

Datenschutzrechtliche Grundsätze bei der dienstlichen/privaten Internet- und E-Mail-Nutzung am Arbeitsplatz

Stand: März 2003

1 Einführung

Der vorliegende Leitfaden zum datenschutzgerechten Umgang mit personenbezogenen Daten bei der Nutzung von Internet- und E-Mail-Diensten am Arbeitsplatz ist in erster Linie für den Bereich der Bundesverwaltung konzipiert. Die dabei entwickelten Grundsätze lassen sich darüber hinaus auch auf die datenschutzrechtliche Ausgestaltung der Nutzung von Informations- und Kommunikationsdiensten durch Beschäftigte in der sonstigen öffentlichen Verwaltung sowie in der Privatwirtschaft übertragen.

Immer mehr Beschäftigten wird der Zugang zum Internet als ein Arbeitsmittel zur Verfügung gestellt. Um diesen Dienst technisch zu ermöglichen, darf der Dienstherr die hierfür erforderlichen personenbezogenen Daten der Beschäftigten verarbeiten. Einige der anfallenden Daten werden auch zur Gewährleistung der Datensicherheit des Netzes benötigt und dürfen zu diesem Zweck in den entsprechenden Protokolldateien vorübergehend gespeichert werden. Ein darüber hinausgehendes Interesse an einer Kenntnisnahme und Auswertung der Daten wird oftmals damit begründet, dass der Dienstherr sich vor dem Verrat von Dienstgeheimnissen schützen müsse und insbesondere Zugriffe der Beschäftigten auf illegale Inhalte und deren Kopie auf den Behördenrechner verhindern wolle. Schließlich hat der Dienstherr ein berechtigtes Interesse daran zu kontrollieren, ob ein Verbot der privaten Nutzung befolgt wird bzw. eine erlaubte private Nutzung sich in dem vorgesehenen Rahmen bewegt.

Damit ergeben sich vielfältige Fragen zur Wahrung der Privatsphäre der betroffenen Mitarbeiter. Je nach der konkreten Ausgestaltung der Nutzungsmöglichkeiten sind die Vorschriften des Teledienstedatenschutzgesetzes (TDDSG), des Telekommunikationsgesetzes (TKG), der Telekommunikations-Datenschutzverordnung (TDSV) sowie des Bundesdatenschutzgesetzes (BDSG) zu beachten. Soweit im Einzelfall Dienstvereinbarungen vorliegen, sind auch diese zu berücksichtigen.

Bei der Beurteilung, ob und inwieweit der Dienstherr die Beschäftigten anhand der Verbindungs- und Nutzungsdaten kontrollieren und überwachen darf, ist es von Bedeutung, ob den Bediensteten neben der dienstlichen auch die private Nutzung des Internet am Arbeitsplatz gestattet wird. Abhängig davon finden die allgemeinen oder die bereits angesprochenen Datenschutzregelungen im Bereich der Tele- und Telekommunikationsdienste Anwendung.

Im Falle der nur dienstlichen Nutzung besteht zwischen Dienstherrn und Beschäftigten kein Anbieter-Nutzer-Verhältnis, da es sich bei der Bereitstellung der Dienste nicht um ein Angebot von Telekommunikation und Telediensten i.S. des Telekommunikationsgesetzes bzw. des Teledienstegesetzes handelt. Die Rechtmäßigkeit einer Verarbeitung personenbezogener Daten richtet sich nach den Vorschriften des BDSG. Danach ist eine Abwägung der Interessen beider Seiten im Hinblick auf die Erforderlichkeit und Verhältnismäßigkeit der vorgesehenen Datenverarbeitung vorzunehmen. Hierbei sind auch verfassungsrechtliche Vorgaben zu berücksichtigen, da Kontrollmaßnahmen durch den Dienstherrn das Recht des Beschäftigten auf informationelle Selbstbestimmung tangieren, d.h. einen Eingriff in die Grundrechte des Beschäftigten darstellen. Denn auch wenn sich der Beschäftigte dem Direktionsrecht seines Dienstherrn unterwirft, kann er sich doch auf seine Grundrechtspositionen berufen.

Als Ergebnis dieser Abwägung ist eine Totalüberwachung und damit eine Vollkontrolle der Beschäftigten im Hinblick auf die Internet-Nutzung unverhältnismäßig und somit datenschutzrechtlich unzulässig. Zur Wahrung der o.g. Interessen des Dienstherrn kann eine regelmäßige stichprobenhafte und auch zeitnahe Auswertung der Protokolldaten als erforderlich und verhältnismäßig betrachtet werden. Soweit diese Daten für Zwecke der Datensicherheit verarbeitet werden, unterliegen sie jedoch der besonderen Zweckbindung des § 14 Abs. 4 BDSG, d.h. sie dürfen für keine anderen Zwecke verwendet werden. Daher müssten Protokolldaten, die der Kontrolle dienen sollen, ob die dienst-/arbeitsrechtlichen Vorgaben für die Nutzung von Internetdiensten eingehalten werden, eigens für diesen Zweck erhoben werden. Die Zulässigkeit richtet sich dann gem. § 12 Abs. 4 BDSG nach § 28 Abs. 1 BDSG. Da diese Daten mit den für die Datensicherheit erhobenen Daten identisch sind, kann jedoch von einer doppelten Datenerhebung abgesehen werden.

Hat der Dienstherr die private Nutzung des Internet erlaubt, so gelten die Vorschriften des Telekommunikationsgesetzes und der Telekommunikations-Datenschutzverordnung bzw. die Regelungen des Teledienstedatenschutzgesetzes, da der Dienstherr in diesem Fall seinen Beschäftigten gegenüber die Funktion eines Telekommunikations- bzw. Telediensteanbieters wahrnimmt. Als solcher hat er das Fernmeldegeheimnis nach § 85 TKG zu beachten. Der Erlaubnisrahmen für die Verarbeitung der Verbindungs-, Nutzungs- und Abrechnungsdaten ist sehr eng gesteckt. Allgemein gesagt, dürfen die genannten Daten nur verarbeitet und genutzt werden, soweit dies für die Erbringung und Abrechnung der Dienste erforderlich ist.

Die sich aus der Rechtslage ergebenden unterschiedlichen Konsequenzen für die Durchführung von Kontrollmaßnahmen stellen den Dienstherrn - will er die private Nutzung des Internet grundsätzlich erlauben - in der Praxis vor das Problem, die

dienstliche von der privaten Nutzung abgrenzen zu müssen. Lösungsmodelle, die von zwei user accounts ausgehen, erfordern nicht nur zusätzlichen Administrationsaufwand. Sie erscheinen auch angesichts der „Natur“ des Internet unrealistisch. Da der Dienstherr andererseits aber nicht verpflichtet ist, die private Nutzung des Internet zu gestatten, und ein berechtigtes Interesse daran hat, Missbrauch oder strafbare Handlungen nicht nur im dienstlichen Bereich, sondern auch bei der privaten Nutzung des dienstlichen Internet-Zugangs zu unterbinden, kann er die Erlaubnis der privaten Nutzung an bestimmte Bedingungen hinsichtlich des Zeitrahmens, der zugelassenen Bereiche und regelmäßig durchzuführender Kontrollen knüpfen.

Eine praktikable und aus Datenschutzsicht vertretbare Lösung geht davon aus, keine technische Trennung der Verbindungs-/Nutzungsdaten nach dienstlicher und privater Nutzung vorzunehmen und dadurch die bei der privaten Nutzung anfallenden Daten in die o.g. Kontrollmaßnahmen für den Bereich der dienstlichen Nutzung einzubeziehen. Entsprechende Regelungen sollten in einer Dienstvereinbarung unter Beteiligung des behördlichen Beauftragten für den Datenschutz festgelegt werden, deren Kenntnisnahme jeder Beschäftigte schriftlich bestätigen sollte. Eine individuelle Einwilligung in die Verarbeitung der bei der privaten Nutzung anfallenden Daten ist dann nicht erforderlich. Denn sobald der Beschäftigte in Kenntnis der Regelungen das Internet privat nutzt, liegt seine Einwilligung konkludent in seinem Verhalten, d.h. wenn er die Kontrollmaßnahmen nicht akzeptieren will, muss er die private Nutzung unterlassen. Dass der Dienstherr von der konkludenten Einwilligung des einzelnen Beschäftigten durch private Nutzung ausgehen kann, setzt aber unbedingt voraus, dass der Beschäftigte umfassend über die Bedingungen und Kontrollen bei der privaten Nutzung informiert ist.

2 Grundsätze im Überblick

2.1 Allgemeines

- Bei der Nutzung von E-Mail und anderen Internetdiensten durch die Beschäftigten sind die eingesetzten Verfahren entsprechend dem Grundsatz von Datenvermeidung und Datensparsamkeit technisch so zu gestalten, dass von vornherein so wenige personenbezogene Daten wie möglich verarbeitet werden. Hierzu sind datenschutzfreundliche Verfahren einzusetzen. Ebenso ist die Kontrolle der Nutzung dieser Dienste durch den Arbeitgeber so zu gestalten, dass sie zunächst ohne, zumindest aber mit so wenigen personenbezogenen Daten wie möglich durchgeführt wird. Dabei sind präventive Maßnahmen gegen unbefugte Nutzung, wie z. B. Positivlisten erlaubter Internet-Adressen, nachträglichen Kontrollen vorzuziehen.

- Um Art und Umfang der Verarbeitung ihrer personenbezogenen Daten nachvollziehen zu können, sind die Bediensteten gemäß § 3 Abs. 5 TDSV bzw. § 4 Abs. 1 TDDSG umfassend darüber zu informieren (Grundsatz der Transparenz).

2.2 Dienstliche Nutzung

- Gestattet der Dienstherr die Nutzung von E-Mail und anderen Internetdiensten ausschließlich zu dienstlichen Zwecken, ist er nicht Anbieter im Sinne des Telekommunikations- (vgl. § 2 Nr. 2 TDSV) bzw. Teledienstrechts (vgl. § 1 Abs. 1 Nr. 1 TDDSG). Die Erhebung und Verarbeitung von Daten über das Nutzungsverhalten der Beschäftigten richtet sich in diesen Fällen nach den Vorschriften des Bundesdatenschutzgesetzes.
- Der Dienstherr hat grundsätzlich das Recht, stichprobenartig zu prüfen, ob die Internet-Nutzung der Beschäftigten dienstlicher Natur ist. Eine automatisierte Vollkontrolle durch den Dienstherrn ist als schwerwiegender Eingriff in das Persönlichkeitsrecht der Beschäftigten hingegen nur bei konkretem Missbrauchsverdacht im Einzelfall zulässig. Es wird empfohlen, eine Dienstvereinbarung abzuschließen, in der die technischen und organisatorischen Fragen der Protokollierung und Auswertung eindeutig geregelt werden.
- Soweit die Nutzung von E-Mail und Internetdiensten zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherung des ordnungsgemäßen Betriebes der Verfahren protokolliert wird, dürfen diese Daten nach dem BDSG und den einschlägigen dienstrechtlichen Bestimmungen nur zu diesen Zwecken genutzt werden. Eine Verwertung zur Verhaltens- und Leistungskontrolle der Beschäftigten ist unzulässig.

2.3 Private Nutzung

- Der Dienstherr ist nicht verpflichtet, den Beschäftigten die private Nutzung des Internet zu erlauben. Entschließt er sich dazu, ist es grundsätzlich zulässig, diese Erlaubnis an einschränkende Voraussetzungen zu knüpfen (z. B. eine angemessene Art der Kontrolle durchzuführen).
- Wenn ein Dienstherr den Beschäftigten die private Nutzung von Internetdiensten oder E-Mail erlaubt, ist er ihnen gegenüber Telekommunikations- bzw. Telediensteanbieter. Ein vom Dienstherrn beauftragter Zugangsanbieter ist zwar diesem gegenüber Telekommunikations- bzw. Telediensteanbieter. Gegenüber den privat nutzenden Beschäftigten sind die Provider aber lediglich Auftragnehmer des dann als Anbieter zu qualifizierenden Dienstherrn.

- Es gelten die Regelungen des Telekommunikationsgesetzes und der Telekommunikations-Datenschutzverordnung sowie des Teledienststedatenschutzgesetzes. Abweichungen davon zu Lasten der Beschäftigten sind nur mit deren individueller Einwilligung gem. § 4a BDSG zulässig.
- Der Dienstherr ist den Beschäftigten gegenüber zur Einhaltung des Telekommunikationsgeheimnisses verpflichtet. Daher sollten die gleichen Regeln wie beim privaten Telefonieren angewendet werden.
- Der Umfang der privaten Nutzung, ihre Bedingungen sowie die Kontrolle, ob diese Bedingungen eingehalten werden, müssen – am sinnvollsten durch Dienstvereinbarung oder -anweisung – geregelt werden. Die Bestimmungen des Personalvertretungsrechts sind dabei zu beachten.
- Eine Protokollierung darf ohne Einwilligung nur erfolgen, wenn sie zu Zwecken der Datenschutzkontrolle, der Datensicherung, zur Sicherung des ordnungsgemäßen Betriebs oder zu Abrechnungszwecken erforderlich ist.

2.4 Besonderheiten bei E-Mail

- Von ein- und ausgehenden dienstlichen E-Mails seiner Beschäftigten darf der Dienstherr im selben Maße Kenntnis nehmen wie von deren dienstlichem Schriftverkehr. Beispielsweise kann der Vorgesetzte verfügen, dass ihm jede ein- oder ausgehende E-Mail seiner Mitarbeiter zur Kenntnis zu geben ist.
- Aus Gründen der Datensicherheit dürfen Teilinhalte oder Anlagen von E-Mails unterdrückt werden, die gefährlichen oder verdächtigen ausführbaren Code enthalten (also insbesondere Mail-bodies oder E-Mails mit ausführbarem Code oder Dateien mit den Erweiterungen .exe, .bat, .com).
- Private E-Mails sind wie private schriftliche Post zu behandeln. So sind eingehende private, aber fälschlich als Dienstpost behandelte E-Mails den betreffenden Mitarbeitern unverzüglich nach Bekanntwerden ihres privaten Charakters zur alleinigen Kenntnis zu geben.
- Der Dienstherr sollte entweder für die Beschäftigten separate E-Mail-Adressen zur privaten Nutzung einrichten oder – falls privates Surfen erlaubt ist – sie auf die Nutzung eines (kostenlosen) Web-Mail-Dienstes verweisen.
- Wie bei der dienstlichen Nutzung dürfen aus Gründen der Datensicherheit eingegangene private E-Mails oder deren Anhänge unterdrückt werden, wenn sie ein Format aufweisen, das ausführbaren Code enthalten kann. Die Verfahrensweise ist den Mitarbeitern zuvor in Form einer Dienstvereinbarung bekanntzugeben. Generell ist der betreffende Mitarbeiter darüber zu unterrichten, wenn eine an ihn

gerichtete oder von ihm abgesendete E-Mail ganz oder teilweise unterdrückt wird oder virenverseucht ist. Eine Untersuchung von virenverseuchten E-Mails mit Kenntnisnahme des Inhalts, etwa durch den Systemadministrator, ist nur unter Einbeziehung des betreffenden Mitarbeiters zulässig. Eine darüber hinausgehende inhaltliche Kontrolle ist nicht zulässig.

3 Protokollierung des Internet-Zugangs

Der Zugriff des einzelnen Beschäftigten auf das Internet kann durch den Proxy Server / Web Server einer Behörde umfänglich protokolliert und ausgewertet werden. Aus diesen Protokollen können nicht nur die Benutzeridentifikation (IP-Adresse, Ethernet-Adresse), Datum und Uhrzeit des Zugriffs sowie die übertragene Datenmenge hervorgehen, sondern vor allem auch die Zieladresse des Zugriffs, d.h. anhand des Protokolls wäre genau nachvollziehbar, wer wann was gelesen hat. Dies kann einen Eingriff in die Persönlichkeitsrechte der Beschäftigten darstellen.

Bei den meisten verwendeten Servern ist es möglich, im einzelnen festzulegen, was konkret protokolliert wird. Es ist daher in einem ersten Schritt zu prüfen, ob ein alle Einzelheiten umfassendes Protokoll überhaupt bzw. welche Angaben unbedingt erforderlich sind.

Folgende Grundsätze sind dabei zu beachten:

- Der Umfang der Protokolldaten muss festgelegt und den Beschäftigten bekannt gegeben werden (z. B. Datum, Uhrzeit, Rechner- oder Benutzerkennung, Fehlercode, Anzahl der übertragenen Bytes, Rechner- oder Benutzeridentifikation, eventuell Zieladresse des angeforderten Dokuments, Fehlercode der Übertragung).
- Die Verwendung der Protokolldaten muss an genau definierte Zwecke gebunden werden, so zum Beispiel zur Aufrechterhaltung der Systemsicherheit, zur Analyse und Korrektur technischer Fehler im Netz, zur Optimierung der Rechnerleistungen im Netzwerk, zur Ermittlung der Kosten verbrauchter Ressourcen zwecks interner Leistungsverrechnung sowie zur Kontrolle der Einhaltung dienst-/arbeitsrechtlicher Vorgaben.
- Der Zugriff auf die Protokolldaten muss auf das technische Personal begrenzt bleiben, das für den Netzwerkbetrieb und die Bereitstellung der verfügbaren Services zuständig ist. Diese Personen sind verpflichtet, sich an die beschriebene (und ihnen bekannt gegebene) Zweckbindung zu halten und außerhalb der beschriebenen Zwecke keine Detailinformationen aus den Protokollen weiterzugeben.

- Die Speicherdauer der Protokolldateien wird so kurz gehalten, wie dies zur Erfüllung der beschriebenen Zwecke erforderlich ist.
- In begründeten Fällen von Missbrauch oder beim Verdacht strafbarer Handlungen kann eine weitergehende Einsicht in die Protokolldaten vorgenommen werden. Dabei sollte ein Verfahren gewählt werden, das die betroffene Person von dem Verdacht in Kenntnis setzt und die zuständige Personalvertretung einbezieht.
- Um die Einhaltung der genannten Regelungen durch den Dienstherrn bzw. seinen Beauftragten zwingend zu machen, kann ein "Beweisverwertungsverbot" verabredet werden, wonach Informationen aus den Protokolldateien, die unter Verletzung der vorgenannten Regelungen gewonnen oder weiterverarbeitet wurden, zur Begründung personeller Maßnahmen nicht verwertet werden dürfen.
- Der Personalvertretung kann das Recht zugesichert werden, in Fällen begründeten Missbrauchs durch den Dienstherrn bzw. seinen Beauftragten technische Sicherungsvorkehrungen zu verlangen, die die Beteiligung der Personalvertretung technisch sicherstellen und die durch die Administration vorgenommenen Zugriffe elektronisch protokollieren.

4 Musterdienstvereinbarung:

**Dienstvereinbarung
zwischen
dem Bundesministerium____
und
dem Personalrat im Bundesministerium____
über die Nutzung elektronischer Kommunikationssysteme
am Arbeitsplatz**

Das Bundesministerium _____ und der Personalrat im Bundesministerium _____ schließen nach § 73 in Verbindung mit § 75 Abs. 3 Nr. 17 und § 76 Abs. 2 des Bundespersonalvertretungsgesetzes die folgende Dienstvereinbarung über die Nutzung elektronischer Kommunikationssysteme am Arbeitsplatz:

§ 1

Gegenstand und Geltungsbereich

Diese Vereinbarung regelt die Grundsätze für den Zugang und die Nutzung der Internetdienste im Bundesministerium _____ und gilt für alle Beschäftigten, deren Arbeitsplätze über einen Internetzugang verfügen.

§ 2

Zielsetzung

Ziel dieser Vereinbarung ist es, die Nutzungsbedingungen sowie die Maßnahmen zur Protokollierung und Kontrolle transparent zu machen, die Persönlichkeitsrechte der Beschäftigten zu sichern und den Schutz ihrer personenbezogenen Daten zu gewährleisten.

§ 3

Nutzung

(1) Der Internet-Zugang steht den Beschäftigten als Arbeitsmittel im Rahmen der Aufgabenerfüllung zur Verfügung und dient insbesondere der Verbesserung der internen und externen Kommunikation, der Erzielung einer höheren Effizienz und der Beschleunigung der Informationsbeschaffung und der Arbeitsprozesse.

(2) Die private Nutzung im geringfügigen Umfang ist zulässig, soweit die dienstliche Aufgabenerfüllung sowie die Verfügbarkeit des IT-Systems für dienstliche Zwecke nicht beeinträchtigt werden und haushaltsrechtliche Grundsätze dem nicht entgegenstehen. Privater eMail-Verkehr darf nur über die kostenlosen Web-Mail-Dienste abgewickelt werden. Das Abrufen von kostenpflichtigen Informationen für den Privatgebrauch ist unzulässig. Im Rahmen der privaten Nutzung dürfen keine kommerziellen oder sonstigen geschäftlichen Zwecke verfolgt werden.

(3) Eine Unterscheidung von dienstlicher und privater Nutzung auf technischem Weg erfolgt nicht. Die Protokollierung und Kontrolle gemäß §§ 6 und 7 dieser Vereinbarung erstrecken sich auch auf den Bereich der privaten Nutzung des Internetzugangs.

(4) Durch die private Nutzung des Internetzugangs erklärt der Beschäftigte seine Einwilligung in die Protokollierung und Kontrolle gemäß §§ 6 und 7 dieser Vereinbarung für den Bereich der privaten Nutzung.

§ 4

Verhaltensgrundsätze

(1) Grundsätzlich gelten die Regelungen der „Dienstanweisung für die Nutzung des IT-Systems im Bundesministerium _____“.

(2) Unzulässig ist jede absichtliche oder wissentliche Nutzung des Internet, die geeignet ist, den Interessen der Dienststelle oder deren Ansehen in der Öffentlichkeit zu schaden, die Sicherheit des Behördennetzes zu beeinträchtigen oder die gegen geltende Rechtsvorschriften und die Dienstanweisung für die Nutzung des IT-Systems gemäß Absatz 1 verstößt. Dies gilt vor allem für

- das Abrufen oder Verbreiten von Inhalten, die gegen persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstoßen,
- das Abrufen oder Verbreiten von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, sexistischen, gewaltverherrlichenden oder pornografischen Äußerungen oder Abbildungen.

(3) Zur Überprüfung der Einhaltung der Regelungen dieser Vereinbarung werden regelmäßige nicht-personenbezogene Stichproben in den Protokolldateien durchgeführt (vgl. § 6 Abs. 3). Ergänzend wird eine Übersicht über das jeweilige Gesamtvolumen des ein- und ausgehenden Datenverkehrs erstellt.

(4) Die bei der Nutzung der Internetdienste anfallenden personenbezogenen Daten werden nicht zur Leistungs- und Verhaltenskontrolle verwendet. Sie unterliegen der Zweckbindung dieser Vereinbarung und den einschlägigen datenschutzrechtlichen Vorschriften.

§ 5

Information und Schulung der Beschäftigten

Die Beschäftigten werden durch die Dienststelle über die besonderen Datensicherheitsprobleme bei der Nutzung der elektronischen Kommunikationssysteme unterrichtet. Sie werden für den sicheren und wirtschaftlichen Umgang mit diesen Systemen qualifiziert und über die einschlägigen Rechtsvorschriften informiert.

§ 6

Protokollierung und Kontrolle

(1) Die Verbindungsdaten für den Internet-Zugang werden mit Angaben von

- Datum / Uhrzeit,

- Adressen von Absender und Empfänger und
- übertragener Datenmenge

protokolliert.

(2) Die Protokolle nach Absatz 1 werden ausschließlich zu Zwecken der

- Analyse und Korrektur technischer Fehler
- Gewährleistung der Systemsicherheit
- Optimierung des Netzes
- statistischen Feststellung des Gesamtnutzungsvolumens
- Stichprobenkontrollen gemäß Absatz 3 und
- Auswertungen gemäß § 7 dieser Vereinbarung (Missbrauchskontrolle)

verwendet.

(3) Die Protokolle werden durch einen von der Behördenleitung schriftlich beauftragten Mitarbeiter regelmäßig stichprobenhaft hinsichtlich der aufgerufenen Websites, aber nicht personenbezogen gesichtet und ausgewertet. Die Auswertung der Übersicht des Gesamtdatenvolumens erfolgt monatlich ebenfalls durch diesen Mitarbeiter. Der behördliche Datenschutzbeauftragte wird beteiligt, wenn er dies wünscht.

(4) Der Zugriff auf die Protokolldateien für die Zwecke der Erstellung der Übersicht, der Durchführung der nicht-personenbezogenen Stichproben und der jeweiligen Auswertung ist auf den von der Behördenleitung beauftragten Mitarbeiter begrenzt. Dieser hat eine entsprechende Verpflichtungserklärung zum Datenschutz unterschrieben. Darüber hinaus ist er hinsichtlich der Einhaltung des Fernmeldegeheimnisses und des Datenschutzes auf die strafrechtlichen Konsequenzen bei Verstößen hingewiesen worden.

(5) Die Protokolldaten werden nach einer Woche automatisch gelöscht.

§ 7

Maßnahmen bei Verstößen / Missbrauchsregelung

(1) Bei Verdacht auf missbräuchliche/unerlaubte Nutzung des Internetzugangs gemäß §§ 3 und 4 dieser Vereinbarung durch einen Mitarbeiter erfolgt unter Beteiligung des behördlichen Datenschutzbeauftragten eine Überprüfung durch eine von der Behördenleitung einzusetzende Untersuchungsgruppe, der auch der nach § 6 Abs. 3 beauftragte Mitarbeiter angehört. Sie veranlasst gegebenenfalls weitere Untersuchungsmaßnahmen (z.B. Offenlegung der IP-Adresse des benutzten PC's oder wei-

tere Überprüfungen). Auf der Basis dieser Untersuchung erstellt sie einen Bericht, der dem Betroffenen ausgehändigt wird. Dieser ist anschließend dazu zu hören.

(2) Im übrigen gelten die einschlägigen Regelungen des Disziplinar- bzw. Tarifrechts.

(3) Ist aufgrund der stichprobenhaften nicht-personenbezogenen Kontrollen bzw. der Auswertung der Übersicht des Datenvolumens eine nicht mehr tolerierbare Häufung von offensichtlich privater Nutzung des Internetzugangs zu erkennen, so werden innerhalb von einer zu setzenden Frist von 2 Wochen die Stichproben weiterhin nicht-personenbezogen durchgeführt. Ergeben diese Stichproben bzw. die Auswertung der Übersicht des Datenvolumens keine Änderung im Nutzungsverhalten, so werden die Protokolle der folgenden 2 Wochen durch eine Untersuchungsgruppe stichprobenhaft personenbezogen ausgewertet. Hierbei wird wie im Falle des Verdachts einer missbräuchlichen Nutzung (Abs. 1) vorgegangen. Zu den Verfahren nach Satz 1 und Satz 2 erfolgt eine entsprechende vorherige schriftliche Mitteilung an alle Beschäftigten.

(4) Ein Verstoß gegen diese Dienstvereinbarung kann neben den dienst- und arbeitsrechtlichen Folgen auch strafrechtliche Konsequenzen haben.

(5) Die Dienststellenleitung behält sich vor, bei Verstößen gegen diese Vereinbarung die private Nutzung des Internetzugangs im Einzelfall zu untersagen.

§ 8

Änderungen und Erweiterungen

(1) Geplante Änderungen und Erweiterungen an den elektronischen Kommunikationssystemen werden der Personalvertretung und dem behördlichen Beauftragten für den Datenschutz mitgeteilt. Es wird dann geprüft, ob und inwieweit sie sich auf die Regelungen dieser Vereinbarung auswirken. Notwendige Änderungen oder Erweiterungen zu dieser Vereinbarung können im Einvernehmen in einer ergänzenden Regelung vorgenommen werden.

(2) Zur Evaluierung dieser Dienstvereinbarung ist nach Ablauf von zwei Jahren ein Erfahrungsbericht vorzulegen.

§ 9

Schlussbestimmungen

(1) Diese Vereinbarung tritt mit ihrer Unterzeichnung in Kraft. Sie kann mit einer Frist von drei Monaten zum Monatsende, frühestens jedoch zum _____ gekündigt wer-

den. Im Falle einer Kündigung bleibt sie bis zum Abschluss einer neuen Vereinbarung gültig.

(2) Jeder Mitarbeiter bestätigt schriftlich die Kenntnisnahme. Ein Abdruck der Vereinbarung wird ihm zusammen mit einer Kopie der Bestätigung ausgehändigt.