GÖRG

GÖRG Partnerschaft von Rechtsanwälten

München

Berlin ▪ Essen ▪ Frankfurt/M. ▪ Köln ▪ München

GÖRG – Wir beraten Unternehmer.

GÖRG

Unternehmerfrühstück 18. Februar 2009
C o m p l i a n c e

IT - Compliance

Rechtliche Aspekte von IT im Unternehmen

GÖRG

Woher stammen die Anforderungen an IT - Compliance

Die Anforderungen stammen sowohl aus allgemeinen wie spezialgesetzlichen Anforderungen, z.B.:

- § 238, 239 HGB (Buchführung)
- Gesellschaftsrecht
  - § 91, 93 AktG,
  - § 43 GmbHG
  - SOX, BilMoG
- Banken und Versicherungen
  - § 25a KWG
  - § 64a VAG
  - Basel II
  - Solvency II
- Telekommunikationsbranche
  - TKG
  - TMG Telemediengesetz
- Arbeitsrechtliche Schutzvorschriften
  - BDSG
  - Bildschirmarbeitsplätze

Was ist IT – Compliance (1)

Die Übereinstimmung der IT-Landschaft selbst sowie der durch sie unterstützten Prozesse und Verfahren mit gesetzlichen Vorschriften, Normen, Standards, z.B.

- Buchhaltung
  - GoBS
  - GdPdU (**G**rundsätze zum **D**atenzugriff und zur **P**rüfbarkeit **d**igitaler **U**nterlagen)
  - IDW-Standards (z.B. Prüfungsgrundsätze für IT-Systeme IDW 300)
- IT-Sicherheit und Umfeld
  - BSI-Grundschutzhandbuch
  - ISO 27002 für Sicherheit und Umfeld
  - MaRisk (Mindestanforderungen an das Risikomanagement
  - MaRisk VA
- Outsourcing + IT-Prozesse
  - ITIL V3
  - ISO 20.0000

Was ist IT – Compliance (2)

- Laufende IT-Projekte und QM
  - DIN 9001-2000
  - DIN 69901 ff
- Internet + eMail am Arbeitsplatz
  - Arbeitsplatzrichtlinie
  - Archivierung von eMails
  - Filterung von Mails, SPAM
  - Protokollierung von Mail- und Internetverkehr
- Sicherheit von Anwendungen
  - Rechte an den Programmen und Systemen (z.B. Internetauftritt, Onlineplattform, Bildern usw.)
  - Bearbeitungsmöglichkeiten
  - Zugriffsmöglichkeiten auf Quellcode / Quellcodehinterlegung

Grundsatz „Ordnungsmäßigkeit“ (am Beispiel Buchhaltung)

- Vollständigkeitsgrundsatz
- Richtigkeit
- Zeitgerechtigkeit
- Ordnungsgrundsatz
- Nachvollziehbarkeit
- Unveränderlichkeit
- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Autorisierung
- Authentizität

GÖRG

Managementgrundsatz (am Beispiel KWG)

Alle Geschäftsleiter (§ 1 Abs. 2 KWG) sind, unabhängig von der internen Zuständigkeitsregelung, für die ordnungsgemäße Geschäftsorganisation und deren Weiterentwicklung verantwortlich. Diese Verantwortung bezieht sich unter Berücksichtigung ausgelagerter Aktivitäten und Prozesse auf alle wesentlichen Elemente des Risikomanagements. Die Geschäftsleiter werden dieser Verantwortung nur gerecht, wenn das Risikomanagement ihnen ermöglicht, die Risiken zu beurteilen und die erforderlichen Maßnahmen zu ihrer Begrenzung zu treffen.

GÖRG

Technischer Grundsatz (am Beispiel MaRisk, 7.2)

- Umfang und Qualität der technisch-organisatorischen Ausstattung haben sich insbesondere an betriebsinternen Erfordernissen, den Geschäftsaktivitäten sowie der Risikosituation zu orientieren.
- Die IT-Systeme (Hardware- und Software-Komponenten) und die zugehörigen IT-Prozesse müssen die Integrität, die Verfügbarkeit, die Authentizität sowie die Vertraulichkeit der Daten sicherstellen. Für diese Zwecke ist bei der Ausgestaltung der IT-Systeme und der zugehörigen IT-Prozesse grundsätzlich auf gängige Standards abzustellen. Ihre Eignung ist regelmäßig von den fachlich und technisch zuständigen Mitarbeitern zu überprüfen.
- Die IT-Systeme sind vor ihrem erstmaligen Einsatz und nach wesentlichen Veränderungen zu testen und von den fachlich sowie auch von den technisch zuständigen Mitarbeitern abzunehmen. Produktions- und Testumgebung sind dabei grundsätzlich voneinander zu trennen.

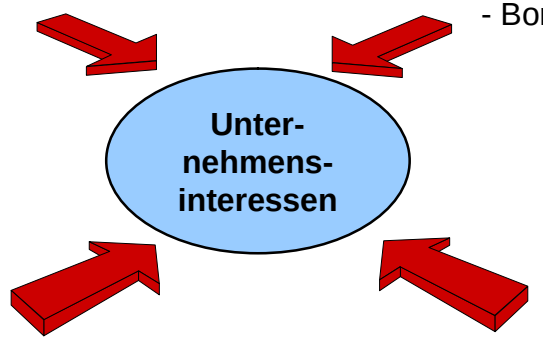
IT-Sicherheit als Compliancekriterium
Risiken für das Unternehmen

Technische Risiken

- Überlastung der Server und Netzwerke
- Daten- und Anwendungssicherheit
- Verfügbarkeit,
- Vertraulichkeit, Integrität

Finanzielle Risiken

- Produktivitätsverluste
- Kostensteigerungen
- verlorene Arbeitszeit
- Schadenersatz an Mitarbeiter oder Dritte
- Bonitätsminderung



Rechtliche Risiken:

Wer steht in der rechtlichen Verantwortung?

Rechtlich geschützte Interessen

- geschützte Personendaten
- IT-System als Ganzes

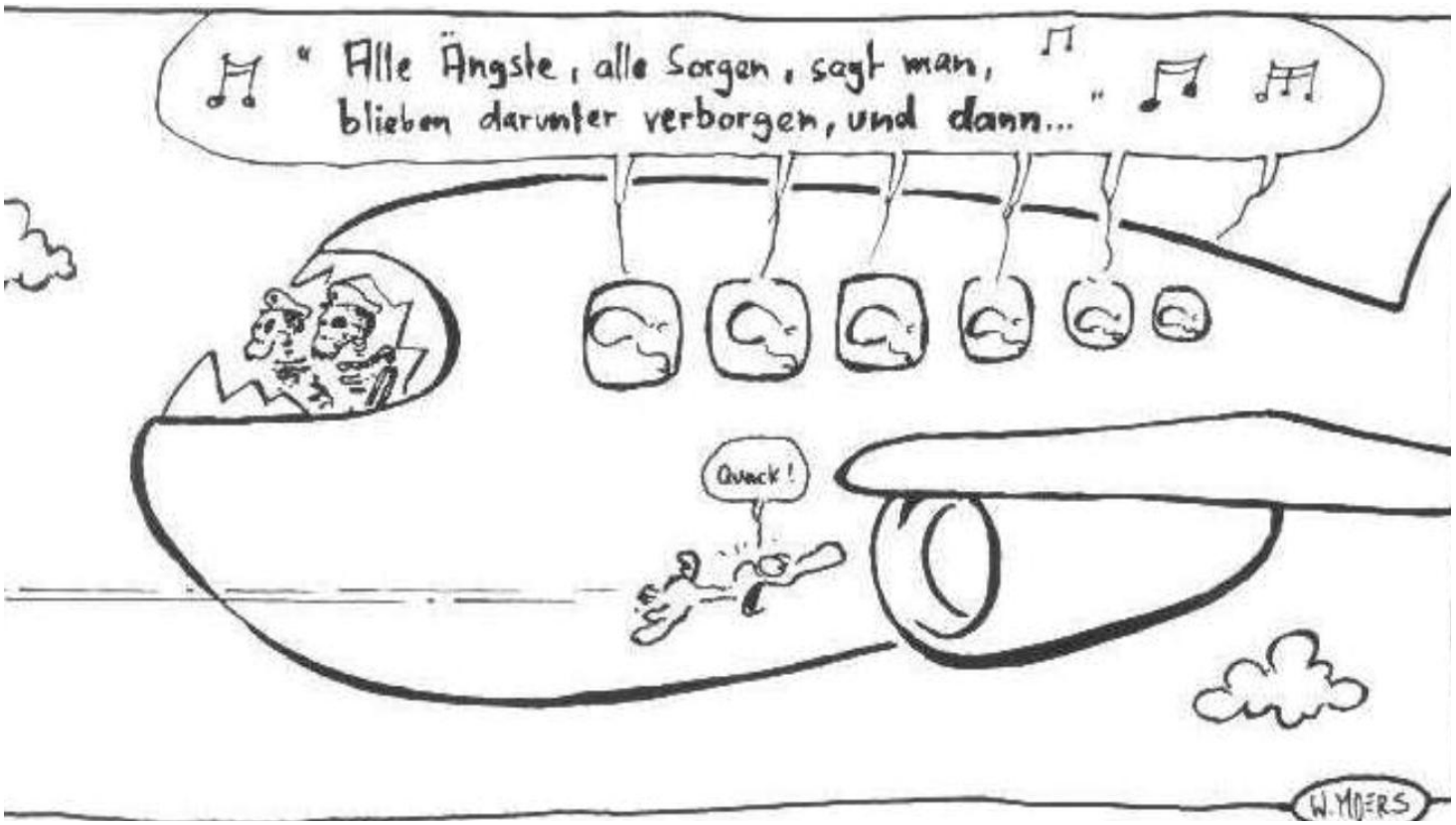
(Computerkriminalität)

- Eingriff in den „Gewerbebetrieb“
- Geschäftsgeheimnisse
- Image / Ruf des Unternehmens

GÖRG

IT - Sicherheit

Nur ca. 35% aller Unternehmer betrachten IT-Sicherheit als sehr wichtiges Thema für das Unternehmen



GÖRG

Datenschutz und Datensicherheit

Angeklagt,

weil er sich Daten stehlen ließ.

GÖRG

Das Management (Organe)

Delegation ist zulässig

- Gewissenhafte Auswahl des Verantwortlichen
- Sorgfältige Überwachung
- Einrichtung eines klaren Berichts- und Entscheidungsprozesses
- IT-Sicherheitsmanual und DS-Manual
- Vordefinierte Notfallpläne
- **Und wenn nicht?**

GÖRG

IT-Compliance ist Chefsache

- Er hatte die Compliance des Unternehmens im Sinn
- Er hatte einen exzellenten Datenschutzbeauftragten
- Er nutzte alle technischen Möglichkeiten
- Er delegierte an den DSB
- Wie kontrollierte er?
- Wie lies er sich berichten?
- Prüfte er die rechtliche Zulässigkeit?
- Er rechtfertigt die Maßnahmen in der Öffentlichkeit!
- Er ist in der rechtlichen Verantwortung!

GÖRG

www.goerg.de

KONTAKT

GÖRG Partnerschaft von Rechtsanwälten

Büro München

Dr. Axel Czarnetzki LL.M.

Prinzregentenstraße 22

D-80538 München

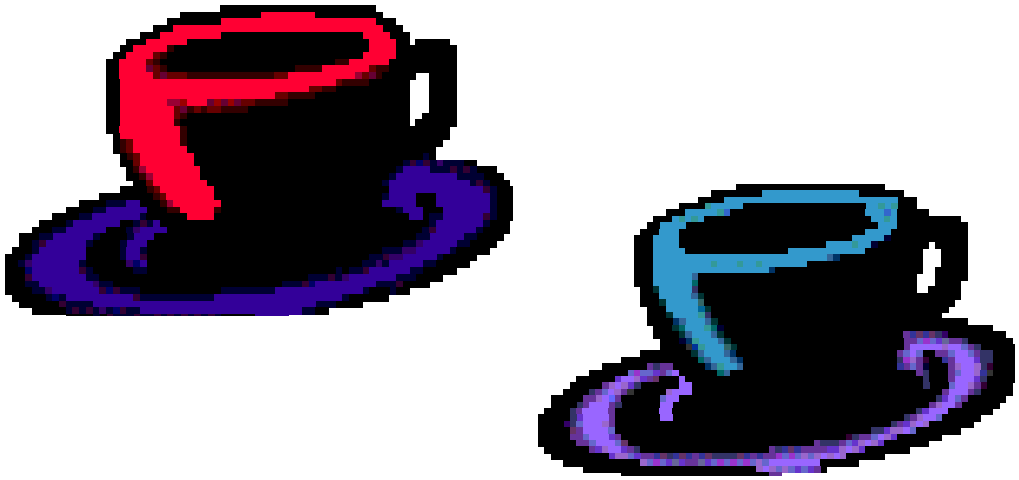
Tel. +49-89-30 90 667-0

Fax + 49-89-30 90 667-90

aczarnetzki@goerg.de

GÖRG

FRÜHSTÜCK & FRAGEN



Dr. Axel Czarnetzki, GÖRG