

# E-Mail und Internet am Arbeitsplatz

## Kontrollen, Mitbestimmung und Datenschutz

Eberhard Kiesche // Arbeitnehmerorientierte Beratung (AoB), Bremen  
Matthias Wilke // Datenschutz- und Technologieberatung (dtb), Kassel

### HIER LESEN SIE:

- die rechtlichen Rahmenbedingungen für die (private) Nutzung von Kommunikationsmitteln in der Arbeitswelt
- wie die Mitbestimmungsrechte den Kontrollmöglichkeiten des Arbeitgebers enge Grenzen setzen
- den Vorschlag für eine Vereinbarung zur Regelung der Nutzung von Internet und E-Mail am Arbeitsplatz

**Die private Nutzung von Kommunikationsmitteln in Betrieb und Dienststelle ist nach wie vor umstritten. Betriebs- und Personalräte suchen derweil nach Wegen, eine geringfügig private Nutzung des Internet für die Beschäftigten zu sichern. Arbeitgeber wollen dagegen zunehmend die Privatnutzung untersagen – um nicht Provider im Arbeitsverhältnis zu werden. In dieser Situation hilft der Abschluss einer Betriebs- oder Dienstvereinbarung zum privaten Surfen beiden Seiten. Der Persönlichkeitsschutz der Beschäftigten und die Interessen des Arbeitgebers an Missbrauchs- und Verhaltenskontrollen können so in Einklang gebracht werden. Das Beispiel einer Betriebsvereinbarung über die Nutzung von Internet und Mail am Arbeitsplatz zeigt, wie derzeit eine Lösung aussehen kann.**

Viele Arbeitgeber und Interessenvertretungen gehen inzwischen davon aus, dass eine gelegentliche private Nutzung von E-Mail und Internet sich nicht völlig verbieten lässt. Wird die Privatnutzung erlaubt, so stellen sich Fragen, inwieweit noch Kontrollen z. B. der Inhalte von E-Mails, der Verkehrsdaten<sup>1</sup> und/oder der aufgerufenen Internetseiten zulässig sind.

Bei der datenschutzrechtlichen Bewertung, inwieweit Arbeitgeber die Nutzung der Telekommunikationsanlagen in Unternehmen und Dienststellen kontrollieren dürfen, ist neben den Vorgaben des Telekommunikationsgesetzes (TKG) das Bundesdatenschutzgesetz (BDSG) zu beachten.<sup>2</sup> Dieses wurde bei der letzten Novellierung im Jahr 2009 verschärft und hat in § 32 BDSG eine erste Regelung zum Beschäftigtendatenschutz aufgenommen. Hier bleibt nachstehend zu untersuchen,

wie die neuen gesetzlichen Regelungen konkret in Betriebs- und Dienstvereinbarungen zu E-Mail und Internet umzusetzen sind.

Im Folgenden sollen datenschutzgerechte Lösungen diskutiert werden, die möglichst den Interessen der Beschäftigten und der Unternehmen gleichermaßen dienlich sind. Ziel ist es dabei, praxisgerecht zu einem möglichst umfassenden Persönlichkeits- und Datenschutz der Beschäftigten bei der privaten Nutzung von Kommunikationsanlagen beizutragen.

Dabei wird nachstehend auf eine pragmatische Regelung im Sinne einer Betriebs- oder Dienstvereinbarung abgezielt, die eine gelegentliche, geringfügige und die Arbeitsleistung nicht beeinträchtigende Nutzung der Internetdienste ermöglicht. Die private Nutzung dienstlicher Mail-Adressen<sup>3</sup> soll dabei im Rahmen einer sol-

chen Regelung zwar ausgeschlossen, die Nutzung eines Webmail-Dienstes für den privaten E-Mail-Verkehr im Betrieb oder in der Dienststelle aber für ein Zeitfenster außerhalb der Arbeitszeit ermöglicht werden.

Mit der Erlaubnis einer Privatnutzung des WWW sind auch Vorteile für Unternehmen und Verwaltungen verbunden. Motivierte Mitarbeiter und moderne attraktive Arbeitsplätze sind hier nur zwei Argumente. Die Erfahrung in Betrieben und Verwaltungen zeigt zudem, dass sich ein absoluter Ausschluss der Privatnutzung kaum durchsetzen lässt. Es ist deshalb eine geeignete Organisationsgestaltung zu finden, um eine geringfügige private Nutzung von Internetdiensten bei der Arbeit rechts- und datenschutzkonform zu ermöglichen – unter Wahrung der gegenseitigen Interessen.

Von daher werden nachstehend kurz die rechtlichen Grundlagen zu E-Mail und

Internet am Arbeitsplatz, das Grundrecht „Fernmeldegeheimnis“ im Arbeitsverhältnis, die datenschutzrechtlichen Zulässigkeitsvoraussetzungen von Kontrollen des Arbeitgebers und die Erlaubisnorm Betriebs-/Dienstvereinbarung erörtert.

Abschließend soll als Ausblick dargestellt werden, ob sich durch das geplante Beschäftigtendatenschutzgesetz erkennbar etwas an der bisherigen Rechtslage ändert. Ziel ist es zusätzlich, Inhalte einer rechtskonformen und datenschutzgerechten Betriebs- bzw. Dienstvereinbarung zu entwickeln.

## Arbeitgeber als Provider und Beschäftigte als Nutzer

Zunächst muss geklärt werden, ob im jeweiligen konkreten Einzelfall der Arbeitgeber die betriebliche Informations- und Kommunikationstechnik auch für private Zwecke zur Verfügung stellt. Von dieser Unterscheidung hängen unterschiedliche Rechtspflichten für den Arbeitgeber bei der Nutzung von Internetdiensten ab.

Die Frage stellt sich, ob bei der betrieblichen Nutzung der Telekommunikation das Fernmeldegeheimnis gemäß §§ 88 ff. TKG anzuwenden ist. Es ist zu untersuchen, ob konkret für die Verarbeitung personenbezogener Daten der Beschäftigten beim Aussenden, Übermitteln und Empfangen von Nachrichten jeglicher Art mittels Telekommunikationsanlagen und -systemen (Fax, Telefon, E-Mail usw.) das Fernmeldegeheimnis gilt.

Nutzen die Beschäftigten die Telekommunikationsanlagen im Betrieb ausschließlich für berufliche Zwecke, wird der Arbeitgeber nicht zum Diensteanbieter im Sinne des § 3 Abs. 6 TKG und des Telemediengesetzes (TMG). Kontrollen des Arbeitgebers sind dann nach dem BDSG bzw. entsprechender Länderdatenschutzgesetze, BetrVG und dem allgemeinen Persönlichkeitsrecht rechtlich zu bewerten.<sup>4</sup>

Nutzen die Beschäftigten die Anlage im Unternehmen dagegen auch für private Zwecke, so erbringt der Arbeitgeber geschäftsmäßig Telekommunikationsdienste.<sup>5</sup> Auf das nachhaltige Angebot von Telekommunikation einschließlich des Angebots von Übertragungswegen für Dritte

(hier der Mitarbeiter) oder das Mitwirken hierbei sind § 88 TKG, das BDSG und das BetrVG anzuwenden.

## Grundrecht „Fernmeldegeheimnis“

Das Grundrecht des Fernmeldegeheimnisses, abzuleiten aus Art. 10 Abs. 1 des Grundgesetzes (GG), umfasst alle mit Hilfe der verfügbaren Telekommunikations-einrichtungen erfolgenden Übermittlungen von Informationen.<sup>6</sup> Betriebliche Eingriffe in das Persönlichkeitsrecht der Beschäftigten, hier in der Ausprägung des Fernmeldegeheimnisses, sind nach dem

**„Die Internetnutzung und Kommunikation mit schweigepflichtigen Personen und Interessenvertretungen sind vor einer Überwachung grundsätzlich zu schützen.“**

Verhältnismäßigkeitsprinzip zu beurteilen. Der verfassungsrechtliche Schutz des Persönlichkeitsrechts gilt mittelbar auch im Arbeitsverhältnis.<sup>7</sup>

§ 88 TKG erstreckt sich auf alle Diensteanbieter, die ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringen und daran mitwirken.<sup>8</sup> Lässt der Arbeitgeber die Privatnutzung von E-Mail und Internet zu, wird der Beschäftigte „Dritter“ im Sinne des TKG – dann erstreckt sich der Schutz des Art. 10 GG auch auf die von Arbeitgebern betriebenen Kommunikationsanlagen.<sup>9</sup> Der Arbeitgeber als Anbieter hat das Fernmeldegeheimnis für alle Inhalte und näheren Umstände der Telekommunikation zu wahren.<sup>10</sup>

Hier müssen Belegschaftsvertretungen und Beschäftigte jedoch wissen, dass nach Beendigung der Übertragung von Nachrichten (E-Mails) das Telekommunikationsgeheimnis<sup>11</sup> die private Korrespondenz des Beschäftigten nicht mehr schützt. Bleiben private Mails im Posteingang oder -ausgang oder auf den lokalen Rechnern im Bereich des Empfängers, unterliegt der Zugriff des Arbeitgebers auf diese Mails im lokalen Endgerät nicht mehr dem Fernmeldegeheimnis.

Der Beschäftigte als Empfänger hat die technische Möglichkeit, die empfangenen Daten zu verarbeiten bzw. insbesondere

zu löschen. Der Schutz der erst nach Abschluss des Übertragungsvorgangs angelegten Dateien erfolgt nunmehr über das Recht auf Datenschutz<sup>12</sup>, das Allgemeine Persönlichkeitsrecht, die Anwendbarkeit des § 32 BDSG und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.<sup>13</sup>

Probleme ergeben sich, wenn die Nachricht mit privaten Inhalten in das Postfach gelangt, der Beschäftigte sie aber noch nicht zur Kenntnis genommen hat.<sup>14</sup> Der Schutzbereich des Art. 10 Abs. 1 GG erstreckt sich zudem auf Mails, die auf dem Server des Providers (hier des Arbeitgebers) gespeichert sind.<sup>15</sup>

Hier sollten Interessenvertretungen durch umfassende Information der Belegschaft dafür sorgen, dass eingehende private Mails in geschützte und als privat gekennzeichnete Ordner des jeweiligen Mail-Systems vom betroffenen Beschäftigten unverzüglich nach Kenntnisnahme verschoben werden. Als alternative Regelungen bieten sich die Löschung nach der Kenntnisnahme bzw. die Weiterleitung an die eigene private E-Mail-Adresse an.

## Protokollierung, Kontrollen des Arbeitgebers und Einwilligung

Es stellt sich die Frage, inwieweit der Arbeitgeber befugt ist, die private und/oder dienstliche Nutzung der Internetdienste zu kontrollieren.

Auch bei einer dienstlichen Nutzung ist eine vollumfängliche oder dauerhafte Kontrolle der Nutzung des Internet und des Mail-Verkehrs seitens des Arbeitgebers nicht zulässig.<sup>16</sup> Stichprobenartige Überprüfungen genügen.<sup>17</sup> Präventive Maßnahmen im Sinne von Aufklärung/Schulung, eindeutige Nutzungsregeln/Sicherheitsrichtlinien und technisch-organisatorische Schutzmaßnahmen sind einer nachträglichen vergangenheitsbezogenen Kontrolle vorzuziehen. Maßnahmen zur

## FRISCH GELESEN ...

■ Die CuA-Schwesterzeitschrift „Arbeitsrecht im Betrieb“ beschäftigt sich in ihrer März-Ausgabe schwerpunktmäßig damit, wie sich **Betriebsräte** für ihre Tätigkeit „gut aufstellen“, um **erfolgreich zu sein**. Im Team lässt sich die immer komplexer werdende Betriebsratsarbeit am besten meistern. So stellt Marcus Schwarzbach die besondere Bedeutung der Strategieplanung für die Arbeitnehmervertretung dar. Die Betriebe sind heutzutage häufig Veränderungen unterworfen. Tätigkeiten verändern sich, neue Managementstrategien und moderne Informations- und Kommunikationstechniken spielen eine große Rolle. Wichtig ist vor allem auch eine rechtzeitige Planung.

■ Die Fachzeitschrift „Der Personalrat“ (3/2011) zeigt **neue Kommunikationswege für Personalräte**. Die CuA-Autoren Rainer Meyer und Ulrich R. Buchholz beschreiben am Beispiel des Bloggens, wie Interessenvertretungen die neuen elektronischen Kommunikationsmöglichkeiten nutzen können, um etwa die Beschäftigten mit aktuellen Informationen, Einblicken in ihre Arbeit und mit Materialien zu versorgen. Aber auch die andere Richtung von Kommunikation wird dargestellt: Wie kann die Personalvertretung eine Rückmeldung der Mitarbeiter erhalten? Wie können sie an Diskussionsprozessen beteiligt werden?

■ In der März-Ausgabe der Fachzeitschrift „gute Arbeit“ erläutert Dr. Ulrich Faber warum beim **Betrieblichen Eingliederungsmanagement** besonders auf den **Datenschutz** geachtet werden muss. Gesundheitsdaten dürfen dabei auf keinen Fall in falsche Hände geraten oder gar krankheitsbedingten Kündigungen Vorschub leisten. Die Eingliederungsteams müssen sich vielmehr der Herausforderung stellen, personenbezogene Gesundheitsdaten sparsam zu erheben oder möglichst zu vermeiden.

## Bestellhinweis

**Einzelexemplare** der hier genannten Zeitschriften können bestellt werden bei:  
Bund-Verlag – Leserservice, 60424 Frankfurt/„M.,  
fon 069 795010-71, abodienste@bund-verlag.de

Überwachung der Beschäftigten bei der privaten Nutzung der Arbeitsmittel (Kommunikationsanlagen) sind an Art. 2 Abs. 1 (Persönlichkeitsrechtsschutz) und Art. 10 (Fernmeldegeheimnis) GG zu messen.

Protokollierung, präventive Kontrolle mit Anonymisierung und Pseudonymisierung sowie anlassbezogene Überprüfung bei Missbrauchsverdacht sind in einer Dienst- bzw. Betriebsvereinbarung zu regeln. Die Internetnutzung und Kommunikation mit schweigepflichtigen Personen<sup>18</sup> und Interessenvertretungen sind vor einer Überwachung grundsätzlich zu schützen.

Zur Protokollierung stellen sich Fragen, die in der Praxis oftmals von Betriebs- und Personalräten nicht ausreichend beantwortet werden. Wie soll die Protokollierung konkret ablaufen? Ein alles umfassendes Protokoll wird nicht benötigt, es verstößt gegen das Gebot der Datenvermeidung und Datensparsamkeit (Systemdatenschutz gemäß § 3 a BDSG) und es ist im Übrigen nicht erforderlich.

Der Umfang der Protokolldaten muss eindeutig festgelegt und die Zwecke der Datenverwendung exakt bestimmt werden. Zudem müssen die Zugriffsberechtigten bzw. die Verantwortlichen benannt, die gegebenenfalls erforderliche Weitergabe an befugte Personen im Unternehmen geregelt, die Speicherdauer der Protokolldaten möglichst kurz gehalten und ein exaktes Verfahren bei personenbezogenen Kontrollmaßnahmen festgelegt werden. Es ist weiterhin von den Betriebsparteien festzulegen, nach welchen Kriterien die Kontrollen technisch von welchen befugten Personen durchzuführen sind. Im Falle eines begründeten Verdachts sind der betriebliche Datenschutzbeauftragte und die Belegschaftsvertretung immer hinzuzuziehen.

Keineswegs sollten Datenschutzbeauftragte Kontrollen mit einer „Spionagesoftware“ durchführen, von der die Belegschaftsvertretung nicht in Kenntnis gesetzt wird.<sup>19</sup>

Die präventiven anonymisierten und bei einem begründeten Verdacht auch personenbezogenen Kontrollverfahren sollten von Betriebs- und Personalräten mitbestimmt und eingegrenzt vereinbart werden. Nur so kann beispielsweise bei den

präventiven Kontrollen die tatsächliche Anonymität der Auswertungen gesichert und von der Interessenvertretung überprüft werden.<sup>20</sup>

Gestattet der Arbeitgeber die private Nutzung des WWW am Arbeitsplatz, kann er die Erlaubnis davon abhängig machen, dass der Beschäftigte einer Protokollierung seiner dabei anfallenden personenbezogenen Daten zur Durchführung einer angemessenen Kontrolle der Netzaktivitäten zustimmt.<sup>21</sup>

Die Einwilligung muss nach § 4 a BDSG freiwillig, ohne Zwang und informiert – das heißt in Kenntnis der Sachlage – erfolgen. Dies hat zur Konsequenz, dass der Beschäftigte über den Kontrollzweck, die Art der für diesen Zweck gespeicherten Daten oder Aufzeichnungen, die Art und Weise der Auswertungen und die Dauer der Speicherung informiert werden muss. Er muss weiterhin auf sein Widerrufsrecht und auf die Folgen seines Widerrufs aufmerksam gemacht werden. Einwilligungen, die die Datenverarbeitung im Bereich des BDSG ermöglichen, bedürfen der Schriftform nach § 4 a Abs. 1 Satz 3 BDSG, so auch die Einwilligung in die Kontrollen der Nutzung von Internetdiensten. Diese Einwilligung kann dem Arbeitgeber allerdings nicht mehr zugestehen, als ihm aufgrund des Arbeitsverhältnisses an Kontrollmöglichkeiten zusteht und darf zudem nicht Schutzgesetzen widersprechen.

Generell ist allerdings die Einwilligung im Beschäftigungsverhältnis problematisch, weil es an der Freiwilligkeit fehlt. Bei der Einwilligung in Kontrollen der geringfügigen Internetnutzung für private Zwecke ist nur ein „Randbereich des Beschäftigungsverhältnisses“ betroffen, so dass ein Ausnahmefall vorliegt und die Einwilligung als eine mögliche Zulässigkeitsvoraussetzung bislang genutzt werden kann.<sup>22</sup>

## Datenschutzgerechte Nutzung von E-Mail und Internet

Zunächst haben die Aufsichtsbehörden für den Datenschutz Hinweise für eine datenschutzgerechte Gestaltung von E-Mail und Internet gegeben.<sup>23</sup> Seit 2009 gibt es eine erste rechtliche Grundlage für einen Be-

schäftigtendatenschutz. § 32 BDSG regelt die Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung im Beschäftigungsverhältnis. Hierfür wurde in 2009 unter § 3 Abs. 11 BDSG der Begriff des Beschäftigten definiert. Er umfasst alle in einem abhängigen Beschäftigungsverhältnis stehenden Personen.

Der § 32 BDSG verlangt als Zulässigkeitskriterium, dass die Datenerhebung, -verarbeitung und -nutzung für die Begründung, Durchführung und Beendigung des Beschäftigungsverhältnisses erforderlich ist.<sup>24</sup> Die Rechtmäßigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten der Beschäftigten richtet sich somit vorrangig nach dem Zweck des Arbeitsverhältnisses.

Stichprobenartige präventive Kontrollen, die die Verkehrsdaten der Telekommunikation speichern und auswerten, sind nach § 32 Abs. 1 Satz 1 BDSG zulässig. Der Arbeitgeber hat das Recht, verhältnismäßige Kontrollen beim dienstlichen E-Mail-Verkehr und der Internetnutzung durchzuführen, weil sich aus dem Arbeitsverhältnis Pflichten für Beschäftigte ergeben und der Arbeitgeber die Einhaltung der Pflichten und die Erledigung der vertraglich vereinbarten Aufgaben kontrollieren kann.<sup>25</sup>

Datenerhebung, -verarbeitung und -nutzung bei schweren vertraglichen Verletzungen sind nach § 32 Abs. 1 Satz 1 BDSG zulässig. Maßnahmen aufgrund eines begründeten Verdachts auf Begehung einer beschäftigungsbezogenen Straftat gegen eine bestimmte Person sind auf Verhältnismäßigkeit/Angemessenheit nach den Vorgaben von § 32 Abs. 1 Satz 2 BDSG in jedem Einzelfall zu überprüfen.

Will der Arbeitgeber die Erhebung und Verwendung von Beschäftigtendaten zur Aufdeckung von Straftaten<sup>26</sup> auf § 32 Abs. 1 Satz 2 BDSG<sup>27</sup> begründen, so müssen die folgenden Anforderungen eingehalten werden:

- „zu dokumentierende tatsächliche Anhaltspunkte
- begründeter Verdacht einer Straftat im Beschäftigungsverhältnis
- Erhebung, Verarbeitung oder Nutzung der Daten ist erforderlich
- schutzwürdiges Beschäftigteninteresse überwiegt nicht
- Art und Ausmaß der Datenverwendung ist im Hinblick auf den Anlass nicht unverhältnismäßig.“<sup>28</sup>

§ 32 Abs. 1 Satz 2 BDSG regelt die Überwachung beim Verdacht auf eine Straftat. Hierfür hat das Bundesarbeitsgericht (BAG) hinsichtlich der Videoüberwachung Grundsätze aufgestellt, die es bei einer Verhältnismäßigkeitsprüfung von personenbezogenen Kontrollen in jedem Einzelfall zu beachten gilt.<sup>29</sup>

### **Betriebs- oder Dienstvereinbarung als vorrangige Erlaubnisnorm**

Gegenüber einer Nutzungsordnung bezüglich E-Mail und Internet am Arbeitsplatz ist eine Betriebs- bzw. Dienstvereinbarung aufgrund deren normativen Wirkung vorzuziehen.

Die Verarbeitung oder Nutzung von personenbezogenen Daten im Rahmen der Durchführung von Telemediendiensten und Telekommunikation kann grundsätzlich durch eine „andere Rechtsvorschrift“

erlaubt sein.<sup>30</sup> Zu den in § 4 Abs. 1 BDSG angeführten „anderen Rechtsvorschriften“ zählen Betriebs- und Dienstvereinbarungen.<sup>31</sup> Sie sind keine „gesetzlichen Vorschriften“ und dürfen somit den Spielraum für eine Kenntnisnahme der Nutzungsdaten bei E-Mail und Internet durch den Arbeitgeber gegenüber den Vorgaben des TKG und des TMG nicht erweitern.<sup>32</sup> Eine Abweichung vom gesetzlichen Datenschutzstandard zum Nachteil des Beschäftigten ist nicht möglich.<sup>33</sup>

Betriebs- und Dienstvereinbarungen dürfen und vor allem sollten jedoch günstigere Regelungen im Sinne des Persönlichkeitsschutzes und des Rechts auf Datenschutz enthalten und Kontrollbefugnisse des Arbeitgebers einschränken. Regelungen in einer Vereinbarung zur E-Mail- und Internetnutzung sind darauf hin zu entwickeln und zu bewerten, inwieweit sie den Persönlichkeitsschutz konkretisieren und verbessern.<sup>34</sup> Deshalb sollten sich Mitarbeitervertretungen z.B. fragen, inwieweit präventive stichprobenartige Kontrollen auch ohne Personenbezug überhaupt erforderlich sind und ob nicht auch vollständig darauf verzichtet werden kann.

Die Speicherung und Auswertung der bei der Nutzung des Internet protokollierten Daten unterliegen der Mitbestimmung nach § 87 Abs. 1 Nr. 6 BetrVG bzw. § 75 Abs. 3 Nr. 17 BPersVG. Betriebs- und Personalrat haben zudem die Aufgabe, die Einhaltung der in diesem Fall einschlägigen Datenschutzvorschriften gemäß § 80 Abs. 1 Nr. 1 BetrVG und § 68 Abs. 1 Nr. 2 BPersVG<sup>35</sup> zu überwachen.

Nachfolgende Vereinbarung, die Vorschläge zur Umsetzung der vorstehenden

Überlegungen entwickelt und auf Beratungen in der Praxis basiert (siehe Kasten ab Seite 19), dient ausdrücklich nicht als „Mustervereinbarung“. Sie erhebt keinen Anspruch, alle erforderlichen Themen im Zusammenhang mit E-Mail und Internet am Arbeitsplatz zu regeln.

So sind z.B. Regelungen für geplante und ungeplante Abwesenheiten<sup>36</sup>, zur Sperrung von Kommunikationspartnern oder Websites durch Filter oder zum Umgang mit Spam ausgespart.<sup>37</sup> Der Vereinbarungstext konzentriert sich auf präventive anonymisierte und nachträgliche personenbezogene Kontrollen einer geringfügigen Internetnutzung bei begründetem Verdacht und dabei zusätzlich auf das grundsätzliche Verbot der Nutzung der dienstlichen E-Mail-Adresse für private Zwecke.<sup>38</sup>

## Ausblick

Ändert sich durch die geplanten Neuregelungen zum Beschäftigtendatenschutz voraussichtlich im Jahr 2011 die Rechtslage? Der durch das Bundeskabinett vorgelegte Gesetzesentwurf zum Beschäftigtendatenschutz sieht dies zurzeit ausdrücklich nicht vor.

Eine Sonderregelung zur erlaubten privaten Nutzung von Telekommunikationsdiensten des Arbeitgebers enthält der Gesetzesentwurf nicht bzw. schweigt dazu. Es bleibt insofern bei der geltenden Rechtslage nach dem TKG, wenn der Arbeitgeber die private Nutzung der Kommunikationsmittel erlaubt, so ausdrücklich das Hintergrundpapier zum Gesetzesentwurf.<sup>39</sup> Eine präventive personenbezogene Missbrauchskontrolle mit Einsicht in private Inhalte wird auch zukünftig ausgeschlossen sein.<sup>40</sup>

Im geplanten § 32i zur Telekommunikation fehlt zudem die Einwilligung. Die Einwilligung wäre nur noch dann erlaubt, wenn sie in den künftigen §§ 32 a–l BDSG ausdrücklich vorgesehen ist. Der Entwurf zur Kontrolle der Nutzung von Telekommunikationsdiensten sieht weiterhin eine sogenannte Verhältnismäßigkeitsprüfung vor, ähnlich wie sie in der ab Seite 19 abgedruckten Betriebsvereinbarung in § 7 vorgesehen ist.

Betriebs- und Personalräten ist anzuraten, die private Nutzung von Kommunikationsanlagen in Unternehmen und Dienststellen und eine damit verbundene Auswertung von Internetverkehrsdaten nur in ganz eng definierten Grenzen zu vereinbaren. Die vorstehenden Ausführungen sollen hierfür ein Diskussionsanstoß sein.

Auf den Seiten 19 bis 21 folgt als weitere Anregung ein Vorschlag für eine Betriebsvereinbarung zum Thema „Internet- und E-Mail-Nutzung am Arbeitsplatz“.

### Autoren

**Dr. Eberhard Kiesche**, Arbeitnehmerorientierte Beratung (AoB), Bremen, eberhard.kiesche@t-online.de, www.aob-bremen.de; **Matthias Wilke**, Datenschutz- und Technologieberatung (dtb), Kassel, info@dtb-kassel.de, www.dtb-kassel.de

### Fußnoten

- 1 § 3 Nr. 30 TKG
- 2 Dies gilt für die Privatwirtschaft und die Bundesverwaltung. Bei den Ländern gelten die entsprechenden Länderdatenschutzgesetze und ggf. vorrangige Bundesspezialgesetze und Länderspezialgesetze, siehe die umfassende Darstellung in: Bergmann/Möhrle/Herb, Datenschutzrecht, 2010 (41. Ergänzungslieferung)
- 3 vorname.nachname@domain des Arbeitgebers
- 4 Siehe auch § 11 Abs. 1 Nr. 1 TMG und Däubler, Gläserne Belegschaften?, 5. Auflage, 2010, Rn. 336 ff. (338); Karg, Arbeitgeber als Provider, in: CuA 6/2010, 18 ff.; auch das jeweilige PersVG
- 5 Siehe § 3 Abs. 6 TKG und Vietmeyer/Byers, Der Arbeitgeber als TK-Anbieter im Arbeitsverhältnis, in: MMR 2010, 808; Behling, Compliance versus Fernmeldegeheimnis, in: BB 2010, 892 ff. (893)
- 6 Gola, Datenschutz und Multimedia am Arbeitsplatz, 3. Auflage, Rn. 94 ff.
- 7 Siehe § 75 Abs. 2 BetrVG
- 8 Vgl. § 3 Nr. 10 TKG
- 9 Bei Internetzugang und Mail-Übertragung als Telemediendienste ist auch das TMG zu beachten. Wegen § 11 Abs. 3 TMG gelten allerdings primär die Datenschutzregelungen des TKG, so Gola, aaO., Rn. 155 und Fn. 148. Die Abgrenzung wird hier nicht weiter dargestellt. Einen guten Überblick bietet die Schrift von Gola, aaO.
- 10 Siehe auch § 206 Strafgesetzbuch (StGB)
- 11 Däubler, aaO., Rn. 332
- 12 Recht auf Informationelle Selbstbestimmung im Sinne des Art. 2 Abs. 1 und Art. 1 Abs. 1 GG (Bundesverfassungsgericht – BVerfG – im Volkszählungsurteil von 1983)
- 13 Gola, aaO., Rn. 100, 98; siehe auch BVerfG vom 2.3.2006, Az.: 2 BvR 2099/04 und VGH Hessen, Beschluss vom 19.5.2009, Az.: 6 A 2672/08.Z (www.lareda.hessenrecht.hessen.de)
- 14 Siehe Vietmeyer/Byers, aaO., 808 ff.
- 15 BVerfG, Beschluss vom 16.6.2009, Az.: 2 BvR 902/06, www.bverfg.de und ausführlich Karg, aaO., 20
- 16 Wedde, Das TKG und die private E-Mail-Nutzung am Arbeitsplatz, in: CuA 3/2007, 9 ff.
- 17 Gola, aaO., Rn. 291
- 18 Siehe die in § 203 StGB genannten Personen; auch Wissenschaftler genießen einen Schutz nach § 40 Abs. 1 BDSG; Däubler, aaO., Rn. 379 ff., Weichert, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Auflage, 2010, § 39 Rn. 1

- 19 Siehe die empfohlene Vorgehensweise des BFD zur Protokollierung, abgedruckt in Gola, aaO., Rn. 110
- 20 Vgl. hierzu grundlegend Roßnagel/Scholz, Datenschutz durch Anonymität und Pseudonymität. Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, in: MMR 2000, 721 ff.; Heinson/Schmidt, IT-gestützte Compliance-Systeme und Datenschutzrecht, in: CR 2010, 540 ff.
- 21 Siehe unter vielen Gola, aaO., Rn. 331
- 22 Bergmann/Möhrle/Herb, aaO., § 32 BDSG, Rn. 20; das könnte sich durch das geplante Beschäftigtendatenschutzgesetz ändern, weil dann die Einwilligung nur noch in definierten Fällen zugelassen werden soll
- 23 Vgl. die Entschließung der 63. Konferenz der Datenschutzbeauftragten (Länder, Bund) zu E-Mail und Internet unter: www.datenschutz.rlp.de/de/ds.php?submenu=grem&typ=dsb&ber=063\_internetarbpl
- 24 Vgl. hierzu Gola, aaO., Rn. 137 ff.
- 25 Wedde, in: Däubler/Klebe/Wedde/Weichert, aaO., § 32 Rn. 91; Däubler, aaO., Rn. 292
- 26 Etwa das Verbreiten von Kinderpornografie oder unberechtigte Weitergabe von Betriebsgeheimnissen
- 27 Nachgebildet § 100 Abs. 3 TKG
- 28 Bergmann/Möhrle/Herb, aaO., § 32 BDSG Rn. 167
- 29 BAG, Beschluss vom 6.8.2008, Az.: 1 ABR 16/07, in: RDV 2008, 238
- 30 Siehe § 12 Abs. 1, 3 TMG, § 4 Abs. 1 BDSG, § 88 Abs. 3 Satz 3 TKG, ausführlich dazu Gola, aaO., Rn. 345 ff. und Däubler, aaO., Rn. 327 ff.
- 31 Allgemein anerkannt, auch vom BAG, siehe Beschluss vom 27.5.1986, Az.: 1 ABR 48/84
- 32 Gola, aaO., Rn. 350
- 33 Bergmann/Möhrle/Herb, aaO., § 4 BDSG, Rn. 25f. mit überzeugenden Argumenten gegen einen veralteten BAG-Beschluss vom 27.5.1986, in: RDV 1986, 199
- 34 Gola, aaO., Rn. 351f.
- 35 Analog entsprechende Landes-Personalvertretungsgesetze
- 36 Bsp.: Urlaub oder Krankheit; siehe auch § 32i Abs. 4 Satz 2 Beschäftigtendatenschutzgesetz (Entwurf)
- 37 So weiter auch die Problematik des Downloads von Software oder die Pflicht des Arbeitgebers zur Bereitstellung von Technik zur Nutzung von E-Mail und Internet, hierzu Gola, aaO., Rn. 4 ff.; 193 ff.
- 38 Die Ausgestaltung der Betriebs- bzw. Dienstvereinbarung greift auf Vorlagen zurück; siehe vor allem Prömper/Römermann, Nutzung von Internet und E-Mail am Arbeitsplatz (Mustervereinbarung), in: MMR 2008, 514 ff.; Speichert, Praxis des IT-Rechts, 2. Auflage, 2007, 186 ff.
- 39 Siehe BMI-Presspapier: www.bmi.bund.de und ausführlich Vietmeyer/Byers, aaO., 807 ff.; Tinnefeld/Petri/Brink, Aktuelle Fragen um ein Beschäftigtendatenschutzgesetz, in: MMR, 733f.
- 40 Vietmeyer/Byers, aaO., 810

## BETRIEBSVEREINBARUNG ÜBER DIE NUTZUNG VON INTERNET UND E-MAIL AM ARBEITSPLATZ

Zwischen der Geschäftsführung der Firma XYZ und dem Betriebsrat der Firma XYZ wird nachstehende Betriebsvereinbarung geschlossen.

### § 1 Gegenstand und Geltungsbereich

- (1) Die Internet- und E-Mail-Nutzung am Arbeitsplatz steht den Beschäftigten als Arbeitsmittel im Rahmen der dienstlichen Aufgabenerfüllung zur Verfügung und dient insbesondere der Verbesserung der internen und externen Kommunikation, der Erzielung einer höheren Effizienz und der Beschleunigung der Arbeitsprozesse.
- (2) Diese Betriebsvereinbarung zeigt die geltenden Grundsätze für den Zugang und die Nutzung der Internet- und E-Mail-Dienste bei der Firma XYZ auf.
- (3) Sie gilt für alle Beschäftigten einschließlich der Auszubildenden, Praktikanten, Aushilfen, Diplomanden und Leiharbeiternehmer, die einen betrieblichen E-Mail- und Internetzugang nutzen.
- (4) Leitende Angestellte im Sinne von § 5 Abs. 3 BetrVG werden auf die Einhaltung und Umsetzung der Regelungen dieser Betriebsvereinbarung schriftlich verpflichtet.

### § 2 Zielsetzung

- (1) Ziel dieser Betriebsvereinbarung ist es, die Nutzungsbedingungen von E-Mail und Internet sowie die Maßnahmen zur Protokollierung von personenbezogenen Daten und, soweit erforderlich, Kontrollmaßnahmen transparent zu regeln, die Persönlichkeitsrechte der Beschäftigten zu sichern und den Schutz ihrer personenbezogenen Daten dauerhaft zu gewährleisten.
- (2) Internet und E-Mail dürfen nicht zur Leistungsbewertung und -kontrolle eingesetzt werden. Die bei der Nutzung der Internetdienste anfallenden personenbezogenen Daten werden nicht zur Leistungs- und Verhaltenskontrolle erhoben, verarbeitet oder genutzt. Die protokollierten Daten unterliegen der Zweckbindung dieser Betriebsvereinbarung und den einschlägigen Datenschutzbestimmungen.

### § 3 Private Nutzung von E-Mail

- (1) Die private Nutzung von E-Mail-Diensten über das betriebliche Mailsystem (z. B. Outlook, Lotus Notes) ist in allen dienstlichen Postfächern untersagt.
- (2) Eingehende private E-Mails an die dienstliche E-Mail-Adresse sind nach inhaltlicher Kenntnisnahme grundsätzlich durch den Beschäftigten entweder zu löschen, in als privat gekennzeichneten Ordnern des Mailprogramms zu verschieben oder erforderlichenfalls an den privaten E-Mail-Account weiterzuleiten. Der Beschäftigte soll den Absender eingehender privater E-Mails auf dem Dienst-Account auf die ausschließliche dienstliche Zweckbestimmung des E-Mail-Verkehrs hinweisen.

- (2) Das Medium Internet kann zusätzlich genutzt werden, private E-Mails über ein Webmail-Konto (wie z. B. www.web.de) zu empfangen und zu versenden, allerdings nur in Pausenzeiten (Zeitfenster ### Uhr bis ### Uhr) oder nach Dienstschluss. Das Zugangspasswort hierfür darf nicht im dienstlichen Bereich hinterlegt und zugänglich gemacht werden.

### § 4 Private Internetnutzung

- (1) Internetdienste werden primär für die geschäftliche Aufgabenerfüllung eingesetzt.
- (2) Die gelegentliche private Nutzung des Internet ist nur in Pausenzeiten oder nach Dienstschluss gestattet.
- (4) Der Internetzugang darf nicht wissentlich oder absichtlich für beleidigende, verleumderische, verfassungsfeindliche, rassistische, sexistische, Gewalt verherrlichende, pornografische Aktivitäten oder sonst rechtswidrige oder gegen die Systemicherheit gerichtete Aktivitäten genutzt werden.
- (5) Im Rahmen der privaten Nutzung dürfen keine kommerziellen oder sonstigen geschäftlichen Zwecke verfolgt werden.
- (6) Unzulässig ist auch jede bewusste, absichtliche oder wissentliche Nutzung des Internetzugangs, die geeignet ist, den Interessen der Firma XYZ oder deren Ansehen in der Öffentlichkeit zu schaden, die Sicherheit des Unternehmensnetzes zu beeinträchtigen oder gegen geltende Rechtsvorschriften verstößt.

### § 5 Einwilligung und Protokollierung

- (1) Durch die private Nutzung der Internetdienste erklärt der Beschäftigte seine Einwilligung in die Protokollierung seiner dabei anfallenden personenbezogenen Daten und in gegebenenfalls erforderliche Kontrollmaßnahmen für den Bereich der dienstlichen und/oder privaten Nutzung.
- (2) Nur denjenigen Beschäftigten wird die private Nutzung von Internet gestattet, die zuvor in einer schriftlichen Einwilligung gegenüber dem Arbeitgeber eine Einverständniserklärung abgeben. Mit dieser (jederzeit widerruflichen) Einwilligung erkennt der Beschäftigte an, dass das Telekommunikationsgeheimnis eingeschränkt wird und Kontrollen entsprechend der Betriebsvereinbarung durchgeführt werden dürfen.
- (3) Soweit der Beschäftigte keine Einwilligung abgibt oder sie widerruft, erhält er Zugang zum Internet ausschließlich zu dienstlicher oder beruflicher Nutzung. Es steht jedem Beschäftigten frei, ob er sich für oder gegen eine Privatnutzung entscheidet.
- (4) Folgende Verkehrsdaten für den Internetzugang und den E-Mail-Verkehr werden protokolliert:
  - Zeitraum (Dauer der Internetsitzung),
  - IP-Adressen von Absender und Empfänger und
  - Anzahl/Häufigkeit der Zugriffe im WWW.

Ausgenommen hiervon sind der Betriebsrat, die Schwerbehindertenvertretung sowie alle schweigepflichtigen Personen im Unternehmen (siehe § 203 StGB).

(5) Die Protokolldatei wird ausschließlich zu Zwecken der

- Analyse und Korrektur technischer Fehler im Netz (Störungsbeseitigung),
- Gewährleistung der Datensicherheit,
- Gewährleistung des ordnungsgemäßen Betriebs der Telekommunikationsnetze oder -dienste,
- anonymisierte nicht personenbezogene Stichproben zur Kontrolle der Einhaltung von arbeits- und strafrechtlichen Vorgaben gemäß § 6 dieser Betriebsvereinbarung und
- personenbezogene Auswertungen gemäß § 7 (Missbrauchskontrolle) dieser Betriebsvereinbarung

verwendet.

### § 6 Anonymisierte präventive stichprobenartige Kontrollen

(1) Zur Überprüfung der Einhaltung der Regelungen dieser Betriebsvereinbarung werden die Protokolldateien von namentlich benannten IT-Systemadministratoren, die für den Netzwerkbetrieb und die Bereitstellung der Internetdienste verantwortlich sind, stichprobenartig und nicht personenbezogen gesichtet und ausgewertet. Hierzu sind maximal zwei Personen aus dem IT-Bereich berechtigt, die sich an die Zweckbindung, die durch diese Betriebsvereinbarung vorgegeben ist, halten müssen.

(2) Auf Anforderung des Betriebsrats werden die technische Ausgestaltung der Kontrolle und die Auswertungen der anonymisierten Stichproben gemeinsam mit dem IT-Bereich entwickelt und durchgeführt.

(3) Die Protokolldatei wird nach Ablauf von # (z. B. drei) Monaten ab Aufzeichnung automatisch durch Überschreiben gelöscht.

(4) Für weitergehende Überprüfungsmaßnahmen dürfen die Protokolle nur nach Maßgabe des § 7 dieser Betriebsvereinbarung genutzt werden.

(5) Die Systemadministratoren haben eine Verpflichtung zur Einhaltung des Datenschutzes und des Fernmeldegeheimnisses zu unterschreiben. Darüber hinaus sind sie hinsichtlich der Einhaltung des Datengeheimnisses nach § 5 BDSG und des Fernmeldegeheimnisses nach § 88 TKG auf die arbeits- und strafrechtlichen Konsequenzen bei Verstößen hinzuweisen. Außerhalb der hier beschriebenen Zwecke und des vereinbarten Verfahrens dürfen sie keine Detailinformationen aus den Protokollen an Vorgesetzte oder an die Personalabteilung weitergeben.

### § 7 Maßnahmen bei begründetem Verdacht

1. Zur Aufdeckung von Straftaten oder einer schweren arbeitsvertraglichen Verfehlung im Zusammenhang mit der privaten Nutzung des Internet wird nach Maßgabe des

§ 32 Abs. 1 Satz 2 BDSG verfahren. Geht es um eine missbräuchliche oder unerlaubte Nutzung der Internetdienste im Sinne einer schweren Verletzung der arbeitsvertraglichen Pflichten oder von Ordnungswidrigkeiten, so gilt § 32 Abs. 1 Satz 1 BDSG und nachfolgend § 7 Abs. 2 dieser Betriebsvereinbarung. Zu wahren ist dabei der Grundsatz der Datenvermeidung und Datensparsamkeit aus § 3 a BDSG und der Grundsatz der Verhältnismäßigkeit.

2. Bei dokumentierten tatsächlichen Anhaltspunkten für einen begründeten und konkreten Verdacht auf eine missbräuchliche oder unerlaubte Nutzung der Internetdienste oder auf Begehung einer Straftat, die sich aufgrund der anonymisierten Kontrollen gemäß § 6 dieser Betriebsvereinbarung ergeben, informiert der Systemadministrator die Personalabteilung. Weitere personenbezogene Überprüfungen wie z. B. Offenlegungen der IP-Adresse des benutzten Computers dürfen nur nach erfolgter Zustimmung sowohl des Betriebsrats als auch des betrieblichen Datenschutzbeauftragten und nach einer einvernehmlichen positiven Zulässigkeits- und Verhältnismäßigkeitsprüfung entsprechend § 32 Abs. 1 Satz 2 BDSG durch den IT-Systemadministrator unter Hinzuziehung des betrieblichen Datenschutzbeauftragten durchgeführt werden. Gegebenenfalls ist die zuständige Aufsichtsbehörde einzuschalten. Die Leitung der IT-Abteilung erstellt nach erfolgter Prüfung einen Bericht, der an den betrieblichen Datenschutzbeauftragten, die Interessenvertretung und die Personalabteilung geht.
3. Nach erfolgter Kontrolle ist der betroffene Beschäftigte von der Datenerhebung und -verwendung unverzüglich zu unterrichten. Sollte der Verdacht auf Missbrauch gegenstandslos werden, sind sämtliche Unterlagen (E-Mails, Tabellen, Ausdrucke usw.) zu vernichten. Die Ergebnisse der Prüfung dürfen nicht für andere Zwecke verwertet werden. Ist der Verdacht nicht ausgeräumt, ist der Ergebnisbericht dem Beschäftigten unverzüglich auszuhändigen. Der Betroffene ist anzuhören. Auf Wunsch des Betroffenen ist der Betriebsrat zur Anhörung hinzuzuziehen.
4. Die gesetzlichen Rechte des Betriebsrats nach dem Betriebsverfassungsrecht bleiben unberührt.
5. Die Firma XYZ behält sich vor, bei Verstößen gegen die Betriebsvereinbarung die private Nutzung der Internetdienste im Einzelfall zu untersagen.
6. Alle Maßnahmen und Informationen sind von allen Beteiligten vertraulich zu handhaben, insbesondere nicht der Belegschaft bekannt zu geben.

### § 8 Mitbestimmung, Öffnungsklausel

(1) Macht der Betriebsrat aufgrund der Erfahrungen mit dieser Vereinbarung geltend, dass die Bestimmungen dieser Betriebsvereinbarungen nicht ausreichen, um neue Kommunikationstechnik, weitere Leistungsmerkmale der vorhandenen Kommu-

nikationstechnik und zusätzliche mitbestimmungspflichtige Maßnahmen des Arbeitgebers im Zusammenhang mit E-Mail und Internet am Arbeitsplatz angemessen zu regeln, so ist in allen Einzelfällen vorher ein Einvernehmen mit dem Betriebsrat über Änderungen oder Ergänzungen der vorliegenden Betriebsvereinbarung erforderlich.

### § 9 Beweisverwertungsverbot

(1) Werden Informationen z. B. aus den Protokolldateien unter Verletzung der Bestimmungen dieser Betriebsvereinbarung gewonnen, weiterverarbeitet und verwendet, dürfen diese zur Begründung personeller und arbeitsrechtlicher Maßnahmen nicht verwertet werden und unterliegen einem Beweisverwertungsverbot. Dies gilt auch für Ermittlungsergebnisse, die unter Verstoß gegen diese Betriebsvereinbarung rechtswidrig zustande gekommen sind. Sie dürfen durch den Arbeitgeber nicht zum Gegenstand einer Sanktion oder eines gerichtlichen Verfahrens gemacht werden.

### § 10 Schlussbestimmungen

- (1) Diese Betriebsvereinbarung tritt mit ihrer Unterzeichnung in Kraft.
- (2) Sie kann mit einer Frist von drei Monaten zum Jahresende gekündigt werden. Nach Ablauf der Kündigungsfrist wirkt die Betriebsvereinbarung nach.

(3) Nach der Kündigung sind unverzüglich Verhandlungen über den Abschluss einer neuen Betriebs-/Dienstvereinbarung aufzunehmen. Unberührt davon bleiben die jederzeitigen einvernehmlichen Änderungen.

(4) Allen Beschäftigten wird diese Betriebsvereinbarung durch die Informationsmedien der Firma XYZ bekannt gemacht.

(5) Bei Meinungsverschiedenheiten kann jede Partei die Einigungsstelle anrufen.

(6) Sollte eine Vorschrift dieser Vereinbarung nicht dem geltenden Recht und dem gültigen Tarifvertrag entsprechen und deshalb unwirksam sein, behalten die übrigen Bestimmungen ihre Gültigkeit. Rechtsunwirksame Vorschriften werden durch die Parteien in vertrauensvoller Zusammenarbeit durch eine rechtskonforme Vorschrift ersetzt, die dem angestrebten Regelungsziel am nächsten kommt.

## EINWILLIGUNGSERKLÄRUNG: EINWILLIGUNG IN KONTROLLEN BEI DER PRIVATEN NUTZUNG DES INTERNET

Ich bin damit einverstanden, dass meine private Nutzung bzw. die Kommunikation per Internet von der Firma XYZ in dem Rahmen protokolliert und kontrolliert werden kann, den die Betriebsvereinbarung zu „E-Mail und Internet am Arbeitsplatz“ vom ##.##.#### allen Beschäftigten vorgibt.

Ich bin darauf hingewiesen worden, dass meine Verkehrsdaten der Internetnutzung (Zeitraum, Adressen von Absender/Empfänger und Anzahl/Häufigkeit der Aufrufe von Webseiten) protokolliert werden.

Ich bin über die Art, die Zweckbestimmung der erhobenen, verarbeiteten und genutzten personenbezogenen Daten und die gegebenenfalls durchgeführte Auswertung und darüber, dass die Daten ausschließlich zur Gewährleistung der Systemsicherheit im Sinne des § 31 BDSG genutzt werden, vom betrieblichen Datenschutzbeauftragten ausreichend informiert worden.

Ich bin darüber unterwiesen worden, dass die protokollierten Daten längstens 3 Monate aufbewahrt werden und zusätzlich für präventive stichprobenartige Kontrollen und bei tatsächlichen Anhaltspunkten für einen Missbrauch auch personenbezogen gemäß §§ 6 und 7 dieser Betriebsvereinbarung ausgewertet werden. Ich stimme zu, dass in einem solchen Fall die Daten an befugte und benannte Personen und Stellen im Unternehmen weitergegeben werden dürfen.

*Mein vorstehendes Einverständnis kann ich jederzeit widerrufen. Es gilt dann die folgende Regelung:*

*Ich bin nicht mit einer Kontrolle meiner privaten Nutzung/Kommunikation per Internet einverstanden. Ich bin darüber informiert worden, dass mir in diesem Fall eine private Nutzung des Internet nicht gestattet ist.*

*Der Mitarbeiter stimmt durch Unterschrift der Protokollierung und den Kontrollen in dem von der Betriebsvereinbarung dargelegten Rahmen zu.*