechtsanwalt Martin Kuhr, LL.M.

**RESMEDIA**  
Kanzlei für IT- und Medienrecht

## IT-Compliance

- **Begriff: IT-Compliance**
  - **IT-Security**
  - **elektronische Archivierung**
  - **Informations- u. Kontrollsystem**
  - **Einhaltung von Datenschutz**
  - **Einhaltung der Datensicherheit**
  - **Kontrolle IT-Nutzung Mitarbeiter**

Rechtsanwalt Martin Kuhr, LL.M.

# IT-Compliance

- **IT-Security**

Rechtsanwalt Martin Kuhr, LL.M.

**RESMEDIA**  
Kanzlei für IT- und Medienrecht

## IT-Compliance

- **IT-Security**

Verpflichtung zu angemessenem

Risikomanagement bzgl. IT-Systemen

IT-Systeme gegen Angriffe von innen und  
außen sichern

Rechtsanwalt Martin Kuhr, LL.M.

**RESMEDIA**  
Kanzlei für IT- und Medienrecht

# IT-Compliance

- **IT-Security**

## **§ 2 Abs. 2 BSIG**

„Sicherheit in der Informationstechnik im Sinne dieses Gesetzes bedeutet die **Einhaltung bestimmter Sicherheitsstandards**, die die **Verfügbarkeit, Unversehrtheit** oder **Vertraulichkeit** von Informationen betreffen, durch Sicherheitsvorkehrungen“

Rechtsanwalt Martin Kuhr, LL.M.

**RESMEDIA**  
Kanzlei für IT- und Medienrecht

## IT-Compliance

- **IT-Security**

Haftung des Vorstands § 93 Abs. 2 AktG

Rechtsanwalt Martin Kuhr, LL.M.

**RESMEDIA**  
Kanzlei für IT- und Medienrecht

## IT-Compliance

- **IT-Security**
  - **gibt es im Unternehmen:**
    - für IT aktuelles Sicherheitskonzept?
    - automatisiertes Backup?
    - Plan für Recovery Maßnahmen?

## IT-Compliance

- **IT-Security**
    - „IT-Grundschutz“ des BSI
      - **IT-Sicherheitsmaßnahmen** gem. Stand der Technik
      - **IT-Grundschutz-Vorgehensweise** des BSI
- zusammen= Maßnahmen+Methodik**

Rechtsanwalt Martin Kuhr, LL.M.

**RESMEDIA**  
Kanzlei für IT- und Medienrecht

## IT-Compliance

- **IT-Security**
  - **gibt es im Unternehmen:**
    - definierte Rollenverteilung für Nutzung der IT einschließlich Festlegung von Lese-, Lösch- und Editierberechtigungen?
    - Funktionstrennung

Rechtsanwalt Martin Kuhr, LL.M.

## IT-Compliance

- **IT-Security**
  - **gibt es im Unternehmen:**
    - effektive Spam-Abwehr?
    - aktuellen Virens Scanner?
    - effektive Firewalls?
  - beachten: Remotezugriff via DSL,  
Hotspot, PDA

Rechtsanwalt Martin Kuhr, LL.M.

# IT-Compliance

- **Archivierung**

Rechtsanwalt Martin Kuhr, LL.M.

**RESMEDIA**  
Kanzlei für IT- und Medienrecht

## IT-Compliance

- **Archivierung**
  - **gibt es im Unternehmen:**
    - Archivierungskonzept, welches Einhaltung der Aufbewahrungsfristen sichert?

## IT-Compliance

- **Archivierung- Archivierungskonzept**
  - § 257 HGB, § 147 AO
  - abgesendete/empfangene Handels- und Geschäftsbriefe
    - Aufbewahrungsfrist 6 Jahre
  - Buchungsbelege, Jahresabschlüsse, etc.
    - Aufbewahrungsfrist bis 10 Jahre

## IT-Compliance

- **Archivierung- Archivierungskonzept**
  - § 257 HGB, § 147 AO
  - betrifft auch E-Mails im Zusammenhang mit Vorbereitung/Abschluss/  
Durchführung des Handelsgeschäfts  
i.S.v. § 343 HGB

## IT-Compliance

- **Archivierung- Archivierungskonzept**
  - §§ 239 Abs. 4, 257 Abs. 3 HGB
  - „Geschäftsbriefe“ (auch Mail+Anhang)  
können auf elektron. Datenträgern  
aufbewahrt werden, wenn entsprechend:  
Grundsätzen der ordnungsgemäßen  
Buchführung (**GOB**) und

## IT-Compliance

- **Archivierung- Archivierungskonzept**  
Grundsätzen der ordnungsgemäßen  
DV-gestützten Buchführungssysteme  
(**GoBS**)

Rechtsanwalt Martin Kuhr, LL.M.

**RESMEDIA**  
Kanzlei für IT- und Medienrecht

## IT-Compliance

- **Archivierung- Archivierungskonzept**
  - Sicherstellen: **Revisionssicherheit**  
Übereinstimmung Daten mit Originalen;  
in Aufbewahrungsfrist verfügbar/lesbar
  - **Unveränderbarkeit der Dokumente**  
**muss gewährleistet sein**

Rechtsanwalt Martin Kuhr, LL.M.

**RESMEDIA**  
Kanzlei für IT- und Medienrecht

# IT-Compliance

- **Archivierung**
  - **gibt es im Unternehmen:**
    - Revisionssicherheit und GDPdU-Konformität des Archivsystems?

## IT-Compliance

- **Archivierung**
  - **GDPdU** (Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen) 2001 zur Konkretisierung der GoBS
  - steuerrelevante Unterlagen (Finanz-, Anlagen-, Lohnbuchhaltung) maschinell auswertbar vorlegen

Rechtsanwalt Martin Kuhr, LL.M.

## IT-Compliance

- **Archivierung**
  - **P: Frage der „Steuerrelevanz“**
  - keine steuerliche Auswirkung nötig
  - Katalog des BMF: auch eingescannte  
Unterlagen= originäre digitale Unterlagen
  - E-Mails sind im Originalformat zu  
speichern

Rechtsanwalt Martin Kuhr, LL.M.

## IT-Compliance

- **Archivierung**
  - Verwendung von Langzeitformaten:  
TIFF-G4 und PDF/A  
und  
proprietäre Originalformate
  - JPEG für farbige Vorlagen

## IT-Compliance

- **Archivierung**
  - **gibt es im Unternehmen:**
    - Sicherstellung des automatisierten Zugriffs auf unternehmensrelevante Informationen?  
z. B. durch Archivierung der Infos in ECM- oder DMS- System?

# IT-Compliance

- **Archivierung**

- Entschlüsselung muss während Aufbewahrungsfrist jederzeit möglich sein

# IT-Compliance

- **E-Mail und Internetnutzung**

Rechtsanwalt Martin Kuhr, LL.M.

**RESMEDIA**  
Kanzlei für IT- und Medienrecht

## IT-Compliance

- **E-Mail und Internetnutzung**
  - wird vom Arbeitgeber private Nutzung von IT durch Mitarbeiter erlaubt?
  - „Mischnutzung“: Fernmeldegeheimnis
  - Kündigung wegen privater Nutzung?

Rechtsanwalt Martin Kuhr, LL.M.

**RESMEDIA**  
Kanzlei für IT- und Medienrecht

## IT-Compliance

- **E-Mail und Internetnutzung**
  - gibt es IT-Richtlinie bzw. E-Mail-Policy sowie konkrete Vorgaben zum Umfang der privaten Nutzung?

Rechtsanwalt Martin Kuhr, LL.M.

**RESMEDIA**  
Kanzlei für IT- und Medienrecht

## IT-Compliance

- **E-Mail und Internetnutzung**
  - „Betreffzeile“
  - funktionsbezogen „vertrieb@firma.de“
  - „Access Delegation“: Krankheit, Urlaub
  - automatische Filterung?

P: § 88 TKG, §§ 202a, 206 StGB

# IT-Compliance

- **Datenschutz**

Rechtsanwalt Martin Kuhr, LL.M.

**RESMEDIA**  
Kanzlei für IT- und Medienrecht

## IT-Compliance

- **Datenschutz**

- gibt es unabhängigen Datenschutzbeauftragten?

Datenschutzbeauftragter, wenn mind.  
10 Personen ständig automatisiert  
mit Verarbeitung personenbezogener  
Daten beschäftigt

Rechtsanwalt Martin Kuhr, LL.M.

# IT-Compliance

- **Datenschutz**
  - Verfahrensübersicht § 4e BDSG

Rechtsanwalt Martin Kuhr, LL.M.

**RESMEDIA**  
Kanzlei für IT- und Medienrecht

## IT-Compliance

- **Datenschutz Verfahrensübersicht § 4e BDSG**
  1. Name oder Firma der verantwortlichen Stelle,
  2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
  3. Anschrift der verantwortlichen Stelle,

Rechtsanwalt Martin Kuhr, LL.M.

## IT-Compliance

- **Datenschutz Verfahrensübersicht § 4e BDSG**

4. Zweckbestimmungen der Datenerhebung,  
-verarbeitung oder -nutzung,
5. eine Beschreibung der betroffenen  
Personengruppen und der  
diesbezüglichen Daten oder Datenkategorien,
6. Empfänger oder Kategorien von Empfängern,  
denen die Daten mitgeteilt werden können,

Rechtsanwalt Martin Kuhr, LL.M.

## IT-Compliance

- **Datenschutz Verfahrensübersicht § 4e BDSG**
  7. Regelfristen für die Löschung der Daten,
  8. eine geplante Datenübermittlung in Drittstaaten

Rechtsanwalt Martin Kuhr, LL.M.

**RESMEDIA**  
Kanzlei für IT- und Medienrecht

## IT-Compliance

- **Datenschutz**
  - werden die „**8 goldenen Regeln**“ des Datenschutzes eingehalten?
  - Anlage zu § 9 BDSG

## IT-Compliance

- **Datenschutz- „8 goldene Regeln“**
  - Zutrittskontrolle (gesicherte Räumlichkeit)
  - Zugangskontrolle (Zugang zum EDV-System)
  - Zugriffskontrolle (Zugriff auf Daten)
  - Weitergabekontrolle (Weitergabe)
  - Verfügbarkeitskontrolle (zufällige Zerstörung)
  - Trennungsgebot (zweckgebundene Verarbeitung)
  - Eingabekontrolle (revisionssichere Protokollierung)
  - **Auftragskontrolle** (Weisung des Auftraggebers)

Rechtsanwalt Martin Kuhr, LL.M.

## IT-Compliance

- **Datenschutz**
  - gibt es Datenschutzpolicy auf Webseite?

Rechtsanwalt Martin Kuhr, LL.M.

**RESMEDIA**  
Kanzlei für IT- und Medienrecht

## IT-Compliance

- **Datenschutz**

- **warum Datenschutz beachten?**

- Verstoß gegen § 11 II 2 oder 4 BDSG:

- Bußgeld bis zu **50.000 Euro oder mehr**

- (wirtschaftl. Gewinn) § 43 III BDSG

## IT-Compliance

- **Datenschutz**
  - **Auftragsdatenverarbeitung** nur, wenn:
    - Verarbeiter der Daten streng weisungsgebunden
    - keinen eigenen Bewertungs- u. Entscheidungsspielraum

## IT-Compliance

- **BDSG seit 01.09.2009: § 11 Auftrag schriftlich erteilen**
  - Gegenstand und Dauer des Auftrags
  - Umfang, Art und Zweck der geplanten Datenverarbeitung
  - erforderl. techn. u. organ. Maßnahmen
  - Kontrollrechte/Weisungsrechte des AG
  - Mitwirkungspflichten des AN

Rechtsanwalt Martin Kuhr, LL.M.

## IT-Compliance

- **BDSG seit 01.09.2009: § 11 Auftrag schriftlich erteilen**
  - Pflichten nicht abschließend geregelt
  - unbestimmt formuliert
    - „die von ihm vorzunehmenden Kontrollen“
  - ordnungswidrig handelt, wer:
    - „einen Auftrag nicht vollständig erteilt“

## IT-Compliance

- **BDSG**
  - **Wenn keine Auftragsdatenverarbeitung:**
  - Rechtfertigung gem. § 28 I 1 Nr 2 BDSG  
möglich:  
wie Outsourcing: Interessenabwägung

# IT-Compliance

- **Fazit: IT-Compliance**
  - IT wird zum Enabler für Compliance
  - IT-Abteilung wird zum Kernbereich eines Unternehmens

Rechtsanwalt Martin Kuhr, LL.M.

**RESMEDIA**  
Kanzlei für IT- und Medienrecht

# IT-Compliance

- **Fazit: IT-Compliance**
  - IT dient der Sicherstellung der regulatorischen und geschäftlichen Anforderungen nach:
    - Schutz, Verfügbarkeit
    - Nachvollziehbarkeit, Transparenz
    - Sorgfalt

# IT-Compliance

- **Fazit: IT-Compliance**

- IT kann die regulatorischen und geschäftlichen Anforderungen erfüllen durch:
  - Informationsschutz, Risikomanagement
  - Informationsmanagement
  - Internes Kontrollsystem
  - Mitwirkungs- u. Informationspflichten

Rechtsanwalt Martin Kuhr, LL.M.

**RESMEDIA**  
Kanzlei für IT- und Medienrecht

# IT-Compliance

- **Fazit: IT-Compliance**

- IT-Compliance kann bewirken:
  - Kalkulieren und Reduzieren von IT-Risiken
  - Vermeiden von Betrugsfällen
  - Steigerung der Effizienz
  - Steigerung der Transparenz

## IT-Compliance

- **Checkliste**
  - IT-Security
  - Archivierung
  - E-Mail und Internetnutzung
  - Datenschutz

Rechtsanwalt Martin Kuhr, LL.M.

# Vielen Dank für Ihre Aufmerksamkeit

---

Rechtsanwalt Martin Kuhr, LL.M.

www: [onlinerechtlich.de](http://onlinerechtlich.de)

Twitter: [itundrecht](https://twitter.com/itundrecht)

Mail: [mku@res-media.net](mailto:mku@res-media.net)

www: [res-media.net](http://res-media.net)

Kanzlei RES MEDIA, Kanzlei für IT- und Medienrecht

E 2/1-3, 68159 Mannheim

---