



# **Die Nutzung von Email und Internet im Unternehmen**

**Rechtliche Grundlagen und  
Handlungsoptionen**

Version 1.3

Copyright 2006

Alle Rechte,  
auch der auszugsweisen Vervielfältigung, bei BITKOM -  
Bundesverband Informationswirtschaft, Telekommunikation,  
und neue Medien e.V., Berlin/Frankfurt

Redaktion:	Dr. Kai Kuhlmann
Redaktionsassistentz:	Karen Schlaberg
V.i.S.d.P.:	Dr. Bernhard Rohleder

Vorwort zur Version 1.3 .....	5
Vorwort zur Version 1.2 .....	5
Vorwort zur Version 1.1 .....	5
Vorwort .....	5
1. Einführung und Hintergrund .....	7
a) Technischer Hintergrund .....	8
b) Interessenlage .....	8
c) Rechtlicher Hintergrund .....	9
d) Rechtliche Grundlagen .....	9
aa) Grundrechte: Das Recht auf informationelle Selbstbestimmung gem. Art.2 I i.V.m. Art.1 Grundgesetz .....	10
bb) Fürsorgepflicht des Arbeitgebers aus §§ 611, 242 BGB .....	10
cc) Normen des Bundesdatenschutzgesetzes .....	10
dd) Informations- und Kommunikationsdienste Gesetze .....	11
• Telekommunikationsgesetz (TKG) .....	11
• Teledienstegesetz (TDG) .....	11
• Teledienstedatenschutzgesetz (TDDSG) .....	11
ee) Tarifverträge und Betriebsvereinbarungen .....	12
ff) Beteiligungsrechte des Betriebsrats .....	12
• Allgemeine Aufgaben: .....	12
• Normsetzungsbefugnis: .....	13
2. Datenschutzverpflichtungen des Arbeitgebers bei der Nutzung von Internet und Email am Arbeitsplatz .....	13
a) Dienstliche Nutzung .....	14
aa) Anwendung des Telekommunikationsgesetzes .....	14
bb) Anwendung von Teledienstegesetz und Teledienstedatenschutzgesetz .....	14
cc) Anwendung des Bundesdatenschutzgesetzes .....	14
b) Private Nutzung .....	15
aa) Anwendung des Telekommunikationsgesetzes .....	15
• Fernmeldegeheimnis gem. § 88 TKG .....	15
• Maßnahmen zum Schutz des Fernmeldegeheimnisses gem. § 109 TKG .....	16
• Zulässige Eingriffe in das Fernmeldegeheimnis gem. §§ 97, 100 TKG .....	16
bb) Anwendung von Teledienstegesetz und Teledienstedatenschutzgesetz .....	17
cc) Anwendung des Bundesdatenschutzgesetzes .....	18
c) Einsatz von nicht dem Unternehmen zugehörigen Arbeitnehmern .....	18
aa) Leiharbeiter .....	18
bb) Werk- oder Dienstverträge mit Auftragnehmern .....	18
d) Service-Provider als Internet-/Emaildienstleister (auch eigene Konzernunternehmen) ..	20
3. Handlungsoptionen .....	21
a) Allgemeines .....	21
b) Regelung im Arbeitsvertrag .....	21
aa) Internet und Email-Nutzung .....	21
bb) Datenerhebung und -nutzung .....	22
c) Regelung durch Betriebsvereinbarung .....	23
d) Kontrollmöglichkeiten des Arbeitgebers .....	24
aa) Technische Sicherheit .....	24
bb) Schutz des Unternehmens .....	24
cc) Kontrollbefugnisse bei ausschließlich dienstlicher Nutzung (Verbot der privaten Nutzung) .....	25
• Kostensteigerung und Überlastung des Netzes .....	26
• Verdacht auf Verletzung von Geschäftsgeheimnissen .....	27
dd) Kontrollbefugnisse bei Erlaubnis der privaten Nutzung .....	27
4. Steuerliche Aspekte der Nutzung von Email und Internet durch den Arbeitnehmer und ertragsteuerliche Beurteilung der Kosten für den Arbeitgeber .....	27

a) Ertragsteuerliche Beurteilung der Kosten für den Arbeitgeber.....	27
b) Lohnsteuerliche Beurteilung der Vorteile für den Arbeitnehmer .....	28
c) Auswirkung der Steuerbefreiung auf die Sozialversicherungspflicht.....	28
d) Umsatzsteuerliche Beurteilung der privaten Nutzung betrieblicher Einrichtungen durch den Arbeitnehmer .....	29
5. Strafrechtliche Situation.....	29
6. Fazit.....	31
7. Beispielformulierung für Arbeitsvertrag, Richtlinie oder Betriebsvereinbarung.....	32
Literaturhinweise/ Weiterführende Links .....	36
Profil .....	39



## Vorwort zur Version 1.3

Anlass für die Aktualisierung zur Version 1.3 war insbesondere die intensive Diskussion, die sich mittlerweile zur Frage der Strafbarkeit des Einsatzes von Emailfiltern entwickelt hat (Abschnitt 5 des Leitfadens). Berücksichtigt wurde aber auch die erste höchstinstanzliche Entscheidung zur fristlosen Kündigung wegen privatem Internetsurfen während der Arbeitszeit (BAG 2 AZR 581/04).

Berlin, den 29. August 2005

## Vorwort zur Version 1.2

Durch die am 26.6.2004 in Kraft getretene Novellierung des Telekommunikationsgesetzes (TKG) haben sich gesetzestechnische Änderungen ergeben, die eine redaktionelle Aktualisierung des vorliegenden Leitfadens erforderlich gemacht haben. So ist das Fernmeldegeheimnis nun in § 88 TKG (bisher § 85) geregelt; die Anforderungen an Maßnahmen zum Schutz des Fernmeldegeheimnisses aus dem ehemaligen § 87 sind in § 109 TKG geregelt. Weiter wurde durch die Novellierung im TKG ein eigener abschließender Datenschutzteil geschaffen, §§ 91-107 TKG. Durch die nun einheitliche gesetzliche Regelung im TKG entfallen die bisher parallel geltende Telekommunikationsdatenschutzverordnung (TDSV) und ihre Ermächtigungsgrundlage, § 89 TKG a. F. Eine inhaltliche Änderung der Version 1.1 ist damit nicht verbunden.

Berlin, den 29. April 2005

## Vorwort zur Version 1.1

Die Nutzung von Email und Internet im Unternehmen ist weiterhin ein viel diskutiertes Feld, in dem der vorliegende Leitfaden die erforderliche Orientierung und Hilfestellung zur eigenverantwortlichen und individuellen unternehmensinternen Regelung gibt. Wegen des stetigen Interesses an dem Leitfaden und der ausgesprochen positiven Resonanz der Leser hat der BITKOM Arbeitskreis Datenschutz die im letzten Jahr erschienene Version 1.0 zur vorliegenden Version 1.1 ausgebaut und aktualisiert. Ergänzungen haben sich vor allem in den Bereichen 2c), 4) und 5) sowie bei den weiterführenden Hinweisen ergeben; geringfügig erweitert wurde das Regelungsbeispiel (Ziffern 3.3, 4.4, 5.1 und 5.5)

Berlin, den 04. März 2004

## Vorwort

Dieser Leitfaden entstand als erste Publikation des BITKOM Arbeitskreises Datenschutz, der sich im Herbst 2001 konstituiert hat. Der Arbeitskreis besteht aus Experten der BITKOM-Mitgliedsfirmen und befasst sich mit aktuellen Themen und datenschutzspezifischen Aspekten der Informations- und Kommunikationstechnik. Ein Profil des Arbeitskreises findet sich am Ende des Leitfadens.

Besonderer Dank gilt folgenden Mitgliedern des Arbeitskreises Datenschutz, die mit ihrer Expertise und wertvollen praktischen Erfahrung ganz maßgeblich zur Entstehung des Leitfadens beigetragen haben:

- Mirko Schmidt, Motorola GmbH
- Regina Wacker-Dengler, Alcatel SEL AG
- Thomas Börner, debitel AG
- Ulrike Schroth, T-Systems Enterprise Services GmbH  
(Vorsitzende des Arbeitskreises)
- Ralf Maruhn, Nokia (Stellvertretender Vorsitzender des Arbeitskreises)
- Helmut Glaser, IBM
- Klaus Gatter, Marconi Communications GmbH
- Stefan Lerbs, Gemplus GmbH
- Eva Stoll, debitel AG
- Anne Bernzen, Detecon International GmbH

Für die zahlreichen Anregungen und die kritische Begleitung der Erstellung dieses Leitfadens aus arbeitsrechtlicher Sicht bedanken wir uns bei Volker Uebbing, Alcatel SEL AG.

Der Leitfaden kann angesichts der komplexen Materie keinen Anspruch auf Vollständigkeit erheben. Zudem ist die dargestellte Materie der fortlaufenden Entwicklung des Rechts und der Technik unterworfen. Letztlich versteht sich dieser Leitfaden daher als Einführung in die Problematik und Aufbereitung möglicher Handlungsmöglichkeiten, der jedoch die Einbindung professioneller unternehmensinterner oder externer Berater nicht überflüssig macht.

Berlin, den 18. Juli 2003



## 1. Einführung und Hintergrund

Der Einsatz von Informationssystemen am Arbeitsplatz und deren rasche technologische Entwicklung wirft eine Vielzahl datenschutzrechtlicher Fragen auf. Moderne Telefonanlagen, Personalcomputer und Telefaxgeräte gehören längst zu unverzichtbaren Hilfsmitteln der Kommunikation am Arbeitsplatz. Zusätzlich ist in den letzten Jahren eine schnell wachsende Entwicklung der Internet- und Emailnutzung in Betrieben zu beobachten.

Gerade weil der betriebliche Einsatz von Internet und E-mail oft zunächst langsam anläuft, werden die Folgen nicht sofort offensichtlich. Zugleich trifft die Einführung dieser neuen Kommunikationstechniken sehr viele Beschäftigte. Die Klärung datenschutzrechtlicher Fragen bezüglich der Internet- und Emailnutzung am Arbeitsplatz kann so zu einem aktuellen Konfliktfeld werden.

Dieser Leitfaden möchte über die möglichen datenschutzrechtlichen Probleme im Zusammenhang mit der Internet- und Emailnutzung in Betrieben aufklären sowie die Vor- und Nachteile der Zulassung von privater Internet- und Emailnutzung aufzeigen. In dem hier gegebenen Rahmen können nicht alle Fragen beantwortet werden. Wenden Sie sich für die Beantwortung offener Fragen daher auch an Ihren betrieblichen Datenschutzbeauftragten. Als Ansprechpartner steht Ihnen daneben die zuständige Aufsichtsbehörde zur Verfügung. Sowohl der betriebliche Datenschutzbeauftragte als auch die Aufsichtsbehörde haben die Ausführung der entsprechenden Datenschutzgesetze sicherzustellen.

Sämtliche im Bereich des Interneteinsatzes in Unternehmen vorgesehenen Maßnahmen sind nicht nur vor dem Hintergrund der hier angesprochenen datenschutzrechtlichen, sondern auch der arbeitsrechtlichen Anforderungen zu sehen. So sind die vorgesehenen Maßnahmen, soweit ein Betriebsrat konstituiert ist, insbesondere hinsichtlich ihrer Auswirkungen auf die Art der Arbeit und die Anforderungen an den Arbeitnehmer mit dem Betriebsrat zu beraten.

Unter bestimmten Voraussetzungen ist eine Kontrolle der Internet- oder Emailnutzung der Arbeitnehmer möglich. Ist in dem betreffenden Betrieb die private Internet- oder Emailnutzung erlaubt, ist der Arbeitgeber zahlreichen speziellen datenschutzrechtlichen Verpflichtungen der Informations- und Kommunikationsdienstegesetze (z.B. aus dem Telekommunikationsgesetz –TKG- und dem Teledienststedatenschutzgesetz -TDDSG-) unterworfen.

Um nicht diesen weit reichenden Datenschutzverpflichtungen zu unterliegen, kann es für den Arbeitgeber ratsam sein, die private Nutzung von Internet und Email über die betrieblichen EDV-Systeme zu untersagen oder im Vereinbarungswege zu regeln. Bei einem ausdrücklichen Verbot der privaten Internet- und Emailnutzung, d.h. einer ausschließlich dienstlichen Nutzung von Internet und Email, brauchen die datenschutzrechtlichen Bestimmungen der Telekommunikationsgesetze nicht beachtet zu werden. Für die rein dienstliche Nutzung des Internets finden nur die subsidiären Datenschutzbestimmungen des Bundesdatenschutzgesetzes Anwendung, wonach eine Interessenabwägung zwischen dem Interesse des Arbeitgebers an einem Schutz vor Missbrauch und Schutz der Datensicherheit und dem Schutz des Arbeitnehmers an der Wahrung der Persönlichkeitsrechte vorzunehmen ist. Dabei zeigt sich, dass je nach geschützter Zielrichtung und Interessenlage die Zulässigkeit von Kontrol-

Soweit nicht anders vermerkt, beziehen sich die folgenden Ausführungen nur auf nicht-öffentliche Stellen i.S.d. Bundesdatenschutzgesetzes. Darüber hinaus wird in den folgenden Ausführungen grundsätzlich nicht zwischen der lediglich internen, unternehmens-eigenen, geschäftlichen oder privaten sowie auch externen Nutzung des Emailanschlusses der Mitarbeiter unterschieden. Sollte es auf diese Unterscheidung ankommen, wird dies besonders ausgeführt.

Ein Glossar mit Erklärungen zu vielen Begriffen rund um das WorldWideWeb steht unter [http://www.bsi-fuer-buerger.de/glossar/glo\\_ef.htm](http://www.bsi-fuer-buerger.de/glossar/glo_ef.htm) zur Verfügung.

len unter Anwendung des Verhältnismäßigkeitsprinzips letztlich im Einzelfall bestimmt werden muss. Insbesondere die inhaltliche Vollkontrolle bleibt dem Arbeitgeber – wie bei dienstlichen Telefonaten – versagt.

## a) Technischer Hintergrund

Durch die zunehmende Vernetzung der Datenverarbeitung in Betrieben gewinnt der Datenschutz am Arbeitsplatz immer mehr an Bedeutung. In der Vergangenheit wurde Informations- und Kommunikationstechnik (IuK-Technik) nur für einzelne betriebliche Funktionen wie Lohn- und Gehaltsabrechnung, Buchführung oder Gleitzeitkontrolle eingesetzt. Dementsprechend ging es im Hinblick auf Datenschutz am elektronischen Arbeitsplatz bislang überwiegend um die Frage der Datenerhebung und -verarbeitung innerhalb begrenzter EDV-Systeme. Dagegen ist die gegenwärtige Situation aufgrund zunehmender technischer Konvergenz geprägt von einer Vernetzung bislang getrennter IuK-Techniken. Diese Vernetzung vollzieht sich in mehreren Schichten: Die Telekommunikationsebene und die Ebene der Dienstleistungen über die Telekommunikationsträger überlagern sich ebenso wie Intranet, Extranet, Internet etc. Die einzelnen Datenflüsse werden dadurch immer weniger überschaubar. Gleichzeitig steigen mit der zunehmenden Komplexität der Netzstrukturen auch die Anforderungen an die datenschutz- und datensicherheitsgerechte Verarbeitung der Datenmengen. Denn zwangsläufig entstehen bei jeder Nutzung von technischen Geräten oder Software der IuK-Technik auch personenbezogene Daten. Der jeweilige Nutzer hinterlässt Datenspuren, die z.B. Zeit, Dauer und Art seiner Nutzung dokumentieren.

Nutzt ein Arbeitnehmer den PC am Arbeitsplatz (aus dienstlichem oder privatem Anlass) um im Internet zu recherchieren oder versendet er eine Email, so entstehen dabei Verbindungsdaten. Je nach Einstellungen der Überwachungsfunktionen in der Firewall werden auch Nutzungsdaten und Inhaltsdaten mit aufgezeichnet. Diese werden auf ihrem Weg zwischen Sender und Empfänger an mehreren Stellen zwischengespeichert, wobei an jeder dieser Stellen die Möglichkeit besteht, die Daten zu kontrollieren. Die Mitarbeiteraktivitäten können direkt am betrieblichen Email-/Internet-Server oder beim Provider kontrolliert werden.

Firewall-System: Wird ein betriebsinternes Informationssystem - Intranet – an das Internet angeschlossen, so müssen Sicherheitsvorkehrungen zum Schutz der Datensicherheit im internen Netz getroffen werden. Kernstück solcher Sicherheitslösungen sind Firewall-Systeme („Brandschutzmauern“), die zwischen beide Netze geschaltet werden, so dass der gesamte Datenverkehr zwischen den beiden Netzen nur über das Firewall-System läuft. Dieses enthält neben Virencannern, die alle eingehenden und bei Bedarf auch die abgehenden Dateien bezüglich versteckter Viren überprüft, leistungsfähige Protokollierungsmöglichkeiten, um sicherheitsrelevante Angriffe auf das betriebsinterne Netz zu erkennen. Je nach Programmierung können in einem Logfile alle ein- und ausgehenden Emails sowie aus dem Internet heruntergeladene Dateien gespeichert werden mit der Möglichkeit, diese Daten auszuwerten. Die Protokollierungen an der Firewall dienen somit der Feststellung von sicherheitsrelevanten Angriffen auf das interne Netz. Sie können jedoch auch dazu benutzt werden, die Internetnutzung der Beschäftigten zu kontrollieren.

In der Praxis kommt der Datenprotokollierung im Firewall-System des Arbeitgebers die größte Bedeutung zu.

## b) Interessenlage

Nutzt der Arbeitgeber IuK-Technik an den Arbeitsplätzen der Mitarbeiter, so bestimmen auch Aspekte der Datensicherheit und des Datenschutzes diese Nutzung. Häufig haben Arbeitnehmer und Arbeitgeber unterschiedliche Interessen bei oder Vorstellungen von der Nutzung. Der Mitarbeiter ist regelmäßig daran interessiert, über die Preisgabe und Verwendung seiner persönlichen Daten selbst zu bestimmen. Er möchte bei der Nutzung moderner IuK-Technik im Rahmen der Vorgaben des Arbeitgebers möglichst überwachungsfrei sein. Der Arbeitgeber hingegen wird häufig ein nachvollziehbares Interesse daran haben, die Sicher-

heit seines Unternehmens zu gewährleisten, die Leistung der Mitarbeiter zu prüfen oder zu fördern und zu diesem Zweck auch personenbezogene Daten der Betroffenen verwenden zu können. Zudem unterliegt ihm die Gestaltung des Arbeitsplatzes und auch die Ausgestaltung der Nutzung von IuK-Technik. Die gesetzlichen Datenschutz- und Datensicherheitsvorschriften legen für die Lösung dieser Interessenkonflikte Wertungen fest, die beim Ausgleich zwingend zu beachten sind.

### c) Rechtlicher Hintergrund

Ein spezielles Gesetz über den Arbeitnehmerdatenschutz existiert (noch) nicht. Nach einer EU-weiten Befragung von Interessenverbänden, Unternehmen und Betroffenen hat die Europäische Kommission jedoch angekündigt, eine Richtlinie zum Arbeitnehmerdatenschutz vorzulegen.

In einem immer komplexer werdenden technischen wie normativen Umfeld ist auch zu beachten, dass Eingriffe in die verfassungsrechtlich geschützten Persönlichkeitsrechte von Arbeitnehmern vermieden werden.

Derzeit bestehen keine speziellen gesetzlichen Regelungen zu Einzelthemen wie etwa Kontrolle der Email- oder Internetnutzung, Videoüberwachung, Umgang mit Bewerberdaten, Erstellung von Persönlichkeitsprofilen usw. So wird die Zulässigkeit der Erhebung und Verarbeitung personenbezogener Daten im Arbeitsverhältnis bisher durch allgemeine gesetzliche Regelungen des Bundesdatenschutzgesetzes, Normen des Individualarbeitsrechts und insbesondere die Überwachung durch technische Überwachungseinrichtungen - soweit ein Betriebsrat existiert - durch im BetrVG festgeschriebenen Mitspracherechte und Mitbestimmungsrechte geregelt.

Mittlerweile liegt zumindest ein erstes höchstinstanzliches Urteil vor, das erste Konturen in dieser „rechtlichen Grauzone“ festschreibt und daher für die betriebliche Praxis einen wichtigen Orientierungspunkt darstellt. Das Bundesarbeitsgericht hat am 7. Juli 2005 über eine fristlose Kündigung wegen privatem Internetsurfen während der Arbeitszeit entschieden. Nach dem Urteil (2 AZR 581/04) verletzt ein Arbeitnehmer durch eine zeitlich intensive private Nutzung des Internet während der Arbeitszeit seine arbeitsvertraglichen Pflichten, auch wenn grundsätzlich die private Internetnutzung am Arbeitsplatz gestattet ist. Dies gilt insbesondere, wenn der Arbeitnehmer auf Internetseiten mit pornographischem Inhalt zugreift. Ein solches Verhalten kann nach Ansicht des Bundesarbeitsgerichts - je nach Schwere des Falles und der Gesamtumstände - sogar eine außerordentliche fristlose Kündigung rechtfertigen. Nach dem Bundesarbeitsgericht soll es für die Wirksamkeit einer Kündigung jedoch maßgeblich darauf ankommen, in welchem zeitlichen Umfang der Arbeitnehmer seine Arbeitsleistung durch das Internetsurfen vernachlässigt hat, ob er dabei seine konkreten Arbeitspflichten verletzt hat und welche Kosten dem Arbeitgeber durch die private Internetnutzung entstanden sind. Außerdem ist erschwerend zu berücksichtigen, wenn das Aufrufen pornographischer Webseiten aufgrund elektronischer Spuren einen Imageschaden für den Arbeitgeber verursacht. Entlastend kann zu werten sein, wenn eine beim Arbeitgeber bestehende Regelung zur privaten Internetnutzung für den Arbeitnehmer inhaltlich unklar ist.

Um der Verunsicherung entgegenzuwirken, die nach wie vor aus dieser „rechtlichen Grauzone“ entsteht, werden im Folgenden Möglichkeiten und Grenzen des Umganges mit personenbezogenen Daten im Arbeitsverhältnis aufgezeigt.

### d) Rechtliche Grundlagen

Unerlässlich ist es, sich zunächst die Normen und andere Rechtsgrundlagen zu vergegenwärtigen, die den Datenschutz am Arbeitsplatz inhaltlich prägen können:

## aa) Grundrechte: Das Recht auf informationelle Selbstbestimmung gem. Art.2 I i.V.m. Art.1 Grundgesetz

Als ein Teilbereich des allgemeinen Persönlichkeitsrechts gem. Art.2 I i.V.m. Art.1 Grundgesetz definiert das informationelle Selbstbestimmungsrecht die Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen er persönliche Lebenssachverhalte offenbart und in welcher Weise seine „Lebensdaten“ verwendet werden sollen. Wie sich das informationelle Selbstbestimmungsrecht auf das Arbeitsverhältnis auswirkt, hängt davon ab, welche Rechtswirkung Grundrechte im Privatrecht und damit auch im Arbeitsrecht entfalten.

Da Grundrechte in erster Linie Abwehrrechte des Bürgers gegen den Staat sind, sind sie auf das Verhältnis der Bürger untereinander nicht unmittelbar anwendbar. Grundrechte verkörpern jedoch gleichzeitig eine generelle objektive Werteordnung, wodurch sie mittelbar auf Rechtsbeziehungen Privater untereinander und damit auch auf das Arbeitsverhältnis einwirken. Das informationelle Selbstbestimmungsrecht kommt dabei über sog. ausfüllungsbedürftige Normen im Arbeitsrecht zur Anwendung. Ein wichtiges Beispiel dafür ist § 75 II des Betriebsverfassungsgesetzes (BetrVG). Nach dieser Norm haben der Arbeitgeber und der Betriebsrat die „freie Entfaltung der Persönlichkeit der Arbeitnehmer zu schützen und zu fördern“. Im Rahmen dieser ausfüllungsbedürftigen Begriffe kann das Recht auf informationelle Selbstbestimmung zur Anwendung kommen.

Mittelbarer Schutz der allgemeinen Persönlichkeitsrechte des Arbeitnehmers, insbesondere des informationellen Selbstbestimmungsrechts gem. Art. 2 I i.V.m. Art. 1 GG, durch § 75 II BetrVG.

Wichtige Begriffe des Datenschutzes im Zusammenhang mit Arbeitnehmerdatenverarbeitung:

- Nicht-öffentliche Stelle: vgl. § 3 BDSG, z.B. Firma.
- Personenbezogene Daten: „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person“ (§ 3 BDSG). Der Begriff ist sehr weit zu verstehen. Es gibt praktisch keine „harmlosen“ personenbezogenen Daten.
- Verarbeiten von personenbezogenen Daten: umfasst das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten gem. § 3 Abs. 4 BDSG.
- Das Datengeheimnis ist die Grundlage für die Verantwortung des Arbeitgebers im Umgang mit personenbezogenen Daten sowie für Sanktionen.

## bb) Fürsorgepflicht des Arbeitgebers aus §§ 611, 242 BGB

Als Nebenpflicht aus dem Arbeitsvertrag gem. § 611 BGB erwächst dem Arbeitgeber eine Fürsorgepflicht gem. § 242 BGB („Treu und Glauben“) für den Arbeitnehmer. Diese umfasst auch den Schutz der Handlungsfreiheit des Arbeitnehmers sowie seine persönliche Integrität einschließlich der Privat- und Intimsphäre.

## cc) Normen des Bundesdatenschutzgesetzes

Das Bundesdatenschutzgesetz (BDSG) ist als ein „Auffanggesetz“ ausgestaltet. Das heißt, dass seine Vorschriften nur zum Tragen kommen, soweit es keine anderen Regelungen oder Normen gibt, die den Sachverhalt schon abschließend regeln (vgl. §§ 1 III und 4 I BDSG). Auf das Arbeitsverhältnis findet insbesondere das kodifizierte Arbeitsrecht, dessen Normen durch die Rechtsprechung interpretiert werden, vorrangig Anwendung.

Das BDSG ist ein „Auffanggesetz“: Vorrang haben daher z.B.:

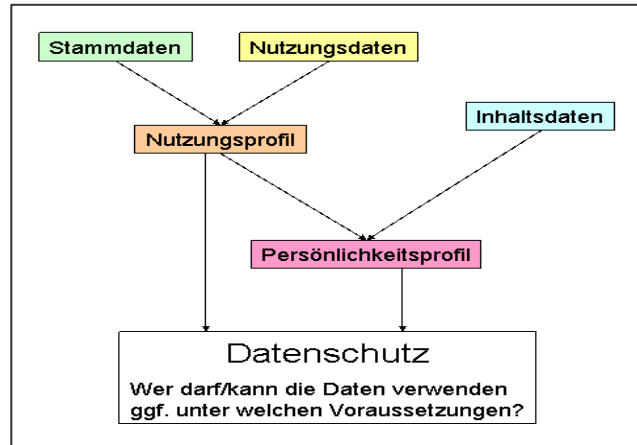
- die Einwilligung des Betroffenen (§ 4 I i.V.m. § 4a BDSG)
- bundesgesetzliche Regelungen (§1 III BDSG)
- andere Rechtsvorschriften (§ 4 I BDSG)
- die Regelungen des BDSG selbst (insb. § 4 I i.V.m. §§ 27 ff. BDSG)

Gibt es keine vorrangigen Regelungen zu beachten, so ist der Anwendungsbereich des BDSG eröffnet, wenn der Arbeitgeber Daten unter Einsatz von Datenverarbeitungsanlagen

erhebt, verarbeitet oder nutzt oder die Daten in oder aus nicht automatisierten Dateien erhebt, verarbeitet oder nutzt. Wichtig ist weiterhin, dass sich das BDSG nur auf personenbezogene Daten bezieht. Für die Datenverarbeitung in der Privatwirtschaft sind insbesondere die Abschnitte 1 und 3 des BDSG maßgeblich (vgl. §§ 1 II; 27 I BDSG)<sup>1</sup>.

## dd) Informations- und Kommunikationsdienste Gesetze

Zu einer besonderen Hürde bei der Verarbeitung betrieblicher Datenflüsse können die Regelungen des Telekommunikationsdatenschutzrechts werden. Die Telekommunikationsgesetze verfolgen (unter anderem) den Zweck, die sich aus der multimedialen Kommunikation ergebenden datenschutzrechtlichen Besonderheiten zu erfassen. Es handelt sich bei ihnen um Bundesgesetze i.S.d. § 1 III BDSG. Soweit die Anwendungsbereiche dieser Gesetze eröffnet sind, haben deren Regelungen Vorrang vor dem BDSG.



- **Telekommunikationsgesetz (TKG)**

Zweck des TKG ist die Förderung des Wettbewerbes und die flächendeckende Versorgung mit Telekommunikationsdiensten und die Wahrung der Interessen der Nutzer. Dieses geschieht grundsätzlich durch die Regulierung der Telekommunikation (vgl. § 1 TKG) sowie speziell durch die Wahrung des Fernmeldegeheimnisses (vgl. § 88 TKG) und des Datenschutzes (vgl. §§ 91-107 TKG) bei der Nutzung von Telekommunikationsdiensten. Die Vorschriften der §§ 88 und 91-107 TKG finden Anwendung, sobald ein Unternehmen geschäftsmäßig Telekommunikationsdienste erbringt. Grundsätzlich ist hierfür ein nachhaltiges Angebot von Telekommunikation einschließlich des Angebotes von Übertragungswegen **für Dritte** auch ohne Gewinnerzielungsabsicht ausreichend. Im Einzelnen wird hierauf noch an späterer Stelle eingegangen.

- **Teledienstegesetz (TDG)**

Das TDG schafft die Rahmenbedingungen für die verschiedenen Nutzungsmöglichkeiten elektronischer Teledienste (vgl. §§ 1f. TDG), wie z.B. Telebanking, Datendienste oder Dienste zur Nutzung des Internets.

- **Teledienstedatenschutzgesetz (TDDSG)**

Zweck des TDDSG ist die Sicherstellung des Schutzes personenbezogener Daten bei Telediensten. Es enthält daher Regelungen zur Verarbeitung personenbezogener Daten bei der Nutzung von Telediensten. Darüber hinaus begründet das TDDSG für die Anbieter von Telediensten besondere Pflichten (vgl. §§ 3-6 TDDSG).

Stammdaten: Daten, die notwendig sind, um die Dienstleistung überhaupt gegenüber einem Nutzer erbringen und ggf. abrechnen zu können.

Nutzungsdaten: Daten, die bei der Nutzung eines Dienstes anfallen, z.B. Aufzeichnungen über Tag, Uhrzeit und Dauer einer Internetverbindung, Email Adresse des Nutzers und des Empfängers (Bestands-, Verbindungs- und Entgeltdaten).

Inhaltsdaten: z.B. der Inhalt der Email bzw. der aufgerufenen Internetseiten.

Profile: vgl. Graphik S.10

<sup>1</sup> Die Vorschriften des 2. Abschnitts des BDSG gelten nur für öffentliche Stellen des Bundes, die nicht als öffentliche Unternehmen am Wettbewerb teilnehmen. Gleiches gilt für die öffentlichen Stellen der Länder, für die die entsprechenden Datenschutzgesetze der Länder einschlägig sind.

Internet, Email und alle anderen Teledienste beruhen auf der Nutzung von Telekommunikationseinrichtungen. Weil bei der Nutzung von Telediensten gleichzeitig auch Telekommunikationsdienste genutzt werden, können die Datenschutzregelungen der Telekommunikationsgesetze zur Anwendung kommen.

### ee) Tarifverträge und Betriebsvereinbarungen

Die Daten schützenden Regelungen aus dem BDSG und den spezialgesetzlichen Regelungen verleihen dem Einzelnen individuelle Rechte zum Schutz seines Rechtes auf informationelle Selbstbestimmung bzw. seines allgemeinen Persönlichkeitsrechts. Zu diesen Rechten können „kollektivrechtliche Datenschutzregelungen“ hinzutreten, sofern ein Betriebsrat im Unternehmen besteht.

Vorgesehene Maßnahmen sind zunächst gem. § 90 Abs.1 Ziffer 2 und 4 BetrVG hinsichtlich ihrer Auswirkungen auf die Art der Arbeit und die Anforderungen an den Arbeitnehmer mit dem Betriebsrat zu beraten. Mitbestimmungspflichtig gem. § 87 Abs.1 Ziffer 1 BetrVG sind Regelungen, die das Verhalten oder die Ordnung der Arbeitnehmer im Betrieb betreffen. Gleiches gilt für die Einführung technischer Überwachungseinrichtungen gem. § 87 Abs. 1 Ziffer 6 BetrVG. Nicht von der Mitbestimmung umfasst ist hingegen das „ob“, d.h. die Frage, ob die Nutzung des Internets überhaupt zugelassen wird. Gem. § 88 BetrVG können die Geschäftsleitung und der Betriebsrat auch außerhalb der erzwingbaren Mitbestimmung, z.B. nach § 87 I BetrVG, einvernehmliche Regelungen treffen. Da die Mitbestimmungsrechte auch die kollektivrechtliche Mitgestaltung zulässiger Eingriffe gewährleisten, können im Rahmen der gesetzlichen Mindestnormen des individuellen Datenschutzes - unter Beachtung des Persönlichkeitsrechtes des Arbeitnehmers - durch Betriebsvereinbarungen von den Parteien spezielle Regelungen geschaffen werden. Darüber hinaus sind auch tarifvertragliche Regelungen durch die Tarifvertragsparteien denkbar.

In ihrer zeitlichen Wirkungsweise sind diese Rechtsgrundlagen verschieden. Die Regelungen des BDSG greifen erst ein, wenn personenbezogene Daten verarbeitet werden, jedoch nicht im Vorfeld dieser Datenverarbeitung. Der „kollektivrechtliche Arbeitnehmerdatenschutz“ eröffnet bereits im Vorfeld, nämlich bei der Einführung einer Daten verarbeitenden Technologie (vgl. unten) die Möglichkeit, interessengerechte Lösungen herbeizuführen.

Kollektivrechtliche Regelungen zum Arbeitnehmerdatenschutz in Form von Tarifverträgen und Betriebsvereinbarungen gelten als „andere Rechtsvorschrift“ i.S.d. § 4 I BDSG und können dadurch besondere Zulässigkeitstatbestände für die Verarbeitung personenbezogener Arbeitnehmerdaten schaffen. Werden datenschutzrelevante Regelungen in einer Betriebsvereinbarung oder einem Tarifvertrag getroffen, so haben diese normative Wirkung. Sie schaffen objektives Recht, das die notwendige Grundlage für bestimmte Datenverarbeitungen bietet.

### ff) Beteiligungsrechte des Betriebsrats

Die im Betriebsverfassungsgesetz normierten Beteiligungsrechte des Betriebsrats ergänzen die datenschutzrechtlichen Bestimmungen. Es ist eine der Aufgaben des Betriebsrates, auch die Einhaltung des Datenschutzes im Unternehmen sicherzustellen. Es handelt sich insbesondere um die nachfolgenden Rechte:

Für Betriebsratsmitglieder gelten Sonderregeln (Schutz der Betriebsratstätigkeit vor jedweden Störungen), wenn die Nutzung von Internet und Email auch in der Funktion als Betriebsrat gestattet wird.

- **Allgemeine Aufgaben:**  
**Überwachungsrecht gem. § 80 I Nr.1 BetrVG**

Auf Grund der Generalklausel des § 75 II BetrVG haben der Arbeitgeber und der Betriebsrat die freie Persönlichkeitsentfaltung der Arbeitnehmer zu schützen und zu fördern (vgl. schon oben aa)). Diese Regelung wird durch das Mitwirkungsrecht des § 80 I Nr.1 BetrVG dahingehend konkretisiert, dass der Betriebsrat die Einhaltung der zugunsten des Arbeitnehmers geltenden Rechtsvorschriften zu überwachen hat. Zu diesen Rechtsvorschriften gehören auch die Regelungen des BDSG und die den Datenschutz betreffenden Bundesspezialgesetze.

### **Informationsanspruch gem. §§ 80 II, 111 BetrVG**

Nach den §§ 80 II, 111 BetrVG hat der Betriebsrat jederzeit einen umfassenden Auskunfts- und Informationsanspruch zur Durchführung seiner Aufgaben. Der Auskunfts- und Informationsanspruch erstreckt sich auf alle betrieblichen Vorgänge und erfasst daher auch die Verarbeitung von Daten der Arbeitnehmer.

#### • **Normsetzungsbefugnis:**

### **Mitbestimmungsrecht gem. § 87 I Nr. 6 BetrVG**

Gemäß § 87 I Nr.6 BetrVG hat der Betriebsrat bei der Einführung und Anwendung von technischen Einrichtungen, die dazu geeignet sind, das Verhalten oder die Leistung der Mitarbeiter zu überwachen, ein Mitbestimmungsrecht (soweit gem. § 87 I BetrVG keine gesetzliche oder tarifliche Regelung besteht). Die Vorschrift dient mehreren Zwecken: Zum einen soll sie als präventiver Schutz rechtlich unzulässige Eingriffe in Persönlichkeitsrechte des Einzelnen bereits im Vorfeld verhindern. Zudem sichert es dem Betriebsrat ein Mitbeurteilungsrecht bei der schwierigen Ermittlung der Grenze zwischen zulässiger und unzulässiger Datenverarbeitung. Schließlich gewährleistet die Mitbestimmung des Betriebsrates, dass zulässige Eingriffe in das Persönlichkeitsrecht auf das unbedingt erforderliche Maß reduziert werden. Besondere Aktualität hat dieses Mitbestimmungsrecht durch den Einsatz neuer IuK-Techniken gewonnen. Ihre Einführung und Anwendung unterliegt dem Mitbestimmungsrecht des Betriebsrats schon dann, wenn das jeweilige IuK-System zur Überwachung geeignet ist. Ob die Überwachung auch tatsächlich erfolgen soll, ist hingegen für das Mitbestimmungsrecht nicht relevant.

#### **Wichtige Beteiligungsrechte des Betriebsrates:**

- Überwachungsrecht gem. § 80 I Nr.1 BetrVG
- Informationsanspruch gem. §§ 80 II, 111 BetrVG
- Mitbestimmungsrecht gem. § 87 I Nr.6 BetrVG

Zur Herbeiführung einer normativen Wirkung sollten mitbestimmte Regelungen in Form einer Betriebsvereinbarung unter Beachtung der entsprechenden Formerfordernisse erfolgen.

## **2. Datenschutzverpflichtungen des Arbeitgebers bei der Nutzung von Internet und Email am Arbeitsplatz**

Mit der Frage, ob den Arbeitnehmern die private Internet- bzw. Emailnutzung gestattet oder verboten ist, verbindet sich eine entscheidende Weichenstellung: Nur, wenn die private Nutzung durch die Arbeitnehmer zugelassen ist, kommen die datenschutzrechtlichen Regelungen des TKG, des TDG und des TDDSG im Verhältnis zum Arbeitgeber zur Anwendung. Ist jedoch dem Arbeitnehmer nur die

! Auch ein völlig regelungsloser Zustand bezüglich der dienstlichen und privaten Nutzung von Email und Internet oder ein nicht überwachtes Verbot der privaten Nutzung kann dazu führen, dass eine sog. „**betriebliche Übung**“ geschaffen wird. Diese kann u.U. als Erlaubnis der privaten Nutzung gewertet werden. (Siehe dazu auch unten S. 25, 3 d cc)

rein dienstliche Nutzung von Internet und Email erlaubt, sind diese Gesetze insoweit für den Arbeitgeber irrelevant. Diese Konstellation, dass dem Arbeitnehmer lediglich die dienstliche Nutzung von Internet und Email erlaubt ist, wird im Folgenden näher erläutert:

## a) Dienstliche Nutzung

### aa) Anwendung des Telekommunikationsgesetzes

Die Anwendbarkeit des TKG setzt voraus, dass ein Dienstleister einem „Dritten“ ein Angebot über eine Telekommunikationsdienstleitung macht. Die Bereitstellung eines Internet-Zugangs durch den Arbeitgeber für die Arbeitnehmer stellt grundsätzlich ein Angebot von Telekommunikation dar. Jedoch ist der Arbeitnehmer im Verhältnis zum Arbeitgeber nur dann „Dritter“, wenn er diese Dienstleistung nicht nur für den Arbeitgeber nutzt, sondern die Nutzung auch für eigene Zwecke des Arbeitnehmers freigegeben ist. Bei rein dienstlicher Nutzung des Internet oder des Emailsystems durch den Arbeitnehmer dient die Erbringung dieses Telekommunikationsdienstes aber nicht fremden, sondern ausschließlich dienstlichen und damit eigenen Zwecken. Der Arbeitnehmer ist daher nicht als „Dritter“ anzusehen, so dass das TKG keine Anwendung findet.

### bb) Anwendung von Teledienstgesetz und Teledienstedatenschutzgesetz

Die Regelungen im TDG und TDDSG knüpfen gem. § 2 TDDSG an die Begriffe des „Diensteanbieters“ und des „Nutzers“ an. Entscheidend ist daher zunächst, ob der einzelne Arbeitnehmer bei rein dienstlicher Nutzung des Internet-Zugangs überhaupt als „Nutzer“ einzustufen ist.

Bei der nur dienstlichen Internetnutzung ist jedoch nicht der Arbeitnehmer, sondern der Arbeitgeber als Inhaber des Internetzugangs als „Nutzer“ anzusehen. Die Folge ist, dass die datenschutzrechtlichen Bestimmungen des TDDSG nicht zur Anwendung kommen. Der Arbeitgeber wäre hiernach nicht gehindert, die gesamte Unternehmenskommunikation nach seinem Ermessen aufzuzeichnen und weiterzuverarbeiten. Eine Grenzziehung für die dabei notwendigerweise anfallenden personenbezogenen Daten der Mitarbeiter ergibt sich aber aus den subsidiären Regelungen des BDSG (vgl. unten cc)).

#### Bei rein dienstlicher Nutzung:

##### Keine Anwendbarkeit des TKG:

Der Arbeitnehmer ist kein Dritter i.S.d. TKG, da die Bereitstellung eines Zuganges nur dienstlichen und damit eigenen Zwecken des Arbeitgebers dient.

##### Keine Anwendung des TDG und des TDDSG:

Bei rein dienstlicher Nutzung ist nur der Arbeitgeber, nicht aber der Arbeitnehmer als Nutzer des Zugangs anzusehen.

### cc) Anwendung des Bundesdatenschutzgesetzes

Die bei der Nutzung des Internets entstehenden Verbindungs-, Nutzungs- und Inhaltsdaten sind personenbezogene Daten, die der Arbeitgeber durch die Einrichtung eines Überwachungssystems erhebt. Aufgrund der fehlenden Anwendbarkeit der Telekommunikations-Datenschutzgesetze richtet sich diese Verarbeitung aller Datenarten nach den Regelungen des BDSG. Es gelten grundsätzlich die Regeln der §§ 4, 27, 28 BDSG. Nach §§ 4 I, 1 III BDSG ist die Verarbeitung personenbezogener Daten und deren Nutzung nur zulässig, wenn sie insbesondere durch

#### Bei rein dienstlicher Nutzung

- richtet sich der Datenschutz nach den §§ 3a, 4, 27 und 28 BDSG.
- ist die Nutzung personenbezogener Daten zulässig, wenn deren Verwendung im Rahmen der Zweckbestimmung des Vertragsverhältnisses zwischen Arbeitgeber und Arbeitnehmer erfolgt.
- oder, wenn die Nutzung dem Zweck der Datensicherung oder dem ordnungsgemäßen Betrieb der Datenverarbeitungsanlage dient, § 31 BDSG.

- die Vorschriften des BDSG

erlaubt ist. Nach § 28 BDSG ist z.B. die Erhebung und Speicherung, Veränderung und Übermittlung der Verbindungs-, Inhalts- und Nutzungsdaten der Arbeitnehmer zulässig,

- wenn die Verwendung der personenbezogenen Daten der Zweckbestimmung des Arbeitsvertragsverhältnisses zwischen Arbeitgeber und Arbeitnehmer dient (§ 28 I Nr.1) oder
- soweit es zur Wahrung berechtigter Interessen des Arbeitgebers erforderlich ist und ein schutzwürdiges Interesse des Arbeitnehmers nicht überwiegt (§ 28 I Nr.2).

Das Gesetz selbst sagt nichts darüber aus, was der “Zweckbestimmung“ des Arbeitsverhältnisses dient und was nicht; es benennt auch nicht konkrete berechnete und schutzwürdige Interessen. Aus der Vorschrift lässt sich jedoch folgern, dass die Nutzung von solchen personenbezogenen Daten der Arbeitnehmer zulässig ist, die zur Erfüllung der Pflichten oder zur Wahrnehmung der Rechte aus dem Arbeitsvertrag erforderlich sind, sofern darin kein unverhältnismäßiger Eingriff in das Persönlichkeitsrecht des Arbeitnehmers liegt.

Zu diesen Daten gehören auch Daten über Tatsachen, die die Verwirklichung des Vertragszwecks gefährden können, also z.B. tatsächliche oder vermeintliche Verletzungen der dem Vertragspartner gegenüber obliegenden Verpflichtungen. Ob die Nutzung dieser Daten zulässig ist, kann aber letztlich nur in einer einzelfallbezogenen Betrachtung ermittelt werden (vgl. unten zu den Kontrollmöglichkeiten des Arbeitgebers). Eine besondere Erlaubnis gibt auch § 31 BDSG. Danach ist eine Protokollierung und Speicherung von Daten zum Zweck der Datensicherung oder der Gewährleistung eines ordnungsgemäßen Betriebs der Datenverarbeitungsanlage möglich. Es ist also zulässig, mit Hilfe der Protokolldaten einen Virenangriff etc. nachzuweisen, nicht aber, diese Daten zur Leistungskontrolle der Arbeitnehmer auszuwerten. Darüber hinaus ist auch der Grundsatz der Datenvermeidung und der Datensparsamkeit zu beachten (§ 3 a BDSG).

## b) Private Nutzung

Ganz anders ist die Situation, wenn der Arbeitgeber die private Nutzung von Internet und Email gestattet oder die Nutzung duldet. Die Duldung kann u.U. zu einer Gestattung aufgrund einer betrieblichen Übung (vgl. Kästchen S. 12) führen.

### aa) Anwendung des Telekommunikationsgesetzes

Gestattet der Arbeitgeber die private Nutzung des Internet-/Emailzugangs – gleichgültig, ob entgeltlich oder unentgeltlich – so wird er zum geschäftsmäßigen Anbieter von Telekommunikationsdiensten, da er den Internetzugang für fremde Zwecke zur Verfügung stellt. Der Arbeitnehmer ist dann nicht mehr als Teil des Unternehmens, dem Betreiber der Anlage, sondern als „Dritter“ gem. § 3 Nr.5 TKG einzuordnen. Somit unterliegt der Arbeitgeber, wenn er den Arbeitnehmern die private Internetnutzung gestattet, den folgenden Verpflichtungen bzw. Einschränkungen des TKG:

- **Fernmeldegeheimnis gem. § 88 TKG**

§ 88 TKG bestimmt, dass „der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war“ dem Fernmeldegeheimnis unterliegen. Zu diesem Fernmeldegeheimnis haben das Bundesverfassungsgericht und das Bundesarbeitsgericht Grundsätze für die Telekommunikation mittels Telefon entwickelt, die auf die Telekommunikation mittels Internet/Email übertragen werden können. Da durch das Fernmeldegeheimnis jede Art der Telekommunikation geschützt ist, werden auch alle Inhalts- und Verbindungsdaten, die Auskunft über die am Internet-/Emailaustausch Beteiligten geben könn-

ten, vor einer Preisgabe geschützt. Aus einer Analogie zu der Rechtsprechung bzgl. der Telefonüberwachung lässt sich herleiten, dass auch die Installation von Überwachungssystemen für die Internetnutzung in das allgemeine Persönlichkeitsrecht bzw. Fernmeldegeheimnis eingreift. Da über die Installation einer Firewall oder eines entsprechenden Protokollierungsprogramms je nach Programmierung die Verbindungsdaten und evtl. die Inhalte der Internet- und Emailnutzung aufgezeichnet werden, ist die Überwachung der Inhalte und Verbindungsdaten der Internet-/Emailnutzung daher unzulässig, soweit keine Rechtfertigung für diesen Eingriff vorliegt. Trennt der Arbeitgeber eine erlaubte private Kommunikation nicht von der dienstlichen Kommunikation, so erstreckt sich die Geheimhaltungspflicht auch auf dienstliche Emails. Eine Aufhebung des Fernmeldegeheimnisses durch eine Betriebsvereinbarung ist nicht möglich.

**Bei Erlaubnis der privaten Nutzung unterliegt der Arbeitgeber erheblichen Verpflichtungen:**

1. Wahrung des Fernmeldegeheimnisses: Jegliche Überwachung der Inhalte sowie der Verbindungsdaten der Internet- und Emailnutzung ist unzulässig.

• **Maßnahmen zum Schutz des Fernmeldegeheimnisses gem. § 109 TKG**

Neben der Wahrung des Fernmeldegeheimnisses ist der Arbeitgeber als Erbringer geschäftsmäßiger Telekommunikationsdienste gem. § 109 I TKG zu angemessenen technischen Vorkehrungen und sonstigen Maßnahmen zum Schutz des Fernmeldegeheimnisses verpflichtet. Diese Maßnahmen werden im Regelfall einen erheblichen Mehraufwand darstellen. Die Verpflichtung bezieht sich nur auf solche Datenverarbeitungssysteme, die bei der geschäftsmäßigen Erbringung von Telekommunikationsdiensten eingesetzt werden, wie z.B. ein PC mit Internet-/Emailzugang.

Als Maßnahmen zum Schutz des Fernmeldegeheimnisses kommen Zutritts- und Zugriffsbeschränkungen, Verschlüsselungen sowie der Schutz der Firewall-Auswertungsprotokolle vor unbefugter Einsichtnahme in Betracht. Da das TKG in erster Linie auf gewerbliche Betreiber von Telekommunikationsanlagen zielt, wird davon ausgegangen, dass die Anforderungen an die zu treffenden technischen Schutzvorkehrungen durch den Arbeitgeber nicht überzogen sein dürfen. Anhand des Einzelfalls muss geprüft werden, ob dem Arbeitgeber die Einhaltung des in § 109 I TKG genannten Katalogs von Sicherheitsanforderungen zuzumuten ist.

2. Schutz des Fernmeldegeheimnisses: Alle Inhalts- und Verbindungsdaten, die Auskunft über die an der Internetnutzung oder am Emailverkehr Beteiligten geben könnten, sind durch angemessene technische Vorkehrungen und sonstige Maßnahmen vor Kenntnisnahme zu schützen.

• **Zulässige Eingriffe in das Fernmeldegeheimnis gem. §§ 97, 100 TKG**

Die gesetzlich zulässigen Eingriffe in das Fernmeldegeheimnis sind in §§ 97 und 100 TKG aufgeführt. Nach § 97 TKG dürfen Verbindungsdaten von Arbeitnehmern, die sich im Internet bewegen, erhoben werden, um das Entgelt für die Telekommunikationsdienste zu ermitteln. Gem. § 100 ist die Verarbeitung ebenfalls zulässig, wenn sie zur Erkennung, Eingrenzung oder Beseitigung von Störungen oder Fehlern an TK-Anlagen und für das Aufklären und Unterbinden rechtswidriger Inanspruchnahme des Internet-/Emailzugangs erforderlich ist. Für den zuletzt genannten Zweck kann daher die Protokollierung der Internetnutzung an der Firewall oder durch ein Überwachungsprogramm zulässig sein. Voraussetzung ist nach § 100 III TKG, dass tatsächliche Anhaltspunkte für eine rechtswidrige Inanspruchnahme vorliegen. Der Verdacht darf sich gerade nicht aus der Protokollierung ergeben, sondern es müssen konkrete Anhaltspunkte für einen Missbrauch der Internet-/Emailnutzung sprechen.

## bb) Anwendung von Teledienstegesetz und Teledienstedatenschutzgesetz

Während das TKG die Sicherheit und den Schutz der Verbindungsdaten gewährleisten soll, regeln das TDG und das TDDSG, was mit den Nutzungsdaten geschehen kann.

Gestattet der Arbeitgeber die private Nutzung des Internetzugangs, so ist er ein „Diensteanbieter“ im Sinne des TDG und der Arbeitnehmer wird zum „Nutzer“, da er unabhängig vom Arbeitsverhältnis das Angebot des Arbeitgebers ablehnen kann (vgl. schon oben 2 a bb)). Damit treffen den Arbeitgeber hinsichtlich der bei der privaten Nutzung des Internet anfallenden Daten insbesondere die Datenschutzverpflichtungen des TDDSG (bzw. des Mediendienstestaatsvertrags -MDSStV-, welcher inhaltsgleiche Regelungen enthält):

- Nach dem Grundsatz des Systemdatenschutzes soll bereits durch die Gestaltung der Systemstrukturen, in denen personenbezogene Daten erhoben und verarbeitet werden, einer unzulässigen Datenverwendung vorgebeugt werden. Der Diensteanbieter soll daher sein Angebot danach ausrichten, so wenig personenbezogene Daten wie möglich zu verarbeiten. Dieser Grundsatz findet seine Ausprägung in § 4 TDDSG, wonach der Arbeitgeber als Diensteanbieter dem Arbeitnehmer als Nutzer die Inanspruchnahme von Email und Internetnutzung gem. § 4 TDDSG anonym oder pseudonym zu ermöglichen hat, soweit dies technisch möglich ist. Diese Regelung dürfte die Auswertung der Internet-/Emailnutzungsprotokolle des Firewall-Systems oder der Kontrollprogramme im betrieblichen Rahmen erschweren.

3. Grundsatz des Systemdatenschutzes: Reduzierung der Erhebung von personenbezogenen Daten auf ein Mindestmaß.

- Zudem unterliegen gem. § 6 I TDDSG alle bei der Internet-Nutzung erhobenen Bestands-, Nutzungs- und Abrechnungsdaten dem Gebot der Erforderlichkeit. Das bedeutet, dass der Arbeitgeber diese Daten nur insoweit erheben darf, als sie zur Abrechnung, Nutzung oder für das Vertragsverhältnis notwendig sind. Die Protokollierung der privaten Nutzung ist nur zu Abrechnungszwecken bzw. nach den Zulässigkeitsnormen des BDSG zulässig oder nach konkret erteilter Einwilligung des Arbeitnehmers. Daher sind nicht benötigte Daten von Arbeitnehmern, die privat das Internet/Email nutzen, nach Ende der jeweiligen Nutzung (z.B. nach Auswertung der Nutzungsprotokolle zur Abrechnung) zu löschen.

4. Grundsatz der Erforderlichkeit: Die Protokollierung der privaten Nutzung ist nur zulässig, soweit sie zu Abrechnungszwecken erforderlich ist. Diese Daten sind unverzüglich nach dem Ende der jeweiligen Nutzung (z.B. nach Auswertung der Nutzungsprotokolle zur Abrechnung) zu löschen.

- Schließlich ist es für den Arbeitgeber ratsam, die im Rahmen des Arbeitsvertrages anfallenden Daten der Nutzung des Internet-/Emailsystems organisatorisch getrennt von den im Rahmen des privaten Nutzungsverhältnisses anfallenden Daten zu speichern. Geschieht das nicht, gilt alle Email und Internetnutzung bzw. Kommunikation – auch die dienstliche – als privat.

5. Trennt der Arbeitgeber die private Emailnutzung nicht logisch oder physisch von der dienstlichen Nutzung, z.B. durch separate Email-Anschriften oder Vorgabe einer Pflicht zur Kennzeichnung als „privat“, so ist jede Kommunikation als privat anzusehen (so die Auffassung der Aufsichtsbehörde in Baden-Württemberg).

Erforderlich ist die gesonderte Speicherung der Daten aus dem privaten Nutzungsverhältnis.

### cc) Anwendung des Bundesdatenschutzgesetzes

Im Gegensatz zur dienstlichen Nutzung bleibt im Bereich der privaten Nutzung von Internet und Email aufgrund der Subsidiarität der Vorschriften des BDSG nur noch ein beschränkter Anwendungsbereich für das BDSG übrig. Nur soweit die Spezialvorschriften des Telekommunikations-Datenschutzes keine Regelungen enthalten und auch eine weitere Verarbeitung von Verbindungs- und Nutzungsdaten hierdurch nicht ausgeschlossen ist, können diese Daten auf der Grundlage des BDSG weiterverarbeitet oder genutzt werden. Das betrifft insbesondere die Erhebung, Verarbeitung oder Nutzung von sog. Inhaltsdaten.

#### Bei privater Nutzung

gelten regelmäßig die Telekommunikations- und Teledienstedatenschutzregelungen.

Das BDSG kommt nur zur Anwendung, soweit

- keine Spezialregelungen greifen.
- eine Verarbeitung durch die telekommunikationsrechtlichen Normen nicht ausgeschlossen ist.

### c) Einsatz von nicht dem Unternehmen zugehörigen Arbeitnehmern

Häufig werden in Unternehmen Personen tätig, die keinen Arbeitsvertrag mit dem Unternehmen haben (bspw. Leiharbeiter, Auftragnehmer). Auch in dieser Situation hängt die Anwendbarkeit der Vorschriften des TKG sowie des TDG und des TDDSG entscheidend davon ab, ob das Unternehmen ein „nachhaltiges Angebot von Telekommunikation einschließlich von Übertragungswegen für Dritte“ erbringt (vgl. § 3 Nr. 5 TKG), bzw. diese Personen als „Nutzer von Telediensten“ auftreten (vgl. § 3 Nr. 2 TDDSG).

#### aa) Leiharbeitnehmer

Der Leiharbeitnehmer wird auf Grundlage des Entleihvertrages in dem entleihenden Unternehmen eingesetzt. Das verleihende Unternehmen erhält dafür die Vergütung. Im Gegenzug tritt das Unternehmen regelmäßig das aufgrund des Arbeitsverhältnisses zwischen dem Leiharbeitnehmer und dem entleihenden Unternehmen bestehende Weisungsrecht an das entleihende Unternehmen ab. Der Leiharbeitnehmer ist an die Weisungen des Entleihers gebunden. Insoweit besteht während der Zeit der Entleihe eine vergleichbar starke Bindung wie zu einem Vertragsarbeitgeber. Leiharbeitnehmer haben sich an bestehende Betriebsvereinbarungen zu halten und können auch durch Betriebsvereinbarungen des Entleihbetriebs erfasst, in die Pflicht genommen oder begünstigt werden.

Aus diesem Grunde sind Leiharbeitnehmer – in dem hier aufgeführten Zusammenhang der Nutzung von Email und Internet – wie Vertragsarbeitnehmer zu behandeln. Es ergeben sich keine Unterschiede zu dem im Vorangegangenen dargestellten.

#### bb) Werk- oder Dienstverträge mit Auftragnehmern

Die Tätigkeit nicht unternehmenszugehöriger Personen in einem Unternehmen erfolgt regelmäßig aufgrund eines Werk- oder Dienstvertrages. Das Unternehmen ist dann der Auftraggeber, die nicht unternehmenszugehörige Person ist ein Auftragnehmer, der selbst oder durch seine Mitarbeiter die vertraglich geschuldete Leistung erbringt. Der Auftragnehmer oder seine Mitarbeiter sind in diesem Rahmen Erfüllungsgehilfen des Auftraggebers (vgl. § 278 BGB).

### **Situation 1**

Stellt der Auftraggeber dem Auftragnehmer zur Erfüllung seiner Aufgaben die notwendigen Ressourcen der Telekommunikation (z.B. durch Telefon oder Internetanschluss) und der Teledienste (z.B. Intranet, Email) zur Verfügung, sind die folgenden Besonderheiten zu beachten:

- **Anwendbarkeit von TKG**

Für die Anwendbarkeit des TKG kommt es u. a. darauf an, ob der Auftragnehmer Dritter i.S. des TKG ist. Der Auftragnehmer ist dann **nicht Dritter** i.S.d. Vorschriften, wenn er die Telekommunikationsmöglichkeiten, die vom Auftraggeber zur Verfügung gestellt werden, nur für Zwecke des Auftraggebers nutzen darf. Dies trifft regelmäßig auf alle Handlungen zu, die der Auftragnehmer oder dessen Mitarbeiter ausschließlich zur Erfüllung des Auftragsverhältnisses vornehmen (vgl. oben: Stellung als Erfüllungsgehilfe). In diesem Fall liegt kein Angebot und keine Erbringung von Telekommunikationsdiensten für andere (Dritte) im Sinne des TKG vor; das TKG ist nicht anwendbar.

- **Anwendbarkeit des TDG, TDDSG**

Soweit die Nutzung von Telediensten (z.B. Internetzugang, Email) durch den Auftragnehmer ausschließlich im Rahmen seiner Tätigkeit als Erfüllungsgehilfe erfolgt, findet das TDG zwar Anwendung (Begriff des „Nutzers“ ist erfüllt, auch wenn z.B. festgestellt wurde, dass der Auftragnehmer nicht Dritter i.S.d. TKG ist). Eine Anwendung des TDDSG entfällt jedoch aufgrund der Regelung in § 2 Abs. 2 Nr. 1 TDDSG. Ausweislich der Gesetzesbegründung soll das TDDSG nur im Verhältnis von Anbietern und (End-) Nutzern von Telediensten gelten. Es geht um den Schutz der personenbezogenen Daten natürlicher Personen, die als Verbraucher Teledienste nachfragen. Vorgänge, die ausschließlich der Steuerung von Arbeits- und Geschäftsprozessen dienen, sollen vom Anwendungsbereich des TDDSG gerade nicht erfasst werden. Hierzu gehören z. B. Systeme zur Erfassung und Abrechnung der erbrachten Dienstleistung, EDI, aber auch Email oder Internetanbindung, soweit diese ausschließlich zur Durchführung entsprechender Arbeitsprozesse eingesetzt werden. Im Ergebnis ist das TDDSG damit ein Schutzgesetz für Endverbraucher.

### **Situation 2**

Handelt es sich um einen nur kurzen Einsatz des Auftragnehmers beim Auftraggeber und/oder stellt der Auftraggeber dem Auftragnehmer zur Erfüllung seiner Aufgaben keine Ressourcen der Telekommunikation und der Teledienste zur Verfügung, weil diese nicht notwendig sind (Beispiel: Der Auftragnehmer bekommt keinen Telefonanschluss in seinem Raum), nutzt der Auftragnehmer aber die sonstigen vorhandenen Ressourcen der Telekommunikation, so kann von folgendem ausgegangen werden:

#### Umsetzungsempfehlungen bei Werk- oder Dienstverträgen mit Auftragnehmern

Grundsätzlich kann der Auftraggeber davon ausgehen, dass das TDSSG aufgrund der Stellung des Auftragnehmers als Erfüllungsgehilfe keine Anwendung findet (keine „Dritten“ i.S.d. TKG). Das gilt ebenso für die Spezialregelung TDDSG.

Einer besonderen Beachtung oder Regelung dieses Themas in den Werk-, Dienst- oder Beratungsverträgen mit dem Auftragnehmer bedarf es nicht. Die Privatnutzung bzw. die Nutzung der Ressourcen des Auftraggebers zu eigenen Zwecken des Auftragnehmers gehört per se nicht zu den Befugnissen oder Aufgaben des Auftragnehmers bzw. seiner Mitarbeiter. Der Auftraggeber hat daher auch insoweit keine besonderen Aufklärungspflichten. Der Auftragnehmer ist vielmehr verpflichtet, bestehende Rahmenbedingungen (Regeln) des Auftraggebers vollständig zu beachten.

Gleichwohl ist es für den Auftraggeber ratsam, den Auftragnehmer über die unternehmensspezifischen Regelungen aufzuklären. Gerade beim Outsourcing kann es – je nach bisheriger Situation im eigenen Unternehmen – sinnvoll sein, den neuen Auftragnehmer auf eine veränderte Situation hinzuweisen und z. B. deutlich zu machen, dass es verboten ist, Email und Internet privat zu nutzen bzw. dass Aufzeichnungen und Kontrollen stattfinden.

- **Anwendbarkeit TKG**

Unabhängig von den Überlegungen zum Status des Auftragnehmers als „Dritter“ i.S.d. TKG fehlt es hier schon an einem „nachhaltigen Angebot von Telekommunikation einschließlich der Übertragungswege“. Die nur gelegentliche Nutzung bereits vorhandener Ressourcen der Telekommunikation, die nicht ausdrücklich dem Auftraggeber oder einem begrenzten Personenkreis von Auftragnehmern zugeordnet sind, erfüllt nicht den Tatbestand des „nachhaltigen Angebots“ i.S.d. TKG.

- **Anwendbarkeit TDG, TDDSG**

Die nur gelegentliche Nutzung bereits vorhandener, aber nicht bereitgestellter Ressourcen an Telediensten (Beispiel: Ein Mitarbeiter lässt den Auftragnehmer über den Internetanschluss des Unternehmens privat im Internet surfen) stellt erst recht kein „Anbieten“ i.S.d. TDG dar. Ein „Anbieter-Nutzer-Verhältnis“ kommt gar nicht zustande. Die Anwendbarkeit des TDG und damit auch des TDDSG entfällt schon aus diesem Grund. An der Anwendbarkeit fehlt es selbstverständlich auch, wenn der Auftragnehmer sich den Zugang zu den Telediensten rechtswidrig erschleicht.

### Sonstige Situationen

In allen anderen Konstellationen kann nur eine genaue Einzelfallbetrachtung Klarheit über die Anwendbarkeit von TKG, TDG und TDDSG schaffen. Ggf. sollten daher Spezialisten zu Rate gezogen werden. Bereiche, die regelmäßig einer besonderen Einzelfallbetrachtung bedürfen, sind insbesondere:

- die erlaubte Nutzung von Ressourcen der Telekommunikation durch den Auftragnehmer für private Zwecke,
- Reisebürofilialen oder Dienstleistungen anderer Art, die ihre Dienste nicht ausschließlich einem Unternehmen zur Verfügung stellen, deren Fax-, Telefon- und Internetanschluss aber über die gleichen Ressourcen abgewickelt werden, wie die des Unternehmens,
- Einrichtungen der Telekommunikation sowie Teledienste in Tagungszentren, Krankenhäusern, Hotels, Restaurants, Corporate Networks.

### **d) Service-Provider als Internet-/E-maildienstleister (auch eigene Konzernunternehmen)**

Die oben dargestellten Punkte sind auch zu beachten, wenn ein Service Provider diese Dienstleistung für das Unternehmen erbringt. Dabei spielt es keine Rolle, ob es sich hierbei um einen externen Provider oder ein konzernangehöriges Unternehmen handelt. Grundlage der Tätigkeit des Service Providers ist regelmäßig ein Auftragsverhältnis. Datenschutzrechtlich kommt eine Auftragsdatenverarbeitung nach § 11 BDSG in Betracht. Der Auftraggeber (=Arbeitgeber) bleibt bei dieser Konstellation für die Rechtmäßigkeit der Verarbeitung der personenbezogenen Daten verantwortlich, vgl. § 11 I BDSG. Der Auftragnehmer hat die Daten nach den Weisungen des Auftraggebers zu verarbeiten und wird datenschutzrechtlich dem Auftraggeber als Teil der verantwortlichen Stelle zugerechnet. Die Anforderungen an einen Auftragnehmer im Falle der Auftragsdatenverarbeitung sind vertraglich sicherzustellen. Zwingend ist die Einstufung als Auftragsdatenverarbeitung aber nicht, es kommt insbesondere auf die Ausgestaltung der vertraglichen Beziehungen sowie auf die übertragene Aufgabe an. Im Falle der Erlaubnis privater Nutzung durch den Mitarbeiter ist der Arbeitgeber als Dienstleister gegenüber dem nun als Nutzer eines Dienstleistungsangebots auftretenden Mitarbeiter anzusehen. Er hat in diesem Falle daher auch alle datenschutzrechtlichen Verpflichtungen zu wahren.

### 3. Handlungsoptionen

Gesetzliche Regelungen, die sich ausdrücklich auf den Umgang mit Internet und Email am Arbeitsplatz sowie auf die Kontrolle dieser Nutzung beziehen, gibt es nicht. Die Rechte und Pflichten in diesem Bereich bestimmen sich daher in erster Linie anhand von

- arbeitsvertraglichen Regelungen und
- Betriebsvereinbarungen (falls ein Betriebsrat besteht).

#### a) Allgemeines

Grundsätzlich entscheidet der Arbeitgeber frei darüber, ob und in welchem Umfang er seinen Arbeitnehmern die Nutzung von Internet und Email ermöglicht. Der Arbeitnehmer hat aufgrund des Arbeitsvertrages kein Recht, Internet und Email für eigene Zwecke zu nutzen. Die private Nutzung bedarf daher der Erlaubnis des Arbeitgebers. Nur in Notfällen darf der Arbeitnehmer auch ohne eine solche Erlaubnis diese Mittel nutzen.

Nutzt der Arbeitnehmer seinen Email-Account für private und dienstliche Zwecke (**Mischnutzung**), gilt das BDSG für alle Mails, d.h. auch für die dienstlichen.

Der Arbeitgeber hat bei der rein dienstlichen Nutzung wesentlich stärkere Kontrollbefugnisse als bei einer auch privaten Nutzung. Für den Arbeitgeber kann es deshalb empfehlenswert sein, eine strenge Trennung zwischen der dienstlichen Nutzung und der Privatnutzung vorzunehmen. Dazu bietet sich die Einrichtung verschiedener Email-Accounts an. Ist die Einrichtung unterschiedlicher Accounts zu aufwändig, wäre eine andere Möglichkeit, die Mitarbeiter zu verpflichten, private Mails besonders zu kennzeichnen, um sie von den übrigen Kontroll- und Überwachungsmaßnahmen trennen zu können. Dies führt aber nicht dazu, dass der Arbeitgeber von der Beachtung der Vorschriften des BDSG entbunden ist. Private Emails sollten darüber hinaus vom Arbeitnehmer unverzüglich gelöscht oder ggf. weitergeleitet werden.

Die Arbeitnehmer sollten umfassend darüber informiert werden, für welche Zwecke sie einen Internetzugang am Arbeitsplatz nutzen dürfen und auf welche Weise der Arbeitgeber die Einhaltung der Nutzungsbedingungen kontrolliert.

Bei der Nutzung von Email und anderen Internetdiensten durch die Beschäftigten sollten die eingesetzten Verfahren technisch so gestaltet sein, dass von vornherein so wenige personenbezogene Daten wie möglich verarbeitet werden (Grundsatz von Datenvermeidung und Datensparsamkeit). Hierzu bietet es sich an, datenschutzfreundliche Verfahren einzusetzen, insbesondere präventive Maßnahmen.

#### b) Regelung im Arbeitsvertrag

##### aa) Internet und Email-Nutzung

Austausch und Kommunikation zwischen den Mitarbeitern (z.B. in der Teeküche oder in der Zigarettenpause) gehörten immer schon zu einem gesunden sozialen Betriebsklima, solange sich das in Maßen hält. Eine Regelung sollte daher mit Augenmaß getroffen werden: Sollte diese Kommunikation etwa durch die Veränderung der Arbeitsumstände aufgrund neuer Arbeitsmittel plötzlich unzulässig sein? Soll einem Telearbeiter wirklich nur der rein geschäftliche Kontakt zu seinen Arbeitskollegen erlaubt sein?

- Will der Arbeitgeber vermeiden, dass er den weitgehenden datenschutzrechtlichen Verpflichtungen von TKG und TDDSG unterliegt, kann er die private Nutzung von Internet und Email verbieten. Der Klarstellung wegen sollte er dies im Arbeitsvertrag regeln

bzw. in internen Richtlinien, mit denen das Direktionsrecht des Arbeitgebers ausgeübt wird. Zwingend notwendig ist das allerdings nicht, da das Anstellungsverhältnis der Mitarbeiter kein Recht auf diese Art der Nutzung beinhaltet. Eine solche Regelung kann allerdings der Entstehung einer ungewünschten „betrieblichen Übung“ entgegenwirken. Auch auf der Grundlage eines Verbotes der privaten Nutzung von Internet und Email ist die *dienstlich motivierte* Privatnutzung jedoch regelmäßig zulässig. Es handelt sich hierbei um die gleichen Grundsätze, die auch in Fällen des Verbotes der privaten Nutzung des Telefons Anwendung finden. Dienstlich motivierte Privatnutzung liegt dann vor, wenn die Notwendigkeit der Kommunikation aus Umständen resultiert, die in der Sphäre des Arbeitgebers begründet sind und deren Gestattung sich aus der Fürsorgepflicht des Arbeitgebers ableitet. Dies gilt z.B., wenn ein privater Termin aus geschäftlichen Gründen nicht eingehalten werden kann und deshalb per Telefon oder Email der Betroffene informiert werden soll. Ebenfalls als zulässig anzusehen ist der private Austausch am Arbeitsplatz in begrenztem Umfang, wie z.B. die Verabredung zum Mittagessen. In beiden Fällen bleibt das Verbot der privaten Nutzung uneingeschränkt bestehen. Ob konkrete Regelungen hierzu sinnvoll sind, lässt sich nicht pauschal feststellen. Sollte jedoch eine Regelung angestrebt werden, so ist schwerpunktmäßig besonders auf klare Abgrenzungskriterien zwischen der noch zulässigen, da dienstlich begründeten privaten Nutzung, der gelegentlichen privaten Nutzung zum rein internen Austausch und der bereits unzulässigen, weil nicht dienstlich begründeten E-Mailkommunikation mit externen Dritten Wert zu legen.

- Hat sich der Arbeitgeber für die Erlaubnis der privaten Nutzung entschieden, sollte er die Zulässigkeit der Privatnutzung zumindest einschränken. Dies ist möglich in zeitlicher und/oder inhaltlicher Hinsicht, z.B. durch die Beschränkung der privaten Nutzung auf Randzeiten und Pausen, durch Vereinbarung eines Entgeltes oder durch eine Regelung, durch die der Arbeitgeber seine Berechtigung ausübt, bestimmte Websites oder auch bestimmte Email-Zieladressen zu sperren.

## bb) Datenerhebung und -nutzung

Der Arbeitgeber ist - wie bereits erwähnt - nicht verpflichtet, die private Nutzung des Internet am Arbeitsplatz zu gestatten. Wenn er dies gleichwohl tut, kann er die Gestattung unter Beachtung der hier genannten Grundsätze davon abhängig machen, dass die Arbeitnehmer einer Protokollierung zur Durchführung einer angemessenen Kontrolle der Netzaktivitäten zustimmen (**Einwilligung, § 4a BDSG**). Die Voraussetzungen, die das Gesetz an die Wirksamkeit einer Einwilligung stellt, sind allerdings hoch.

- Der Betroffene muss sein Einverständnis zeitlich vor Beginn des Verarbeitungsprozesses freiwillig erteilen, eine nachträgliche Genehmigung hat keine rechtfertigende Wirkung für die Vergangenheit.
- Die Einwilligungserklärung bedarf grundsätzlich der Schriftform (vgl. § 126 BGB). Unter besonderen Umständen kann von dem Schriftformerfordernis des § 4a BDSG abgewichen werden und eine andere Form gewählt werden (z.B. telefonische Befragung und die hierfür notwendige Einwilligung zur Datenverarbeitung, eine besondere Eilbedürftigkeit kann das Schriftformerfordernis lockern, wenn die Schriftlichkeit der Einwilligung bloße „Förmelei“ wäre). Auch kann eine gesetzliche Regelung die Lockerung der Formvorschriften vorsehen (vgl. hierzu § 4 Abs.2 TDDSG und § 94 TKG).
- Die Einwilligungserklärung ist besonders hervorzuheben, wenn sie zusammen mit anderen Erklärungen erteilt werden soll. Dies kann etwa durch Fettdruck oder als gesondert unterzeichneter Anhang geschehen.
- Schließlich ist der Betroffene vor Abgabe der Einwilligungserklärung auf die Zwecke der Datenverarbeitung hinzuweisen; dazu gehört auch die Information über die Arten

der Daten, die verarbeitet werden sollen. Entsprechende Klauseln können gem. § 94 BetrVG der Mitbestimmung unterliegen.

In diesem Zusammenhang wird häufig die konkludente Einwilligung erörtert, d.h. eine Einwilligung, die sich durch schlüssiges Handeln ergibt. Bei dieser Art der Einwilligung wird lediglich auf die ausdrückliche Äußerung der Willenserklärung verzichtet. Nicht jedoch auf die Willenserklärung selbst. Daher müssen die Voraussetzungen des § 4a BDSG (insbesondere die Freiwilligkeit, die Information des Betroffenen, die zeitlich vorherige Abgabe der Willenserklärung vorliegen. Da von der Schriftform gem. § 4a BDSG nur unter besonderen Umständen abgewichen werden kann, und diese durch eine andere Form zu ersetzen ist, kommt die konkludente Einwilligung nur sehr begrenzt zur Anwendung.

### c) Regelung durch Betriebsvereinbarung

Insbesondere für große Unternehmen ist der Weg, die Zulässigkeit einer Datenerhebung und -nutzung durch individuelle Einwilligung (§ 4 a BDSG) sicherzustellen, häufig wenig praktikabel. Zum einen ist hiermit ein nicht unerheblicher Verwaltungsaufwand verbunden, zum anderen kann die Verweigerung der Einwilligung durch einzelne Arbeitnehmer den Nutzen eines Datenverarbeitungssystems und den Wert, der mit ihm erzielten Ergebnisse maßgeblich verringern. Besteht daher Bedarf nach einer einheitlichen Regelung, so kommt hierfür - sofern ein Betriebsrat oder sogar Gesamt- oder Konzernbetriebsrat besteht - der Abschluss einer (Gesamt-/Konzern-) Betriebsvereinbarung in Betracht. Dem Betriebsrat steht ohnehin hinsichtlich der Einführung und Anwendung eines Datenverarbeitungssystems ein Mitbestimmungsrecht zu (vgl. § 87 I Nr. 6 BetrVG). Dieses Recht entfällt auch nicht durch die Einholung einer individuellen Einwilligung zur Datenerhebung oder -verarbeitung. Die Möglichkeit, die Internetnutzung am Arbeitsplatz und deren Kontrolle im Rahmen der Verhandlung zu regeln, ist allerdings nicht schrankenlos. Nach der Rechtsprechung des Bundesarbeitsgerichts sind Betriebsvereinbarungen zwar Erlaubnisnormen i.S.d. § 4 BDSG, sie dürfen jedoch nicht gegen zwingende Normen des BetrVG verstoßen und auch nicht die individuellen Rechte der Betroffenen beeinträchtigen.

Die inhaltliche Gestaltungsfreiheit von Arbeitgeber und Betriebsrat beim Abschluss einer Betriebsvereinbarung über die Zulässigkeit und den Umfang von Kontrollen der Internetnutzung wird durch § 75 II BetrVG eingeschränkt, wonach Arbeitgeber und Betriebsrat die freie Entfaltung der Persönlichkeit der Arbeitnehmer zu fördern und zu schützen haben. Eine Vereinbarung über die Einführung von Kontrollsystemen darf also stets nur so weit gehen, wie es das allgemeine Persönlichkeitsrecht der Arbeitnehmer aus Art. 2 I GG i.V.m. Art. 1 GG erlaubt, denn die Zulässigkeit von Eingriffen in die Persönlichkeitsrechte kann nicht durch das Mitbestimmungsrecht erweitert werden.

In einer entsprechenden Betriebsvereinbarung kann auch die private Nutzung und deren Einschränkung geregelt werden.

Aufgrund der Regelungen in einer Betriebsvereinbarung kann der private Datenaustausch mittels Internet am Arbeitsplatz gestattet, verboten und/oder unter besondere Voraussetzungen gestellt werden. **Vorteil:** Die praktische Durchführung wird durch eine Betriebsvereinbarung erleichtert. Denn nach § 77 IV S.1 BetrVG gilt eine Betriebsvereinbarung unmittelbar und zwingend. Sie hat normative Wirkung auf die einzelnen Arbeitsverhältnisse, sogar ohne Wissen und Wollen neuer Arbeitnehmer.

Ein instruktives **Beispiel für eine Betriebsvereinbarung** mit erläuternden Hinweisen ist abgedruckt in: Betriebs-Berater (BB), Heft 38, 2001 S.1950, 1954 ff.

## d) Kontrollmöglichkeiten des Arbeitgebers

- Vereinbarung von Nutzung und Kontrollrechten

Die einfachste und für alle Beteiligten transparenteste Lösung ist, Kontrollrechte des Arbeitgebers umfassend in der Betriebsvereinbarung zu regeln. Bei der Festlegung des Umfangs kann sich dabei an den unten stehenden Grundsätzen orientiert werden.

- Keine Vereinbarung von Nutzung und Kontrollrechten

Sollte hingegen nur eine Gestattung oder ein Verbot der privaten Nutzung ausgesprochen oder vereinbart worden sein, stellt sich die Frage, wie die tatsächliche Einhaltung solcher Vereinbarungen kontrolliert werden kann. Denn jede Vereinbarung, deren Einhaltung in der Praxis nicht (lückenlos) kontrolliert werden kann, ist auf Dauer faktisch wertlos. Auch zu beachten sind in diesen Fällen mögliche Mitbestimmungsrechte des Betriebsrats.

Existiert kein Betriebsrat, sind die Mitarbeiter persönlich von den Kontrollen zu informieren (§ 33 BDSG).

In das Recht auf informationelle Selbstbestimmung kann bei der Auswertung von Protokollen eines Log-Systems bzw. anderer Überwachungseinrichtungen dadurch eingegriffen werden, dass die Verbindungs- und Inhaltsdaten der Nutzung durch die Beschäftigten eingesehen werden. Das Recht des Arbeitnehmers auf informationelle Selbstbestimmung ist jedoch nicht schrankenlos, sondern findet dort seine Grenze, wo die Kontrollmaßnahmen des Arbeitgebers rechtlich zulässig sind. Von entscheidender Bedeutung ist daher die Frage, unter welchen konkreten Voraussetzungen diese Eingriffe in die Rechte des Arbeitnehmers individualrechtlich zulässig sind.

### aa) Technische Sicherheit

Aus Gründen der Datensicherheit ist eine Überwachung und Kontrolle der technischen Einrichtungen zur Aufrechterhaltung des Betriebs und im Falle der Wartung möglich. Dem Arbeitgeber muss die Auswertung der entsprechenden Protokolle möglich sein, um Gefährdungen der Datensicherheit frühzeitig zu erkennen. Das gilt zunächst einmal unabhängig von der rein geschäftlichen oder auch privaten Nutzung sowohl des Email- als auch des Internetanschlusses. Die Wahrung der Datensicherheit rechtfertigt jedoch nicht die unbeschränkte und vollständige Überwachung der Beschäftigten. Insoweit ist insbesondere zu beachten, dass

- personenbezogene Daten bei diesen Maßnahmen so weit wie möglich vermieden werden,
- die Verwendung dieser Informationen regelmäßig beschränkt ist (vgl. z.B. § 31 BDSG) und nur in besonderen Fällen (z.B. Einwilligung des Betroffenen oder Verfolgung strafrechtlicher Tatbestände durch die Verfolgungsbehörden) durchbrochen werden darf bzw. kann,
- keine sonstigen Vereinbarungen (z.B. Betriebsvereinbarungen) entgegenstehen.

Soweit die entstandenen Protokolle nicht mehr benötigt werden, sind diese zu vernichten oder zu sperren.

### bb) Schutz des Unternehmens

Der Arbeitgeber muss ebenso befugt sein, sich selbst präventiv vor möglichen Eingriffen seitens der Strafverfolgungsbehörden zu schützen. Das gewinnt ganz besonders an Bedeutung, wenn es um Tier- oder Kinderpornographie geht. Schon wenn nur der begründete Verdacht besteht, dass sich auf den Computern des Unternehmens Informationen mit strafrechtlicher Relevanz (z.B. auch Beweise) befinden, dann besteht die Gefahr, dass diese Arbeits-

mittel durch die Strafverfolgungsbehörden beschlagnahmt werden. Wird ein Server komplett beschlagnahmt, kann das das Aus für die interne oder externe weitere Kommunikation bedeuten (z.B. Email- oder Internet-Cache-Server). Dem Arbeitgeber ist es hier ebenfalls gestattet, sich im Wege präventiver Maßnahmen- und bei begründetem Verdacht auch nachträglich- vor diesen Gefahren angemessen zu schützen. Letzten Endes ist aber immer eine Einzelfallbetrachtung notwendig, denn die eingesetzten Mittel müssen auch in einem angemessenen Verhältnis zum erstrebten Zweck stehen.

So sollte vom Arbeitgeber zunächst die Sperrung bestimmter WWW-Adressen erwogen werden. Sollte hiervon eine Internetadresse betroffen sein, die fälschlicherweise nicht angezeigt wird, kann dem Benutzer die Möglichkeit gegeben werden, über ein Formblatt (z.B. auch eine Webseite im Intranet) die Freischaltung zu beantragen. Daneben steht es dem Arbeitgeber aus seinem Direktionsrecht zu, die Freischaltung des Internetanschlusses je nach Arbeitsaufgabe einzugrenzen oder durch Kontrollsoftware das Herunterladen unerwünschter Inhalte aus dem Internet automatisch zu sperren.

### cc) Kontrollbefugnisse bei ausschließlich dienstlicher Nutzung (Verbot der privaten Nutzung)

Gestattet der Arbeitgeber die Nutzung von Email und Internet ausschließlich zu dienstlichen Zwecken, ist er nicht Anbieter im Sinne des Telekommunikations- bzw. Teledienstrechts (vgl. oben sowie § 1 I Nr. 1 Teledienstschutzgesetz, TDDSG); die Erhebung und Verarbeitung von Daten über das Nutzungsverhalten der Beschäftigten richtet sich in diesen Fällen nach den einschlägigen Vorschriften des BDSG.

Der Arbeitgeber hat grundsätzlich das **Recht, stichprobenartig zu prüfen**, ob das Surfen bzw. Email-Versenden der Arbeitnehmer dienstlicher Natur ist. Die Durchführung von Stichproben (und ggf. die Aussprache von Abmahnungen bzw. Verhängung von Sanktionen) ist auch ratsam, um der **Entstehung einer betrieblichen Übung** entgegenzuwirken, denn ein nicht überwachtes Verbot kann u. U. wie eine Erlaubnis der privaten Nutzung gewertet werden (vgl. Kästchen S.12). Eine automatisierte Vollkontrolle durch den Arbeitgeber ist als schwerwiegender Eingriff in das Persönlichkeitsrecht der Arbeitnehmer hingegen nur bei konkretem Missbrauchsverdacht im Einzelfall zulässig. Auf mögliche Überwachungsmaßnahmen und in Betracht kommende Sanktionen sind die Arbeitnehmer vorab hinzuweisen.

Kontrollen bei ausschließlich dienstlich erlaubter Nutzung: Stichproben sind zulässig

Von ein- und ausgehenden **dienstlichen Emails** seiner Beschäftigten darf der Arbeitgeber im selben Maße Kenntnis nehmen, wie von deren dienstlichem Schriftverkehr. Beispielsweise könnte der Vorgesetzte verfügen, dass ihm jede ein- oder ausgehende Email seiner Mitarbeiter zur Kenntnis zu geben ist. Ein direkter Zugriff des Vorgesetzten auf das elektronische Postfach des Mitarbeiters ohne eine vorab bestehende Vertretungsregel sollte nicht gestattet sein. Grund hierfür ist, dass es E-mailkommunikation (z.B. zwischen der Personalabteilung und dem Mitarbeiter) gibt, die einem Vorgesetzten nicht zugänglich sein darf (z.B. Information über eine Pfändung des Arbeitseinkommens). Eine sichere Lösung bietet hier z.B. der Einsatz einer PKI (Public Key Infrastructure).

Der Arbeitgeber kann den Arbeitnehmer jederzeit auffordern, ihm die dienstlichen Emails zugänglich zu machen.

Die **Kontrolle der Verbindungs- und Inhaltsdaten** der Internetnutzung ist gem. § 28 I Nr.1 BDSG zulässig, wenn die Verwendung der Daten im Rahmen der Zweckbestimmung eines Vertragsverhältnisses mit dem Betroffenen liegt (vgl. 2 a cc)).

Aus dem Arbeitsvertrag ergibt sich die Verpflichtung des Arbeitnehmers zur Erbringung einer Arbeitsleistung, die in einem angemessenen Austauschverhältnis zur Zahlung von Arbeitsentgelt steht. Diese Verpflichtung kann z.B. dadurch verletzt sein, dass der Arbeitnehmer ei-

nen unangemessenen Anteil seiner Arbeitszeit Internet und Email privat nutzt. Um eine solche Verletzung der arbeitsvertraglichen Pflichten feststellen zu können, benötigt der Arbeitgeber entsprechende Daten über die Nutzung.

Ob diese Datenerhebung zulässig ist, ist immer durch eine Abwägung zwischen den Interessen des Arbeitgebers und des Arbeitnehmers zu ermitteln. Die entscheidende Frage bei dieser **Abwägung** ist, ob sich die Nutzung der Daten zu Kontrollzwecken aus einem überwiegenden Interesse des Arbeitgebers rechtfertigen lässt.

Weitere Verpflichtungen aus dem Arbeitsvertrag kommen in Betracht, aufgrund derer der Arbeitgeber ein Interesse an einer Kontrolle der Nutzungsdaten haben kann:

- Aufgrund der zunehmenden wirtschaftlichen Bedeutung von Datensicherheit hat der Arbeitgeber regelmäßig ein legitimes Interesse daran, die Datenströme zwischen Intranet und Internet zu überwachen und so der Gefahr von Viren, Sabotage und unbefugtem Zugriff auf sensible betriebsinterne Daten zu begegnen.
- Zudem hat er ein Interesse daran festzustellen, wie der Internetzugang von den Beschäftigten genutzt wird, damit auf diesem Wege Geschäftsgeheimnisse nicht unrechtmäßig weitergegeben werden oder eine Überlastung des Firmennetzes sowie evtl. eine Kostensteigerung durch ausschweifende Inanspruchnahme des Internet-Zugangs unterbleibt.

Der Arbeitnehmer wiederum hat in erster Linie ein Interesse an der Wahrung seines Rechtes auf informationelle Selbstbestimmung.

Zudem besteht auf Arbeitnehmerseite das Interesse am Schutz vor einer umfassenden Kontrolle der Internet-Nutzung und den damit unter Umständen einhergehenden arbeitsrechtlichen Konsequenzen.

Die Zulässigkeit einer Kontrolle beruht letztlich immer auf einer **Einzelfallentscheidung**.

#### **Beispielfälle:**

- **Kostensteigerung und Überlastung des Netzes**

Bei einer Kontrolle aus Gründen der erheblichen Kostensteigerung oder Überlastung des Netzes sollte unterschieden werden: Stellt der Arbeitgeber allgemein eine Kostensteigerung fest, wird der Arbeitgeber vor einer mitarbeiterbezogenen Kontrolle zunächst abzuwägen haben, ob er stattdessen präventive Maßnahmen ergreifen kann, die dem Recht des Arbeitnehmers auf Datenschutz Rechnung tragen. Denn will der Arbeitgeber eine Kostensteigerung und die Überlastung des Netzes durch private Internet- und Emailnutzung vermeiden, so kann er dieses Ziel schon durch temporäre Zugangssperren oder dadurch erreichen, dass ein bestimmtes Passwort vor der Email eingegeben werden muss, um es als private Email zu kennzeichnen und dann bei einer Netzüberlastung nicht zur Übertragung zuzulassen.

Ist die Zuordnung der Kostensteigerung jedoch zu einem bestimmten Mitarbeiter möglich, kann dies einen Missbrauchsverdacht begründen, der die Kontrolle der Verbindungs- und Inhaltsdaten rechtfertigt.

- **Verdacht auf Verletzung von Geschäftsgeheimnissen**

Ob der Arbeitnehmer die arbeitsvertragliche Nebenpflicht verletzt, über Geschäftsgeheimnisse Stillschweigen zu bewahren, kann der Arbeitgeber nur durch eine inhaltliche Kontrolle der Emails feststellen. Die nachträgliche inhaltliche Vollkontrolle zu diesem Zweck setzt aber einen konkreten Verdacht voraus. Insoweit bleibt dem Arbeitgeber zunächst die Möglichkeit, durch ein dichtes Netz von Zugangsberechtigungen und Passwortabfragen seine wertvollen Unternehmensinformationen präventiv zu schützen.

Ob die Kontrolle der Verbindungs- und Inhaltsdaten im Übrigen zulässig ist, muss durch eine Interessenabwägung in jedem Einzelfall geprüft werden. Hierbei ist aufgrund der geschützten Interessen der Arbeitnehmer restriktiv vorzugehen: Der Arbeitgeber muss zur Erreichung seines Ziels ein anderes, die Datenschutzinteressen der Arbeitnehmer weniger berührendes Mittel als die Kontrolle wählen, wenn ein solches zur Verfügung steht und zur Zielerreichung geeignet ist.

Soweit die Nutzung von Email und Internet nur zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherung des ordnungsgemäßen Betriebs der Verfahren protokolliert wird, dürfen diese Daten nach dem BDSG auch nur zu diesen Zwecken genutzt werden, nicht aber zur Verhaltens- und Leistungskontrolle.

#### **dd) Kontrollbefugnisse bei Erlaubnis der privaten Nutzung**

Wenn ein Arbeitgeber seinen Arbeitnehmern die private Nutzung von Internet oder Email erlaubt, ist er ihnen gegenüber Telekommunikations- bzw. Telediensteanbieter, vgl. oben 2 b) aa, bb). Der Arbeitgeber ist daher den Arbeitnehmern gegenüber zur **Einhaltung des Telekommunikationsgeheimnisses** verpflichtet, es gelten die gleichen Grundsätze wie beim privaten Telefonieren. Eingehende private, aber fälschlich als Dienstpost behandelte Emails sind daher den betreffenden Mitarbeitern unverzüglich nach Bekanntwerden ihres privaten Charakters zur alleinigen Kenntnis zu geben.

Eine Protokollierung der Nutzung darf ohne Einwilligung erfolgen, wenn sie nur zu Zwecken der Datenschutzkontrolle, der Datensicherung, zur Sicherung des ordnungsgemäßen Betriebs der Verfahren oder zu Abrechnungszwecken erforderlich ist, oder der Verdacht auf eine strafrechtlich relevante Nutzung vorliegt. Sollte der Mitarbeiter zur Kostenerstattung verpflichtet sein, können aber die Abrechnungsdaten festgehalten werden. Bezüglich der **Filterung und Löschung von Spam-Emails** gelten die Ausführungen zu 5) (vgl. unten) entsprechend: Durch die vorherige Einwilligung des Arbeitnehmers kann der Arbeitgeber die Anwendbarkeit der §§ 206 Abs.2, 303 a StGB sicherheitshalber ausschließen.

Eine darüber hinaus gehende Kontrolle ist nicht zulässig. Das heißt: Ohne eine entsprechende Regelung in einer Vereinbarung, Weisung, Richtlinie oder Betriebsvereinbarung oder ohne die Einwilligung des Arbeitnehmers hat der Arbeitgeber letztlich **keinerlei Kontrollbefugnisse**.

## **4. Steuerliche Aspekte der Nutzung von Email und Internet durch den Arbeitnehmer und ertragsteuerliche Beurteilung der Kosten für den Arbeitgeber**

### **a) Ertragsteuerliche Beurteilung der Kosten für den Arbeitgeber**

Die Kosten, die der Arbeitnehmer zur Durchführung seiner betrieblichen Aufgaben bei der Nutzung von Personalcomputern und Telekommunikationseinrichtungen verursacht, gehören zu den betrieblichen Kosten des Arbeitgebers. Der Arbeitgeber kann sie als Betriebsausgaben von der steuerlichen Bemessungsgrundlage seines Unternehmens abziehen. Unerheblich ist

dabei, ob der Arbeitgeber die zur Erbringung der Arbeitsleistung notwendigen Einrichtungen selbst anschafft und ihren Betrieb selbst finanziert oder dem Arbeitnehmer die Auslagen erstattet, die diesem durch Anschaffung und Betrieb der notwendigen Ausrüstung entstehen (vgl. Schmidt, Kommentar zum Einkommensteuergesetz (EStG), 19. Aufl. § 4 Rz 501). Voraussetzung für den Betriebsausgabenabzug ist aber, dass der Arbeitgeber die Kosten tatsächlich trägt und die vom Arbeitnehmer verursachten Kosten zumindest teilweise auch betrieblich veranlasst sind (§ 4 Abs. 4 EStG). Eine betriebliche Veranlassung besteht, wenn der Arbeitgeber dem Arbeitnehmer eine Einrichtung als Arbeitsmittel zur Verfügung stellt, damit der Arbeitnehmer seine Funktion im Betrieb wahrnehmen kann (vgl. Schmidt, Kommentar zum EStG, 19. Aufl. § 4 Rz 481, 520 Stichwort "Arbeitsmittel").

## **b) Lohnsteuerliche Beurteilung der Vorteile für den Arbeitnehmer**

Soweit der Arbeitnehmer Internet und E-Mail nutzt, um seine betrieblichen Aufgaben zu erfüllen, hat er keine besonderen, steuerlich relevanten Nutzungsvorteile. Im Ergebnis steuerfrei ist auch die private Nutzung betrieblicher Einrichtungen durch den Arbeitnehmer. Bis zum Jahr 2000 war jedoch umstritten, ob die Vorteile eines Arbeitnehmers aus der privaten Nutzung von betrieblichen Personalcomputern, betrieblichem Internetzugang und anderen betrieblichen Kommunikationsmöglichkeiten der Lohnsteuer zu unterwerfen sind. Der im Jahre 2000 eingeführte § 3 Nr. 45 EStG stellt aber nunmehr klar, dass Vorteile des Arbeitnehmers aus der privaten Nutzung betrieblicher Personalcomputer und Telekommunikationseinrichtungen einkommensteuerfrei bleiben. Die Nutzung dieser Einrichtungen durch den Arbeitnehmer erhöht also nicht seinen zu versteuernden Arbeitslohn. Dies gilt unabhängig davon, welchen Gegenwert der Arbeitnehmer aus der Nutzung zieht. Auf das Verhältnis von betrieblicher und privater Nutzung kommt es nicht an (Verfügung der Oberfinanzdirektion Berlin v. 12.6.2001, St 177 – S 2350 – 1/01; veröffentlicht in DStR 2001 (Heft 39) S. 1662). Unbeachtlich ist zudem, ob der Arbeitnehmer betriebliche Geräte am Arbeitsplatz oder in seiner Wohnung privat nutzt. Zu den lohnsteuerfrei nutzbaren Geräten gehören neben dem Computer selbst auch das erforderliche Zubehör wie Monitor, Drucker, Scanner, Modem/ISDN-Karte sowie die installierte Software (vgl. Abschn. 21 e der Lohnsteuer-Richtlinien 2004). Typische Telekommunikationsgeräte, die lohnsteuerfrei genutzt werden können, sind z.B. Telefone, Faxgeräte und Handys. Die Steuerfreistellung umfasst auch die Gebühren und sonstigen Verbindungsentgelte (z.B. Provider-Gebühren), die der Arbeitnehmer verursacht (Verfügung der OFD Berlin v. 12.6.2001, St 177 – S 2350 – 1/01; veröffentlicht in DStR 2001 (Heft 39) S. 1662).

Voraussetzung für die Befreiung von der Lohnsteuer ist jedoch immer, dass betriebliche Einrichtungen genutzt werden. Die Steuerfreistellung gilt nur, solange die genutzte Einrichtung zum Betrieb des Arbeitgebers gehört. Gibt der Arbeitgeber Geräte im Wege der Schenkung oder des verbilligten Erwerbs an den Arbeitnehmer ab, sind die Vorteile des Arbeitnehmers aus dem vergünstigten Erwerb nach § 40 Abs. 1 Nr. 5 EStG pauschal mit 25 % zu versteuern. Schuldner der pauschalen Lohnsteuer ist der Arbeitgeber (§ 40 Abs. 3 S. 2 EStG).

## **c) Auswirkung der Steuerbefreiung auf die Sozialversicherungspflicht**

Gestattet der Arbeitgeber die Privatnutzung von Internet und E-Mail, ohne die Privatnutzung betrieblicher Einrichtungen auf den geschuldeten Arbeitslohn anzurechnen, sind die dadurch entstehenden Vorteile des Arbeitnehmers auch sozialversicherungsfrei (§ 1 der Arbeitsentgeltverordnung). Gewährt der Arbeitgeber die Vorteile bei der Nutzung betrieblicher Einrichtungen anstelle eines Teils des vertraglich geschuldeten Arbeitslohns, sind die Nutzungsvorteile zwar steuerfrei, aber sozialversicherungspflichtig. Die Vorteile des Arbeitnehmers aus einem vergünstigten Erwerb von Computern und EDV-Zubehör vom Arbeitgeber sind ebenfalls sozialversicherungsfrei (§ 2 Abs. 1 Nr. 2 der Arbeitsentgeltverordnung).

## d) Umsatzsteuerliche Beurteilung der privaten Nutzung betrieblicher Einrichtungen durch den Arbeitnehmer

Die private Nutzung betrieblicher Einrichtungen durch den Arbeitnehmer unterliegt der Umsatzsteuer. Uneingeschränkt gilt dieser Grundsatz jedoch nur dann, wenn der Arbeitgeber für die Privatnutzung betrieblicher Einrichtungen vom Arbeitnehmer ein Entgelt verlangt. Grundlage für die Besteuerung ist das Entgelt für die Nutzung. Abweichend davon sind für die Berechnung der Steuer die durch die Nutzung entstandenen Kosten des Arbeitgebers zugrunde zu legen, wenn sie das vereinbarte Entgelt übersteigen (§ 10 Abs. 5 Nr. 2 UStG).

Nutzt der Arbeitnehmer gegen den Willen des Arbeitgebers Internet und E-Mail zu privaten Zwecken, kann keine Leistung im Sinne des UStG vorliegen. Infolge dessen entfällt eine Besteuerung.

Die unentgeltliche private Nutzung betrieblicher Gegenstände durch den Arbeitnehmer mit Zustimmung des Arbeitgebers unterliegt nach § 3 Abs. 9a Nr. 1 UStG der Umsatzsteuer. Wegen der schwierigen und aufwändigen Ermittlung der steuerlich relevanten Nutzungsvorteile verzichtet die Finanzverwaltung aber auf eine Besteuerung, wenn der Zugang des Arbeitnehmers zu E-Mail, Internet und sonstigen Kommunikationseinrichtungen überwiegend durch das betriebliche Interesse des Arbeitgebers veranlasst ist. Ein Nutzungsvorteil des Arbeitnehmers ist demnach nicht zu versteuern, wenn die Möglichkeit der privaten Nutzung nur eine Begleiterscheinung des Zugangs zu Computer und Internet ist und durch den betrieblichen Zweck des Zugangs zu Kommunikationseinrichtungen überlagert wird (vgl. Abschnitt 12 Abs. 4 der Umsatzsteuer-Richtlinien 2000). Die dargestellte umsatzsteuerrechtliche Beurteilung ist in einer Verfügung der Oberfinanzdirektion München vom 12.11.2001, S 7100 – 212 St 432 zusammengefasst (veröffentlicht in DStR 2001 (Heft 48), S. 2073). Sie geht zurück auf ein Schreiben des Bundesministeriums der Finanzen an die Wirtschaftsverbände vom 11. April 2001 (Az. IV B 7 - S 7109 - 14/01).

Weiterführende Links:

- Einkommensteuergesetz (EStG)  
<http://bundesrecht.juris.de/bundesrecht/estg/index.html>
- Umsatzsteuergesetz (UStG)  
[http://bundesrecht.juris.de/bundesrecht/ustg\\_1980/index.html](http://bundesrecht.juris.de/bundesrecht/ustg_1980/index.html)

## 5. Strafrechtliche Situation

### Allgemeine Hinweise zur Strafbarkeit

Das Internet ist kein „rechtsfreier Raum“. Strafbare Handlungen können auch im Internet begangen werden. Das Strafgesetzbuch (StGB) enthält in den §§ 201 ff und 303 ff StGB Vorschriften, die Verletzungen des persönlichen Lebens- und Geheimbereichs sowie Sachbeschädigung unter Strafe stellen. Wo den besonderen Anforderungen an die Tatumsstände von Straftaten über oder mittels Telekommunikationseinrichtungen, des Internets (und seiner Dienste) oder Computern Rechnung getragen werden muss, hat der Gesetzgeber besondere bzw. ergänzende Vorschriften geschaffen (vgl. rechter Kasten). Bei bestimmten Handlungen im Bereich der Tele- und Mediendienste sowie der Telekommunikation sind diese Vorschriften unbedingt zu beachten.

#### 1a) Grundnorm:

§ 201 StGB, „Verletzung der Vertraulichkeit des Wortes“ und § 33 Kunsturhebergesetz (Verbot unbefugter Verbreitung und Veröffentlichung von Bildnissen)

#### 1b) spezifische Ergänzung:

§ 201a StGB, „Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen“

#### 2a) Grundnorm:

§ 202 StGB „Verletzung des Briefgeheimnisses“

#### 2b) spezifische Ergänzung:

§ 202 a StGB „Ausspähen von Daten“

Die Strafbarkeit trifft immer eine natürlich Person – in erster Linie also den für das Unternehmen handelnden Arbeitnehmer. Jedoch können Straftaten über die allgemeinen Regeln der Täterschaft und Teilnahme (Anstiftung und Beihilfe) Personen zugerechnet werden, die nicht unmittelbar gehandelt haben, aber dennoch über die erforderliche sog. Tatherrschaft verfügen.

3 a) Grundnorm:  
§ 303 StGB „Sachbeschädigung“

3b) spezifische Ergänzungen:  
§§ 303 a und 303 b StGB „Datenveränderung“ und „Computersabotage“.

#### Im Besonderen: § 206 StGB „Verletzung des Fernmeldegeheimnisses“

Ein aktuelles und besonderes praxisrelevantes Problem stellt die automatisierte **Filterung und Löschung von Emails** dar. Unter welchen Voraussetzungen eine Handlung eine Verletzung des Fernmeldegeheimnisses darstellt und wie eine Strafbarkeit gleichwohl vermieden werden kann, befindet sich in der Rechtswissenschaft noch in der Diskussion. Hierbei geht es vor allem um die Frage, ob der Einsatz von Spam-Filtern in strafbarer Weise das Fernmeldegeheimnis verletzt (vgl. § 206 Abs. 2 Nr. 2 StGB), weil die Emailunterdrückung einen unbefugten Eingriff in den Übermittlungsvorgang darstellen könnte. Einigkeit besteht mittlerweile über die folgenden Punkte:

- Bei der ausschließlich dienstlichen Nutzung eines Emailpostfaches entfällt die Strafbarkeit des Löschens von Spam-Emails. Über den gesamten elektronischen Posteingang kann das Unternehmen bestimmen. Das Restrisiko, dass geschäftliche Emails, die für den Benutzer relevant sind, als Spam-Email eingestuft und daher gelöscht werden, trifft allein die Unternehmensleitung.
- Der Straftatbestand kann überhaupt nur erfüllt werden, wenn die private Nutzung von Email im Unternehmen erlaubt ist, da nur dann das Unternehmen eine Telekommunikationsdienstleistung gegenüber Dritten erbringt (vgl. § 3 Nr. 10 TKG), was eine der Voraussetzungen des § 206 Abs. 2 Nr. 2 StGB ist.
- Für die strafrechtliche Betrachtung wichtig ist der Zeitpunkt, in dem die Anfrage zur Übermittlung von Daten den Mailserver des Unternehmens erreicht und der übermittelnde Mailserver die Daten dem empfangenden Server übermittelt (strafrechtlich als „Gewahrsamerlangung“ bezeichnet). Daher fallen Filtermaßnahmen, aufgrund derer es zu einer Übertragung und Gewahrsamerlangung (z.B. durch Speicherung) von „header“ (Kopfzeile) und „body“ (eigentlicher Inhalt) der Email gar nicht kommt (z.B. „Blacklists“) nicht unter § 206 Abs. 2 Nr. 2 StGB und sind nach überwiegender Meinung unbedenklich. Vorzugswürdig erscheinen allerdings Vorgehensweisen bei denen es nicht zu einer Löschung der Email kommt, sondern zur Aufbewahrung in einem separaten Ordner des Empfängers, dessen Regelkonfiguration sowohl durch den Nutzer, als auch durch die für den E-maildienst verantwortliche Abteilung vorgenommen werden kann. Letztere Lösung hat allerdings den praktischen Nachteil, dass die Spam-Email zunächst übertragen wird, die Belastung des Unternehmens also unverändert besteht. Der Vorteil besteht darin, dass der Benutzer des Postfachs die endgültige Entscheidung zur Löschung selber trifft.

Verbietet das Unternehmen die private Nutzung, kann eine Strafbarkeit nach § 206 Abs. 2 Nr. 2 StGB beim Einsatz von Spam-Filtern nicht vorliegen.

Einigkeit besteht (bei Unterschieden im Detail) auch letztendlich darüber, dass – bei gestatteter privater Nutzung - eine Einwilligung in die Filterung von Email der Strafbarkeit nach § 206 Abs. 2 Nr. 2 StGB entgegenstehen kann. Unterschiedlich beantwortet wird jedoch die Frage, *wer* in die Filterung einwilligen muss. Das OLG Karlsruhe betont in einem aktuellen Beschluss (1 Ws 152/04 vom 10.01.2005), dass die Einwilligung von allen an dem konkreten Fernmeldeverkehr Beteiligten erteilt werden muss, d.h. von Empfänger *und* Versender. Demgegenüber wird in der rechtswissenschaftliche Literatur mit beachtlichen Argumenten

vertreten, dass die Einwilligung des Empfängers ausreicht. Hingewiesen wird darauf, dass es nicht nur rechtsdogmatisch unzutreffend ist, zusätzlich die Einwilligung des Versenders zu verlangen, sondern auch völlig praxisfern.

Ist § 206 Abs. 2 Nr. 2 StGB erfüllt, wird regelmäßig ebenfalls eine strafbare Datenveränderung gemäß § 303a StGB durch Löschung bzw. Unterdrückung der Email gegeben sein.

Wegen der zahlreichen, unterschiedlichen Meinungen in der Literatur und der erst beginnenden Aufarbeitung dieser Frage durch die Rechtsprechung kann auch an dieser Stelle noch keine endgültige Aussage getroffen werden. Sobald sich die Meinungen festigen, wird an dieser Stelle erneut eine Aktualisierung vorgenommen.

#### Literaturhinweise:

- CR (Computer und Recht) 2005, S. 450: V. Kitz (BITKOM): Meine Emails les´ ich nicht – Zur Einwilligung in die Spamfilterung
- MMR 2005 S. 343: M. Schmidl: E-Mail-Filterung am Arbeitsplatz
- DuD 2005 S. 163: Strafbarkeit der Ausfilterung von E-Mails – Anmerkung zum Beschluß des OLG Karlsruhe vom 10.1.2005 – 1 WS 152/04
- DuD 2005 S. 267: M. Schmidl: Private E-Mail-Nutzung – Der Fluch der guten Tat
- MMR 2005 S. 78: Beschluss des OLG Karlsruhe zum Ausfiltern von E-Mails (mit Anmerkung von J. Heidrich)
- CR 2005 S. 290: Urteilsanmerkung von M. Lejeune zum Beschluss OLG Karlsruhe
- CR 2004 S. 437: G. Spindler/S. Ernst: Vertragsgestaltung für den Einsatz von Emailfiltern
- MMR 2004 S. 75: J. Heidrich/S. Tschoepe: Rechtsprobleme der E-Mail-Filterung
- NJW 2004 S. 3513: T. Hoeren

## 6. Fazit

Beim Datenschutz am elektronischen Arbeitsplatz richtet sich der Umfang des Arbeitnehmerdatenschutzes danach, ob dem Arbeitnehmer die private Nutzung der Informations- und Kommunikationstechniken gestattet ist oder nicht.

Während der Arbeitnehmerdatenschutz bei der privaten Internet-/Emailnutzung durch die bereichsspezifischen Regelungen der Telekommunikations- und Telekommunikationsgesetze sehr weitgehend ist, bleibt bei Anwendung des BDSG bei einer dienstlichen Nutzung des Internet/Email die Frage offen, wann die Voraussetzungen gem. §§ 4, 27, 28 BDSG vorliegen und damit eine Ausnahme vom Datenverarbeitungsverbot zu bejahen ist. Aufgrund der noch ausstehenden Rechtsprechung in diesem Bereich, besteht die Möglichkeit, überwiegende Interessen des Arbeitgebers anzunehmen und dem Arbeitgeber so einen großen Spielraum bei der Wahrnehmung seiner Datenverarbeitungsinteressen zu gewähren.

Die Diskussion über den Umfang des Datenschutzes bei neuen Kommunikationsformen am Arbeitsplatz wie Internet und Email steht aber erst am Anfang. Zur Vermeidung späterer Streitigkeiten über den Umfang der Kontrollbefugnisse des Arbeitgebers ist es daher in jedem Fall empfehlenswert, klare Regelungen über die dienstliche Nutzung und die Gestattung der privaten Nutzung des Internet zu treffen.

## 7. Beispielformulierung für Arbeitsvertrag, Richtlinie oder Betriebsvereinbarung

### Hintergrund und Anwendungsbereich

Wie schon im Laufe der vorangegangenen Darstellung erläutert, hat der Arbeitnehmer keinesfalls aufgrund seines Arbeitsvertrages ein Recht, Internet und Email für eigene Zwecke zu nutzen. Die Entscheidung, ob und in welchem Umfang er den Arbeitnehmern die private Nutzung von Internet und Email ermöglicht, liegt allein beim Arbeitgeber. Diese Ausgangssituation legt den Schluss nahe, dass eine Regelung, insbesondere ein ausdrückliches Verbot nicht erforderlich ist, wenn der Arbeitnehmer den ihm zur Verfügung gestellten Zugang nicht privat nutzen soll. In der Praxis ist jedoch dringend davon abzuraten, das Ob und das Wie der Nutzung ungeregelt zu lassen, denn auch ein regelungsloser Zustand bezüglich der dienstlichen und privaten Nutzung von Email und Internet kann durch ein Gericht als Duldung einer stattfindenden Nutzung gewertet werden und dazu führen, dass eine sog. „betriebliche Übung“ geschaffen wird. Letztlich ist es also möglich, dass die Regelungslosigkeit faktisch wie eine Erlaubnis der privaten Nutzung gewertet wird.

Der Arbeitgeber hat verschiedene Möglichkeiten, um eine Regelung vorzunehmen. Zunächst kann er eine Regelung im jeweiligen Arbeitsvertrag mit dem Arbeitnehmer vornehmen. Mit steigender Zahl der Arbeitnehmer ist diese Möglichkeit jedoch wegen des hohen Aufwands unpraktikabel, insbesondere, wenn bestehende Arbeitsverträge ergänzt werden müssen. Um zu vermeiden, dass eine große Anzahl von Einzelvereinbarungen mit den Arbeitnehmern abgeschlossen werden muss, kann der Arbeitgeber die Regelung jedoch auch in einer unternehmensinternen Richtlinie zusammenfassen, die als Teil des Arbeitsvertrages gilt. Schließlich kann er, sofern ein Betriebsrat besteht, auch mit diesem eine Betriebsvereinbarung abschließen, die die Modalitäten der Nutzung regelt. Auch hierbei gilt: Nicht von der Mitbestimmung umfasst ist, ob die Nutzung des Internets überhaupt zugelassen wird.

Bei allen Vorgehensweisen sind die regelungsbedürftigen Punkte weitestgehend identisch. Für die Situation, dass der Arbeitgeber eine private Nutzung in begrenztem Maß erlaubt, ist im Folgenden daher als Beispiel für eine mögliche Formulierung eine Kernregelung aufgeführt, die gleichermaßen Aufnahme in den Arbeitsvertrag, eine unternehmensinterne Richtlinie oder eine Betriebsvereinbarung finden kann. Die Beispielformulierungen sind selbstverständlich unverbindlich und sollten in jedem Fall unternehmensintern verhandelt bzw. geprüft, angepasst oder ergänzt werden (z.B. Ziffer 3.1)

## Kernregelung

### 1. Gegenstand und Geltungsbereich

Diese [Vereinbarung/Weisung/Richtlinie/Betriebsvereinbarung] regelt die Grundsätze für die private Nutzung der Internet- und Email-Dienste von [Unternehmen] [falls vorhanden: ...und Tochterfirmen] und gilt für alle Mitarbeiter, deren Arbeitsplätze über einen geschäftlichen Internet- bzw. Email-Zugang verfügen.

### 2. Zielsetzung

Ziel dieser [Vereinbarung/Weisung/Richtlinie/Betriebsvereinbarung] ist es, die Nutzungsbedingungen sowie die Maßnahmen zur Protokollierung und Kontrolle transparent zu machen, die Persönlichkeitsrechte der Mitarbeiter zu sichern und den Schutz ihrer personenbezogenen Daten zu gewährleisten.

### 3. Internet und Email

#### 3.1

[Unternehmen] gestattet\* die nur gelegentliche und im Verhältnis zur geschäftlichen Nutzung eindeutig unerhebliche\*\* private Nutzung des geschäftlichen Internet- und Email-Anschlusses sowie der damit verbundenen Email-Adresse.

#### 3.2

Eine solche unerhebliche Nutzung wird nicht disziplinarisch sanktioniert bzw. geahndet, solange dabei keine Gesetze [soweit vorhanden: ...oder interne Richtlinien] verletzt oder überschritten werden und die Verfügbarkeit des IT-Systems für dienstliche Zwecke nicht beeinträchtigt wird. [soweit vorhanden: Insbesondere die Regelungen der Richtlinie XXX (zur Datensicherheit) sind zu beachten.]

#### 3.3

Absender und Empfänger von Emails sind allein für deren weitere Verwendung verantwortlich; sie entscheiden über Speicherung, Löschung und Weiterleitung im Rahmen der gesetzlichen und betrieblichen Regelungen. Unbeschadet dessen behält sich [Unternehmen] vor, Spam - Emails herauszufiltern und sofort zu löschen.

### 4. Einwilligung und Vertretungsregelung

#### 4.1

Eine Unterscheidung von dienstlicher und privater Nutzung auf technischem Weg erfolgt nicht. Die Protokollierung und Kontrolle gemäß Ziffer 5 dieser [Vereinbarung/Weisung/Richtlinie/Betriebsvereinbarung] erstrecken sich auch auf den Bereich der privaten Nutzung des Internetzugangs.

#### 4.2

Durch die private Nutzung des Internetzugangs erklärt der Mitarbeiter seine Einwilligung in die Protokollierung und Kontrolle gemäß Ziffer 5 dieser [Vereinbarung/Weisung/Richtlinie/Betriebsvereinbarung] für den Bereich der privaten Nutzung. Insoweit stimmt er auch einer Einschränkung des Telekommunikationsgeheimnisses zu.

#### 4.3

Bei der Einrichtung einer Vertretungsregelung muss der Mitarbeiter damit rechnen, dass auch private Emails vom Vertreter gelesen werden können.

#### 4.4

Nach dem Ausscheiden oder bei längerer, insbesondere krankheitsbedingter Abwesenheit des Mitarbeiters steht dem Arbeitgeber der Zugriff auf die Emails des Mitarbeiters in dem Umfang zu, den der ordnungsgemäße Geschäftsgang oder betriebliche Ablauf erfordert. Der Zugriff ist im Beisein des betrieblichen Datenschutzbeauftragten [falls vorhanden: und des Betriebsrats] durchzuführen. Der Mitarbeiter muss damit rechnen, dass auch private Emails dabei gelesen werden können.

## 5. Leistungs- und Verhaltenskontrolle/Datenschutz für Email- und Internetnutzung/Sanktionen

### 5.1

Soweit personenbezogene oder –beziehbare Daten aufgezeichnet werden, dürfen diese ausschließlich für die genannten Zwecke dieser [Vereinbarung /Weisung/ Richtlinie/ Betriebsvereinbarung] verwendet werden. Daten über das Benutzerverhalten dürfen ausschließlich zur Gewährleistung der Systemsicherheit, zur Optimierung und Steuerung des Systems, zur Fehleranalyse und -korrektur sowie zur kostenstellenbezogenen Abrechnung der Systemkosten verwendet werden. Die Zugriffe auf diese Funktionen bleiben auf die mit der technischen Administration des Systems betrauten Personen begrenzt; diese Personen sind gem. § 5 BDSG und § 88 TKG verpflichtet. Der Mitarbeiter willigt ein, dass Daten, die den Verdacht bezüglich eines Verstoßes gegen die vorliegende [Vereinbarung /Weisung/ Richtlinie/ Betriebsvereinbarung] begründen, an die Geschäftsleitung weitergegeben werden. Soweit strafrechtlich relevante Inhalte betroffen sind, dürfen diese Daten auch an die Strafverfolgungsbehörden weitergegeben werden.

### 5.2

Eine Verwendung der vorgenannten Daten zur weitergehenden Leistungs- oder Verhaltenskontrolle ist nicht gestattet. Die Regelungen der Absätze 5.3 – 5.5 bleiben hiervon unberührt.

### 5.3

Bei einem ausreichend begründeten Verdacht kann [*falls vorhanden*: ...mit Zustimmung des örtlichen Betriebsrates] eine gezielte Überprüfung eines Internet- und/oder Email-Accounts stattfinden. Bei der Überprüfung ist der betriebliche Datenschutzbeauftragte hinzuzuziehen.

### 5.4

Maßnahmen, die den Missbrauch von Internet und/oder Email verhindern oder beweisen helfen, können bei Gefahr im Verzug (begründeter Verdacht) unmittelbar durchgeführt werden. In diesen Fällen ist der betriebliche Datenschutzbeauftragte [*falls vorhanden*: und der Betriebsrat] anschließend unverzüglich zu informieren.

### 5.5

Ein Verstoß kann neben den arbeitsrechtlichen Folgen auch strafrechtliche Konsequenzen haben. [Unternehmen] behält sich vor, bei Verstößen gegen diese Vereinbarung die private Nutzung des Internet-/Email-Zugangs im Einzelfall zu untersagen. Darüber hinaus kann ein Verstoß uneingeschränkte zivilrechtliche Schadensersatzpflichten auslösen, z. B. bei rechtswidriger Nutzung kostenpflichtiger Internetseiten.

## 6. Verhaltensgrundsätze

### 6.1

Bei der privaten Nutzung sind die gesetzlichen Vorschriften [*falls vorhanden*: ...und die XXX internen Richtlinien] zu beachten.

### 6.2

Darüber hinaus ist - im Rahmen der Einschränkungen gem. Ziffer 3 - nur eine solche Nutzung erlaubt, die

- das Geschäft von [Unternehmen] nicht stört oder mit ihm im Wettbewerb steht,
- die eigene oder die Arbeit anderer Mitarbeiter nicht behindert oder stört,
- keine zusätzlichen Kosten für [Unternehmen] verursacht,
- keine geschäftsmäßige Werbung beinhaltet,
- Dritten keine Informationen über oder Listen von Mitarbeitern zukommen lässt,
- keine geschäftsmäßigen oder privaten Verteilerlisten einbezieht.

### 6.3

Generell unzulässig ist das Aufrufen kostenpflichtiger Internet-Seiten und das Zugreifen auf oder Verteilen von Material, das von anderen Personen als geschmacklos, Anstoß erregend oder respektlos angesehen werden könnte; Beispiele hierfür sind:

- Material, das sexuell eindeutige Bilder und Beschreibungen enthält
- Material, das illegale Aktionen befürwortet
- Material, das Intoleranz gegen Andere befürwortet

#### 6.4

Generell unzulässig ist auch die Verwendung der [Unternehmen] - UserID in öffentlichen „Chat-Räumen“ oder bei anderen Anlässen, bei denen es zur Zusendung von Werbe- oder sogenannten Spam-Mails kommen kann.

*\* Diese Formulierung kann durch den Zusatz „...unter dem Vorbehalt des jederzeitigen Widerrufs...ergänzt werden, da es sich um eine freiwillige Leistung des Arbeitgebers handelt und auf diese Weise einer Selbstbindung entgegen gewirkt werden kann.*

*\*\* Die Unerheblichkeit der Nutzung in Ziffer 3.1 muss vom jeweiligen Unternehmen genauer definiert werden, z.B. durch eine beispielhafte, nicht abschließende Aufzählung*



## Literaturhinweise/ Weiterführende Links

- Nils Adams, Nutzwert maximieren? Praxistipps zur Email-Nutzung, in: Anwalt 4/2001, S. 46
- Dirk M. Barton, E-Mail-Kontrolle durch Arbeitgeber – Drohen unliebsame strafrechtliche Überraschungen?, in: CR 11/2003, S. 839
- Martin Beckschulze/Wolfram Henkel, Der Einfluss des Internets auf das Arbeitsrecht, in: Der Betrieb (DB)2001, S. 1491 ff.
- Bernd-Christoph Bijok/Thomas Class, Arbeitsrechtliche und datenschutzrechtliche Aspekte des Internet-Einsatzes (insbesondere Email), in: RDV 2001, S. 52 ff.
- Bernd Borgmann, Das Dilemma des Admins – Arbeitsrechtliche Fragen bei der Email-Überwachung, in: iX 2000, Ausgabe 11, S. 138 ff.
- Datenschutzpraxis, Internet am Arbeitsplatz, in: Datenschutzberater (DSB) 2002, Ausgabe 4, S. 11
- Wolfgang Däubler, Nutzung des Internet durch den Arbeitnehmer, in: Kommunikation & Recht (K&R) 2000, S. 323 ff.
- Der Datenschutzbeauftragte für den Datenschutz, Surfen am Arbeitsplatz - Datenschutzwegweiser, Februar 2005
- Robert Dickmann, Inhaltliche Ausgestaltung von Regelungen zur privaten Internetnutzung im Betrieb, NZA 2003, S.1009 ff
- DUD Report, Datenschutzgerechte Nutzung von Email und anderen Internet-Diensten am Arbeitsplatz, in: Datenschutz und Datensicherheit (DuD) 2002, S. 4
- Stefan Ernst, Der Arbeitgeber, die Email und das Internet, in: Neue Zeitschrift für Arbeitsrecht (NZA) 2002, S. 585 ff.
- Andreas Grote, Ausgesurft? Kosten von Web-Missbrauch und Surfkontrolle im Büro, in: c't 24/2000, S. 272
- Peter Hanau/Thomas Hoeren, Private Internetnutzung durch Arbeitnehmer, 2003, Beck Juristischer Verlag
- Joerg Heidrich/Sven Tschoepe, Rechtsprobleme der E-Mail-Filterung, in: MMR 2004 S. 75 ff
- Joachim Heilmann/Claudia Tege, Informationstechnologie? Rechte und Pflichten bei der Kommunikation, in: AuA 2001, S. 52
- Bernhard Hörl/Antje Buddee, Private Email-Nutzung am Arbeitsplatz, in: ITRB 7/2002, S. 160 ff.
- Manuel Kiper, Betriebs- und Dienstvereinbarungen zu Email und Internet (1)+(2), in: Computer Fachwissen 9/2004, S. 15 ff und 10/2004, S. 6 ff

- Manuel Kiper, Spione im Büro – Überwachung am Arbeitsplatz, in: Christiane Schulzki-Haddouti: Bürgerrechte im Netz, 2003, S. 92 f..
- Manuel Kiper/Bruno Schierbaum, Arbeitnehmer-Datenschutz bei Internet- und E-Mail-Nutzung, 2000, S. 33 f.
- Michael Kliemt, Vertrauen ist gut, Kontrolle ist besser? Internet- und E-Mail-Nutzung von Mitarbeitern, in: AuA 2001, S. 532
- Gerhard Kronisch; Privates Internet-Surfen am Arbeitsplatz, in AUA 1999, S. 550 ff
- Jan Krosch, Spitzel im Netz, in: iX 2000, Ausgabe 11, S. 136 ff.
- Achim Lindemann/Oliver Simon, Betriebsvereinbarungen zur Email, Internet und Intranetnutzung, in: Arbeits- und Sozialrecht 2001, S. 1950 ff.
- Anja Mengel, Kontrolle der Email- und Internetkommunikation am Arbeitsplatz – Wege durch einen juristischen Irrgarten, in: BB 2004, S. 2014 ff.
- Alexander Mayerhöfer/Christian Schlesiger, Spione im Büro? PC-Überwachung, in: Capital 22/2001, S. 162
- Jan-Bernd Meyer, Firmenalltag? Die Jagd nach Sex und der Moorhuhn-Overkill, Computerwoche, Heft 38/2000, S. 9
- Andreas Müller, Datenschutz beim betrieblichen Mailing, in: RDV 1998, S. 205 ff.
- Stefan Nägele/Lars Meyer: Internet und Email am Arbeitsplatz: Rechtliche Rahmenbedingungen der Nutzung und Kontrolle sowie die Reaktion auf Missbrauch, in: K&R 2004, S. 312 ff.
- Anke Naujock, Internet-Richtlinien: Nutzung am Arbeitsplatz, in: Datenschutz und Datensicherheit (DuD) 2002, S. 592 ff.
- Anna Ohlenburg, Der neue Telekommunikationsdatenschutz, in: Multimedia und Recht (MMR) 2004, S. 431 ff.
- OLG Karlsruhe: Strafbarkeit des Ausfilterns von Emails in „Unternehmen“ (OLG Karlsruhe vom 10.1.2005), in: CR 4/2005, S. 288 ff.
- Matthias Pierson/David Seiler, Internet-Recht im Unternehmen, S. 211 ff
- Thomas Reimann, Datenschutz im neuen TKG, in: Datenschutz und Datensicherheit (DuD) 2004, S. 421 ff.
- Michael Schmidl, Private Email-Nutzung – Der Fluch der guten Tat - § 206 StGB als Folge der Gestattung privater Email-Nutzung am Arbeitsplatz, DuD 2005, S. 267
- Brunhilde Steckler, Interessenkonflikte – Darf der Arbeitgeber den E-Mail-Verkehr am Arbeitsplatz überwachen?, in: c't 24/2000, S. 266
- Thorsten Vehslage, Privates Surfen am Arbeitsplatz, in: AnwBl 3/2001, S. 145
- Peter Wedde, Private Email-Nutzung am Arbeitsplatz, Computer Fachwissen 6/2004, S. 25 ff.

- Elmar Weißnicht, Die Nutzung des Internet am Arbeitsplatz, in: MultiMedia und Recht (MMR) 7/2003, S. 448 ff.

### Weiterführende Links:

- Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.:  
<http://www.bvdnet.de/>
- Deutsche Vereinigung für Datenschutz DVD e.V.  
<http://www.aktiv.org/DVD/index.htm>
- Gesellschaft für Datenschutz und Datensicherheit (GDD)  
<http://www.gdd.de/>
- Hamburger Datenschutzgesellschaft e.V.  
<http://www.hamdg.de>
- Zeitschrift Datenschutz-Berater  
<http://www.vhb.de/datenschutz-berater/index.html>
- Zeitschrift DuD Datenschutz und Datensicherheit  
<http://www.dud.de/>
- Zeitschrift Datenschutz-Nachrichten (DANA)  
[http://www.aktiv.org/DVD/Themen/dana/dana\\_start.html](http://www.aktiv.org/DVD/Themen/dana/dana_start.html)
- Zeitschrift IT-Sicherheit  
[http://www.it-sicherheit-fachzeitschrift.de/it-sicherheit/sich\\_hauptframe.htm](http://www.it-sicherheit-fachzeitschrift.de/it-sicherheit/sich_hauptframe.htm)
- Zeitschrift Recht der Datenverarbeitung (RDV)  
[http://www.rdv-fachzeitschrift.de/rdv/recht\\_hauptframe.htm](http://www.rdv-fachzeitschrift.de/rdv/recht_hauptframe.htm)
- Datenschutzrechtliche Grundsätze bei der dienstlichen und privaten Internet und E-Mail-Nutzung am Arbeitsplatz  
<http://www.bfd.bund.de/information/Leitfaden.pdf>
- Gesetz über die Nutzung von Telediensten  
<http://bundesrecht.juris.de/bundesrecht/tdg/index.html>
- Virtuelles Datenschutzbüro  
<http://www.datenschutz.de/>

## Profil

### Arbeitskreis Datenschutz

Datenschutz ist ein wichtiger Akzeptanzfaktor der Informationsgesellschaft. Seine rechtliche Gestaltung beeinflusst die Entwicklung einer modernen Wirtschaft. Er ist der entscheidende Vertrauensfaktor, der es ermöglicht, in der Informationsgesellschaft personenbezogene Daten zu erheben, zu verarbeiten und zu nutzen. Insbesondere beim elektronischen Handel und der elektronischen Verwaltung kann Datenschutz das notwendige Vertrauen in die elektronische Kommunikation schaffen und verbreiteten Befürchtungen vor Missbrauch entgegenwirken. Ein moderner und technikadäquater Datenschutz ist damit auch ein bedeutender Wettbewerbsvorteil und Standortfaktor.

Dem trägt das bisherige Datenschutzrecht in Deutschland nur bedingt Rechnung. Es ist auch nach seiner Novellierung immer noch zu sehr auf das Konzept der räumlich abgegrenzten Datenverarbeitung fixiert, nimmt neue Formen personenbezogener Daten und deren Verarbeitung nur ungenügend auf und berücksichtigt nicht ausreichend die Chancen neuer Techniken der Datenverarbeitung. Darüber hinaus ist es in seinen Formulierungen häufig widersprüchlich und durch seine Normierung in Hunderten von speziellen Gesetzen unübersichtlich und schwer zu handhaben.

Für die BITKOM-Mitglieder ist nicht nur die datenschutzrechtliche Einbettung ihrer Geschäftsmodelle von täglicher Relevanz, sondern auch die Fragen des unternehmensinternen Datenschutzes. Der Umgang mit Mitarbeiterdaten, die Nutzung moderner Kommunikationsmittel am Arbeitsplatz und der konzerninterne Datenaustausch stellen die Unternehmen vor vielfältige Herausforderungen.

### Aufgaben und Ziele

- BITKOM fordert ein datenschutzrechtliches Regelwerk, das am Wert und den Erfordernissen eines modernen Datenschutzes ausgerichtet ist.
- Der Arbeitskreis dient zum einen dem Informations- und Wissensaustausch der BITKOM-Mitglieder, zum anderen unterhält und fördert der Arbeitskreis den Kontakt zu den auf öffentlicher und staatlicher Seite verantwortlichen Entscheidungsträgern.

### Aktivitäten

- Erarbeitung von Stellungnahmen zu aktuellen datenschutzrechtlichen Gesetzgebungsverfahren und Problemen.

- Aktive Beteiligung an den im Bereich Datenschutz erforderlichen Änderungen.
- Zusammenarbeit mit benachbarten BITKOM Gremien, insbesondere aus dem Bereich der Medienpolitik
- Entwicklung vertraglicher Lösungskonzepte für die Auftragsdatenverarbeitung.
- Erstellung von Publikationen und Praxishilfen
- Veranstaltung von Workshops
- Kritische Begleitung der Rechtsentwicklung im Bereich Datenschutz

### Themen (Auswahl)

- RFID
- VoIP
- Datenschutzaudit (-Gesetz) und Gütesiegel
- Auftragsdatenverarbeitung
- Customer Relation Management
- Nutzung von Internet und Email am Arbeitsplatz
- Datentransfer in Drittländer
- Betrieblicher Datenschutz
- Schulungstools
- Arbeitnehmerdatenschutz
- BDSG in der Fassung von 05/2002
- Zweite Stufe der Novellierung des BDSG
- Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, 97/66/EG
- Neufassung der Richtlinie 97/66/EG
- Evaluation der Richtlinie 95/46/EG
- Umsetzung der Richtlinie 02/58/EG

#### Vorsitzende:

Ulrike Schroth, T-Systems International GmbH

#### Stellvertretender Vorsitzender:

Ralf Maruhn, Nokia GmbH

### Ihr Ansprechpartner bei BITKOM:

#### Dr. Kai Kuhlmann



030/27576-131 fax 030/27576-139

[k.kuhlmann@bitkom.org](mailto:k.kuhlmann@bitkom.org)

