Mittelstandsdialog Informationssicherheit 6. Mai 2010

Identity Management und Gesetz: Spannungsfeld Compliance <-> Datenschutz

RA Dr. Michael Karger
Wendler Tremml Rechtsanwälte, München

NIFIS e.V.

- Nationale Initiative für Internet- und Informations-Sicherheit
- Selbsthilfeorganisation der Wirtschaft, um Unternehmen im Kampf gegen die wachsenden Gefahren aus dem Internet technisch, organisatorisch und rechtlich zu stärken
- Derzeit 46 Mitglieder aus der ganzen Republik
- Mitglieder sowohl Anbieter als auch Anwender von IT-Sicherheit

Rechtsanwalt Dr. Michael Karger

- Partner Wendler Tremml Rechtsanwälte München
- www.law-wt.de // MKarger@law-wt.de
- Fachanwalt für Informationstechnologierecht und Verwaltungsrecht
- Beratung im IT-Recht (Projekte, Outsourcing, Web 2.0) und Datenschutzrecht (auch externer Datenschutzbeauftragter)
- **Beck-Blog IT-Recht:** http://blog.beck.de/category/it-recht

Überblick:

1. Compliance
2. Datenschutzrecht
3. Allgemeine Anforderungen an datenschutzkonforme Systeme und IM
4. Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Compliance-Kontext
5. Sonderthema: Maßnahmen zur Aufdeckung von Straftaten von Beschäftigten
6. Fazit

Um was geht es ?

- Compliance / Risikomanagement:
  - Maximal mögliche Kontrolle aller Unternehmensvorgänge und
  - maximal verfügbare Information über Mitarbeiter, Kunden, Geschäftspartner wünschenswert

contra

- Datenschutzrecht
  - Nutzung personenbezogener Daten nur in Grenzen zulässig
  - Persönlichkeitsrechte des Einzelnen sind zu wahren
  - Setzt Compliance-Maßnahmen deutliche Grenzen

-> Konflikt zwischen rechtlichem Müssen und rechtlichem Dürfen ?

Compliance

Aktuell: “Compliance-Skandale”

- Betroffene Unternehmen u.a.:
  - Deutsche Bahn, MAN,
  - Bosch, Siemens, Lidl
- Themen u.a.:
  - Bestechungszahlungen
  - Ausforschen von Mitarbeitern
  - Weitergabe vertraulicher Daten
  - Kartellabsprachen
  - Verletzung Arbeitsschutzvorschriften
  - Überhöhte Rechnungen

Aktuell: Compliance-Urteil des BGH

- Urteil vom 17.07.2009 (5 StR 394/08)
- **Compliance-Beauftragter** (Leiter der Rechtsabteilung und der Innenrevision) …
- hat trotz Kenntnis überhöhte Abrechnungen nicht verhindert …
- ist verantwortlich als “Garant” für Rechtskonformität …
- ist wegen Beihilfe zum Betrug **strafbar**

-> Untätigkeit ist keine Option !

Was bedeutet “Compliance”?

- Unternehmen muss sich **rechtskonform** verhalten
- Begriff seit ca. 20 Jahren in Gebrauch
- „Compliance“:
  - Blickwinkel des Unternehmens (Normadressat)
- „Corporate Governance“:
  - Blickwinkel des Regulierers (Normgeber)

Compliance -> IT-Sicherheit -> Identitätsmanagement

1. Compliance: Rechtskonformität
2. Rechtsverstöße = Haftung = wirtschaftliches Risiko
3. Risikomanagement: Vermeidung von Haftungsrisiken durch vorbeugende Unternehmensorganisation
4. IT ist zentrales Element der Unternehmensorganisation
5. IT-Sicherheit ist bedeutender Aspekt des Risikomanagements
6. Identitätsmanagement ist (auch) ein Aspekt der IT-Sicherheit (z.B. Berechtigungskonzepte)

Rechtliche Grundlagen für Organisationspflichten (zB)

- Strafrecht:
  - Keine ausdrückliche Pflicht, aber Organe können aus "Garantenstellung" wegen Beihilfe strafbar sein
- Ordnungswidrigkeitenrecht
  - § 130 OWiG
- Gesellschaftsrecht
  - § 91 II AktG
  - § 93 I AktG
  - Grundsätze gelten auch für die GmbH (§ 43 GmbHG)

§ 130 Ordnungswidrigkeitengesetz

(1) Wer als Inhaber eines Betriebes oder Unternehmens vorsätzlich oder fahrlässig die Aufsichtsmaßnahmen unterläßt, die erforderlich sind, um in dem Betrieb oder Unternehmen Zuwiderhandlungen gegen Pflichten zu verhindern, die den Inhaber treffen und deren Verletzung mit Strafe oder Geldbuße bedroht ist, handelt ordnungswidrig, wenn eine solche Zuwiderhandlung begangen wird, die durch gehörige Aufsicht verhindert oder wesentlich erschwert worden wäre. Zu den erforderlichen Aufsichtsmaßnahmen gehören auch die Bestellung, sorgfältige Auswahl und Überwachung von Aufsichtspersonen. (…)

(3) Die Ordnungswidrigkeit kann, wenn die Pflichtverletzung mit Strafe bedroht ist, mit einer Geldbuße bis zu einer Million Euro geahndet werden. (…).

§§ 91, 93 Aktiengesetz

§ 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."

§ 93 Abs. 2 AktG:

> "Vorstandsmitglieder, die ihre Pflichten verletzen, sind der Gesellschaft zum Ersatz des daraus entstehenden Schadens (…) verpflichtet. Ist streitig, ob sie die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters angewandt haben, so trifft sie die Beweislast."

Compliance: Themen mit Relevanz für IT-Sicherheit und Identitätsmanagement und Datenschutz, z.B.

- Verhinderung von Straftaten durch Mitarbeiter
- Korruptionsbekämpfung
- Überwachung von E-Mail- und Internet-Nutzung der Mitarbeiter
- Schutz von Betriebs- und Geschäftsgeheimnissen
- Verhinderung von Straftaten durch Kunden/Nutzer im Online-Bereich (z.B. Online-Plattformen)

Datenschutzrecht

Datenschutzrecht

- schützt alle in den Systemen erfassten **personenbezogenen** Daten
- „Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person“
- insbesondere Daten von Mitarbeitern und Kunden
- regelt die Zulässigkeit von
  - Erheben
  - Speichern, Verändern, Übermitteln
  - Sperren, Löschen
  - Nutzen
- Bundesdatenschutzgesetz // Telemediengesetz (Online)

Aktuelle Verschärfungen im BDSG 2009:

- §3a: Zwang zur Anonymisierung und Pseudonymisierung von Daten
- § 11: Auftragsdatenverarbeitung
- § 32: Daten von Beschäftigten

Aktuelle Verschärfungen im BDSG 2009:

- § 38: Befugnisse der Aufsichtsbehörde
- § 42a: Informationspflicht bei unrechtmäßiger Kenntniserlangung Dritter („Data Breach“)
  - Sensible Daten
  - Bank-, Kreditkartendaten
- § 43: Bußgelder bis 300.000 € und darüber hinaus

Höheres Gewicht Datenschutz durch Rechtsprechung

- Entscheidungen des Bundesverfassungsgerichts
  - „Bundestrojaner“ (BKA-Gesetz)
  - Vorratsdatenspeicherung
- Haben auch Auswirkungen auf den privatwirtschaftlichen Bereich

Allgemeine Anforderungen

an datenschutzrechtskonforme Systeme

und Identitätsmanagement

Allgemeine datenschutzrechtliche Anforderungen an Systeme und Identitätsmanagement

1. Differenzierung nach Art und Schutzgrad der Daten im System muss möglich sein:
   a) Nicht personenbezogene Daten
   b) Personenbezogene Daten
   c) Besondere Arten personenbezogener Daten
      - Ethnische Herkunft, politische Meinungen, religiöse Überzeugung, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben

Allgemeine datenschutzrechtliche Anforderungen an Systeme und Identitätsmanagement

2. Vorkehrungen zur Datenvermeidung (§ 3a)

- Auswahl System am Ziel auszurichten, so wenig wie möglich Daten zu erheben, zu speichern oder zu nutzen
- Daten sind nach Möglichkeit zu anonymisieren oder pseudonymisieren

Allgemeine datenschutzrechtliche Anforderungen an Systeme und Identitätsmanagement

3. Berichtigung, Löschung und Sperrung (§ 35 BDSG)

- Unrichtige Daten müssen berichtigt werden können
- Datenlöschung erforderlich, wenn Zweck entfallen
- Sperrung statt Löschung, wenn z.B. gesetzliche Aufbewahrungsfristen (AO, HGB: 10 Jahre) zu beachten
- Löschung und Sperrung oft in „Data Retention Policy“ geregelt

Allgemeine datenschutzrechtliche Anforderungen an Systeme und Identitätsmanagement

4. Technische und organisatorische Maßnahmen (§ 9)
   - Erforderliche Maßnahmen (kein unverhältnismäßiger Aufwand)
   - Zugangskontrolle
   - Zugriffskontrolle
   - Weitergabekontrolle
   - Eingabekontrolle
   - Auftragskontrolle
   - Verfügbarkeitskontrolle

Realisierung: Übergreifendes Projekt

1. IT-Leitung
2. Security-Beauftragter
3. Compliance-Beauftragter
4. Datenschutzbeauftragter
5. Wirtschaftprüfer
6. Rechtsabteilung
7. Unternehmensleitung
8. Betriebsrat

Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Compliance-Kontext

Datennutzung im Compliance-Kontext

- nicht bereits zulässig, nur weil es um „Compliance“ geht
- Zulässig, wenn ausdrückliche **Einwilligung** des Betroffenen
- Zulässig, wenn **Erlaubnis** in Datenschutzgesetzen
  - § 28 Abs. 1 Nr. 1 und Nr. 2 BDSG
  - § 32 BDSG (nur für Beschäftigte)
- Bzgl. Arbeitnehmern teilweise dann zulässig, wenn von **Betriebsvereinbarung** gedeckt

Sonderthema:

Maßnahmen zur Aufdeckung von Straftaten von Beschäftigten

Maßnahmen zur Aufdeckung von Straftaten

1. Pauschale, unlimitierte Überwachung (E-Mail, Internet-Nutzung) und Zugriff auf alle verfügbaren personenbezogenen Daten unzulässig
2. Zulässigkeit des Zugriffs auf Daten nach § 32 BDSG
   - Verdacht aufgrund konkreter Anhaltspunkte
   - Dokumentation der Anhaltspunkte
   - Erforderlich zur Aufdeckung der Straftat
   - Nicht unverhältnismäßig
3. Im Zweifelsfall: Abstimmung mit Aufsichtsbehörde

Fazit

1. Spannungsverhältnis Compliance <-> Datenschutzrecht (+)
2. aber nur bei personenbezogenen Daten
3. Datenschutzrecht 2009 verschärft
4. IT-Systeme: Was ist nach Datenschutzrecht gefordert ?
5. Nutzung von Daten: Einwilligung oder gesetzliche Erlaubnis erforderlich
6. Aufdeckung von Straftaten Beschäftigter: Neuer § 32 BDSG

Vielen Dank für Ihre Aufmerksamkeit!

Weitere Informationen unter www.nfis.de