UNIVERSITÄTSLEHRGANG
FÜR INFORMATIONSRECHT UND RECHTSINFORMATION
AN DER RECHTSWISSENSCHAFTLICHEN FAKULTÄT DER UNIVERSITÄT WIEN

Privacy am Rechnerarbeitsplatz

Datenschutzrechtliche Probleme durch die

Protokollierung von Log-Files und e-Mails am

Arbeitsplatz

MASTER THESIS

zur Erlangung des akademischen Grades

MASTER OF LAWS (LL.M.)
Informationsrecht und Rechtsinformation

an der Universität Wien
(Universitätslehrgang für Informationsrecht und Rechtsinformation)

vorgelegt von

Mag. Thomas Streitberger

begutachtet von

ao. Univ.-Prof. Dr. Dietmar Jahnel

im September 2003

Hinweise

Dieses Layout basiert auf der Typoskriptvorlage der Österreichischen Rechtswissenschaftlichen Studien (ÖRSt). Die Verwendung, Bearbeitung und allfällige Veröffentlichung der Bearbeitung erfolgt mit freundlicher Genehmigung des Manz-Verlages. Ansonsten wird auf das UrhG verwiesen.

Paragraphenangaben, denen keine Gesetzesbezeichnung beigefügt ist, beziehen sich auf das im jeweiligen Kapitel in der Hauptsache behandelte Gesetz.

Vorliegende Arbeit orientiert sich im Wesentlichen an den AZR (*Friedl/Loebenstein* (Hrsg), Abkürzungs- und Zitierregeln der österreichischen Rechtssprache und europarechtlicher Rechtsquellen[5] (2000)). Zeitschriftenartikel werden mit der Anfangsseitenzahl zitiert, um eine leichtere Auffindbarkeit in der RDB zu ermöglichen.

Die URLs wurden zuletzt am 1.9.2003 überprüft.

Vorwort:

Die Verwendung neuer Kommunikationstechnologien wie Internet und e-Mail am Arbeitsplatz ermöglicht dem Arbeitgeber eine umfassende Überwachung der Arbeitnehmer, die diese Dienste nutzen. Dies ist eine Tatsache, die bei weitem nicht allen Arbeitnehmern bekannt ist. Viele fühlen sich beim Surfen im Internet oder beim Versenden und Empfangen von e-Mails am Arbeitsplatz völlig unbeobachtet.
Dass dadurch auch rechtliche Probleme entstehen ist nicht verwunderlich. Während jedoch zur arbeitsrechtlichen Problematik der Verwendung neuer Medien am Arbeitsplatz bereits zahllose Literatur existiert, so wurde im Gegensatz dazu der datenschutzrechtliche Aspekt in gewissem Maße vernachlässigt. Diese Arbeit soll dazu beitragen etwas Licht ins datenschutzrechtliche Dunkel zu bringen, das in Bezug auf die Verwendung von Internet und e-Mail am Arbeitsplatz und die daraus resultierenden datenschutzrechtlichen Folgen auf Arbeitgeber- und Arbeitnehmerseite herrscht.
Die kurze Abhandlung zum Thema Privacy am Rechnerarbeitsplatz behandelt speziell jene datenschutzrechtlichen Probleme, die sich in Unternehmen, die ihren Mitarbeitern den Internetzugang über einen eigenen Webserver ermöglichen, ergeben können. Dies soll anhand der beiden Hauptproblembereiche, nämlich der Protokollierung von e-Mails und Log-Files aufgezeigt werden.
Besonderer Dank gilt meinem Betreuer, Herrn ao. Univ. Prof. Dr. Dietmar Jahnel, der Dank seiner wertvollen Anregungen und Hinweise, sowie seiner ständigen Ansprech- und Hilfsbereitschaft wesentlich zum Gelingen dieser Arbeit beigetragen hat.

Wien, im Sommer 2003 Thomas Streitberger

Inhaltsverzeichnis

I. Einleitung

Zahlreiche Unternehmen nutzen moderne Kommunikations-technologien. Internet und e-Mail sind aus der heutigen Arbeitswelt kaum mehr wegzudenken. Dass dabei Daten über diejenigen Arbeitnehmer anfallen, die Internet und e-Mail an ihrem Arbeitsplatz nutzen ist vielen nicht bekannt. Der Durchschnittsarbeitnehmer fühlt sich beim Surfen im Internet und beim Versenden von e-Mails unbeobachtet und sicher. Dass für den Arbeitgeber jeder seiner Schritte nachvollziehbar ist, ist ihm meist nicht bewußt. Auf die daraus entstehende datenschutzrechtliche Problematik soll in der folgenden Arbeit eingegangen werden.

Den Ausgangsfall für diese Arbeit stellt dabei ein Unternehmen dar, dass seinen Mitarbeitern Zugang zum Internet über einen eigenen Server gewährt und ihnen ebenso das Versenden und Empfangen von e-Mails ermöglicht.

II. Technischer Hintergrund

Im Folgenden soll dabei kurz auf die technischen Abläufe, die beim Zugriff auf Internetseiten und beim Versenden von e-Mails erfolgen, eingegangen werden, da die Kenntnis dieser Abläufe die Grundlage für das Verständnis der datenschutzrechtlichen Problematik darstellt.

A. Log-Files

Beim Zugriff auf Internetseiten führt der Rechner vom Benutzer unbemerkt mehrere Operationen durch. Nach Eingabe der URL[1] wird zunächst im Cache[2] des Browsers[3] direkt am Rechner des Benutzers nach der gewünschten Seite gesucht. Wird der Rechner dort nicht

---

[1] Uniform Resource Locator – bestehend aus der Bezeichnung der Art des Dienstes (http, ftp, etc.), der Internet-Adresse und evtl. dem Namen des jeweiligen Verzeichnisses und der jeweiligen Datei. Sie dient der eindeutigen _Bezeichnung von Dateien im Web.

[2] Zwischenspeicher in dem häufig aufgerufene Dokumente gespeichert werden.

[3] zB Netscape Navigator, Microsoft Internet Explorer, Mozilla. Im Browser des Benutzers werden zudem die Adressen der zuletzt gelesen Webseiten gespeichert (History).

fündig, so geht die Suche nach dem gewünschten Dokument im Cache des Proxy-Servers[4] des Unternehmens weiter. Ist das Dokument auch dort nicht zu finden, so fordert der Proxy-Server das gewünschte Dokument über das Internet vom Rechner des Anbieters an, kopiert es, speichert es in seinem Cache und leitet es an den anfordernden Rechner weiter. Das gesuchte Dokument wird daraufhin im Browser des Benutzers angezeigt und auch im Cache des anfordernden Rechners gespeichert.

Dabei erfolgt am Proxy-Server des Unternehmens eine Protokollierung der Internetzugriffe. Die relevanten Daten werden dabei in Form sogenannter **Log-Files** (auch Web-Logs[5] genannt) gespeichert. Der Proxy-Server kann aber auch so eingestellt werden, dass keine oder nur eine eingeschränkte Protokollierung der Internetzugriffe erfolgt. Es ist dabei auch möglich die Protokollierung auf Anforderungen aus dem Internet zu beschränken bzw. auch Übermittlungen aus dem Cache des Proxy-Servers einzubeziehen. Welche Informationen diese Log-Files enthalten sollen läßt sich durch den Administrator genau einstellen. Meist sind in den Log-Files Datum und Uhrzeit der Anforderung, die IP-Adresse[6] des anfordernden Rechners, die Art des Zugriffs, Dauer und Datenmenge der Übertragung und eventuell auch die Benutzerkennung, die Adresse des angeforderten Dokuments, etc enthalten[7]. Die Protokollierung von Daten in den Log-Files ist auf sämtliche Eingaben des Benutzers erweiterbar, sodass auch beim Gebrauch einer Suchmaschine verwendete Suchbegriffe, oder Kreditkartenangaben bei Online-bestellungen erfasst werden können.

B. e-Mails

Eine e-Mail besteht aus einem Vorspann (Header) und dem eigentlichen Text (Body). Der Header enthält in der Regel zumindest

---

[4] Auf diesem Server werden, genau wie im „Browser-Cache“ der einzelnen Rechner, aus dem Internet abgerufene Seiten gespeichert um so Zeit und Übertragungskapazität zu sparen.

[5] *Jahnel*, Spamming, Cookies, Web-Logs, LBS und die Datenschutzrichtlinie für elektronische Kommunikation, wbl 2003, 108

[6] Eine IP-Adresse besteht aus einer 32 Bit langen Binärzahl, wobei die Bytes als Dezimalzahlen getrennt durch Punkte angezeigt werden. Sie dient der eindeutigen Identifizierung des jeweiligen Rechners im Internet.

[7] zB 212.93.16.112 - - [22/Jun/2000:04:47:57 +0200] "GET /prog/down/guldrad.exe HTTP/1.1" 200 629257 www.rendle.de "http://www.freeload.de/spiele1.html" "Go!Zilla 3.5 (www.gozilla.com)"

Angaben über den Absender („From"), den Empfänger („To"), das Thema („Subject") und das Datum. Diese Angaben dienen zur Weiterleitung bzw. Rücksendung bei Zustellungsproblemen[8].

Beim Versenden einer e-Mail wird diese zunächst vom Rechner des Benutzers an einen im Mailprogramm eingetragenen Mail-Server (SMTP[9]-Server) übermittelt. Dieser steht entweder bei einem externen Internetserviceprovider oder, sofern der Arbeitgeber selbst als ISP fungiert, im Unternehmen selbst. Der Server sendet die in seinem Speicher eingegangene e-Mail über das Internet an den Server der Zieladresse. Dieser Zielserver (POP-Server[10]) kann wiederum bei einem ISP stehen oder im Unternehmen selbst. Dort angekommen wird die E-Mail in der Mailbox des Empfängers abgelegt und dort für ihn zum Abruf oder zur Bearbeitung bereit gehalten.

Über den Mail-Server können hierbei sämtliche Aktionen protokolliert werden. Wie bei den Log-Files erfolgt aber auch hier die Protokollierung nicht zwingender Weise. Wird aber protokolliert, so entsteht für jede e-Mail eine Protokollzeile mit Angaben über den Absender, den Empfänger, das Datum und den Zeitpunkt der Nachricht, sowie die Anzahl der übermittelten Bytes. Bei den meisten Mail-Servern läßt sich der Umfang der zu protokollierenden Informationen einstellen. Neben diesen Vermittlungsdaten ist es auch möglich den Inhalt der gesendeten Nachrichten zu speichern und so für den Arbeitgeber zugänglich zu machen.

Auch der POP-Server kann ein Protokoll über alle eingehenden e-Mails anlegen, das dann ebenfalls Absender, Empfänger, sowie Datum und Uhrzeit der Übertragung enthält.

---

8 *Hobert*, Datenschutz und Datensicherheit im Internet² (2000) 39
9 Simple Mail Transmission Protocol.
10 Post Office Protocol - Server

III. rechtliche Problematik

Es geht im Folgenden um jene datenschutzrechtlichen Bestimmungen, die der Arbeitgeber in Bezug auf Log-Files und e-Mails zu beachten hat, wenn sein Unternehmen einen eigenen Server besitzt, über den er seinen Dienstnehmern den Zugang zum Internet ermöglicht. Er ist in diesem Fall in Bezug auf seine Arbeitnehmer mit einem ISP vergleichbar, da er ihnen genau wie dieser den Zugang zum Internet ermöglicht. Es wird dabei davon ausgegangen, dass sich das Unternehmen, von dem aus auf das Internet zugegriffen wird bzw e-Mails versendet werden in Österreich befindet. Alle anderen an den jeweiligen Kommunikationsvorgängen beteiligten können sich dagegen sowohl im Ausland, als auch im Inland befinden.

Die datenschutzrechtliche Problematik entsteht allerdings nur unter der Voraussetzung, dass über den Server des Unternehmens protokolliert wird, da sie bei nicht erfolgter Protokollierung entschärft ist. Für den Fall, dass sich der Arbeitgeber eines externen Internetproviders bedient und selbst über keinen Proxy-Server verfügt, so kann er die bereits oben aufgezeigten Möglichkeiten nicht nutzen, weil sein Provider dem TKG unterliegt und daher derartige Informationen nicht weitergeben darf.[11]

Dabei soll zuerst auf jene datenschutzrechtlichen Probleme eingegangen werden, die bei der Protokollierung von Log-Files und e-Mails gleichermaßen auftreten. Später wird dann in einem gesonderten Abschnitt auf jene Problembereiche eingegangen, die speziell durch die Protokollierung von Log-Files bzw speziell durch die Protokollierung von e-Mails am Arbeitsplatz entstehen können.

A. Log-Files und e-Mails – gemeinsame Problematik

1. Sind Log-Files und e-Mails personenbezogene Daten?

Um zur Anwendung datenschutzrechtlicher Bestimmungen zu kommen stellt sich vorerst die Frage, ob es sich bei Log-Files und e-Mails überhaupt um personenbezogene Daten handeln kann. So geht zB

[11] *Obereder*, E-Mail und Internetnutzung aus arbeitsrechtlicher Sicht, DRdA 2001, 75ff; genauere Ausführungen zu den Pflichten eines externen ISP finden sich bei *Jahnel*, Das Versenden von e-Mails aus datenschutzrechtlicher Sicht in e-Mail, elektronische Post im Recht, *it-law.at (Hrsg)*, (2003) 89

Rotter davon aus, dass bei der Registrierung von Internetkontakten überhaupt keine personenbezogenen Daten des Arbeitnehmers gespeichert werden, sondern bloß das Ziel seiner Zugriffe[12].

Dass dem nicht so ist, und es sich sowohl bei e-Mails als auch bei Log-Files unter bestimmten Voraussetzungen um **personenbezogene Daten** handeln kann, soll im Folgenden aufgezeigt werden. Gemäß § 4 Z 1 DSG 2000 sind unter personenbezogenen Daten Angaben über Betroffene zu verstehen, deren Identität bestimmt oder bestimmbar ist. Als Betroffenen definiert § 4 Z 3 DSG 2000 jede vom Auftraggeber verschiedene natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet werden. Eine weitere Unterscheidung erfolgt in der Z 1 noch dahingehend, dass zwischen **„direkt personenbezogenen“** und **„indirekt personenbezogenen“** Daten unterschieden wird, wobei unter „indirekt personenbezogenen Daten“ solche zu verstehen sind, deren Personenbezug derart ist, dass der jeweilige Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann.

a) e-Mails:

Am Einfachsten läßt sich der Personenbezug im Bereich der e-Mails aufzeigen. Es ist hier dahingehend zu unterscheiden, dass dann kein Personenbezug herstellbar ist, wenn die e-Mails von einer Adresse abgeschickt werden, die keinem Dienstnehmer eindeutig zugeordnet werden kann (z.B. office@firma.at). Dies natürlich unter der Voraussetzung, dass sich nicht nachvollziehen läßt, wer zum Zeitpunkt der Übermittlung am jeweiligen Rechner, von dem aus die Übermittlung erfolgte, tätig war. Besonders in kleineren Unternehmen wird es jedoch häufig der Fall sein, dass sich auch bei einer solchen e-Mail-Adresse klar feststellen läßt, wer den Rechner zu diesem Zeitpunkt benutzte und in der Folge von wem die e-Mail stammte. Ist aber nicht herauszufinden von wem die jeweilige e-Mail stammt, so ist auch kein Personenbezug herstellbar.

In den meisten größeren Unternehmen ist es aber so, dass den Mitarbeitern eigene e-Mail-Adressen zugeteilt werden, die sich aus Vorname und Zuname des jeweiligen Mitarbeiters, sowie dem Firmennamen zusammensetzen (zB josef.maier@firma.at). In diesem Fall ist der Personenbezug offensichtlich. Dieser kann hier in

[12] *Rotter*, Internet-Zugang für Arbeitnehmer, Mustervereinbarung, ASoK 1999, 118

zweifacher Hinsicht gegeben sein, und zwar sowohl in Richtung des Absenders, als auch in Richtung des Empfängers[13]. Es reicht in diesem Fall bereits die Protokollierung der „Header-Daten" aus um einen Personenbezug herzustellen, ohne dass es notwendig ist dafür auf den Inhalt der Nachricht zuzugreifen.

Zusammenfassend kann also gesagt werden, dass es sich bei der Protokollierung von e-Mails am Server des Unternehmens, je nach Zusammensetzung der e-Mail Adresse des jeweiligen Arbeitnehmers, um personenbezogene Daten handeln kann, dies jedoch nicht zwingend der Fall sein muß und dass selbst bei einer anonymen e-Mail-Adresse in zahlreichen Fällen ein Personenbezug herstellbar sein kann.

b) Log-Files:

Etwas komplexer stellt sich die Unterscheidung im Bereich der Log-Files dar. So geistert in zahlreichen wissenschaftlichen Beiträgen noch die Auffassung umher, dass sich nur dann ein Personenbezug herstellen läßt, wenn der jeweilige PC des Arbeitnehmers paßwortgesichert ist (siehe zB *Dellisch*, private Internet und E-Mail Nutzung am Arbeitsplatz[14], ebenso *Gruber* anläßlich einer Diskussion der österreichischen Juristenkommission[15]). In diesem Fall wären auf jeden Fall personenbezogene Daten gegeben, da der Arbeitgeber den Log-Files sowohl das Paßwort des jeweiligen Arbeitnehmers entnehmen kann, als auch welche Internetseiten von diesem wann und wie lange besucht wurden. Dass dadurch bloß die Ziele der jeweiligen Zugriffe der Arbeitnehmer aufscheinen verhindert nicht, so wie *Rotter*[16] annimmt, das Entstehen personenbezogener Daten. Es fallen in diesem Fall Daten, also Angaben über den Betroffenen, in unserem Fall den Arbeitnehmer, an, aus denen klar hervorgeht auf wen sie sich beziehen. Auch dass nur die Ziele der jeweiligen Zugriffe aufscheinen ist nicht richtig, da es, wie bereits im Rahmen des technischen Hintergrundes erwähnt, auch möglich ist, Suchbegriffe bei der Verwendung von Suchmaschinen, oder Kreditkartennummern bei Onlinebestellungen zu protokollieren. Und selbst wenn nur die Ziele der jeweiligen Zugriffe

---

[13] ähnlich *Funk/Kreijci/Schwarz,* Zur Registrierung von Ferngesprächen durch den Arbeitgeber am Beispiel der Universität Graz, RdA 1984, 285

[14] *Dellisch*, Private E-Mail- und Internet-Nutzung am Arbeitsplatz, ASoK 2001, 316

[15] *Gruber* in: *Öst. Juristenkommission (Hrsg),* Grundrechte in der Informationsgesellschaft (2001) 201

[16] *Rotter*, Internet-Zugang für Arbeitnehmer, Mustervereinbarung, ASoK 1999, 118

aufscheinen würden, so würde dadurch das Entstehen personenbezogener Daten nicht verhindert, wenn sich genauestens zuordnen läßt, welche Internetseiten von welchem Arbeitnehmer besucht wurden. So geht auch *Simitis* davon aus, dass es angesichts der Möglichkeiten der modernen Datenverarbeitung „kein belangloses Datum" mehr gibt[17].

Es ist jedoch nicht unbedingt notwendig, dass der jeweilige Arbeitnehmer einen paßwortgesicherten PC verwendet, um zurückzuverfolgen, wo dieser sich im Internet bewegt hat. Dies ist auch über die jeweilige IP-Adresse des Rechners problemlos möglich, sofern jedem Arbeitnehmer eindeutig ein bestimmter Arbeitsplatz zugewiesen ist, auf den zum entsprechenden Zeitpunkt nur dieser Arbeitnehmer Zugriff hatte. Zudem ist im Rahmen der Rückverfolgbarkeit der derzeit noch gebräuchlichen IPv4[18] - Adressen zwischen statischen und dynamischen IP-Adressen zu unterscheiden[19].

Unter **statischen IP-Adressen** versteht man solche, die ständig demselben Rechner zugeordnet sind. In diesem Fall ist es für den Arbeitgeber überhaupt kein Problem über die IP-Adresse zurückzuverfolgen von welchem Rechner und in der Folge von welchem Arbeitnehmer auf bestimmte Web-Inhalte zugegriffen wurde.

Von einer **dynamischen IP-Adresse** spricht man, wenn dem jeweiligen Rechner für jede Internet-Session eine neue IP-Adresse zugeteilt wird. In diesem Fall werden verschiedenen Benutzern im Lauf der Zeit dieselben IP-Adressen zugeteilt. Doch auch in diesem Fall ist dem Arbeitgeber eine Rückverfolgung ähnlich wie bei statischen IP-Adressen möglich, und zwar dadurch, dass eine Software verwendet wird, die protokolliert, wann welchem Rechner im Firmennetzwerk welche IP-Adresse zugeteilt wurde.

Die nächste Generation von IP-Adressen (IPv6) soll sogar die lebenslange eindeutige Identifikation jedes Rechners im Internet ermöglichen[20], sodass spätestens mit deren Einführung davon auszugehen ist, dass es dem Arbeitgeber, sofern jedem Arbeitnehmer ein Rechner zugewiesen ist auf den nur er Zugriff hat, möglich ist,

---

17 *Simitis* in *Simitis/Dammann,* BDSG-Kommentar[4] (1992), § 1 RN 181

18 Internet Protocol version 4

19 Um eine bessere Lesbarkeit der Arbeit zu ermöglichen, erfolgt die Erklärung der Unterschiede nicht im Rahmen der technischen Grundlagen sondern an gegebener Stelle

20 Cp European Commission, „Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6", http://europa.eu.int/comm/internal_market/en/dataprotect/wpdocs/wp58_en.pdf (1/20/2003).

genau zurückzuverfolgen auf welche Inhalte im WWW seine Mitarbeiter zugegriffen haben.

Abschließend ist also zu sagen, dass es sich auch bei Log-Files, ähnlich wie bei e-Mails, unter bestimmten Voraussetzungen um personenbezogene Daten handeln kann.

c) Liegen direkt oder indirekt personenbezogene Daten vor?

Liegen personenbezogene Daten vor, so handelt es sich im Fall der Protokollierung von Log-Files und e-Mails durch den Arbeitgeber wohl meist um direkt personenbezogenen Daten im Sinne des § 4 Z 1 DSG 2000. Direkt personenbezogene Daten liegen demnach dann vor, wenn Angaben über Betroffene vorliegen, deren Identität bestimmt oder bestimmbar ist, es also für den Verwender der Daten, in unserem Fall den Arbeitgeber, möglich ist den vorhandenen Personenbezug zB in Form einer laufenden oder sprechenden Nummer, auf eine in ihrer Identität bestimmte Person zurückzuführen[21]. Dass dies dem Arbeitgeber aufgrund der Protokollierung unter bestimmten Voraussetzungen möglich ist wurde bereits gezeigt. Gemäß § 4 Z 1 DSG 2000 muß die Identität des Betroffenen weiters mit rechtlich zulässigen Mitteln bestimmbar sein. Nach den erläuternden Bemerkungen zu § 4 Abs 1 leg cit wird dadurch die **Bestimmbarkeit** des Betroffenen auf **legale Mittel** eingeschränkt. Gemäß Erwägungsgrund 26 der dem DSG 2000 zu Grunde liegenden Datenschutzrichtlinie[22] ist als mögliches Mittel der Identifikation nur ein solches anzusehen, das vernünftigerweise angewendet wird, dh das also weder seiner Art nach, noch seinem Aufwand nach vollkommen ungewöhnlich ist. Solange also die Identität des Betroffenen für den Arbeitgeber mit legalen Mitteln, die weder nach ihrer Art, noch nach ihrem Aufwand vollkommen ungewöhnlich sind, bestimmbar ist, liegen direkt personenbezogene Daten vor. Dies wird bei der Protokollierung von Log-Files und e-Mails am Arbeitsplatz durch den Arbeitgeber wohl in den meisten Fällen gegeben sein.

2. Anwendbarkeit der Datenschutzbestimmungen des TKG

Es stellt sich auch die Frage, ob in Bezug auf die Protokollierung von Log-Files und e-Mails am Arbeitsplatz nicht auch die Anwendbarkeit der Datenschutzbestimmungen im 12. Abschnitt des

[21] Siehe dazu die EB der RV zu 4 Z 1 DSG 2000
[22] Richtlinie 95/46/EG

Telekommunikationsgesetzes gegeben ist, da der Arbeitgeber seinen Arbeitnehmern ähnlich einem Access-Provider den Zugang zum Internet und das Versenden und Empfangen von e-Mails ermöglicht. Die folgende Prüfung dieser Frage erfolgt sowohl nach den Bestimmungen des bis 20. August 2003 in Geltung stehenden **TKG 1997**, als auch nach denen des ab diesem Zeitpunkt gültigen **TKG 2003**. Dadurch sollen etwaige Veränderungen der Rechtslage aufgrund der Novellierung des TKG aufgezeigt werden.

a) Nach dem TKG 1997

Um die Anwendbarkeit der Datenschutzbestimmungen des TKG zu gewährleisten muß es sich nach § 88 Abs 2 und § 91 TKG beim Arbeitgeber um einen **Betreiber**, oder eine Person, die an der Tätigkeit des Betreibers mitwirkt, handeln. Unter einem Betreiber ist gemäß § 87 Abs 3 Z 1 TKG ein Anbieter von **öffentlichen Telekommunikations-diensten** im Sinne des 3. Abschnittes des TKG zu verstehen. Es stellt sich also die Frage, ob es sich bei einem Arbeitgeber, der seinen Arbeitnehmern über einen eigenen Server die Verwendung von Internet und e-Mail ermöglicht, um einen Anbieter von öffentlichen Telekommunikationsdiensten im Sinne des 3. Abschnittes des TKG handelt.

Der OGH hat diese Frage in einem ähnlich gelagerten Fall[23] dahingehend entschieden, dass es sich bei einem Arbeitgeber der eine neue Telefonanlage installiert und diese seinen Mitarbeitern zur Verfügung stellt nicht um einen Betreiber im Sinne des § 87 Abs 3 Z 1 TKG handelt. Er begründete dies damit, dass § 3 Z 14 TKG den „Telekommunikationsdienst“ als eine **gewerbliche Dienstleistung**, die in der Übertragung und/oder Weiterleitung von Signalen auf Telekommunikationsnetzen besteht, einschließlich des Angebotes von Mietleitungen, definiert. Das zur Verfügung stellen einer Telefonanlage durch den Arbeitgeber, der damit seinen Mitarbeitern das Führen dienstlicher und auch privater Gespräche ermöglicht, könne jedoch nicht als gewerbliche Dienstleistung angesehen werden, weshalb der Arbeitgeber in diesem Fall nicht dem Fernmeldegeheimnis und dem telekommunikationsrechtlichem Datenschutz, der im 12. Abschnitt des TKG 1997 (§§ 87 bis 101 TKG) normiert ist, unterliege.

Obwohl dem OGH im Ergebnis zuzustimmen ist, so ist die Begründung, mit der er zu diesem Ergebnis kommt, keineswegs zufriedenstellend. So ist mE nicht ohne weiteres klar, warum es sich

[23] OGH, 13 .06. 2002, 8 Ob A 288/01p, wbl 2002, 353

beim zur Verfügung stellen der Telefonanlage für private und dienstliche Gespräche der Arbeitnehmer nicht um eine gewerbliche Dienstleistung handeln kann.

Gemäß § 1 Abs 2 GewO 1994 wird eine Tätigkeit dann gewerblich ausgeübt, wenn sie selbständig, regelmäßig und in der Absicht betrieben wird, einen Ertrag oder sonstigen wirtschaftlichen Vorteil zu erzielen, gleichgültig für welche Zwecke dieser bestimmt ist. Eine Gewinnerzielungsabsicht ist in diesem Zusammenhang nicht notwendig, es reicht bereits, wenn lediglich die Unkosten abgedeckt werden sollen. Ebenso liegt Ertragserzielungsabsicht vor, wenn die Tätigkeit letzten Endes der Erreichung des mit dem Gewerbebetrieb verbundenen geschäftlichen Zieles dient[24]. Zudem stellen nach der Judikatur des VwGH[25] alle Handlungen eines Gewerbebetriebes im Rahmen seines Gewerbes eine gewerbliche Tätigkeit dar, auch wenn diese ansonsten isoliert betrachtet von der Anwendbarkeit, wegen Fehlens eines Tatbestandsmerkmals ausgenommen sind. Es ist also für das Vorliegen der Gewerblichkeit keinesfalls notwendig, dass das Erbringen von Telekommunikationsdienstleistungen den Hauptzweck des Geschäftes darstellt. Insoweit kann also festgestellt werden, dass auch der Arbeitgeber gegenüber seinen Arbeitnehmern, zumindest sofern er auch den privaten Internetgebrauch durch diese duldet, Telekommunikationsdienste im Sinne des § 3 Z 14 erster Halbsatz TKG erbringt.

Diese Argumentation findet sich auch in der Glosse *Thieles*[26] zu dieser Entscheidung, der zudem aber noch darauf hinweist, dass die einschlägigen, zur Zeit der Erlassung des TKG 1997 maßgeblichen EU-Richtlinien[27] in ihren Begriffsbestimmungen keinerlei Hinweise auf eine Gewerblichkeit enthalten. Da nach den erläuternden Bemerkungen zum TKG 1997[28] die Begriffsbestimmungen der einschlägigen Telekom-RL der EG in das österreichische Recht übernommen werden, um so eine vollständige Umsetzung der Richtlinien zu gewährleisten, geht er davon aus, dass die österreichische Regelung eher zu restriktiv umgesetzt worden ist, was jedoch durch eine europarechtskonforme

[24] VwGH 13. 10. 1993, 92/03/0054, VwSlg 13.921 A/1993, wbl 1994, 283 = ZfVB 1995/1765 mwN zur Vorjudikatur betreffend den unentgeltlichen Transport von Skischülern durch den Betreiber einer Skischule

[25] VwGH 10. 12. 1985, 85/04/0126

[26] OGH, 13 .06. 2002, 8 Ob A 288/01p, wbl 2002, 353

[27] RL 90/388/EWG; RL 90/387/EWG; RL 94/46/EG

[28] RV BlgNR GP XX RV 759 zu § 3; AB 824, S 81 im Allg Teil

Interpretation korrigiert werden könne. Dieser Ansicht kann wohl zugestimmt werden.

Thiele geht jedoch in seiner Glosse zur OGH Entscheidung[29] weiters davon aus, dass es sich in diesem Fall bei den Arbeitnehmern um „Benutzer" im Sinne des § 87 Abs 3 Z 3 handelt, da sie den Telekommunikationsdienst für private oder geschäftliche Zwecke nutzen, ohne den Dienst zwangsläufig abonniert zu haben. Hier widerspricht sich *Thiele* jedoch selbst, da es sich gemäß § 87 Abs 3 Z 3 bei einem „Benutzer" um eine natürliche Person handeln muß, die einen öffentlichen Telekommunikationsdienst nutzt. *Thiele* selbst argumentiert in der Folge zu Recht gegen das Vorliegen eines öffentlichen Telekommunikationsdienstes.

Denn aus dem bloßen Erbringen eines Telekommunikations-dienstes im Sinne des § 3 Z 14 TKG durch den Arbeitgeber folgert noch nicht automatisch die Anwendbarkeit des 12. Abschnittes des TKG. Dieser ist gemäß § 87 Abs 3 Z 1 leg cit nur auf „Betreiber" anwendbar, worunter Anbieter von öffentlichen Telekommunikations-diensten im Sinne des 3. Abschnitts des TKG (§§ 12 - 23 TKG) zu verstehen sind.

Dieser Begriff der „**Öffentlichen Telekommunikationsdienste**" wird im TKG nicht näher definiert. Die einschlägigen europarechtlichen Bestimmungen gewähren lediglich eine negative Abgrenzung, derzufolge ein Dienst jedenfalls dann nicht als öffentlich erbracht gilt, wenn er der Kommunikation innerhalb einer geschlossenen Benutzergruppe dient.

In der Folge gehen jedoch *Parschalk, Zuser* und *Otto*[30] davon aus, dass es wohl bereits als Erbringen eines öffentlichen Dienstes gelten muß, wenn den Teilnehmern einer geschlossenen Benutzergruppe nicht nur die interne (Sprach-) Kommunikation sondern auch die Kommunikation mit beliebigen anderen, nicht gruppenzugehörigen Teilnehmern (öffentlicher Netze) angeboten wird. Würde man dieser Ansicht folgen, so müßte man zu dem Schluß kommen, dass in unserem Fall der Arbeitgeber sehr wohl ein Anbieter von öffentlichen Telekommunikationsdiensten ist, da er ja seinen Arbeitnehmern, also einer geschlossenen Benutzergruppe, den Zugang zum Internet und das Versenden von e-Mails ermöglicht, wodurch diese mit beliebigen anderen, nicht ihrer Gruppe zugehörigen, Nutzern des Internets kommunizieren können. Gegen diese Ansicht spricht jedoch das

[29] OGH, 13 .06. 2002, 8 Ob A 288/01p, wbl 2002, 353
[30] *Parschalk/Zuser/Otto*, Telekommunikationsrecht (2002) 51

Positionspapier der TKC zur Konzessionspflicht[31], in dem es heißt, dass der Telefondienst, der einer **geschlossenen Benutzergruppe** angeboten wird sowohl die Herstellung von Telefonverbindungen innerhalb der Gruppe, als auch zwischen Teilnehmern der Gruppe einerseits und beliebigen anderen außerhalb der Gruppe andererseits umfassen kann. Weiters spricht gegen diese Ansicht das in den Erwägungsgründen 6, 12, 33, 37 und 46 zur Datenschutzrichtlinie für elektronische Kommunikation[32] vom 12. Juli 2002 stets von **öffentlich zugänglichen** elektronische Kommunikationsnetzen die Rede ist. Es kommt demnach also darauf an, ob der Zugang zum Netz der Öffentlichkeit angeboten wird, oder eben wie in diesem Fall, nur einer geschlossenen Benutzergruppe, also den Arbeitnehmern des Unternehmens und nicht darauf, ob Außenstehende über dieses Netz erreichbar sind oder nicht. Ein Arbeitgeber, der seinen Arbeitnehmern eine Telefonanlage zum Führen sowohl dienstlicher als auch privater Telefongespräche zur Verfügung stellt ist demzufolge kein Betreiber im Sinne des § 87 Abs 3 Z 1 TKG, da er den Telekommunikationsdienst nicht öffentlich anbietet, weshalb auch die Datenschutzbestimmungen des TKG nicht auf ihn anwendbar sind.

Auch *Thiele* geht in seiner Glosse[33] zum vorliegenden Fall davon aus, dass es an der Öffentlichkeit der Telekommunikations-diensteerbringung mangelt und beruft sich dabei auf die ausführliche Definition geschlossener Benutzergruppen im Erlaß der obersten Fernmeldebehörde[34].

In unserem Fall geht es zwar um keine Telefonanlage, sondern um einen Arbeitgeber, der seinen Arbeitnehmern über einen eigenen Server den Zugang zum Internet ermöglicht, die Argumente zur oben angeführten Entscheidung des OGH lassen sich aber auch in diesem Fall ins Felde führen.

So findet man auch in einer Arbeit von *Otto* zur Konzessionspflicht von Internet Service Providern[35] nach dem TKG die Ansicht, dass ein öffentliches Telekommunikationsnetz jedenfalls dann nicht vorliegt, wenn es nur zur Erbringung von

---

31 Siehe dazu das (noch) von der TKC publizierte Positionspapier für den Sprachtelefondienst, vom 26. 06. 1998, Version 2.1., 14 (im weiteren: Positionspapier zur Konzessionspflicht), zu finden unter http://www.tkc.at/web.nsf/lookuid/01D619D19CD2B97EC1256CF00054CA4E/$file/Konzessionspflicht%20f%C3%BCr%20den%20Sprachtelefoniedienst.pdf

32 Richtlinie 2002/58/EG

33 OGH, 13 .06. 2002, 8 Ob A 288/01p, wbl 2002, 353

34 GZ 108271/IV-JD/96

35 *Otto*, Konzessionspflicht für ISP, 7f, zu finden unter www.it-law.at

Telekommunikationsdiensten, die ausschließlich geschlossenen Benutzergruppen zur Verfügung stehen, genutzt wird. Charakteristisch für **geschlossene Benutzergruppen** ist demzufolge, dass der Kreis der Benutzer von vornherein durch bestimmte Kriterien festgelegt ist. Otto zufolge ist dabei hinsichtlich ISP zu beachten, dass es sich auch um eine geschlossene Benutzergruppe handelt, wenn Daten außerhalb des eigenen Netzes weitergeleitet werden, solange der Zugang nur von bestimmten Personen in Anspruch genommen werden kann. Somit sei z.B. auch ein internes Computernetzwerk im Unternehmen, welches mit dem Internet verbunden ist, nicht öffentlich.

Auf unseren Arbeitgeber bezogen, der seinen Mitarbeitern den Zugang zum Internet ermöglicht und somit ihnen gegenüber die Funktion eines ISP übernimmt, kann somit festgestellt werden, dass er keine öffentlichen Telekommunikationsdienste anbietet und somit auch die Datenschutzbestimmungen des TKG nicht auf ihn anwendbar sind.

b) Anwendbarkeit des TKG 2003

Damit die Datenschutzbestimmungen des TKG 2003 auf den Arbeitgeber anwendbar sind, muss es sich bei diesem um einen Betreiber von öffentlichen Kommunikationsdiensten im Sinne des § 92 Abs 3 Z 1 handeln. Unter einem Kommunikationsdienst ist gemäß § 3 Z 9 eine gewerbliche Dienstleistung zu verstehen, die ganz oder überwiegend in der Übertragung von Signalen über Kommunikationsnetze besteht.

Es kann also in aller Kürze gesagt werde, dass auch die datenschutzrechtlichen Bestimmungen des TKG 2003 **nur auf Betreiber von öffentlichen Telekommunikationsdiensten anwendbar** sind. Dafür ist die Gewerblichkeit sowie die Öffentlichkeit der Diensteerbringung notwendig. Da es in unserem Fall an der Öffentlichkeit der Diensteerbringung fehlt, wie bereits im Abschnitt a aufgezeigt werden konnte, ist auch die Anwendbarkeit der Datenschutzbestimmungen des TKG 2003 auf einen Arbeitgeber, der seinen Arbeitnehmern den Zugang zum Internet über einen eigenen Server ermöglicht, nicht gegeben.

3. Potentiell sensible Daten:

Nachdem nun bereits geklärt werden konnte, dass es sich bei der Protokollierung von Log-Files und e-Mails durch den Arbeitgeber unter bestimmten Voraussetzungen um personenbezogene Daten handeln kann, und diese somit auch dem Schutz des DSG 2000 unterliegen,

führt dies zu einer weiteren wichtigen Frage. Nämlich der nach dem Schutzniveau, dass das DSG 2000 für diese Daten vorsieht. Es stellt sich also die Frage, ob es sich dabei auch um **sensible** Daten im Sinne des § 4 Abs 2 DSG 2000 handeln kann, oder ob durch die Protokollierung nur **nicht-sensible** Daten anfallen. Unter sensiblen Daten sind besonders schutzwürdige Daten, nämlich gemäß § 4 Abs 2 DSG 2000 Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben zu verstehen. Hier wird man nach eingehender Prüfung zu dem Schluß kommen, dass sowohl das Vorliegen sensibler, als auch nicht-sensibler Daten möglich ist.

So läßt sich beispielsweise über die Log-Files nicht nur feststellen, welcher Arbeitnehmer wann, wie lange, welche Seiten im Internet abgerufen hat und wieviel seiner Arbeitszeit er im Internet zubringt, sondern es sind durch die Erfassung der Internetadressen fallweise auch Rückschlüsse auf Interessen, Hobbys, sexuelle Vorlieben, die politische Gesinnung usw. möglich, sofern die Zugriffe privater Natur waren. Besonders hingewiesen werden soll in diesem Fall noch einmal auf die Möglichkeit der Protokollierung von Suchbegriffen bei der Verwendung von Suchmaschinen.

Bei der Protokollierung des e-Mail-Verkehrs verhält es sich ebenso. So ist eine Inhaltskontrolle oft gar nicht mehr erforderlich um zu überprüfen, ob es sich dabei um private oder dienstliche Korrespondenz handelt, sofern die e-Mail-Adresse des Empfängers erfasst wird. Auf Grund der in ihr enthaltenen Angaben (zB …@gruene.at; ...@oegb.or.at; …@dioezese-linz.at; …@aidshilfe.or.at) sind auch hier ohne weiteres Rückschlüsse auf die politische Gesinnung, die Religion, Gesundheit, Gewerkschaftszugehörigkeit etc. möglich. Dies ist sowohl durch Erfassen der e-Mail Adresse des Empfängers, als auch durch Erfassen der e-Mail Adresse des Absenders, also in beide Richtungen, möglich.

Gruber sprach in diesem Zusammenhang erstmals vom Vorliegen **„potentiell sensibler" Daten**.[36] Dieser Begriff ist in zweifacher Hinsicht zutreffend. Zum Ersten kann daraus, dass ein Arbeitnehmer eine e-Mail an die Aidshilfe geschickt hat oder er die Web-Site des ÖGB besucht hat, noch nicht geschlossen werden, dass er an HIV erkrankt oder Gewerkschaftsmitglied ist. Das Auswerten von

[36] *Gruber*, Überwachung der dienstlichen Verwendung von Internet und E-Mail, in *Österreichische Juristenkommission (Hrsg)*, Grundrechte in der Informationsgesellschaft (2001) 172

Suchbegriffen und die kombinierte Auswertung von Log-Files und e-Mails kann aber auf jeden Fall Aufschlüsse über Neigungen, Einstellung, Absicht oder Gesinnungen des jeweiligen Arbeitnehmers geben. Weiters ist es für den Arbeitgeber vor Speicherung, bzw vor Kontrolle und Auswertung, der Daten nicht möglich, zu erkennen, ob es sich dabei um sensible oder nicht-sensible Daten handelt. Mit der Speicherung bzw der Kontrolle und Auswertung derselben ist der Rechtsbruch jedoch dann möglicherweise bereits erfolgt. Da es dem Arbeitgeber vor Sichtung der Daten somit nicht möglich ist zu beurteilen, ob es sich dabei um sensible oder um nicht-sensible Daten handelt ist mE auf Grund des gesetzlichen Schutzzweckes in diesem Zusammenhang im Zweifel wohl immer die strengere datenschutzrechtliche Bestimmung des § 9 DSG 2000 anzuwenden und somit vom Vorliegen sensibler Daten auszugehen[37].

B. Protokollierung und Kontrolle von Log-Files durch den Arbeitgeber – Rechte und Pflichten des AG

Gemäß § 3 Abs 1 DSG 2000 ist dieses Gesetz auf die Verwendung personenbezogener Daten im Inland anzuwenden. Wie bereits gezeigt wurde kann es sich bei Log-Files um personenbezogene Daten im Sinne des § 4 Z 1 DSG 2000 handeln. Demzufolge muß geprüft werden, ob die Protokollierung, also die Speicherung der Log-Files durch den Arbeitgeber nach den Bestimmungen des DSG 2000 rechtmäßig erfolgt, oder nicht.

Die wichtigste Frage, die sich in diesem Zusammenhang stellt ist die, ob der Arbeitgeber in diesem Zusammenhang als **Auftraggeber** im Sinne des § 4 Z 4 DSG 2000 zu betrachten ist. Unter einem Auftraggeber sind natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft oder die Geschäftsapparate solcher Organe zu verstehen, wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten für einen bestimmten Zweck zu verarbeiten und zwar unabhängig davon, ob sie die Verarbeitung selbst durchführen oder hiezu einen anderen heranziehen. Dem Arbeitgeber als Eigentümer des Servers obliegt in diesem Zusammenhang die Entscheidung ob und wenn ja, in welchem Ausmaß eine Protokollierung der Log-Files erfolgen soll. Werden am Unternehmensserver keine Log-Files protokolliert, so

[37] siehe auch *Jahnel*, Das Versenden von e-Mails aus datenschutzrechtlicher Sicht, in *it-law.at (Hrsg)*, e-Mail, elektronische Post im Recht (2003) 96

erfolgt auch keine Verarbeitung von Daten. Die Entscheidung, ob protokolliert wird liegt hierbei allein beim Arbeitnehmer. Somit ist er nach § 4 Z 4 DSG 2000 Auftraggeber. Werden dabei personenbezogene Daten eines Arbeitnehmers protokolliert, so ist dieser **Betroffener** im Sinne des § 4 Z 3 DSG 2000.

1. Speicherung durch den Arbeitgeber

Werden die Log-Files auf dem Server des Unternehmens gespeichert, so ist in diesem Fall der Eigentümer des Unternehmens, also der Arbeitgeber, wie oben bereits erwähnt, Auftraggeber im Sinne des DSG 2000. Daten dürfen gemäß § 7 Abs 1 DSG 2000 nur dann verarbeitet werden, soweit Zweck und Inhalt der Datenanwendung von den gesetzlichen Zuständigkeiten oder den rechtlichen Befugnissen des jeweiligen Auftraggebers gedeckt sind und die schutzwürdigen Geheimhaltungsinteressen der Betroffenen nicht verletzt sind. Betroffener ist auch in diesem Fall der jeweilige Arbeitnehmer, dessen Daten protokolliert werden. Die rechtliche Befugnis des Arbeitgebers zur Verarbeitung der anfallenden Daten läßt sich in diesem Fall aus seinem Eigentum am Server und der **Unverletzlichkeit des Eigentums** gemäß Art 5 StGG ableiten. Das Verarbeiten von Daten umfasst gemäß § 4 Z 9 DSG 2000 auch das Erfassen und Speichern der Daten, wie dies bei einer Protokollierung am Web-Server erfolgt.

Es ist also als nächstes zu prüfen ob **schutzwürdige Geheimhaltungsinteressen** des Betroffenen, hier also des jeweiligen Arbeitnehmers, verletzt werden. Man trifft dabei wieder auf die bereits oben erwähnte Problematik, ob es sich bei Log-Files um sensible oder um nicht-sensible Daten im Sinne des DSG 2000 handelt, da demnach zu prüfen sein wird, ob schutzwürdige Interessen des Arbeitnehmers im Sinne des § 8 oder des § 9 DSG 2000 vorliegen.

a) Überprüfung nach § 8 DSG 2000

Geht man davon aus, dass es sich bei Log-Files um nicht-sensible Daten handelt, so käme § 8 DSG 2000 zur Anwendung. Dieser enthält eine Generalklausel in Abs 1 und eine demonstrative Liste mit einzelnen wichtigen Beispielen in den Absätzen 2-4. Daraus wird ersichtlich unter welchen Umständen die Speicherung erlaubt ist und schutzwürdige Geheimhaltungsinteressen der Arbeitnehmer im Sinne des § 1 Abs 1 DSG 2000 nicht verletzt werden. In diesem Zusammenhang fallen insbesondere § 8 Abs 1 Z 2 und 4 ins Auge. Gemäß Ziffer 2 werden die schutzwürdigen Geheimhaltungsinteressen

des Betroffenen dann nicht verletzt, wenn er der Verwendung seiner Daten zugestimmt hat.

Gemäß § 4 Z 14 DSG 2000 ist unter **Zustimmung** die gültige, insbesondere ohne Zwang abgegebene, Willenserklärung des Betroffenen, dass er in Kenntnis der konkreten Sachlage für den konkreten Fall in die Verwendung seiner Daten einwilligt, zu verstehen. Aus den EB zu § 4 Z 14 DSG 2000 geht hervor, dass diese Zustimmung nicht mehr unbedingt ausdrücklich oder schriftlich erfolgen muß. Dies läßt sich auch daraus schließen, dass § 9 Z 6 für die Verwendung sensibler Daten die ausdrückliche Zustimmung des Betroffenen verlangt, wogegen in § 8 Abs 1 Z 2 in Bezug auf nicht-sensible Daten nur von Zustimmung die Rede ist. Auch in der dem DSG 2000 zugrunde liegenden Datenschutzrichtlinie[38] findet sich diese Unterscheidung. So findet sich auch im Art 8 Abs 2 a der Datenschutzrichtlinie als ausnahmebegründend zum Verwendungsverbot sensibler Daten die **ausdrückliche** Einwilligung der betroffenen Person, wogegen im Art 7 a von einer „Einwilligung der betroffenen Person ohne jeden Zweifel" gesprochen wird. Die Qualität einer ausdrücklichen Einwilligung ist in diesem Fall höher anzusetzen, da auch eine konkludente Einwilligung „ohne jeden Zweifel" gegeben werden kann[39]. Auch den EB zu § 4 Z 14 DSG 2000 ist zu entnehmen, dass **Ausdrücklichkeit nur bei sensiblen Daten** notwendig ist.

Ziffer 4 gestattet die Verwendung nicht-sensibler Daten dann, wenn **überwiegende berechtigte Interessen** des Auftraggebers oder eines Dritten die Verwendung erfordern. In diesem Fall hätte also eine Interessenabwägung dahingehend zu erfolgen, ob das Interesse des Arbeitgebers an der Speicherung der Log-Files überwiegt, oder das schutzwürdige Geheimhaltungsinteresse des Arbeitnehmers in Bezug auf die über ihn vorliegenden nicht-sensiblen Daten. Dabei lägen wohl die besseren Argumente auf Seiten des Arbeitgebers. Dies schon auf Grund dessen, dass bei exzessiver Nutzung von Internet und e-Mail Kosten für ihn entstehen und vor allem Arbeitszeit des Arbeitnehmers verloren geht. Zudem hat der Arbeitgeber ein vitales Interesse daran, dass die Speichermöglichkeiten des Rechners für betriebliche Zwecke freigehalten werden, das Einschleppen von Viren verhindert wird, keine illegalen Inhalte auf seiner Festplatte abgelegt werden (zB kinderpornographische oder rassistische Inhalte) und durch das

[38] Richtlinie 95/46/EG

[39] Siehe auch *Hofer*, datenschutz@internet (2002) 48

Herunterladen und Einspielen von Programmen nicht in das Urheberrecht Dritter eingegriffen wird[40].

Wie aber bereits erwähnt, ist es für den Arbeitgeber vor Auswertung der Log-Files nicht erkennbar, ob es sich dabei um sensible oder um nicht-sensible Daten handelt. Es handelt sich um potentiell sensible Daten. Da aber bereits die Speicherung der Daten am Server eine Verarbeitung derselben im Sinne des DSG 2000 bedeutet, wäre beim Vorliegen von sensiblen Daten bereits mit der Speicherung ein Rechtsbruch erfolgt, sofern nicht einer der Ausnahmetatbestände des § 9 DSG 2000 vorliegt. Auf Grund des gesetzlichen Schutzzweckes ist in diesem Fall wohl, wie oben bereits ausgeführt, bei der **Protokollierung von Log-Files** stets vom Vorliegen **sensibler Daten** auszugehen. Demzufolge ist dem Arbeitgeber die Protokollierung nur dann erlaubt, wenn einer der Ausnahmetatbestände des § 9 DSG 2000 vorliegt.

b) Überprüfung nach § 9 DSG 2000

§ 9 DSG 2000 enthält eine taxative Liste, in der jene Ausnahmetatbestände aufgelistet sind, unter deren Voraussetzung schutzwürdige Geheimhaltungsinteressen der Betroffenen bei Verwendung sensibler Daten nicht verletzt werden.

Ziffer 1 greift nicht, da im Rahmen der Protokollierung kaum davon ausgegangen werden kann, dass der Arbeitnehmer seine Daten selbst öffentlich gemacht hat. In den meisten Fällen wird dem Arbeitnehmer wohl nicht einmal bewußt sein, dass der Web-Server des Arbeitgebers protokolliert auf welche Inhalte er im Internet zugegriffen hat. Doch auch wenn ihm dies zB aufgrund der Informationspflicht des Arbeitgebers bewußt ist, so ist durch sein Wissen von der Protokollierung noch kein öffentlich machen, wie es Z 1 verlangt gegeben. Das es sich bei den Log-Files um direkt personenbezogene Daten handeln kann wurde bereits erwähnt, weshalb auch Ziffer 2 nicht zur Anwendung kommt. Auch ein öffentliches Interesse im Sinne der Ziffer 3 oder ein Auftraggeber des öffentlichen Bereichs nach Ziffer 4 dürften bei einem privatwirtschaftlichen Unternehmen schwer zu finden sein. Ziffer 5 ist in unserem Fall ebenfalls nicht anwendbar. Lebensnotwendige Interessen des Arbeitgebers oder eines Anderen im Sinne der Ziffern 7 und 8 dürften im Normalfall auch nicht gegeben sein. Auch die Anwendbarkeit der Ziffer 9 ist kaum vorstellbar, da

[40] Siehe auch *Dellisch*, Private E-Mail- und Internet-Nutzung am Arbeitsplatz, ASoK 2001, 316

nicht erkennbar ist, wie die sensiblen personenbezogenen Arbeitnehmerdaten dem Arbeitgeber bei der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor einer Behörde helfen könnten. Auch die Ziffern 10, 12 und 13 greifen in Bezug auf die Protokollierung der Log-Files durch den Arbeitgeber nicht.

Als wirklich relevante Ausnahmetatbestände, welche die Speicherung sensibler Arbeitnehmerdaten auf dem Web-Server des Arbeitgebers ermöglichen, verbleiben die Ziffern 6 und 11.

Laut Ziffer 6 werden schutzwürdige Geheimhaltungsinteressen bei der Verwendung sensibler Daten dann nicht verletzt, wenn der Betroffene, also in unserem Fall der Arbeitnehmer, seine **Zustimmung** zur Verwendung der Daten **ausdrücklich** erteilt. Diese Zustimmung kann im Gegensatz zu der nach § 8 Abs 1 Z 1 DSG 2000 nicht konkludent erteilt werden, sondern hat ausdrücklich, ohne Zwang und in Kenntnis der konkreten Sachlage zu erfolgen[41]. Die Zustimmung kann vom Arbeitnehmer jederzeit widerrufen werden und bewirkt die Unzulässigkeit der weiteren Verwendung der Daten. Zu beachten ist allerdings hierbei, dass der Arbeitnehmer bei Abschluß des Arbeitsvertrages und während des aufrechten Dienstverhältnisses vielfach unter einem nicht zu unterschätzenden wirtschaftlichen Druck agiert und man nur beschränkt von einer freien Entscheidung des Arbeitnehmers ausgehen kann[42].

Ziffer 11 gestattet die Verwendung sensibler Daten, sofern die Verwendung erforderlich ist, um den Rechten und Pflichten des Auftraggebers auf dem Gebiet des Arbeits- oder Dienstrechts Rechnung zu tragen, und sie nach besonderen Rechtsvorschriften zulässig ist, wobei die dem Betriebsrat nach dem Arbeitsverfassungsgesetz zustehenden Befugnisse im Hinblick auf die Datenverwendung unberührt bleiben.

Mit dieser Ziffer 11 sollte Art 8 Abs 2 b der Richtlinie 95/46/EG umgesetzt werden, welcher die Verarbeitung sensibler personenbezogener Daten unter der Bedingung gestattet, dass die Verarbeitung erforderlich ist, um den Rechten und Pflichten des für die Verarbeitung Verantwortlichen auf dem Gebiet des Arbeitsrechts Rechnung zu tragen, sofern dies aufgrund von einzelstaatlichem Recht, das angemessene Garantien vorsieht, zulässig ist.

Auftraggeber (für die Verarbeitung Verantwortlicher im Sinne der Richtlinie) ist, wie bereits oben erwähnt, in diesem Zusammenhang der

41 *Hofer*, datenschutz@internet (2002) 86

42 *Löschnigg*, Verarbeiten und Übermitteln von Arbeitnehmerdaten in *Jahnel/Schramm/Staudegger,* Informatikrecht² (2002) 153

Arbeitgeber. Auch was unter den Rechten und Pflichten des Auftraggebers (des für die Verarbeitung Verantwortlichen) auf dem Gebiet des Arbeits- und Dienstrechts zu verstehen ist bereitet keine großen Probleme.

Schwierigkeiten bereitet dagegen der Begriff „…und nach besonderen Rechtsvorschriften zulässig ist." *Löschnigg* geht davon aus, dass der Hinweis auf die **besonderen Rechtsvorschriften** wohl so verstanden werden muß, dass darin die Verwendung der sensiblen Daten ausdrücklich erwähnt wird oder dass der in den Rechtsvorschriften verankerte Regelungszweck ausschließlich durch die Verwendung der sensiblen Daten erreicht werden kann[43]. In der österreichischen Rechtsordnung findet sich der Begriff der sensiblen Daten jedoch nur im DSG 2000, in der Datenschutzverordnung des BMGU, in der Gewerbeordnung 1994, im Sicherheitspolizeigesetz, in der Strafprozeßordnung 1975 und in der Übertragungsverordnung. Keine dieser Normen stellt jedoch eine Rechtsvorschrift dar, wie sie § 9 Z 11 DSG 2000 verlangt.

Gemäß § 96 Abs 1 Z 3 ArbVG bedarf die Einführung von Kontrollmaßnahmen und technischen Systemen zur Kontrolle der Arbeitnehmer durch den Betriebsinhaber der Zustimmung des Betriebsrates. Nach § 96a Abs 1 Z 1 ArbVG bedarf die Einführung von Systemen zur automationsunterstützten Ermittlung, Verarbeitung und Übermittlung von personenbezogenen Daten des Arbeitnehmers, die über die Ermittlung von allgemeinen Angaben zur Person und fachlichen Voraussetzungen hinausgehen ebenfalls der Zustimmung des Betriebsrates. Für Betriebe ohne Betriebsrat ist eine Zustimmung der jeweiligen Arbeitnehmer nach § 10 AVRAG notwendig.

Die Frage die sich nun stellt ist, ob eine in diesem Sinne geschlossene **Betriebsvereinbarung** bzw die Zustimmung nach § 10 AVRAG eine **besondere Rechtsvorschrift** im Sinne des § 9 Z 11 DSG darstellt. Die erläuternden Bemerkungen zum DSG 2000 geben keinerlei Aufschluß darüber, was unter den besonderen Rechtsvorschriften zu verstehen ist.

Bei einer Betriebsvereinbarung handelt es sich, wie bei einem Kollektivvertrag, um einen zweiseitigen Normenvertrag privatrechtlicher Natur[44], allerdings anders als beim Kollektivvertrag, um einen einseitig korporativen Normenvertrag. Die normativen Bestimmungen einer Betriebsvereinbarung sind wie jene eines

[43] *Löschnigg*, Verarbeiten und Übermitteln von Arbeitnehmerdaten in *Jahnel/Schramm/Staudegger,* Informatikrecht² (2002) 153

[44] *Tomandl*, Arbeitsrecht 1³ (1993) 196

Kollektivvertrages unmittelbar rechtsverbindlich, dh sie ziehen wie ein formelles Gesetz auch ohne Wissen und Willen der Normunterworfenen Rechtsfolgen nach sich. Die Ausstattung solcher Normen mit rechtsverbindlicher Wirkung sprengt allerdings das Vertragsmodell. Für die Subsumierbarkeit einer Betriebsvereinbarung könnte die herrschende Meinung sprechen, nach der die normativen Bestimmungen einer Betriebsvereinbarung ebenso wie jene des Kollektivvertrages wie Gesetze nach den Regeln der §§ 6 ff ABGB auszulegen sind[45]. Ob dies aber ausreicht um eine Betriebsvereinbarung als besondere Rechtsvorschrift, wie sie vom DSG 2000 verlangt wird, auszuzeichnen darf bezweifelt werden. Wäre die Betriebsvereinbarung jedoch nicht als solche qualifizierbar, so bliebe dem Arbeitgeber, der Log-Files und e-Mails seiner Mitarbeiter protokollieren will, nichts anderes übrig als sich von jedem seiner Arbeitnehmer die **Zustimmung zur Protokollierung** im Sinne des § 9 Z 6 DSG 2000 zu holen. Auch in Betracht darauf welche Auswirkungen dies auf viele größere Unternehmen haben könnte, wäre eine präzisere Formulierung des Gesetzestextes wünschenswert gewesen. Artikel 8 Abs 2 b der umzusetzenden Richtlinie spricht von der Zulässigkeit der Verarbeitung sensibler Daten, sofern die Verarbeitung erforderlich ist, um den Rechten und Pflichten des für die Verarbeitung Verantwortlichen auf dem Gebiet des Arbeitsrechtes Rechnung zu tragen, sofern dies aufgrund von einzelstaatlichem Recht, das angemessene Garantien vorsieht zulässig ist. Es ist also hier von einzelstaatlichem Recht, das angemessene Garantien vorsieht die Rede und nicht von besonderen Rechtsvorschriften.

Gemäß § 9 Z 11 DSG 2000 bleiben die dem Betriebsrat nach dem Arbeitsverfassungsgesetz zustehenden Befugnisse im Hinblick auf die Datenanwendung unberührt. Diese Bestimmung ist insofern zu eng formuliert, als wohl nicht nur die Mitwirkungsrechte nach dem ArbVG, sondern auch solche, die dem Betriebsrat bzw der Belegschaft nach anderen Bestimmungen zustehen, unberührt bleiben sollen. Die Regelung des § 9 Z 11 ist weiters wohl dahingehend zu verallgemeinern, dass das DSG 2000 nicht in die Betriebsverfassung eingreifen will[46].

Dass die Befugnisse des Betriebsrates im Hinblick auf die Datenanwendung unberührt bleiben trägt jedoch auch nicht zur Lösung der Frage ob eine Betriebsvereinbarung eine besondere

[45] OGH, Arb 9997/1981; aA *Tomandl*, Arbeitsrecht 1³ (1993) 196

[46] *Löschnigg*, Verarbeiten und Übermitteln von Arbeitnehmerdaten in *Jahnel/Schramm/Staudegger,* Informatikrecht² (2002) 155

Rechtsvorschrift im Sinne des DSG darstellt bei. Auch wenn das DSG 2000 nicht die Befugnisse des Betriebsrates berührt, so läßt dies dennoch nicht den Umkehrschluß zu, dass auch die Befugnisse des Betriebsrates, im konkreten Fall zum Abschluß einer Betriebsvereinbarung, nicht in das DSG 2000 eingreifen, also in diesem Fall das Verwenden sensibler Daten ermöglichen.

Dafür, dass es sich bei einer Betriebsvereinbarung um eine besondere Rechtsvorschrift im Sinne der Z 11 handelt, spricht, dass man auch in Deutschland davon ausgeht, dass es sich bei Dienst- und Betriebsvereinbarungen, sowie bei Tarifverträgen um Rechtsvorschriften gemäß § 4 Abs 1 BDSG handelt, in denen – bezogen auf das Dienst- oder Arbeitsverhältnis – die Erlaubnis und die Grenzen der Verarbeitung von Arbeitnehmerdaten bestimmt werden können[47].

Abschließend kann wohl gesagt werden, dass der Arbeitgeber die Log-Files seiner Arbeitnehmer auf jeden Fall mit deren Zustimmung nach Z 6 protokollieren darf. Ob der Abschluß einer Betriebsvereinbarung mit dem Betriebsrat den Ausnahmetatbestand der Z 11 erfüllt konnte hingegen im Rahmen dieser Arbeit nicht abschließend geklärt werden. Im Gegensatz zu *Drobesch/Grosinger*[48], welche in ihren Anmerkungen zu § 9 Z 11 davon ausgehen, dass unter einer „besonderen Rechtsvorschrift" eine gesetzliche Vorschrift, wie sie in § 9 Z 3 verlangt wird, zu verstehen ist und sich somit gegen die Subsumierbarkeit einer Betriebsvereinbarung aussprechen, bin ich der Meinung, dass in diesem Fall auch in § 9 Z 11 von gesetzlichen Vorschriften und nicht von besonderen Rechtsvorschriften die Rede wäre. Ist auch in den EB zum DSG 2000 nichts dazu zu finden, so bin ich dennoch der Meinung (und Hoffnung), dass hier nicht grundlos verschiedene Formulierungen gewählt wurden, sondern dass die „besonderen Rechtsvorschriften" wohl mehr umfassen sollen als die „gesetzlichen Vorschriften" in Z 3. Die unterschiedlichen Formulierungen in Z 3 und Z 11 sprechen daher mE eher für die Subsumierbarkeit von Betriebsvereinbarungen unter „besondere Rechtsvorschriften", wie sie § 9 Z 11 verlangt.

Die Zulässigkeit der Protokollierung durch den Arbeitgeber erfordert gemäß § 7 Abs 3 DSG 2000 noch zusätzlich, dass der Eingriff in das Grundrecht auf Datenschutz nur im **erforderlichen Ausmaß** und mit den gelindesten zur Verfügung stehenden Mitteln erfolgt. Dies

[47] *Schaar*, Datenschutz im Internet (2002) RZ 762
[48] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000) 146

bedeutet, dass der Arbeitgeber die Log-Files nur in dem Ausmaß, das für die Erreichung der Kontrollzwecke unbedingt erforderlich ist, protokollieren darf. Weiters müssen die Grundsätze des § 6 DSG 2000 eingehalten werden. Diese besagen unter anderem dass Daten nur **nach Treu und Glauben** und auf rechtmäßige Weise verwendet werden dürfen. Dafür ist es nach den Erläuternden Bemerkungen zum § 6 Abs 1 Z 1 vor allem wichtig, dass die Bestimmungen des 4. Abschnitts des DSG 2000 eingehalten werden und der Betroffene über die Umstände des Datengebrauchs und das Bestehen sowie die Durchsetzbarkeit seiner Rechte nicht irregeführt oder im Unklaren gelassen wird.

2. Recht des Arbeitgebers auf Kontrolle

In Bezug auf die Kontrollrechte des Arbeitgebers ist es möglich sich kurz zu fassen, da eine Kontrolle der Log-Files ebenso eine **Verarbeitung von Daten** darstellt, wie die Speicherung oder die Löschung derselben. Das heißt die Kontrolle der Daten ist unter den selben Voraussetzungen zulässig.

Was jedoch in diesem Zusammenhang noch zu besprechen bleibt sind die Auswirkungen des Verbotes, bzw der Erlaubnis der Privatnutzung durch den Arbeitgeber auf sein Recht zur Speicherung bzw Kontrolle der Log-Files.

So macht es in Bezug auf die Notwendigkeit der Protokollierung von Log-Files im Gegensatz zur Protokollierung von e-Mails keinerlei Unterschied, ob eine Vereinbarung über **eingeschränkte Privatnutzung**, ein **Nutzungsverbot**, die **Erlaubnis der umfassenden Privatnutzung** oder **keinerlei Vereinbarung** vorliegt. Sollte eine Vereinbarung über eingeschränkte Privatnutzung vorliegen (im Arbeitsvertrag oder im Rahmen einer Betriebsvereinbarung), so ist eine umfassende Protokollierung der Log-Files zur Überwachung der Einhaltung dieser Vereinbarung notwendig. Beim Fehlen einer Vereinbarung ist die Privatnutzung im „ortsüblichen" Ausmaß gestattet und zwar abhängig von den konkreten Umständen des Einzelfalls während oder außerhalb der Arbeitszeit[49]. Zur Kontrolle ob dieses Ausmaß eingehalten wird, ebenso wie zur Kontrolle der Einhaltung eines Nutzungsverbotes ist ebenfalls eine **umfassende Protokollierung** notwendig. Im Gegensatz zur e-Mail ist aber bei Log-Files selbst dann, wenn keinerlei Einschränkung der Privatnutzung durch den Arbeitgeber

[49] *Laimer/Mayr*, Rechtsprobleme bei der Internetnutzung am Arbeitsplatz, ecolex 2003, 113 (114); ebenso *Posch*, die e-Mail Nutzung aus arbeitsrechtlicher Sicht, in *it-law.at (Hrsg*), e-Mail, elektronische Post im Recht (2003) 75

erfolgt, eine umfassende Protokollierung, wenn auch nicht zu Kontrollzwecken im Hinblick auf die Arbeitnehmer, notwendig. Die Log-Files stellen nämlich für den jeweiligen Netzwerkadministrator ein unerläßliches Instrument zur Fehlerbehebung dar. Nur mit Hilfe der Log-Files lassen sich oft die Gründe für Verbindungsfehler finden und Fehlkonfigurationen beheben. Sie stellen somit ein unerläßliches Instrument für die **Wartung und Optimierung des Firmennetzwerkes** dar. Auch in diesem Fall ist eine umfassende Protokollierung der Log-Files notwendig. Eine eingeschränkte nicht personenbezogene Protokollierung wird wohl in diesem Fall nicht möglich sein, da es für en Administrator auch notwendig ist zu erkennen, von welchem Rechner aus der Zugriff auf das Netzwerk bzw das Internet nicht oder nur fehlerhaft funktioniert und von welchem Rechner im Netzwerk die Probleme ausgehen.

An dieser Stelle ist noch darauf hinzuweisen, dass der Arbeitgeber gemäß § 14 Abs 2 Z 7 DSG 2000 auch zur **Protokollierung seiner Kontrollzugriffe** auf die Log-Files verpflichtet ist, damit seine Abfragen im Hinblick auf ihre Zulässigkeit nachvollzogen werden können. Sollte er dieser Pflicht nicht nachkommen, so ist gemäß § 52 Abs 2 Z 4 DSG 2000 die Verhängung einer Verwaltungsstrafe bis zur Höhe von 9445 Euro möglich.

3. Informationspflichten des Arbeitgebers

Gemäß § 24 Abs 1 DSG 2000 hat der Auftraggeber einer Datenanwendung aus Anlaß der Ermittlung von Daten den Betroffenen in geeigneter Weise über den Zweck der Datenanwendung für die Daten ermittelt werden und über Namen und Adresse des Auftraggebers zu informieren, sofern diese Informationen dem Betroffenen nach Umständen des Falles nicht bereits vorliegen. Das Bekanntgeben von Name und Adresse des Auftraggebers erübrigt sich in diesem Zusammenhang. Die Arbeitnehmer sind demzufolge bei ihrem Arbeitsantritt davon zu informieren, dass Log-Files in dem jeweiligen Unternehmen protokolliert werden. Die Ausnahmetatbestände des § 24 Abs 3 DSG 2000 kommen im Fall der Protokollierung von Log-Files am Arbeitsplatz nicht in Betracht. Auch bei **Nichterfüllung der Informationspflichten** ist gemäß § 52 Abs 2 Z 3 die Verhängung einer Verwaltungsstrafe bis zur Höhe von 9445 Euro möglich.

4. Pflicht des Arbeitgebers zur Löschung

Gemäß § 6 Abs 1 Z 5 DSG 2000 dürfen die Log-Files nur solange in ihrer personenbezogenen Form aufbewahrt bleiben, als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist. Die Log-Files sind also nach **Erreichen des Zweckes**, für den sie ermittelt wurden, vom Arbeitgeber sofort zu **löschen**. In diesem Zusammenhang ist aber noch zu sagen, dass auch das Löschen von Daten gemäß § 4 Z 9 DSG 2000 eine Verarbeitung von Daten darstellt. Demzufolge hat hier die Überprüfung der Zulässigkeit der Löschung der Log-Files nach denselben Maßstäben wie die Prüfung der Zulässigkeit der Speicherung zu erfolgen. Es darf also, wenn man dem Gesetzeswortlaut folgt, nur mit Zustimmung des Arbeitnehmers oder des Betriebsrates (Abschluß einer dementsprechenden Betriebsvereinbarung) gelöscht werden. Dies könnte theoretisch zu Widersprüchlichkeiten führen, wenn der Arbeitgeber einerseits gemäß § 6 Abs 1 Z 5 zur Löschung der Daten verpflichtet ist, andererseits aber die Arbeitnehmer, bzw der Betriebsrat ihre Zustimmung zur Löschung verweigern.

C. Zur Abwicklung des e-Mail Verkehrs

Dass es sich bei e-Mails genau wie bei Log-Files um direkt personenbezogene Daten handeln kann, konnte bereits gezeigt werden. Schwieriger erweist sich jedoch im Zusammenhang mit e-Mails die Beantwortung der Frage wer denn Auftraggeber im Sinne des DSG 2000 ist.

1. Wer ist Auftraggeber, wer Betroffener?

Wie bei den Log-Files, so stellt sich auch hier am Anfang die Frage, wer Auftraggeber im Sinne des DSG 2000 ist. Gemäß § 4 Z 4 DSG 2000 ist Auftraggeber eine natürliche oder juristische Person, eine Personengemeinschaft oder Organ einer Gebietskörperschaft wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen hat, Daten für einen bestimmten Zweck zu verarbeiten, und zwar unabhängig davon, ob sie die Verarbeitung selbst durchführt oder hiezu einen anderen heranzieht. Die Definition des Auftraggebers im DSG 2000 ist jedoch für den Fall der Protokollierung von e-Mails höchst unglücklich formuliert, was im Folgenden noch zu zeigen sein wird. Es stellt sich beim Versenden von e-Mails durch den Arbeitnehmer über den Server des Arbeitgebers nämlich die Frage wer von beiden in

diesem Zusammenhang der Auftraggeber im Sinne des DSG 2000 ist. Der Arbeitnehmer, der die Nachricht verfaßt hat und per Mausklick versendet oder der Arbeitgeber über dessen Server, auf dem die entsprechenden Daten protokolliert werden, die Nachricht schließlich versendet wird?

Beim Versenden von e-Mails hat der Arbeitgeber einerseits gar keine Möglichkeit die Verarbeitung von Daten zu verhindern, selbst wenn nicht protokolliert wird, da in diesem Fall aufgrund der technischen Gegebenheiten dennoch eine kurze **Zwischenspeicherung** der e-Mails auf dem SMTP-Server erfolgt, worunter gemäß 4 Z 9 DSG 2000 Verarbeiten von Daten zu verstehen ist. Er hat jedoch die Möglichkeit die Protokollierung zu unterbinden, wodurch der Datenfluß nicht mehr zuordenbar ist.

Im Erwägungsgrund 47 zur Datenschutzrichtlinie[50] findet man eine Erklärung dahingehend, dass bei einer über Telekommunikations-dienste oder durch elektronische Post übermittelten Nachricht, die personenbezogene Daten enthält, die Person, von der die Nachricht stammt, als Verantwortlicher für die Verarbeitung der in der Nachricht enthaltenen personenbezogenen Daten anzusehen ist. Die Person, die den Dienst anbietet ist dagegen als verantwortlich für die Verarbeitung der personenbezogenen Daten, die zusätzlich für den Vertrieb des Dienstes erforderlich sind[51], anzusehen. Auf unseren Sachverhalt bezogen wäre dies dahingehend zu verstehen, dass der Arbeitnehmer, der die e-Mail abschickt für den Inhalt der e-Mail verantwortlich ist, der Arbeitgeber, der die Infrastruktur zur Verfügung stellt, hingegen für die Vermittlungsdaten.

Dem Folgendend schrieb auch *Jahnel* dass beim Versenden elektronischer Post der Versender Auftraggeber ist und nicht der Provider. Dieser sei nur für die Daten, die neben der Nachricht zum Betrieb des Dienstes erforderlich sind Auftraggeber[52]. In einer neueren Publikation geht *Jahnel* jedoch davon aus, dass der Arbeitgeber Auftraggeber im Sinne des DSG 2000 ist[53]. Er argumentiert dies dahingehend, dass beim Versenden von privaten e-Mails der Arbeitnehmer die Entscheidung trifft, Daten für einen bestimmten Zweck zu verarbeiten, und sich für die Verarbeitung des Arbeitgebers

50 Richtlinie 95/46/EG

51 Siehe auch *Hofer*, datenschutz@internet (2002) 45

52 *Jahnel,* Datenschutzrecht in *Jahnel/Schramm/Staudegger*, Informatikrecht² (2002) 247

53 *Jahnel*, Das Versenden von e-Mails aus datenschutzrechtlicher Sicht, in *it-law.at (Hrsg*), e-Mail, elektronische Post im Recht (2003) 89

bedient, der dadurch zum (zivilrechtlichen) Auftragnehmer im Sinne des § 4 Z 4 DSG 2000 wird. Der (zivilrechtliche) Auftragnehmer wird für den Fall, dass ihm die Verarbeitung der Daten untersagt wird ebenso, wie in den Fällen in denen er die Vornahme der Datenverarbeitung auf Grund von **Rechtsvorschriften**, Standes- oder Verhaltensregeln gemäß § 6 Abs 4 DSG 2000 **eigenverantwortlich** zu treffen hat zum (datenschutzrechtlichen) Auftraggeber. Dem folgend geht *Jahnel* davon aus, dass auf den Arbeitgeber zwar nicht die datenschutzrechtlichen Bestimmungen, wohl aber die sonstigen Bestimmungen des TKG anwendbar sind, da er zwar nicht Betreiber im Sinne des § 87 Abs 3 Z1 TKG ist, aber dennoch Anbieter eines gewerblichen Telekommunikationsdienstes. Das TKG kennt neben § 3 Z 1 leg cit neben dem speziellen Begriff des „Betreibers" in § 87 Abs 3 Z1 TKG auch den allgemeinen Begriff des „Betreibens" in § 3 Z 1 leg cit. Demnach bedeutet „Betreiben" das Ausüben der rechtlichen und tatsächlichen Kontrolle über die Gesamtheit der Funktionen, die zur Erbringung des jeweiligen Telekommunikationsdienstes notwendig sind. Die rechtliche und tatsächliche Kontrolle des Arbeitgebers bietet somit laut *Jahnel* zumindest gute Argumente für eine Eigenverantwortung des Arbeitgebers iSd § 4 Z 4 DSG 2000, aus der seine Eigenschaft als datenschutzrechtlicher Auftraggeber folgt. Weiters spricht dafür, dass der Arbeitnehmer die Betroffenenrechte – wie insb das Recht auf Auskunft – nur beim Arbeitgeber geltend machen kann.

Diese Argumentation kann ohne Zweifel gefolgt werden. Sie führt in Bezug auf das DSG 2000 zu einem zufriedenstellenden Ergebnis, da sich bei einem anderen Ergebnis bereits die Ausübung der Betroffenenrechte durch die Arbeitnehmer als äußerst schwierig erweisen würde.

Folgt man dieser Argumentation, wonach der Arbeitgeber in Bezug auf eine von seinem Arbeitnehmer versendete e-Mail Auftraggeber und der Arbeitnehmer Betroffener ist, so ergibt sich jedoch noch das Problem, dass dies mit dem Erwägungsgrund 47 zur Datenschutzrichtlinie nicht vollständig übereinstimmt, wonach in unserem Fall der Arbeitnehmer in Bezug auf den Inhalt der e-Mail, und der Arbeitgeber in Bezug auf die Vermittlungsdaten der e-Mail für die Verarbeitung verantwortlich ist.

In Bezug auf die Vermittlungsdaten, also die Protokollierung der „Header-Daten" ergibt sich dabei kein Problem, da in Bezug auf diese der Arbeitgeber als Auftraggeber ebenso nach dem Erwägungsgrund 47 der Richtlinie, als auch nach der Argumentation von *Jahnel* anzusehen

ist. Der Arbeitnehmer ist in diesem Fall Betroffener. In Bezug auf den Inhalt der e-Mail aber stehen wir vor dem Problem, dass es dem Erwägungsgrund 47 der Richtlinie widerspricht den Arbeitgeber als Auftraggeber anzusehen, der Arbeitnehmer als Auftraggeber gemäß § 4 Z 3 DSG 2000 aber nicht gleichzeitig Betroffener sein kann und somit einer Protokollierung der Inhalte seiner e-Mails durch den Arbeitgeber schutzlos ausgeliefert wäre.

Es stellt sich also die Frage, ob das DSG 2000 richtlinienwidrig umgesetzt wurde und ob in der Folge eine **direkte Anwendbarkeit** der Richtlinie gegeben ist. Da das DSG 2000 in diesem Fall aber nicht den Richtlinienvorschriften selbst widerspricht, sondern nur einem Erwägungsgrund, der zur Auslegung der Richtlinie dient, kann wohl von einer richtlinienkonformen Umsetzung ausgegangen werden. Selbst wenn man von einer rechtswidrigen Umsetzung der Richtlinie ausgeht, so ist dennoch die direkte Anwendbarkeit der Richtlinie nicht gegeben, da nur eine **Richtlinienvorschrift**, die inhaltlich unbedingt und hinreichend genau ist unmittelbar in Anspruch genommen werden kann.[54] Hier handelt es sich jedoch nicht um eine Richtlinienvorschrift, der das DSG 2000 widerspricht, sondern nur um einen Erwägungsgrund, der zur Auslegung der Richtlinienvorschriften dient. Eine direkte Anwendbarkeit der Richtlinie ist deshalb wohl nicht gegeben, da es an der hinreichenden Bestimmtheit der Richtlinienvorschriften selbst fehlt..

Deshalb ist für den Fall der Protokollierung von Arbeitnehmer-e-Mails durch den Arbeitgeber nach dem DSG 2000 entgegen Erwägungsgrund 47 der Richtlinie davon auszugehen, dass der Arbeitgeber sowohl in Bezug auf den Inhalt der e-Mail, als auch in Bezug auf die Vermittlungsdaten als Auftraggeber anzusehen ist.

2. Zulässigkeit der Speicherung/Übermittlung der e-Mails

Wie bereits gezeigt handelt es sich bei e-Mails um potentiell sensible Daten, die unter bestimmten Voraussetzungen einen Personenbezug aufweisen können.

Die Datenverwendung besteht bei e-Mails zunächst im Speichern der Nachricht auf dem Mail-Server, worunter gemäß § 4 Z 9 eine **Verarbeitung** von Daten zu verstehen ist und im Weiterleiten an den Zielserver, worunter gemäß § 4 Z 12 eine **Übermittlung** von Daten zu verstehen ist (ausgenommen der Fall, wo der Arbeitnehmer vom Arbeitsplatz aus eine e-Mail an sich selbst versendet).

[54] *Fischer/Köck/Karollus*, Europarecht[4] (2002) 630, Rz 1273

Das Speichern der e-Mails auf dem SMTP-Server ist dem Arbeitgeber nur bei Bestehen eines der Ausnahmetatbestände des § 9 DSG 2000 erlaubt. Auch hier kommen, wie bereits im Zusammenhang mit der Protokollierung von Log-Files erwähnt, die Ziffern 6 und 11 in Betracht. Die rechtliche Befugnis des Arbeitgebers zur Speicherung der Daten, wie sie § 7 Abs 1 DSG 2000 verlangt, ergibt sich auch hier wiederum aus seinem Eigentum am Server. Zudem dürfen die Daten gemäß § 6 Abs 1 Z 1 DSG 2000 nur nach Treu und Glauben und auf rechtmäßige Weise verwendet werden und hat der Eingriff in das Grundrecht auf Datenschutz nur im erforderlichen Ausmaß und mit den gelindesten zur Verfügung stehenden Mitteln zu erfolgen.

Im Verhältnis zwischen dem Arbeitgeber und dem ISP des Empfängers liegt eine Übermittlung von Daten vor, die nach § 7 Abs 2 DSG 2000 zu beurteilen ist. Die Daten stammen dabei, wie bereits oben festgestellt, aus einer zulässigen Datenanwendung gemäß § 7 Abs 1 DSG 2000 und auch die rechtliche Befugnis des Empfängers, wie sie von § 7 Abs 2 Z 2 leg cit verlangt wird steht außer Zweifel, da es ja der Wunsch des Absenders der e-Mail war, dass der Empfänger diese erhält. In Bezug auf die Frage ob **schutzwürdige Geheimhaltungs-interessen des Arbeitnehmers** durch die Übermittlung verletzt werden ist wiederum zu prüfen, ob entweder die ausdrückliche Zustimmung des Arbeitnehmers gemäß § 9 Z 6, oder eine besondere Rechtsvorschrift im Sinne des § 9 Z 11 gegeben ist. Liegen beide nicht vor, so sind schutzwürdige Geheimhaltungsinteressen des Arbeitnehmers verletzt.

Erfolgt eine Übermittlung an einen Zielserver im Ausland, so liegt eine Datenübermittlung ins Ausland vor. Diese Übermittlung ist genehmigungsfrei, da entweder die Übermittlung in einen Mitgliedsstaat der europäischen Union, oder in einen Drittstaat mit angemessenem Datenschutz gemäß DSAV[55] erfolgt oder ansonsten davon ausgegangen werden kann, dass der Betroffene – durch das Versenden der e-Mail – ohne jeden Zweifel die Zustimmung zur Übermittlung seiner Daten ins Ausland gemäß § 12 Abs 3 Z 5 gegeben hat.

[55] Verordnung des Bundeskanzlers über den angemessenen Datenschutz in Drittstaaten (Datenschutzangemessenheits-Verordnung - DSAV), BGBl. II Nr. 521/1999

3. Kontrolle der e-Mails durch den Arbeitgeber

Bei einer Kontrolle der e-Mails am Server durch den Arbeitgeber handelt es sich ebenso wie bei der Kontrolle von Log-Files um ein Verarbeiten von Daten. Es sind also dieselben datenschutzrechtlichen Bestimmungen wie beim Speichern der Daten zu beachten. Im Gegensatz zur Kontrolle von Log-Files kommt hier jedoch der Unterscheidung zwischen dem Vorliegen einer **Vereinbarung über die eingeschränkte Privatnutzung**, dem **Fehlen einer Vereinbarung**, einem **Nutzungsverbot** oder der **umfassenden Erlaubnis der Privatnutzung** eine entscheidende Bedeutung zu. So liegt sowohl beim Vorliegen eines Nutzungsverbotes, als auch bei einer Vereinbarung über die eingeschränkte Privatnutzung ein Interesse des Arbeitgeber an der Kontrolle der Einhaltung des Verbotes bzw der Vereinbarung vor. Auch im Fall einer fehlenden Vereinbarung liegt ein Interesse des Arbeitgebers vor, zu kontrollieren, ob das ortsübliche Ausmaß der Nutzung nicht überschritten wird. In allen drei Fällen ist wohl zu Kontrollzwecken eine umfassende Protokollierung des e-Mail-Verkehrs notwendig.

Für den Fall, dass die umfassende Privatnutzung erlaubt ist und keinerlei Einschränkung von Seiten des Arbeitgebers vorliegt, so entfällt auch die Notwendigkeit der Protokollierung, der beim e-Mail-Verkehr anfallenden Daten. Die Daten sind daher in diesem Fall sofort nach Übertragung vom Mail-Server zu löschen.[56]

Tätigt der Arbeitgeber Kontrollzugriffe auf die Protokolldateien, so sind genau wie bei den Log-Files auch diese Zugriffe nach § 14 Abs 2 Z 7 zu protokollieren

4. Informationspflicht des Arbeitgebers

Hier sei auf die Informationspflicht des Arbeitgebers im Zusammenhang mit der Protokollierung von Log-Files im Kapitel III.B.3 verwiesen.

5. Pflicht des Arbeitgebers zur Löschung

Auch in Bezug auf die e-Mails dürfen vom Arbeitgeber gemäß § 6 Abs 1 Z 5 DSG 2000 sowohl die Vermittlungsdaten, als auch der Inhalt, nur solange aufbewahrt werden, als dies für die Erreichung der

[56] siehe auch *Jahnel*, Das Versenden von e-Mails aus datenschutzrechtlicher Sicht, in *it-law.at (Hrsg)*, e-Mail, elektronische Post im Recht (2003), 89 (99)

Zwecke, für die sie ermittelt wurden, erforderlich ist. Danach sind Sie zu löschen. Dies bedeutet, dass, wie bereits oben erwähnt, beim Vorliegen keinerlei Einschränkung der Privatnutzung die Daten sofort zu löschen sind, ansonsten hingegen nach Erreichen des jeweiligen Kontrollzweckes.

D. Die Betroffenenrechte der Arbeitnehmer

1. Das Auskunftsrecht des Arbeitnehmers

Der Auftraggeber, also in unserem Fall der Arbeitgeber hat dem Betroffenen nach § 26 Abs 1 DSG 2000 Auskunft über die zu seiner Person verarbeiteten Daten zu geben, wenn der Betroffene dies schriftlich verlangt und seine Identität in geeigneter Form nachweist. Mit Zustimmung des Auftraggebers kann das Auskunftsbegehren auch mündlich gestellt werden. Der Nachweis der Identität stellt in unserem Fall kein Problem dar. Die Auskunft hat die verarbeiteten Daten, die verfügbaren Informationen über ihre Herkunft, allfällige Empfänger oder Empfängerkreise von Übermittlungen, den Zweck der Datenverwendung, sowie die Rechtsgrundlage hiefür in allgemein verständlicher Form zu enthalten. Ein **Auskunftsverweigerungsrecht** gemäß § 26 Abs 2 steht dem Arbeitgeber wohl im Normalfall nicht zu. Die Auskunft ist binnen 8 Wochen nach Einlangen des Begehrens zu erteilen. Sie ist unentgeltlich, sofern sie eine aktuelle Datenanwendung betrifft und der Betroffene im laufenden Jahr noch kein Auskunftsersuchen an den Auftraggeber zum selben Aufgabengebiet gestellt hat. Ansonsten kann vom Auftraggeber ein pauschalierter Kostenersatz in der Höhe von € 18,89 verlangt werden. Gemäß § 26 Abs 10 kann der Betroffene sein Auskunftsbegehren im Falle der auf Grund von Rechtsvorschriften, Standes- oder Verhaltensregeln gemäß § 6 Abs 4 eigenverantwortlichen Entscheidung über die Durchführung einer Datenanwendung durch einen Auftragnehmer gemäß § 4 Z 4, dritter Satz, zunächst auch an denjenigen richten, der die Herstellung des Werkes aufgetragen hat. Folgt man im Bereich des Versendens von e-Mails am Arbeitsplatz der Argumentation *Jahnels*, wonach der Arbeitnehmer Auftraggeber und der Arbeitgeber Auftragnehmer idS ist, so ist diese Bestimmung obsolet, da sie in diesem Fall dem Arbeitnehmer ermöglicht an sich selbst ein Auskunftsbegehren zu stellen.

2. Das Recht auf Richtigstellung oder Löschung

Gemäß § 27 Abs 1 hat der Auftraggeber unrichtige oder entgegen den Bestimmungen dieses Bundesgesetzes verarbeitete Daten richtigzustellen oder zu löschen, und zwar aus eigenem, sobald ihm die Unrichtigkeit von Daten oder die Unzulässigkeit ihrer Verarbeitung bekannt geworden ist, oder auf begründeten Antrag des Betroffenen. Auf Grund des automatisierten Ablaufs der Protokollierung von Log-Files und e-Mails ist das Entstehen unrichtiger Daten wohl nur durch Manipulation oder durch einen Fehler der Maschine möglich. **Entgegen den Bestimmungen des DSG 2000** erfolgte oder **unrichtige Protokollierungen** sind demnach vom Arbeitgeber zu **löschen**. Der Beweis der Richtigkeit der Daten obliegt dem Auftrageber, also dem Arbeitgeber. Innerhalb von acht Wochen nach Einlangung eines entsprechenden Antrages hat die Richtigstellung oder Löschung zu erfolgen oder ist dem Betroffenen eine Mitteilung zu machen, warum die verlangte Löschung oder Richtigstellung nicht vorgenommen wird.

3. Das Widerspruchsrecht

Gemäß § 28 Abs 1 DSG 2000 hat jeder Betroffene, sofern die Verwendung von Daten nicht gesetzlich vorgesehen ist, das Recht gegen die Verwendung seiner Daten wegen der Verletzung überwiegender schutzwürdiger Geheimhaltungsinteressen, die sich aus seiner besonderen Situation ergeben, beim Auftraggeber der Datenanwendung Widerspruch zu erheben. Beim Vorliegen dieser Voraussetzungen hat der Auftraggeber die Daten des Betroffenen **binnen 8 Wochen** aus seiner Datenanwendung zu löschen und allfällige Übermittlungen zu unterlassen. Liegt also keine Zustimmung des Arbeitnehmers gemäß § 9 Z 6 DSG 2000 oder eine besondere Rechtsvorschrift gemäß § 9 Z 11 leg cit vor, so kann der Arbeitnehmer Widerspruch gegen die Protokollierung der Log-Files und e-Mails erheben.

IV. Zusammenfassung

Abschließend lassen sich die Ergebnisse dieser Arbeit dahingehend zusammenfassen, dass sowohl durch die Protokollierung von e-Mails, als auch durch die Protokollierung von Log-Files personenbezogene Daten entstehen können. Der Arbeitgeber der Log-Files und e-Mails auf dem unternehmenseigenen Server protokolliert unterliegt dabei nicht den datenschutzrechtlichen Bestimmungen des TKG. Bei Log-Files und e-Mails handelt es sich um potentiell sensible Daten, welche demgemäß nur bei Vorliegen eines Ausnahmetatbestandes gemäß § 9 DSG 2000 protokolliert werden dürfen. Auch konnte die Problematik der Begriffsdefinitionen „Auftraggeber“ und „Betroffener“ im DSG 2000 aufgezeigt werden[57]. Weiters wurden die unterschiedlichen Auswirkungen beim Vorliegen von keinerlei Nutzungsbeschränkungen auf die Protokollierung von e-Mails und auf die Protokollierung von Log-Files hingewiesen.

[57] vgl die Kritik an dieser Regelung bei *Jahnel*, Datenschutzrecht in *Jahnel/Schramm/Staudegger* (Hrsg), Informatikrecht² (2002) 241 (247); *Dohr/Pollierer/Weiß*, DSG² (2002) § 4 Anm 5

Abkürzungsverzeichnis

aA	=	anderer Ansicht
aaO	=	am angegebenen Ort
AB	=	Ausschussbericht
ABGB	=	Allgemeines bürgerliches Gesetzbuch, JGS 946/1811
abl	=	ablehnend
ABl	=	Amtsblatt der Europäischen Gemeinschaften
AGB	=	Allgemeine Geschäftsbedingungen
arg	=	argumento
BG	=	Bundesgesetz
BGBl	=	Bundesgesetzblatt
BlgNR	=	Beilage(-n) zu den stenographischen Protokollen des Nationalrates
BR	=	Bundesrat
bspw	=	beispielweise
bzw	=	beziehungsweise
Datenschutz-RL	=	Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl L 281 vom 23. 11. 1995, 31
Datenschutz-RL für elektronische Kommunikation	=	Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl L 201 vom 31.7.2002, 37
dh	=	das heißt
div	=	diverse
DSG 2000	=	Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000), BGBl I 165/1999
DSG 1978	=	Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz), BGBl 565/1978
DSK	=	Datenschutzkommission
E	=	Entscheidung
EB	=	Erläuternde Bemerkungen
EMRK	=	Europäische Menschenrechtskonvention, BGBl 210/210
Entw	=	Entwurf
ErwGr	=	Erwägungsgrund
et alt	=	und andere
etc	=	et cetera
EuGH	=	Gerichtshof der Europäischen Gemeinschaften
EWR	=	Europäischer Wirtschaftsraum

f, ff	=	folgende, fortfolgende
FAQ	=	frequently asked questions
FN	=	Fußnote
G	=	Gesetz
gem	=	gemäß
GewO	=	Gewerbeordnung 1994, BGBl 194/1994
GP	=	Gesetzgebungsperiode
Hrsg	=	Herausgeber
iaR	=	in aller Regel
idF	=	in der Fassung
idR	=	in der Regel
idS	=	in diesem Sinne
ieS	=	im engeren Sinn
insbes	=	insbesondere
IP	=	Internet Protokoll
iS	=	im Sinne
iSd	=	im Sinne des, - der
ISP	=	Internet Service Provider
iSv	=	im Sinne von
iVm	=	in Verbindung mit
iwS	=	im weiteren Sinn
JA	=	Justizausschuss
Jud	=	Judikatur
leg cit	=	legis citatae (der zitierten Vorschrift)
Lfg	=	Lieferung
Lit	=	Literatur
lit	=	litera
maW	=	mit anderen Worten
mE	=	meines Erachtens
mA	=	meiner Ansicht
mwH	=	mit weiteren Hinweisen
mwN	=	mit weiteren Nachweisen
Nov	=	Novelle
NR	=	Nationalrat
oa	=	oder ähnliches
OGH	=	Oberster Gerichtshof
RdA	=	Österreichisches Recht der Arbeit
RdW	=	Österreichisches Recht der Wirtschaft
RL	=	Richtlinie der Europäischen Gemeinschaften
RN	=	Randnummer
Rs	=	Rechtsache
Rsp	=	Rechtsprechung
Rz	=	Randzahl
RV	=	Regierungsvorlage
S	=	Satz, Seite
Slg	=	Sammlung
SMS	=	Short Message Service
sog	=	sogenannt, -e, -er, -es

SPG	=	Sicherheitspolizeigesetz, BGBl 566/1991
StF	=	Stammfassung
StGB	=	Strafgesetzbuch, BGBl 1974/60
StGG	=	Staatsgrundgesetz, RGBl 142/1867
StPO	=	Strafprozessordnung 1975, BGBl 631/1975
StProt	=	stenographische(s) Protokoll(e)
stRsp	=	ständige Rechtsprechung
SZ	=	Entscheidungen des österreichischen Obersten Gerichtshofes in Zivilsachen
TKG	=	Telekommunikationsgesetz
TKG 1997	=	Telekommunikationsgesetz, BGBl 100/1997
TKG 2003	=	Telekommunikationsgesetz 2003, BGBl 70/2003
ua	=	und andere
udgl	=	und dergleichen
URL	=	Uniform Resource Locator
uU	=	unter Umständen
va	=	vor allem
vgl	=	vergleiche
VO	=	Verordnung
VfGH	=	Verfassungsgerichtshof
VwGH	=	Verwaltungsgerichtshof
wbl	=	Wirtschaftsrechtliche Blätter
Z	=	Ziffer
zB	=	zum Beispiel
ZfRV	=	Zeitschrift für Rechtsvergleichung
zT	=	zum Teil

Literaturverzeichnis

Offline:

Dohr/Pollierer/Weiß, Datenschutzgesetz² (2002)
Drobesch/Grosinger, Das neue österreichische Datenschutzgesetz (2000)
Fischer/Köck/Karollus, Europarecht⁴ (2002)
Hobert, Datenschutz und Datensicherheit im Internet² (1998)
Hofer, datenschutz@internet (2002)
Parschalk/Zuser/Otto, Telekommunikationsrecht (2002)
Schaar, Datenschutz im Internet (2002)
Simitis/Dammann, BDSG-Kommentar⁴ (1992)
Tomandl, Arbeitsrecht 1³ (1993)

Brodil, Nutzung und Kontrolle von neuen Medien am Arbeitsplatz, ecolex 2001, 853
Damjanovic, Schwerpunkte des Entwurfs für ein neues Kommunikationsgesetz, wbl 2003, 101
Dellisch, Private E-Mail- und Internet-Nutzung am Arbeitsplatz, ASoK 2001, 316
Funk/Kreijci/Schwarz, Zur Registrierung von Ferngesprächen durch den Arbeitgeber am Beispiel der Universität Graz, RdA 1984, 285
Gruber, Überwachung der dienstlichen Verwendung von Internet und E-Mail, in: *Öst. Juristenkommission (Hrsg),* Grundrechte in der Informationsgesellschaft (2001) 167
Jahnel, Datenschutzrecht in *Jahnel/Schramm/Staudegger* Informatikrecht² (2002) 240
Jahnel, Cookies, Web-Logs, LBS und die Datenschutzrichtlinie für elektronische Kommunikation, wbl 2003, 108
Jahnel, Das Versenden von e-Mails aus datenschutzrechtlicher Sicht, in *it-law.at (Hrsg*), e-Mail, elektronische Post im Recht (2003) 89
Lachmaier, Die neue Datenschutzrichtlinie für elektronische Kommunikation, RdW 2003/3
Laimer/Mayr, Rechtsprobleme bei der Internetnutzung am Arbeitsplatz, ecolex 2003, 113
Löschnigg, Verarbeiten und Übermitteln von Arbeitnehmerdaten in *Jahnel/Schramm/Staudegger* Informatikrecht² (2002) 147
Obereder, E-Mail und Internetnutzung aus arbeitsrechtlicher Sicht, RdA 2001, 75
Otto/Parschalk, Anzeige- und Konzessionspflicht von Internet Service Providern nach dem TKG, MR 2001, 420
Posch, die e-Mail Nutzung aus arbeitsrechtlicher Sicht, in *it-law.at (Hrsg*), e-Mail, elektronische Post im Recht (2003) 75
Rotter, Internet-Zugang für Arbeitnehmer, Mustervereinbarung, ASoK 1999, 118
Thiele, Internet am Arbeitsplatz – Erste arbeitsrechtliche Konfliktfälle, ecolex 2001, 613

Online:

Mosing, Cookies and Log-Files – The "Transparent Internet User" or Data Protection on the Internet inn the EU, www.it-law.at
Otto, Konzessionspflicht für ISP, www.it-law.at
Posch, Neue Medien im Lichte des Arbeitsvertrages, www.it-law.at
Buschina, Arbeitnehmerüberwachung im Hinblick auf Grund- und Menschenrechte, www.it-law.at

Judikatur:

OGH 13. 06. 2002, 8 Ob A 288/01p, wbl 2002, 353
OGH, Arb 9997/1981
VwGH 10. 12. 1985, 85/04/0126
VwGH 13. 10. 1993, 92/03/0054, VwSlg 13.921 A/1993, wbl 1994, 283 = ZfVB 1995/1765

Sonstige Quellen und online Datenbanken (annotiert)

http://europa.eu.int/comm/internal_market/en/dataprotect/wpdocs/wp-58_en.pdf
http://www.rdb.at
http://www.ris.bka.gv.at
http://www.parlament.gv.at
http://www.tkc.at/web.nsf/lookuid/01D619D19CD2B97EC1256CF00054CA4E/$file/Konzessionspflicht%20f%C3%BCr%20den%20Sprachtelefoniedienst.pdf