



# Rechtsfragen der IT-Sicherheit

## Autor



- Rechtsanwalt, Kanzlei esb in Stuttgart, spezialisiert auf IT-Recht
- Seminarleiter Internet-Recht, IT-Sicherheit, Datenschutz
- Ausbilder für Datenschutzbeauftragte
- Fachbuchautor „IT-Recht in der Praxis“, Vieweg, 2. Auflage, Dez. 2006
- Lehrbeauftragter der Universität Stuttgart für Medienrecht
- E-Mail: [horst@speichert.de](mailto:horst@speichert.de)
- Internet: [www.kanzlei.de](http://www.kanzlei.de), [www.speichert.de](http://www.speichert.de)

## Vorwort

Das vorliegende Dokument ist ein genereller Leitfaden. Es kann nicht die verbindliche Rechtsauskunft durch einen Fachanwalt ersetzen. Websense bittet Sie um Ihr Verständnis, dass trotz sorgfältiger Recherche keine Garantie oder Gewährleistung übernommen werden kann für die Richtigkeit oder Eignung der enthaltenen Richtlinien. Grundsätzlich sollte sich ein Unternehmen vor einer Implementierung von Richtlinien individuell rechtlich von einem Spezialisten beraten lassen.

## Websense Firmenprofil

Websense (Nasdaq: WBSN), eines der führenden Unternehmen im Bereich integrierter Web-, Messaging- und Data-Protection-Technologien, schützt weltweit mehr als 42 Millionen Mitarbeiter in über 50.000 Unternehmen, Behörden und öffentlichen Organisationen vor externen Angriffen und internen Sicherheitslücken. Distribuiert über ein globales Netz von Channelpartnern helfen Websense-Software und gehostete Security-Lösungen Unternehmen dabei, sich vor böartigem Programmcode jeder Art zu schützen, den Verlust vertraulicher Daten zu verhindern und für die Einhaltung verbindlicher Regeln bei der Internetnutzung zu sorgen. Weitere Informationen: [www.websense.de](http://www.websense.de).

<b>Inhalt:</b>	<b>Mit Rechtssicherheit zur Informationssicherheit .....</b>	<b>5</b>
	<b>Haftungsfragen – Alles, was Recht ist! .....</b>	<b>6</b>
	• Strafverfolgung und Auskunftspflichten .....	6
	• Verkehrssicherungspflichten.....	8
	• Störerhaftung für ungesicherte Netzwerke, offene W-LAN.....	10
	• Haftungsszenario.....	11
	• Rechtsfolgen.....	12
	• Eigenhaftung der Mitarbeiter .....	12
	• Haftung nach TDG.....	14
	<b>Compliance und Risikomanagement.....</b>	<b>14</b>
	• Haftung der Geschäftsleitung nach KonTraG.....	15
	• Anerkannte Standards und Zertifizierung .....	16
	• Vorgaben nach Basel II .....	16
	• Compliance nach SOX .....	18
	<b>Archivierungspflichten – mit Sicherheit Recht behalten!.....</b>	<b>19</b>
	• Handelsrechtliche Pflichten .....	20
	• Steuerrechtliche Pflichten .....	20
	• Ordnungsgemäße Buchführung nach GoBS.....	20
	• Elektronische Betriebsprüfung nach GDPdU.....	21
	• Digitale Rechnungen .....	22
	• Archivierung im Eigeninteresse .....	23
	<b>Rechtssichere https-Scanserver.....</b>	<b>23</b>
	• Zulässigkeitsvoraussetzungen.....	24
	• Best-Practice-Beispiel.....	24
	<b>Mitarbeiterkontrolle versus Datenschutz – mit einem Bein im Gefängnis ? .....</b>	<b>25</b>
	• Private Nutzung, Fernmeldegeheimnis.....	25
	• Dienstliche Nutzung, unerlaubte Privatnutzung.....	26
	• Surfen im Internet .....	26
	• Versendung von E-Mails.....	27

- Interessenausgleich durch rechtliche Gestaltung ..... 27
- Mitbestimmung der Betriebs- und Personalräte ..... 28
- Betriebs- oder Dienstvereinbarungen ..... 29
- Anhang** ..... 32
- Gestaltungsbeispiel einer Betriebsvereinbarung ..... 32
- Checkliste ..... 36

## Mit Rechtssicherheit zur Informationssicherheit

IT-Sicherheit ist eine von Haus aus technisch dominierte Disziplin, die jedoch in starkem Umfang organisatorische Maßnahmen erfordert und zwingend die rechtlichen Rahmenbedingungen einhalten muss. Es handelt sich um eine ganzheitliche Aufgabe, deren technische, organisatorische und rechtliche Komponenten in enger Wechselbeziehung miteinander verzahnt sind. Die technische Sicherheit wird flankiert von organisatorischen Maßnahmen wie Policies, Nutzungsrichtlinien oder Zertifizierungen. Technik und Organisation wiederum werden in Verträgen oder Betriebsvereinbarungen rechtlich gestaltet und umgesetzt. Überdacht wird das System von einem verbindlichen Risikomanagement, das durch die Leitungsebene des Unternehmens umzusetzen ist. Insgesamt ergibt sich eine vielschichtige Pflichtenstruktur, die sich aus einer breiten Palette von Maßnahmen zusammensetzt.



Daraus ergibt sich eine ausgeprägte Ganzheitlichkeit der Informationssicherheit. Filtersysteme, Hard- und Software für die IT-Sicherheit unterfallen der Mitbestimmung des Betriebsrates, sofern sie auch zur Mitarbeiterkontrolle geeignet sind. Spätestens wenn der Betriebsrat den Einsatz der Sicherheitstechnik sperrt, wird erkennbar, dass die technische Komponente nicht alleine steht, sondern in ein juristisches Regelwerk eingebunden ist. Die Beispiele lassen sich fortsetzen. Zur Vermeidung von Haftung und Schadensersatz etwa ist nicht allein der Einsatz von Technik, sondern sind insbesondere auch organisatorische Maßnahmen wie Nutzungsrichtlinien, Schulung und Beaufsichtigung von Mitarbeitern sowie die rechtliche Gestaltung in IT-Verträgen und Betriebsvereinbarungen erforderlich. Auch hier zeigt sich die enge Verzahnung von Technik, Organisation und Recht.

Wer diesen Strukturen gerecht wird und das Thema ganzheitlich umsetzt, hebt die IT-Sicherheit auf die höhere Qualitätsstufe der Informationssicherheit im Sinne der Standards nach BSI-Grundschutz oder ISO 27001.

## Haftungsfragen – Alles, was Recht ist!

Die IT-Verantwortlichen in Unternehmen und Behörden fragen sich immer häufiger und dringlicher, inwieweit illegale Vorgänge und Inhalte zur Mitverantwortung des Arbeitgebers bzw. der Mitarbeiter und Geschäftsleitung führen. Ein einführendes Beispiel mag dies zunächst verdeutlichen.

### Strafverfolgung und Auskunftspflichten

Medienbericht vom 23.05.2006: „Staatsanwaltschaft Köln ermittelt gegen ca. 3.500 P2P-Nutzer. Rund 130 Durchsuchungen wurden im Rahmen einer koordinierten Aktion gegen Tauschbörsennutzer heute zeitgleich im gesamten Bundesgebiet durchgeführt. Zahlreiche PCs und andere Beweismittel wurden beschlagnahmt. Bei den Ermittlungen kam eine speziell zu diesem Zweck entwickelte Software zum Einsatz, die innerhalb von zwei Monaten über 800.000 Datensätze und mehr als 14 Gigabyte Log-Dateien zusammenstellte. Mit diesen Daten ist es gelungen, die Nutzer zu identifizieren.“



Seit Anfang 2005 wurden ca. 20.000 derartiger Strafverfahren eingeleitet. Es stellt sich die Frage nach einer möglichen Mitverantwortlichkeit

- des Unternehmens
- der Geschäftsleitung
- der Mitarbeiter

für solch illegale und strafbare Inhalte.



Bei strafbarem Verhalten (→ z.B. illegale Pornografie, raubkopierte Inhalte) erstatten die Geschädigten verstärkt Strafanzeige. Die Behörden versuchen daraufhin die zur Strafverfolgung notwendigen Daten zu ermitteln. Nach der neueren Rechtsprechung werden Auskunftsansprüche der TK-Anbieter (Provider) nach §§ 89 VI, 113 TKG allgemein anerkannt. Auch der Arbeitgeber wird bei erlaubter Privatnutzung zum TKAnbieter. Demnach müssen

- die öffentlichen Provider → die IP-Adresse herausgeben,
- die Arbeitgeber → anhand der IP-Adresse die persönliche Zuordnung zum konkreten Mitarbeiter vornehmen.

Solche Ermittlungen der Behörden bringen die Verantwortlichen in den Unternehmen nicht selten in schwierige Situationen, insbesondere wenn die Passwort- bzw. Identitätsverwaltung beim Arbeitgeber so unzureichend ist, dass die persönliche Zuordnung der IP-Adresse auch den Falschen treffen kann. Je sensibler der verfolgte Straftatbestand ist, desto empfindlicher wird ein zu Unrecht beschuldigter Mitarbeiter reagieren. Denn die persönliche Zuordnung der IP-Adresse und Herausgabe der Daten führt zu unmittelbaren Ermittlungsmaßnahmen gegen den Mitarbeiter.

## Verkehrssicherungspflichten

Zum besseren Verständnis der Haftungssystematik ist die obergerichtliche Rechtsprechung des Bundesgerichtshofes (BGH) zu den Verkehrssicherungspflichten sowie die Vorgaben des KonTraG für ein verbindliches Risikomanagement zu betrachten. Der BGH spricht im Rahmen der Haftungssystematik von Verkehrssicherungspflichten:

---

*„Wer eine Gefahrenquelle eröffnet oder sich an ihr beteiligt, muss Dritte schützen und hierfür geeignete Schutzmaßnahmen ergreifen.“*

---

- die Kommunikationsvorgänge in Intranet und Internet eröffnen vielfältige Gefahren, sind also Gefahrenquellen im Sinne der Verkehrssicherungspflichten
- die Verkehrssicherungspflichten bestehen im Wesentlichen aus:
  - Organisationspflichten bezüglich betrieblicher (technischer) Abläufe
  - Aufsichtspflichten des Arbeitgebers gegenüber seinen Mitarbeitern
- 100%ige Sicherheit kann im Rahmen der Verkehrssicherungspflichten nicht verlangt werden, aber Maßnahmen nach der Verkehrserwartung, die wirtschaftlich zumutbar sind
- auch die vertraglichen Schutzpflichten orientieren sich an den Verkehrssicherungspflichten



Die Verkehrssicherungspflichten ergeben sich aus einer Vielzahl gesetzlicher und ertraglicher Bestimmungen sowie der Rechtsprechung. Nachfolgend einige Beispiele.

- 
- Besondere Verschwiegenheitsverpflichtung und eine strafbewehrte Garantenstellung für besonders sensible Daten
    - bei Amts-, Berufs- und Privatgeheimnissen, § 203 StGB
    - bei Geschäfts- und Betriebsgeheimnissen, § 17 UWG
    - Garantenstellung nach § 13 StGB
    - begehbar auch durch Unterlassen von Sicherungsmaßnahmen, Verletzung von Sorgfaltspflichten
  - § 25a Abs. 1 Nr. 2 KWG: Kredit- und Finanzinstitute müssen über angemessene Sicherheitsvorkehrungen für die Datenverarbeitung verfügen, diese werden konkretisiert durch Richtlinien des BaFin (MaRisk), welche ein Risikomanagement für Banken und Finanzdienstleister verlangen
  - Vorgaben der Finanzbehörden nach der GoBS oder GDPdU: Risiken für die steuerlich relevanten Datenbestände sind zu vermeiden
  - § 9 BDSG plus Anlage → Die Vorschrift enthält die Grundsätze ordnungsgemäßer Datenverarbeitung, also Vorgaben für die technischorganisatorische Datensicherheit. Es ist ein technisches Sicherheitskonzept zu entwickeln, das unbefugten Zugriff auf personenbezogene Daten verhindert. Im Einzelnen bedeutet dies:
    - Zutrittskontrolle → räumliche, physische Sicherung, Authentifizierung
    - Zugangskontrolle → Passwort, Firewall, Festplattenverschlüsselung
    - Zugriffskontrolle → effektive, rollenbasierte Rechteverwaltung
    - Weitergabekontrolle → Datensicherung, Verschlüsselung
    - Verfügbarkeitskontrolle → Virenschutz, Backup, sichere Archivierung
- 

Die konkretisierenden Normen werden von der Rechtsprechung als Maßstab für die angemessenen Sicherungserwartungen herangezogen. Der Umfang der Verkehrssicherungspflichten bestimmt sich insbesondere nach

- den Sicherheitserwartungen der beteiligten Verkehrskreise
- der Marktüblichkeit der Sicherheits-Hardware und -Software, z.B. hinsichtlich der notwendigen Update-Intervalle eines Viren-Scanners
- der Quantität der Datenverarbeitung
- der Gefährlichkeit des Tuns
- dem Prinzip der Verhältnismäßigkeit, also der Erforderlichkeit und Angemessenheit von Maßnahmen
- der wirtschaftlichen Zumutbarkeit, also der Größe und Leistungsfähigkeit eines Unternehmens

Nach der Rechtsprechung ist im gewerblichen Bereich eine zuverlässige, zeitnahe und umfassende Sicherung der IT-Systeme erforderlich. Ansonsten können betriebliche Brandherde - wie etwa raubkopierte Software oder der strafbare Download von mp3-Files aus P2P-Netzwerken - zur Mitverantwortlichkeit in Unternehmen und Behörden führen. Umgesetzt werden die Pflichten zur Haftungsprävention durch ein Bündel von Maßnahmen, bestehend aus Technik, Nutzungsrichtlinien und rechtlicher Gestaltung:

- Ganzheitlichkeit: abgestimmter Mix aus technischen, organisatorischen und rechtlichen Maßnahmen
- Technisch: upgedateter Virenschutz, Archivierung, URL-Filter, Content-, Spam-Filter etc.
- Organisatorisch: Zuständigkeits-, Verantwortlichkeitsverteilung, Policy, Nutzungsrichtlinien, Kontrolle der Beschäftigten etc.
- Rechtliche Gestaltung: Betriebs-/ Dienstvereinbarung, Steuerung durch Verträge, SLA, AGB etc.
- Transparenz der Regeln: erzeugt Vertrauen + Warnfunktion mit Lenkungswirkung

### Störerhaftung für ungesicherte Netzwerke, offene W-LAN

Das Landgericht Hamburg hat am 26.07.2006 entschieden, dass der Betreiber eines offenen W-LAN für urheberrechtswidrige, strafbare Down- bzw. Uploads aus P2P zumindest im Rahmen der Störerhaftung verantwortlich ist. Bei einem offenen WLAN ohne Passwortschutz ist die Datenübertragung nicht gesichert. So können z.B. strafbare mp3-Files missbräuchlich über das offene W-LAN durch externe Dritte heruntergeladen werden. Im Rechtssinne handelt es sich dabei um ein öffentliches Zugänglichmachen von Musikfiles über P2P. Dem Betreiber eines W-LAN obliegen umfangreiche Verkehrssicherungspflichten. Wer seine Internet-Verbindung drahtlos betreibt, muss für die Sicherung des Netzwerkes sorgen, andernfalls verstößt er gegen zumutbare Prüfungspflichten.

Das Urteil reiht sich in eine mittlerweile Vielzahl von Entscheidungen ein, welche die Störerhaftung für unsichere Netzwerke oder Plattformen bejahen. So haben etwa auch der BGH oder das OLG Brandenburg jüngst entschieden, dass für Markenpiraterie zu Schleuderpreisen auf Internet-Verkaufsplattformen das Auktionshaus haftet.

- Es besteht eine Vorsorgepflicht gegen bekannte Missstände
- Der Einsatz von präventiver Filter-Software ist zumutbare Prüfungspflicht (so auch LG Berlin vom 22.05.2005)
- Bei eindeutigen Hinweisen (bedingter Vorsatz) → Schadensersatzpflicht



Die dargestellte Rechtsprechung ist auf unsichere Netzwerke, Systeme oder Plattformen gleichermaßen anzuwenden. So wird man in Zukunft auch bei offenen Mail-Relays, über die Spam-Attacken oder Hacker-Angriffe erfolgen, eine Haftung des Betreibers bejahen müssen.

Überträgt man die dargestellten Haftungssysteme auf die spezielle Situation in der IT, so ergibt sich das nachfolgende **Haftungsszenario**.

## Haftungsszenario

---

- Rechtswidrige E-Mail-Anhänge oder Download von Mitarbeitern, z.B. Raubkopien, illegale mp3-Files, führen zu Strafverfolgungsmaßnahmen im Unternehmen (Durchsuchung der Geschäftsräume, Beschlagnahme von Firmenrechnern etc.)
  - Eintragungen von außen im eigenen System, z.B. in Blogs, Gästebüchern oder Foren → Gefahr illegaler Inhalte wie Beleidigungen, Obszönitäten, Persönlichkeits-, Marken- oder Urheberrechtsverletzungen etc.
  - Fremdinhalte von Dritten (z.B. Kundendaten oder Webspaces für Dritte)
    - ebenfalls Gefahr, dass die gehosteten Inhalte illegal sind
  - Jugendschutz bei Minderjährigen, z.B. Azubis oder Praktikanten
    - Verstoß gegen Jugendschutz, der Arbeitgeber hat hier eine Garantenstellung
  - Schutz des Persönlichkeitsrechts am Arbeitsplatz vor Belästigung, Beleidigung etwa durch Spam oder E-Mail-Anhänge, konkretisiert z.B. im Beschäftigtenschutzgesetz (BeschSG)
  - Viren und Spam in Kombination mit Hacker-Angriffen: Verletzung von
    - Eigentum und Gewerbebetrieb durch Datenbeschädigung oder –verlust
    - Persönlichkeitsrecht, etwa wenn ein Virus personenbezogene Daten ausspioniert und versendet
  - Verlust von Arbeitszeit, Performance, Bandbreite, Verfügbarkeit
-

## Rechtsfolgen



- 
- Bei Verstoß gegen die Pflichten:
    - mit Verschulden → Schadensersatz und möglicherweise Strafbarkeit des Unternehmens, der Geschäftsleitung und der Mitarbeiter
    - ohne Verschulden → Störerhaftung, Unterlassung, Abmahnung, Vertragsstrafe
  - Bei Erfüllung der dargestellten Pflichten: präventive **Haftungsfreizeichnung**, denn für Schäden, die trotz Pflichterfüllung eintreten (=Restrisiko), wird nicht gehaftet
- 

### Eigenhaftung der Mitarbeiter

Die Vermeidung persönlicher Eigenhaftung ist für die handelnden Mitarbeiter, wie etwa IT-Leiter, Sicherheitsbeauftragte, Administratoren, sonstige IT-Verantwortliche, ein entscheidender Faktor. Hierbei ist zwischen der

- zivilrechtlichen (→ Schadensersatz),
- arbeitsrechtlichen (→ Abmahnung, Kündigung) und
- strafrechtlichen (→ Geld- oder Freiheitsstrafe)

Haftung zu unterscheiden.



Aus dem Arbeitsverhältnis treffen grundsätzlich jeden Mitarbeiter sog. arbeitsvertragliche Nebenpflichten

- Schutz-, Mitwirkungs-, Geheimhaltungs- und Aufklärungspflichten
- Als Sorgfaltsmaßstab gilt ein besonnener Mensch mit durchschnittlichen Fähigkeiten in der Situation des Arbeitnehmers
- Also individuell unterschiedlich: höhere Sorgfaltsanforderungen an leitende Mitarbeiter
- Beweislast des Arbeitgebers, § 619a BGB

**Schadensersatzansprüche** des Arbeitgebers wegen Verletzung der arbeitsvertraglichen Nebenpflichten sind in der Praxis nicht häufig, aber möglich. Aufgrund der Fremdbestimmtheit der Arbeitsleistung trägt der Arbeitgeber das Unternehmensrisiko. Für Tätigkeiten mit erhöhtem Risiko gelten deshalb nach der Rechtsprechung des BAG die Grundsätze zur schadensgeneigten Tätigkeit:

- Für vorsätzliches/ grobfahrlässiges Verhalten → volle Haftung des Mitarbeiters
- Mittlere Fahrlässigkeit → Schadensteilung zwischen Arbeitgeber und Mitarbeiter
- Leichte Fahrlässigkeit → keine Haftung des Mitarbeiters

Diese Haftungserleichterung für den Mitarbeiter gilt grundsätzlich nur im Verhältnis zum Arbeitgeber. Im Verhältnis zu geschädigten Dritten besteht ein Freistellungsanspruch des Arbeitnehmers gegen den Arbeitgeber.

Für eine mögliche **Strafbarkeit** gilt dagegen der Grundsatz der vollständigen Eigenverantwortung. Ein Arbeitnehmer macht sich also selbst strafbar, die arbeitsvertragliche Haftungserleichterung ist nicht anwendbar. Auch gilt kein Befehlsnotstand, so dass ein Mitarbeiter, der auf Anweisung seines Vorgesetzten handelt, deswegen nicht gerechtfertigt ist.

Strafbarkeit ist möglich, etwa nach § 206 StGB oder nach BDSG:

- Fahrlässige Verletzung: Ordnungswidrigkeit, bis 250.000 € Bußgeld
- Bei Übermitteln/Abrufen gegen Entgelt oder Bereicherungs- /Schädigungsabsicht liegt eine Straftat vor

Nicht von der Haftungserleichterung erfasst sind auch die Sanktionen der **Abmahnung oder Kündigung**, welche bei Pflichtverstößen des Mitarbeiters stets eintreten können.

---

Zur **Vermeidung von Eigenhaftung** kann ein verantwortlicher Mitarbeiter nachfolgende Eigenschutzmaßnahmen ergreifen

- gewissenhafte Aufgabenerfüllung
- regelmäßige Information der Geschäftsleitung über mögliche Risiken
- Lösungsvorschläge für Sicherheitsmängel erarbeiten, Projekte vorschlagen, angemessenes Budget beantragen
- Hinzuziehung externer Berater

Reaktion der IT-Verantwortlichen bei Ablehnung der vorgeschlagenen Maßnahmen durch die Geschäftsleitung

- Risiken erneut aufzeigen
- Ablehnung und eigenes Verhalten protokollieren und dokumentieren, etwa durch Besprechungsprotokolle oder schriftliche Fixierung in Briefen
- „Mitwisser schaffen“ oder E-Mail mit Cc
- schriftliche Bestätigung einfordern

Konsequenz → Verlagerung der Verantwortlichkeit auf die vorgesetzte Ebene

---

### Haftung nach TDG

Der Gesetzgeber unterscheidet im Teledienstegesetz (TDG) zwischen eigenen und **Fremdinhalten**. Die gesetzliche Haftungssystematik bleibt allgemein und schablonenhaft, so dass sich die praktischen Fälle mit dem TDG allein nicht befriedigend lösen lassen. Eindeutig ist aber, dass ein Anbieter – wie z.B. ein Provider - für fremde Inhalte jedenfalls dann haftet, wenn er trotz **Kenntnis** bzw. trotz eindeutiger Hinweise nichts unternimmt. Im Übrigen arbeitet die Rechtsprechung mit den geschilderten Verkehrssicherungspflichten. Diese lassen sich wie gesehen aus einer Vielzahl von gesetzlichen und vertraglichen Bestimmungen entnehmen.

### Compliance und Risikomanagement

Compliance, also die Einhaltung fremdgesetzter (gesetzlicher) und selbstgesetzter Standards (z.B. in der Policy), ist nicht nur ein Marketing-Schlagwort, sondern erfordert konkrete Maßnahmen.



### Haftung der Geschäftsleitung nach KonTraG

Die Unternehmensleitung von Kapitalgesellschaften (AG, GmbH) hat für ein wirksames Risikomanagement-System zu sorgen. Im **KonTraG** schreibt der Gesetzgeber Sicherungsmaßnahmen vor, nach denen ein Überwachungssystem einzurichten ist, das bestandsgefährdende Entwicklungen frühzeitig erkennt. Dieses Frühwarnsystem erfordert u.a. eine präventive Überwachung und Erkennung von Fehlentwicklungen in der IT-Sicherheit. Auch das BSI verweist in seinen Standards ausdrücklich auf die Vorgaben des KonTraG (etwa im „Leitfaden IT-Sicherheit“).

- KonTraG = Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
- Eingriff des Gesetzgebers in die „Corporate Governance“ (=Führung und Überwachung) des Unternehmens
- Anwendungsbereich: mittlere und große AG, entsprechende Anwendung auf vergleichbar große GmbH
- Zweck des KonTraG
  - Verpflichtung des Vorstands zu Risikomanagement
    - Risikomanagement = Risikoklassifizierung und -Controlling
  - Früherkennung von gefährlichen Schief lagen = Frühwarnsystem
    - präventive Überwachung und Erkennung von Fehlentwicklungen, z.B. Viren, illegale Inhalte, IT-Sicherheit
  - soll die Prüfung von Unternehmen erleichtern für Anleger und Wirtschaftsprüfer
- Organisations- und Sorgfaltspflichten des Vorstands nach § 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.“
- Persönliche Haftung des Vorstands mit dem eigenen Vermögen

## Anerkannte Standards und Zertifizierung

- Effektivster Schutz vor persönlicher Haftung und Organisationsverschulden
- Nachweis der geprüften Sicherheit nach außen, etwa für Anforderungen von externen Dritten:
  - Wirtschaftsprüfer (KonTraG)
  - Kreditgeber (Basel II), denn IT-Sicherheit ist Rating-Faktor im Rahmen von Basel II
- Erwerb durch Audit eines zertifizierten Auditors

## Anerkannte Standards

- ISO/IEC 13335
  - allgemeine Leitlinie für die Initiierung und Umsetzung des IT-Sicherheitsmanagementprozesses
- ISO/IEC 17799
  - Rahmenwerk für das IT-Sicherheitsmanagement, kaum konkrete technische Hinweise, eine von mehreren Möglichkeiten, die Anforderungen des ISO-Standards 27001 zu erfüllen
- ISO/IEC 27001
  - der erste internationale Standard zum IT-Sicherheitsmanagement, der auch eine Zertifizierung ermöglicht, aber keine Hilfe für die praktische Umsetzung
- BSI-Standards zur IT-Sicherheit, IT-Sicherheitsmanagement
  - 100-1 Managementsystem für Informationssicherheit (ISMS)
  - 100-2 IT-Grundschatz-Vorgehensweise
  - 100-3 Risikoanalyse auf der Basis von IT-Grundschatz
  - ISO 27001 Zertifizierung auf der Basis von IT-Grundschatz

## Vorgaben nach Basel II

Am 26. Juni 2004 wurden die neuen Eigenkapitalanforderungen für Banken, kurz Basel II, am Sitz der Bank für internationalen Zahlungsausgleich unter dem Namen "International Convergence of Capital Measurement and Capital Standards: a Revised Framework" verabschiedet. Am 14. Juli 2004 hat die Europäische Kommission einen Richtlinienentwurf veröffentlicht, mit dem Basel II in Europa Gesetz wurde. Voraussichtlich Ende 2007 treten die neuen Bestimmungen auch bei uns in Kraft.

- Basel II regelt die Kreditvergabe und die Kreditbedingungen
- Gesetzlich noch nicht verbindlich, wird aber im Hinblick auf die baldige gesetzliche Umsetzung bereits heute allgemein beachtet und angewendet



Die Beherrschung der IT-Risiken gilt als wichtiger Rating-Faktor des Unternehmens im Rahmen der Kreditvergabe nach Basel II. Das BSI sagt ausdrücklich in seinem Leitfadens IT-Sicherheit:

---

*„Auch Banken sind inzwischen gezwungen, bei der Kreditvergabe IT-Risiken des Kreditnehmers zu berücksichtigen, was sich unmittelbar auf die angebotenen Konditionen auswirken wird (Stichwort: Basel II).“*

---

Ein hohes Sicherheitsniveau sowie ein effizientes Risiko- bzw. Sicherheitsmanagementsystem, das die Messung der verbleibenden Rest-Risiken erleichtert, führt zu einer reduzierten Eigenkapitalunterlegung bei den Kreditgebern (→ Banken müssen ihre vergebenen Kredite mit Eigenkapital als Sicherheit unterlegen).

- Das vorhandene Sicherheitsniveau kann z.B. durch Zertifizierungen (etwa BSI-Grundschutz oder ISO 27001) dokumentiert werden
- Es ist allgemein anerkannt, dass im Rahmen der Rating-Faktoren „Risikomanagement, -bewertung und -Controlling“ die IT-Risiken berücksichtigt werden
- insbesondere im Rahmen der operationellen Risiken von Unternehmen, welche die Eigenkapitalquote der Bank für die Kreditsicherung erhöhen
- was sich in einem erhöhten Zinssatz für den Kreditnehmer auswirkt

Aus der Sicht des Kreditgebers (Banken und Finanzdienstleister) hat Basel II noch weit reichendere Auswirkungen, umgesetzt in den so genannten **MaRisk** (= Mindestanforderungen an das Risikomanagement des BaFin vom Dez. 2005). Die MaRisk schreiben verbindlich vor:

- IT-Sicherheit gehört zu den Adressausfallrisiken
- Gesamtverantwortung der Geschäftsleitung für Risikomanagement
- Internes Kontrollsystem (IKS)
  - Regelungen zur Aufbau- und Ablauforganisation
  - Einrichtung von Risikosteuerungs- und -Controlling-Prozessen
- Organisationsrichtlinien
- Dokumentation
- Technisch-organisatorische IT-Sicherheit
- Gängige Standards wie BSI oder ISO sind zu beachten
- Test und Abnahme durch Verantwortliche
- Notfallkonzept
- Regelungen für Outsourcing

## Compliance nach SOX

In den letzten Jahren erfolgten weit reichende Eingriffe in die Corporate Governance von Kapitalgesellschaften durch amerikanische Gesetze, die zum Teil auch bei uns Auswirkungen haben.

- Sarbanes-Oxley Act (SOX), US-Gesetz von 2002
- regelt persönliche Verantwortlichkeit und Haftung des Managements (insbes. CEO, CFO)



### Anwendungsbereich

SOX gilt für

- US-börsennotierte Unternehmen
- Ausländische (also z.B. deutsche) Unternehmen, die an US-Börsen oder der NASDAQ gelistet sind
- Ausländische (also z.B. deutsche) Töchter von US-Gesellschaften

SOX ist bereits seit 30.07.2002 in Kraft. Es gab allerdings eine Schonfrist für ausländische Unternehmen, die US-börsennotiert sind, für die SOX erst seit dem 15.07.2006 verbindlich ist.

Zweck von SOX:

- Verschärfung der Rechnungslegungsvorschriften in Folge gravierender Bilanzskandale (z.B. Enron oder Worldcom)
- Wiederherstellung des Vertrauens der Anleger
- Section 404 des SOX: Unternehmensprozesse und Kontrollverfahren müssen definiert und festgelegt werden, um das Risiko einer falschen Bilanz zu minimieren
- u.a. **weit reichende Archivierungspflichten** für E-Mail und elektronische Kommunikation

Section 404 fordert

- wirksames **internes Kontrollsystem (IKS)**
- IT hat im IKS über die Finanzberichterstattung hohen Stellenwert
- Datensicherheit und Backup
- Erfüllung der Compliance-Anforderungen
- Integration in operative Abläufe
- SOX bedeutet Regelbetrieb, also jährlich wiederkehrende Prüfung
- jährliche Bewertung durch eidesstattliche Versicherung (Certification) des CEO und CFO

- Abschlussprüfer
  - bewertet Vorgehen des Managements
  - eigene Stellungnahme zu IKS
- Offenlegungspflicht von Abschlussprüfer und Management bezüglich Fehler im IKS
- Dokumentationspflicht
- Berechtigungsvergabe und Transaktions-Monitoring
- Funktionstrennung, Schnittstellenüberwachung, allgemeine IT-Kontrollen
- Auswertungs- und Berichtsfunktionalitäten zwingend

Überwachung durch US-Behörden

- SEC = Securities and Exchange Commission = Börsenaufsicht in den USA
- PCAOB = Public Company Accounting Oversight Board = US-Aufsichtsbehörde für Wirtschaftsprüfer
- SEC und PCAOB veröffentlichen Leitfäden und Richtlinien für die Umsetzung von SOX

### Archivierungspflichten – mit Sicherheit Recht behalten!

Die Umstellung auf die elektronischen Kommunikationsformen sollte nicht darüber hinwegtäuschen, dass die umfangreichen gesetzlichen Archivierungspflichten auch für die elektronische Buchung und den E-Mail-Verkehr gelten. In Unternehmen und Behörden muss auf breiter Front Datensicherung betrieben werden. Dabei verursachen Archivierungs- und Backup-Systeme erhebliche Kosten. Auch unter dem Gesichtspunkt der Kostenvermeidung sind deshalb die gesetzlichen Aufbewahrungspflichten insbesondere aus Handels- und Steuerrecht zu beachten.



## Handelsrechtliche Pflichten

- Jeder Kaufmann (GbR, GmbH, AG) hat nach § 257 Abs. 1 HGB die Pflicht zur geordneten Aufbewahrung von geschäftlichen Unterlagen
- Hierzu gehören Handelsbücher, Inventare, Eröffnungsbilanzen, Jahresabschlüsse, Konzernabschlüsse, Konzernlageberichte sowie die erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen, empfangene und versandte **Handelsbriefe, Buchungsbelege**
- Dabei ist der Begriff des Handelsgeschäfts nach der Rechtsprechung des BGH weit definiert. Es genügt ein entfernter, lockerer Zusammenhang mit betrieblichen Interessen, z.B. Angebot, Annahme, Auftragsbestätigung, Mängelrüge, Arbeitsverträge, Bau von Gebäuden usw.
- Nicht umfasst sind lediglich reine Privatgeschäfte des Kaufmannes

Zur Vereinfachung kann die **gesamte Geschäftskorrespondenz** als aufbewahrungspflichtig eingestuft werden.

Die vorsätzliche Verletzung von gesetzlichen Aufbewahrungsfristen ist gemäß § 283 b Abs. 1 Nr. 2 StGB, sofern Zahlungseinstellung oder Insolvenz vorliegen, mit Geldstrafe oder Freiheitsstrafe bis zu 2 Jahren bedroht; bei Überschuldung oder Zahlungsunfähigkeit, Strafbarkeit nach § 283 Abs. 1 Nr. 6 StGB

## Steuerrechtliche Pflichten

Daneben gelten steuerliche Aufbewahrungspflichten

- bzgl. sämtlicher kaufmännischer Unterlagen von oben
- und sonstiger Unterlagen, soweit sie für die Besteuerung bedeutsam sind, § 147 Abs. 1 AO

Bei Verletzung der Archivierungspflichten liegt keine ordnungsgemäße Buchführung vor und es erfolgt eine **Schätzung** der Besteuerungsgrundlagen, § 162 AO. Möglicherweise handelt es sich auch um strafbare Steuerhinterziehung.

## Ordnungsgemäße Buchführung nach GoBS

Es gelten die Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) des Bundesfinanzministeriums vom 07.11.1995.

Danach ist keine bestimmte Technologie vorgeschrieben, möglich sind:

- Bildträger (Mikrofilm, Fotokopie), COM
- maschinenlesbare Datenträger (Disketten, Magnetbänder, elektrooptische Speichermedien)
- Dokumentenmanagementsysteme
- digitale Datenträger (CD-Rom, DVD), § 147 Abs. 2 AO
- Ausnahme: Eröffnungsbilanzen, Jahresabschlüsse

Dabei ist sicherzustellen:

- die **Unveränderlichkeit** (Revisionssicherheit), § 146 Abs. 4 AO
  - Erfassung aller Informationen, ohne Unterdrückung

- einmal erfolgte Buchung darf nicht rückgängig gemacht werden
  - Fehlerkorrektur nur durch nachvollziehbare Änderungen (Storno)
- das Vorliegen **systematischer Verzeichnisse**
  - geordneter Zugriff des Prüfers auch ohne Fremdhilfe muss möglich sein
  - zeitlich geordnete Ablage
- ein internes **Kontrollsystem (IKS)**
  - Sicherung und Schutz der vorhandenen Informationen vor Verlusten aller Art
  - Bereitstellung vollständiger, genauer, aussagefähiger und zeitnaher Aufzeichnungen
  - Förderung der betrieblichen Effizienz durch Auswertung und Kontrolle der Aufzeichnungen
  - Unterstützung der Befolgung der Regeln der vorgeschriebenen Geschäftspolitik

### Elektronische Betriebsprüfung nach GDPdU

Für den **Behördenzugriff** ist sicherzustellen:

- die jederzeitige Verfügbarkeit und Lesbarkeit, § 147 Abs. 5 AO
- es besteht: Vorlagepflicht des Steuerpflichtigen auf Verlangen der Behörde
- Kostentragungspflicht des Steuerpflichtigen
- **Außenprüfung** durch Behörde möglich, Einsichtnahme im System des Steuerpflichtigen: nur Lesezugriff, keine Fernabfrage (Online-Zugriff)
- es gelten: die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU), am 16.07.2001 vom Bundesfinanzministerium erlassen, <http://www.aufbewahrungspflicht.de/edfs/gdpdu.pdf>

**Zugriffsmöglichkeiten** nach GDPdU bei elektronischer Betriebsprüfung:

- Z1: Unmittelbarer Zugriff  
Inhouse-Prüfung unmittelbar im System des Steuerpflichtigen
- Z2: Mittelbarer Zugriff  
Das Unternehmen oder ein beauftragter Dritter werten die Daten nach Vorgaben des Prüfers aus
- Datenträgerüberlassung  
Überlassung der Daten an den Prüfer auf einem geeigneten Medium

**Wichtig:** freie Wahlmöglichkeit des Prüfers zwischen den verschiedenen Zugriffsmöglichkeiten, auch kumulativ; nur Zugriffsrecht auf steuerrechtlich relevante Unterlagen, also nicht zu viele Daten zur Verfügung stellen.

Es gelten die folgenden **Aufbewahrungsfristen**:

- Handels- oder Geschäftsbriefe, sowie alle sonstigen Unterlagen, soweit für die Besteuerung bedeutsam, 6 Jahre lang, § 147 Abs. 3 AO
- Bücher, Jahresabschlüsse, Buchungsbelege etc., 10 Jahre lang
- Ablaufhemmung: die Frist läuft nicht ab, solange die Unterlagen für die Besteuerung von Bedeutung sind, 147 Abs. 3 Satz 3 AO
- kürzere Aufbewahrungsfristen nach HGB bleiben unberührt, § 147 Abs. 3 Satz 2 AO



## Archivierung im Eigeninteresse

Neben Handels- und Steuerrecht existieren eine ganze Reihe weiterer Aufbewahrungspflichten:

- alle gesetzlichen Bestimmungen, die Ansprüche auf Auskunft und Rechnungslegung gewähren, so etwa §§ 259, 666, 667 BGB
- Vorlegungspflichten und Beweislast im Prozess
- bei Verletzung nach § 444 ZPO wird ohne Beweisverfahren der vom Gegner behauptete Vortrag als bewiesen angesehen, OLG Düsseldorf
- bei Verletzung von Aufbewahrungspflichten droht Prozessverlust
- bei Fristsetzung des Gerichts muss rechtzeitiger Zugriff auf Archivdaten gewährleistet sein, ansonsten Präklusion bezüglich der Darlegungs- und Beweismöglichkeiten
- ordentliche Geschäftsführung erfordert: grundsätzliche Aufbewahrungs- und Archivierungspflicht - etwa die gesamte **E-Mail-Korrespondenz**, Protokolle von Meetings, Entwürfe und Notizen aller Art etc., die im Streitfall gebraucht werden könnten

## Rechtssichere https-Scanserver

Die gleichzeitige gesetzliche Forderung nach Verschlüsselung auf der einen und Virenschutz auf der anderen Seite, etwa in Anlage zu § 9 BDSG, erzeugt einen technischen Widerspruch, da verschlüsselte Verbindungen nicht ohne Weiteres auf Viren oder Malware untersucht werden können.



- Spannungsfeld zwischen Datenschutz und Systemschutz
- beides wesentliche Eckpfeiler zur Umsetzung der datenschutzrechtlichen Anforderungen
- https gewährleistet die Vertraulichkeit der übertragenen Daten
- Scannen der Verschlüsselung steht der Vertraulichkeit scheinbar entgegen, gewährleistet aber den vergleichbar wichtigen Virenschutz

Immer mehr Missbrauch und Malware erfolgt über https und erzeugt so ein Sicherheitsvakuum. Das technisch unbestritten notwendige https-Scanning muss datenschutzkonform betrieben werden.

Dies erfordert zunächst die Vermeidung von **möglichen Straftatbeständen**

- § 202a StGB Ausspähen von Daten
- § 206 StGB Bruch des Fernmelde-/ Telekommunikationsgeheimnisses
- Ordnungswidrigkeit nach § 43 BDSG

Insbesondere darf der Scan-Vorgang nicht zur Kenntnisnahme der Inhalte führen, muss also in einer Blackbox ablaufen

### Zulässigkeitsvoraussetzungen

- Anlass für das Scannen ist ein konkretes Gefährdungspotential, worunter in erster Linie der Virenschutz fällt, sowie Abwehr vergleichbarer Malware; sonstige Filtermaßnahmen sind kein ausreichender Anlass
- Die Maßnahme muss erforderlich zur Gefahrenabwehr sein, z.B. um das Eindringen von Viren zu verhindern
- Möglichkeit zu optionalen Ausnahmen, besonders sensible https-Verbindungen, etwa Online-Banking, können vom Scan-Vorgang ausgenommen werden
- Der Scan-Vorgang der Verschlüsselung, die Virenfilterung und das erneute Verschlüsseln müssen in einem geschlossenen System ablaufen
- Scan-Vorgang und Antiviren-Software arbeiten in einer Blackbox, führen also nicht zur Kenntnisnahme von Inhalten durch Administratoren oder sonstige Dritte

Zusätzliche optionale Maßnahmen, welche die juristische Sicherheit erhöhen

- Deutliche Hinweise gegenüber dem Nutzer vor dem Scan-Vorgang
- Einwilligung des Nutzers
  - schriftlich nach § 4a BDSG in Nutzungs- oder Betriebsvereinbarung
  - in elektronischer Form nach § 4 Abs. 2, 3 TDDSG, etwa durch Popup- Fenster

### Best-Practice-Beispiel

- Schutz des Berliner Landesnetzes vor Viren
- Datenschutzrechtliche Abwägung des Landesdatenschutzbeauftragten (LDSB) Berlin fiel zugunsten des Virenschutzes und https-Scannings aus
- Unter den dargestellten Voraussetzungen hatte der LDSB Berlin keine rechtlichen Bedenken geäußert und empfohlen, das https-Scan-Verfahren wieder einzusetzen

## Mitarbeiterkontrolle versus Datenschutz – mit einem Bein im Gefängnis ?

Der Arbeitgeber hat ein vitales Interesse daran, das private Surfen, Chatten oder Mailen am Arbeitsplatz sinnvoll zu begrenzen. Neben dem Verlust von Arbeitszeit und Bandbreite lauern hier vielfältige Haftungsrisiken. Die legale Kontrolle der Mitarbeiter, um Missbräuche einzuschränken, ist deshalb überall in den Unternehmen und Behörden ein Thema mit hoher Priorität.

### Private Nutzung, Fernmeldegeheimnis

Bei Kontrollmaßnahmen stellt sich zunächst die Ausgangsfrage, ob der Arbeitgeber die private Nutzung erlaubt oder verboten hat. Bei erlaubter Privatnutzung wird der Arbeitgeber zum Telekommunikationsanbieter, da die Möglichkeit des Arbeitnehmers zur Privatnutzung von E-Mail und Internet als Dienstleistung ihm gegenüber einzustufen ist. Daraus resultiert die Geltung des Fernmeldegeheimnisses, da sich der Arbeitnehmer auf die Vertraulichkeit der privaten Kommunikation verlassen darf. Kontrollmaßnahmen unter dem Regime des Fernmeldegeheimnisses sind weit gehend unzulässig. Die reine „Erhebung“ von Daten zur technischen Datensicherheit, Notfallprävention, Störungsbeseitigung, Datenschutzkontrolle ist möglich. Die Auswertung dieser Daten ist dagegen nur ausnahmsweise nach § 89 TKG möglich:

- zur Abrechnung, etwa der privaten Nutzung
- bei Gefahr im Verzug → z.B. akuter Virus
- bei Vorliegen einer Einwilligung aufgrund einer rechtfertigenden Nutzungsvereinbarung



## Dienstliche Nutzung, unerlaubte Privatnutzung

Ist dagegen die Privatnutzung verboten und nur eine dienstliche Nutzung möglich, kommt das Fernmeldegeheimnis nicht zur Anwendung. Die dienstliche Nutzung steht dann jedoch unter dem Schutz des **Bundesdatenschutzgesetzes (BDSG)**. Zwar sind hier weiter gehende Kontrollen als unter dem Fernmeldegeheimnis möglich, trotzdem besteht kein schrankenloser Freibrief zur Einsicht in E-Mails oder Web-Inhalte. Eine Kontrolle der dienstlichen Nutzung ist nach den Vorgaben des BDSG nur zulässig, wenn aufgrund einer Güterabwägung nach dem Verhältnismäßigkeitsprinzip die Kontrollmaßnahme erforderlich und angemessen ist. In diese Gesamtabwägung der relevanten Belange sind alle beteiligten Interessen mit einzubeziehen. Daraus ergibt sich die grobe **Faustformel**, dass

- äußere Verbindungsdaten wie URL, Empfänger- oder Absenderadresse eingesehen werden dürfen,
- Inhaltskontrollen, wie das Mitlesen von E-Mails oder von Eintragungen des Arbeitnehmers auf den Web-Seiten, aber unzulässig sind.

Unterscheidet man nach den Hauptnutzungsarten, so ergibt sich für die dienstliche Nutzung im Überblick die nachfolgende Kontrollsituation.

### *Surfen im Internet*



- Trotz Verbot der Privatnutzung keine unbeschränkte Kontrolle möglich
- Betroffen ist in erster Linie die Überwachung der Logfiles
- Faustformel: kontrolliert werden können die besuchten URLs, Dauer des Surfens, Umfang der Downloads, nicht aber die auf den Seiten vorgenommene Eintragungen

## Versendung von E-Mails



- Vollständiges Verbot privater E-Mails von Arbeitnehmern anders als bei der Telefonnutzung möglich
- Aber: private E-Mails können trotz Privatnutzungsverbot nicht vollständig verhindert werden, da auch ein Eingang von außen möglich ist, der vom Arbeitnehmer nicht beherrscht wird
- Faustformel: nur Kontrolle der Adressdaten zulässig, das ständige Mitlesen der E-Mails - wie in den USA üblich – ist nicht erlaubt
- Denn es existiert ein gegenüber der Inhaltskontrolle milderer Mittel: die Herausgabe der geschäftlichen E-Mails durch den Arbeitnehmer an den Arbeitgeber

### Interessenausgleich durch rechtliche Gestaltung

Unabhängig davon, ob Fernmeldegeheimnis oder Bundesdatenschutzgesetz gelten, bedeuten unregelte Zustände hinsichtlich der Mitarbeiterkontrolle einen ständigen **rechtlichen Graubereich** und Unsicherheit, da die Bestimmungen in TKG und BDSG unklar sind. Es herrscht große Verunsicherung bei Arbeitgeber, Administrator und Arbeitnehmer, da die notwendige Güterabwägung der beteiligten Interessen im Einzelfall alle Betroffenen überfordert. Das Datenschutzrecht eröffnet jedoch nach dem Grundsatz „präventives Verbot mit Erlaubnisvorbehalt“ einen **Gestaltungsspielraum**, um durch Vereinbarungen legale Handlungsgrundlagen zu schaffen. Nach dem Gesetzeswortlaut besteht zwar zunächst ein generelles Verbot, das aber durch Vereinbarungen, die als Erlaubnisvorbehalt wirken, in Grenzen modifiziert werden kann. Solche Vereinbarungen bringen Vorteile für alle Beteiligten.

Im Überblick stellt sich die Situation bei der Mitarbeiterkontrolle wie folgt dar:

- Präventives Verbot mit Erlaubnisvorbehalt → eröffnet Gestaltungsspielraum
- Vereinbarungen als legale Handlungsgrundlage entsprechen dem Wunsch des Gesetzgebers, solange ein klärendes Arbeitnehmerdatenschutzgesetz nicht existiert
- Klare Verhältnisse für Admin: keine illegale Kontrolle/keine Strafbarkeit wegen Verstoß gegen das Fernmeldegeheimnis
- Transparenz für Arbeitnehmer: schafft Vertrauen, hat aber auch Warnfunktion und damit Lenkungswirkung
- Haftungsprävention für den Arbeitgeber durch legale Kontrolle, da die Beaufsichtigung der Arbeitnehmer zur Erfüllung der Verkehrssicherungspflichten gehört

#### Mitbestimmung der Betriebs- und Personalräte

Da die Fragen der Mitarbeiterkontrolle der Mitbestimmungspflicht im Sinne des Betriebsverfassungsgesetzes unterliegen, müssen Betriebs-/Personalräte am Entscheidungsprozess in Form von Vereinbarungen beteiligt werden. Hier kommen insbesondere die Anpassung der **Arbeitsverträge** und der Abschluss von **Betriebs-/Dienstvereinbarungen** mit entsprechenden Nutzungs- und Kontrollregelungen für die E-Mail- und Internet-Nutzung in Betracht. Im Bereich Fernmeldegeheimnis, das auf ein Grundrecht zurückgeht, ist neben Kollektivvereinbarungen die individuelle Zustimmung der beteiligten Arbeitnehmer von Vorteil. Ergänzend zu entsprechenden Betriebs-/Dienstvereinbarung kann deshalb eine zusätzliche Legitimation und Information durch eine persönliche Zustimmung des betroffenen Arbeitnehmers erfolgen. Im Einzelnen ist die Situation wie folgt:

- Mitbestimmungsrechte des Betriebs-/Personalrates
- Anpassung der Arbeitsverträge
- Betriebs-/Dienstvereinbarung mit Nutzungsrichtlinien
- Ergänzend: individuelle Zustimmung: dadurch zusätzliche Legitimation und Information der Arbeitnehmer



## Betriebs- oder Dienstvereinbarungen

Bei der Betriebs-/Dienstvereinbarung handelt es sich um einen schriftlichen Vertrag zwischen Arbeitgeber und Mitarbeitervertretung, der zur Lösung des Kontroll- und Nutzungsproblems geschlossen wird. In Betrieben ab einer Größe von fünf Mitarbeitern sind Betriebsräte und damit Betriebsvereinbarungen möglich. Während der Arbeitgeber den Missbrauch einschränken will, befürchtet der Betriebsrat die Ausforschung der Arbeitnehmer. Die Betriebs-/Dienstvereinbarung hat rechtssetzenden Charakter und wirkt modifizierend auf die Inhalte der Arbeitsverträge ein.



Im Überblick gilt für die Betriebsvereinbarung:

- Zweck: Lösung gemeinsamer Probleme
- Internet/E-Mail-Nutzung durch Arbeitnehmer:
  - Arbeitgeber befürchtet Missbrauch
  - Mitarbeitervertretung befürchtet Ausforschung
- Mitbestimmungsrecht der Mitarbeitervertretung/des Betriebsrates gemäß §87 Abs. 1 Nr. 1 und 6 BetrVG für die Bereiche:
  - Ordnung des Betriebes, Arbeitnehmersverhalten
  - technische Kontrolleinrichtungen
- Schriftlicher Vertrag zwischen Arbeitgeber und Mitarbeitervertretung
- In Betrieben ab fünf Mitarbeitern, §1 BetrVG
- Rechtssetzender Charakter, der den Arbeitsvertrag abändert
- Endet durch Kündigung oder Fristablauf

Insbesondere die Missbrauchskontrolle und Abwesenheitsproblematik bedarf einer detaillierten Regelung. Zur inhaltlichen Gestaltung von Betriebs-/Dienstvereinbarung der nachfolgende **Gesamtüberblick**, wonach Regelungen zu folgenden Punkten enthalten sein sollten:

- Umfang einer erlaubten Privatnutzung, beispielsweise Beschränkungen nach Umgang, Dauer oder Art und Weise der E-Mail- und Internet-Nutzung
- Verbotene Nutzungen, Aufzählung im Einzelnen, z.B. sexistisch, rechtsradikal, gewaltverherrlichend etc.
- Welche Daten werden zur Kontrolle erfasst:
  - Protokollierung von E-Mail- und Internet-Aktivitäten
  - Gesamtdatenvolumen etc.
- Technische Einrichtungen, die optional der Kontrolle dienen:
  - Firewall, Proxy, Spam-Filter etc.
  - Reporting-Tool URL-Filter
  - https-Scanning
- Monitoring-Funktionen etc.
- Abwesenheitsregelung: Umgang mit der Mailbox im Falle von Urlaub, Krankheit, Kündigung etc.
- Kontrollprozedere: aus Gründen der Verhältnismäßigkeit, welche ständige personenbezogene Inhaltskontrollen verbietet, ist ein abgestuftes Kontrollverfahren erforderlich:
  - zunächst nur anonymisierte Stichprobenkontrolle
  - nur bei grobem Missbrauch oder Straftat: personenbezogene Kontrolle, möglichst unter Beteiligung des Betriebsrates/ Datenschutzbeauftragten nach dem Vier-Augen-Prinzip
- Regelung der Beteiligung von Betriebsrat, Datenschutzbeauftragtem
- Löschungspflichten
- Konsequenzen bei Nichteinhaltung
- Kündigung, Evaluierung

Zur Verdeutlichung der rechtmäßigen Kontrollprozedere:

zunächst nur anonymisierte Stichprobenkontrolle:

The screenshot displays the SurfControl Web Filter Manager interface. The main window is titled 'Monitored Data - [Summary (5 rows, 1 selected) - Detailed (44 rows, 1 selected)]'. It features a navigation pane on the left, a central data table, and an information pane on the right.

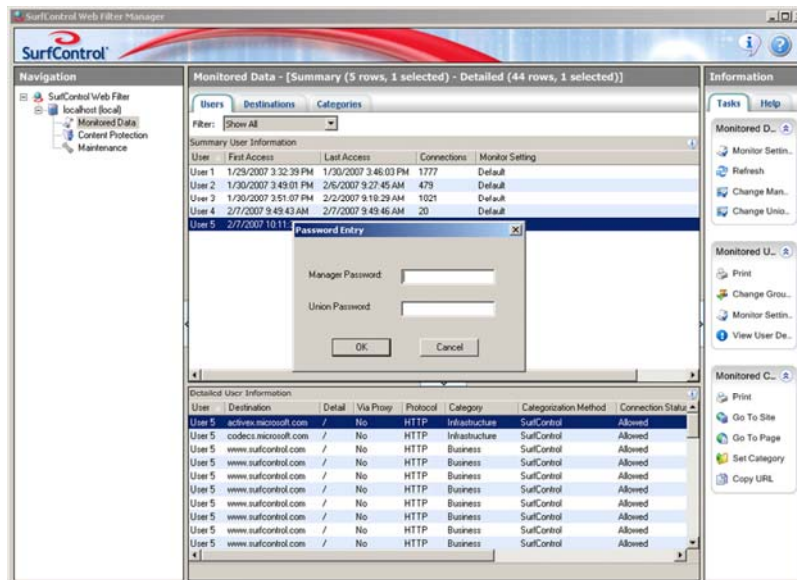
**Summary User Information Table:**

User	First Access	Last Access	Connections	Monitor Setting
User 1	1/29/2007 3:32:39 PM	1/30/2007 3:46:03 PM	1777	Default
User 2	1/30/2007 3:49:01 PM	2/6/2007 9:27:45 AM	479	Default
User 3	1/30/2007 3:51:07 PM	2/2/2007 9:18:29 AM	1001	Default
User 4	2/7/2007 9:49:43 AM	2/7/2007 9:49:46 AM	20	Default
User 5	2/7/2007 10:11:30 AM	2/7/2007 12:09:26 PM	27	Default

**Detailed User Information Table:**

User	Destination	Detail	Via Proxy	Protocol	Category	Categorization Method	Connection Status
User 5	activex.microsoft.com	/	No	HTTP	Infrastructure	SurfControl	Allowed
User 5	codexs.microsoft.com	/	No	HTTP	Business	SurfControl	Allowed
User 5	www.surfcontrol.com	/	No	HTTP	Business	SurfControl	Allowed
User 5	www.surfcontrol.com	/	No	HTTP	Business	SurfControl	Allowed
User 5	www.surfcontrol.com	/	No	HTTP	Business	SurfControl	Allowed
User 5	www.surfcontrol.com	/	No	HTTP	Business	SurfControl	Allowed
User 5	www.surfcontrol.com	/	No	HTTP	Business	SurfControl	Allowed
User 5	www.surfcontrol.com	/	No	HTTP	Business	SurfControl	Allowed
User 5	www.surfcontrol.com	/	No	HTTP	Business	SurfControl	Allowed
User 5	www.surfcontrol.com	/	No	HTTP	Business	SurfControl	Allowed

bei grobem Missbrauch oder Straftat: personenbezogene Kontrolle, möglichst unter Beteiligung des Betriebsrates/Datenschutzbeauftragten nach dem Vier-Augen-Prinzip:



## Anhang

### Gestaltungsbeispiel einer Betriebsvereinbarung

#### Wichtiger Hinweis!

Der nachfolgende Entwurf kann die Vielzahl der Problemstellungen nicht annähernd vollständig erfassen oder lösen, sondern dient lediglich der Veranschaulichung wichtiger Aspekte und schlägt einen Aufbau vor. Eine Problemlösung im Einzelfall ist nur durch eine individuelle Gestaltung möglich. Insbesondere handelt es sich nicht um ein Musterformular, das die rechtliche Gestaltung im Einzelfall, die stets einen individuellen Zuschnitt erfordert, ersetzen kann. Eine ungeprüfte Übernahme ohne substantielle Anpassungen und Ergänzungen ist deshalb - wie auch bei der AGB-Gestaltung - nicht möglich und führt zwangsläufig zu Rechtsverstößen des Verwenders.

#### **Betriebsvereinbarung für die Internet- und E-Mail-Nutzung am Arbeitsplatz**

Die XY GmbH (im Folgenden XY GmbH) und der Betriebsrat schließen entsprechend § 77 in Verbindung mit § 87 Abs. 1 Nr. 1 und 6 BetrVG die folgende Vereinbarung über die Internet- und E-Mail-Nutzung am Arbeitsplatz

#### § 1 Zweck und Geltungsbereich

1. Die vorliegende Vereinbarung regelt die Nutzung der E-Mail- und Internet-Dienste am Arbeitsplatz. Ziel der Vereinbarung ist es, die Nutzungsbedingungen sowie die Maßnahmen zur Protokollierung und Kontrolle transparent zu machen, die Persönlichkeitsrechte der Beschäftigten zu sichern und den Schutz ihrer personenbezogenen Daten zu gewährleisten.
2. Diese Betriebsvereinbarung gilt für alle Mitarbeiterinnen und Mitarbeiter der XY GmbH. Hierzu zählen alle (intern und extern) Beschäftigten, Auszubildende, freie Mitarbeiter, Praktikanten und Aushilfen, mit denen Verträge zur Leistungserbringung vereinbart wurden.
3. Bei der E-Mail- und Internet-Nutzung durch die Mitarbeiter sind die einschlägigen Arbeits- und Sicherheitsanweisungen – insbesondere der Kommunikationsrichtlinie – zu beachten, deren verbindliche Geltung unberührt bleibt. Die vorliegende Vereinbarung greift vielmehr die gemäß § 87 Abs. 1 Nr. 1 und 6 BetrVG mitbestimmungspflichtigen Bereiche aus den einschlägigen Arbeits- und Sicherheitsanweisungen heraus und bildet mit diesen eine abgestimmte Einheit.

#### § 2 Nutzungsrichtlinien

1. E-Mail- und Internet-Zugang stehen den Mitarbeitern als Arbeitsmittel im Rahmen der Aufgabenerfüllung zur Verfügung und dienen insbesondere der Verbesserung der internen und externen Kommunikation, der Erzielung einer höheren Effizienz und der Beschleunigung der Informationsbeschaffung und der Arbeitsprozesse.
2. Unzulässig ist jede wissentliche oder fahrlässige Nutzung des Internet, die geeignet ist, den Interessen oder dem Ansehen der XY GmbH in der Öffentlichkeit zu schaden, die Sicherheit des Netzwerkes zu beeinträchtigen oder die gegen die geltenden Rechtsvorschriften oder einschlägigen Arbeits- und Sicherheitsanweisungen für die Nutzung der IT-Systeme verstößt. Untersagt ist insbesondere das Abrufen oder Verbreiten von Inhalten, die gegen persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstoßen, sowie das Abrufen oder Verbreiten von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, sexistischen, gewaltverherrlichenden oder pornografischen Äußerungen oder Abbildungen.

3. Zur Überprüfung der Einhaltung der Regelungen dieser Vereinbarung werden regelmäßige, nicht personenbezogene Stichproben in den Protokolldateien gemäß § 8 Missbrauchskontrolle durchgeführt.

### § 3 Private Nutzung

1. Die private Internet- und E-Mail-Nutzung ist in eingeschränktem und verhältnismäßigem Umfang, außerhalb der Arbeitszeiten und in den definierten Pausenzeiten zulässig. Während der Privatnutzung hat der Mitarbeiter sich aus dem Zeiterfassungssystem auszubuchen.
2. Dienstliche Belange haben stets Vorrang. Die private Nutzung ist nur zulässig, soweit sie die dienstliche Aufgabenerfüllung sowie die Verfügbarkeit der IT-Systeme für dienstliche Zwecke nicht beeinträchtigt. Private E-Mails dürfen nur ohne Anhänge verschickt werden. Eine Nutzung von Web-Mailern über SSL ist nicht gestattet. Im Rahmen der privaten Internet-Nutzung sind Downloads jeder Art untersagt.
3. Jeder Mitarbeiter erhält die vorliegende Vereinbarung per E-Mail mit der Aufforderung, den Antrag nach Anlage 1 innerhalb von sechs Wochen unterschrieben zurückzusenden. Mitarbeitern, die keinen fristgemäßen Antrag nach Anlage 1 gestellt und unterschrieben haben, ist die private E-Mail- und Internet-Nutzung nicht gestattet.

### § 4 Technische Filtereinrichtungen

1. Trotz der Privatnutzungserlaubnis ist die XY GmbH berechtigt, den Zugriff auf Internet-Inhalte und E-Mails durch den nachfolgenden Einsatz von Filtersystemen einzuschränken:
  - a) Viren- und Spyware-Filter
  - b) Spam-Filter
  - c) URL-Filter
  - d) Firewall und Proxy-Server
  - e) https-Scan-Verfahren
  - f) im Übrigen eingesetzte Filtertechnik gemäß Anlage 2

Zur Unterstützung bei technischen Problemen kann sich der Systemadministrator der XY GmbH auf das EDV-System per Fernzugriff aufschalten. Der beabsichtigte Zugriff wird stets durch eine entsprechende Systemmeldung auf dem System des Mitarbeiters angekündigt und erst nach ausdrücklicher Bestätigung der Anfrage zugelassen.

2. Auf Anforderung hat der betroffene Mitarbeiter dem Vorgesetzten dienstlich veranlasste E-Mails – notfalls unter Löschung privater Passagen - zugänglich zu machen.

### § 5 E-Mail-Regelung bei Abwesenheit

1. Bei Abwesenheit eines Mitarbeiters infolge Urlaub, Krankheit, Kündigung oder anderer Gründe ist der Informationsfluss durch eine verhältnismäßige Abwesenheitsregelung sicherzustellen. Hierfür kommen grundsätzlich zwei Möglichkeiten in Betracht:
  - a) automatisierte Nachricht an den Absender
  - b) Weiterleitung an einen Stellvertreter

2. Scheidet der Mitarbeiter aus der XY GmbH aus, so bereinigt er sein Postfach um private Inhalte und übergibt die geschäftlichen Inhalte nach Aufforderung an den Vorgesetzten oder Nachfolger. Mit dem letzten Arbeitstag wird sein E-Mail-Postfach geschlossen, so dass weiterhin ankommende E-Mails versehen mit einer Nachricht über die Nichtzustellung (Non-Delivery-Report, NDR) zurückgehen.
3. Werden dem Mitarbeiter mobile Endgeräte (Laptop, Blackberry etc.) zur Nutzung überlassen, ist er während seiner geschäftlichen Abwesenheit verpflichtet, seine angemessene Erreichbarkeit und Weiterleitung der E-Mails bezüglich dieser Endgeräte sicherzustellen.

#### **§ 6 E-Mail-Archivierung**

1. Aufgrund verschiedener gesetzlicher Vorschriften ist die E-Mail-Kommunikation zum Teil archivierungspflichtig. Zur Gewährleistung dieser notwendigen Archivierung ist eine automatisierte Komplettarchivierung oder eine Trennung der Gemengelage zwischen privaten und dienstlichen E-Mails durch eine manuelle Weiterleitung (Indizierung) oder Bereinigung zulässig und erforderlich.
2. Die XY GmbH betreibt aus Gründen der Datensicherung ein Backup-System verschiedener Generationen zur Wiederherstellung verlorener oder beschädigter Daten.

#### **§ 7 Protokollierung von E-Mail- und Internet-Aktivitäten**

1. Auf den hierzu vorgesehenen Servern (Proxy-Server etc.) und Filtereinrichtungen (Firewall, URL-Filter etc.) werden die Verbindungsdaten der E-Mail und Internet-Nutzung protokolliert. Dies ist aus Datensicherheitsgründen und für eine Störungsbeseitigung erforderlich. Aus den Protokollen gehen die Aktivitäten der Benutzer hervor.
2. Die Protokolldaten dürfen nicht zur Leistungs- und Verhaltenskontrolle verwendet werden. Sie unterliegen der Zweckbindung dieser Vereinbarung und werden automatisiert nach einer Frist von spätestens 3 Monaten gelöscht.

#### **§ 8 Missbrauchskontrolle**

1. Die Protokolle werden durch einen technisch ausgebildeten Mitarbeiter stichprobenartig und ohne Personenbezug ausgewertet. Der Betriebsrat oder der Datenschutzbeauftragte werden auf Wunsch an den Stichprobenkontrollen beteiligt.
2. Ergibt sich ein konkreter Verdacht auf eine strafbare oder missbräuchliche E-Mail- oder Internet-Nutzung, erfolgt nach vorheriger Absprache mit dem Betriebsrat und dem Datenschutzbeauftragten eine personenbezogene Überprüfung des Vorgangs durch denbeauftragten Mitarbeiter. Der Zugriff kann nur nach dem Vier-Augen-Prinzip erfolgen.

#### **§ 9 Konsequenzen bei Nichteinhaltung**

1. Bei Zuwiderhandlung gegen diese Vereinbarung oder unsachgemäßer Nutzung können die E-Mail- oder Internet-Zugänge zur Wahrung der Sicherheit deaktiviert werden.
2. Bei gravierenden Verstößen gegen diese Vereinbarung muss der Mitarbeiter mit arbeitsrechtlichen Konsequenzen bis hin zur Kündigung des Arbeitsverhältnisses sowie Strafanzeige und Schadensersatzansprüchen rechnen.

3. Erhebt die XY GmbH personenbezogene Daten unter Verstoß gegen die Vorgaben dieser Vereinbarung, so unterfallen die Daten einem Beweisverwertungsverbot mit der Folge, dass sie für arbeitsrechtliche Sanktionen nicht verwendet werden können.

## § 10 Schlussbestimmungen

1. Geplante Änderungen oder Erweiterungen der elektronischen Kommunikationssysteme werden dem Betriebsrat sowie dem Datenschutzbeauftragten rechtzeitig mitgeteilt, soweit sie sich auf die Regelungen dieser Betriebsvereinbarung auswirken.
2. Notwendige Änderungen oder Erweiterungen dieser Betriebsvereinbarung können im Einvernehmen in einer ergänzenden Regelung vorgenommen werden.
3. Die Betriebsvereinbarung kann mit einer Frist von drei Monaten zum Monatsende gekündigt werden. Sie hat eine Laufzeit von einem Jahr und verlängert sich bei Nichtkündigung um ein weiteres Jahr. Im Falle einer Kündigung bleibt sie bis zum Abschluss einer neuen Vereinbarung gültig.
4. Zur Evaluierung dieser Betriebsvereinbarung ist nach Ablauf von zwei Jahren ein Erfahrungsbericht vorzulegen.
5. Diese Betriebsvereinbarung tritt mit Unterzeichnung in Kraft.

....., den \_\_\_\_\_  
XY GmbH \_\_\_\_\_  
Personalrat \_\_\_\_\_

### Anlage 1: Antrag und Einwilligung zur privaten E-Mail- und Internet-Nutzung

Name: \_\_\_\_\_ Vorname: \_\_\_\_\_  
Abteilung: \_\_\_\_\_  
....., den \_\_\_\_\_  
Unterschrift \_\_\_\_\_

### Anlage 2: Technische Filtereinrichtungen

.....

## Checkliste

---

- Existiert ein Notfallszenario/eine Zuständigkeitsverteilung in Fällen wie Virenbefall, Platten-Crash, Systemzusammenbruch?
  - Haben die Anwender einen definierten Ansprechpartner beim Auftauchen gefährlicher oder illegaler Inhalte (Viren, Trojaner, mp3s etc.)?
  - Haben sie eine datenschutzkonforme Abwesenheitsregelung (Krankheit, Urlaub, Kündigung) für den Fortbetrieb der Mailboxen?
  - Haben Sie Spam/URL/Content-Filter im Einsatz?
  - Haben Sie einen Spam-Filter mit einer niedrigen False-Positive-Rate?
  - Hat der Enduser Zugriff auf die ausgefilterten Spam Mails?
  - Haben Sie eine rechtliche Gestaltung (Betriebsvereinbarung, Arbeitsvertrag), die den rechtssicheren Einsatz der Filtersysteme gewährleistet?
  - Betreiben Sie ein datenschutzkonformes Lizenzmanagement?
  - Haben Sie eine datenschutzkonforme Regelung zur Missbrauchskontrolle der Mitarbeiter getroffen?
  - Sind die Passwörter am Monitor gepostet oder im Kollegenkreis bekannt gemacht?
  - Kann jeder Mitarbeiter beliebige Software auf seinem PC installieren?
  - Kann die Geschäfts-Software für den privaten Gebrauch kopiert werden?
  - Gibt es Richtlinien zur Wahrung der Vertraulichkeit von Daten/E-Mails?
  - Kann jeder Mitarbeiter auf alle vorhandenen Daten zugreifen?
  - Wird die Virenschutz-Software ständig und automatisiert upgedatet ?
  - Wird ein brandschutzsicheres Backup-System betrieben?
  - Sind die Firmen-Laptops in das Sicherheitskonzept integriert?
  - Werden als Passwörter die Namen enger Angehöriger oder allgemeine Begriffe verwendet?
  - Sind gefährliche Dateianhänge wie .exe, .bat, .vbs, etc. verboten?
  - Wurden die Mitarbeiter/Innen durch Schulung in die Internet-Nutzung eingewiesen?
  - Kommt eine Firewall zum Einsatz?
  - Existiert eine Regelung zur Archivierung von E-Mails?
  - Kann sichere Verschlüsselungstechnik für die externe und interne Kommunikation eingesetzt werden?
  - Ist das Patchmanagement auf dem letzten Stand der Dinge?
-