

Datenschutzgerechte Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz

Orientierungshilfe

des Arbeitskreises Medien¹ der Ständigen Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Stand: 24. September 2007

Viele Beschäftigte im öffentlichen Dienst haben heute die Möglichkeit, das Internet auch am Arbeitsplatz zu nutzen. Öffentliche Stellen des Bundes und der Länder haben beim Umgang mit den dabei anfallenden personenbezogenen Daten der Beschäftigten, ihrer Kommunikationspartner und anderer Betroffener (beispielsweise Dritter, deren Namen in einer E-Mail genannt werden) bestimmte datenschutzrechtliche Anforderungen zu beachten, die davon abhängen, ob den Bediensteten neben der dienstlichen die private Nutzung des Internet am Arbeitsplatz gestattet wird. E-Mail und andere Internetdienste sind geeignet, das Verhalten und die Leistung der Beschäftigten zu überwachen. Die Orientierungshilfe stellt die bei der Nutzung dieser Dienste geltenden datenschutzrechtlichen Anforderungen dar.

I. Allgemeines

- a. Bei der Nutzung von E-Mail und anderen Internetdiensten durch die Beschäftigten sind die eingesetzten Verfahren technisch so zu gestalten, dass von vornherein so wenige personenbezogene Daten wie möglich verarbeitet werden (Grundsatz von Datenvermeidung und Datensparsamkeit). Hierzu bietet es sich an, 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 nachträglichen Kontrollen vorzuziehen.
- b. Die Bediensteten sind mit den technischen Möglichkeiten vertraut zu machen, wie die eingesetzten Verfahren datenschutzgerecht angewendet werden können. Um Art und Umfang der Verarbeitung ihrer personenbezogenen Daten nachvollziehen zu können, sind die Bediensteten umfassend darüber zu informieren (Grundsatz der Transparenz).

¹ Die Orientierungshilfe wurde unter Beteiligung des AK Personalwesen erstellt. Sie richtet sich in erster Linie an öffentliche Stellen des Bundes und der Länder. Die hier dargestellten Grundsätze können auch auf den nicht-öffentlichen Bereich übertragen werden.

² Zur Vereinfachung bezeichnet „Arbeitgeber“ sowohl den Arbeitgeber als auch den öffentlich-rechtlichen Dienstherren.

- c. Es sind geeignete Maßnahmen zu treffen, um die Vertraulichkeit und Integrität der Kommunikation zu gewährleisten. Insbesondere sollte jeder internetfähige PC mit leicht bedienbarer, auch bei den Kommunikationspartnern vorhandener Verschlüsselungssoftware ausgestattet sein, um zu verhindern, dass aus Bequemlichkeit personenbezogene oder andere sensible Daten unverschlüsselt übertragen werden.
- d. Automatisierte zentrale und wegen einer Verschlüsselung auch lokale Virenchecks sind notwendig. Um aktive Inhalte zu überprüfen, empfiehlt sich der Einsatz von lokaler Sandbox-Software.
- e. Es gibt eine Vielzahl an Möglichkeiten zur Abwehr unerwünschter Nachrichten (Spam), die in verschiedensten Kombinationen und Ausprägungen eingesetzt werden können. Welche Maßnahmen dafür grundsätzlich in Betracht kommen, kann etwa der Anti-Spam-Studie des BSI³ entnommen werden. Die auf dieser Grundlage denkbaren Lösungen unterscheiden sich sowohl hinsichtlich ihrer Eignung als auch hinsichtlich des Ausmaßes, in dem sie in die Persönlichkeitsrechte der Kommunikationspartner oder Dritter eingreifen. Daher sollte jede Stelle, bevor sie Maßnahmen zur Spam-Abwehr ergreift, eine schriftliche Konzeption hierfür erstellen, der zu entnehmen ist, dass unter den in Betracht kommenden Varianten die datenschutzfreundlichste gewählt wurde.

Die Konzeption sollte dabei folgenden Grundsätzen Rechnung tragen:

- Filter, die Header oder Inhalt elektronischer Post automatisch auf unerwünschte Nachrichten (Spam) prüfen, sollten erst an einem Punkt eingesetzt werden, der außerhalb der Reichweite des Fernmeldegeheimnisses liegt.
- Die (zentrale) Markierung spamverdächtiger Nachrichten ist dabei der zentralen Löschung von E-Mails ohne Kenntnis des Empfängers vorzuziehen.
- Um Verletzungen von Vertraulichkeit und Integrität zu vermeiden, sollten die Empfänger der Nachrichten in größtmöglicher Autonomie über den Umgang mit den an sie gerichteten E-Mails selbst entscheiden können.

II. Dienstliche Nutzung

- a. Gestattet der Arbeitgeber die Nutzung von E-Mail und Internet ausschließlich zu dienstlichen Zwecken, ist er nicht Anbieter im Sinne des Telekommunikations- (TK-) bzw. Telemedienrechts (vgl. § 11 Abs. 1 Nr. 1 Telemediengesetz, TMG); die Erhebung und Verarbeitung von Daten über das Nutzungsverhalten der Beschäftigten richtet sich in diesen Fällen nach den jeweils einschlägigen, am Erforderlichkeitsmaßstab orientierten Vorschriften des Beamtenrechts sowie des BDSG bzw. der Landesdatenschutzgesetze.
- b. Der Arbeitgeber hat grundsätzlich das Recht, stichprobenartig zu prüfen, ob das Surfen bzw. E-Mail-Versenden der Beschäftigten dienstlicher Natur ist. Eine automatisierte Vollkontrolle durch den Arbeitgeber ist als schwerwiegender Eingriff in das Persönlichkeitsrecht der Beschäftigten hingegen nur bei konkretem Missbrauchsverdacht im Einzelfall zulässig. Es wird empfohlen über die Nutzung von E-Mail und Internet eine Dienstvereinbarung mit dem Personalrat abzuschließen, in der die Fragen der Protokol-

³ www.bsi.de/literat/studien/antispam/antispam.pdf

lierung, Auswertung und Durchführung von Kontrollen eindeutig geregelt werden. Auf mögliche Überwachungsmaßnahmen und in Betracht kommende Sanktionen sind die Beschäftigten hinzuweisen.

- c. Bei Beschäftigten, denen in ihrer Tätigkeit persönliche Geheimnisse anvertraut werden und die deshalb in einem besonderen Vertrauensverhältnis zu den betroffenen Personen stehen, muss eine Kenntnisnahme des Arbeitgebers vom Inhalt der Nachrichten und den Verkehrsdaten, die einen Rückschluss auf die betroffenen Personen zulassen, ausgeschlossen werden.
- d. Der Arbeitgeber darf die Nutzungs- und Verkehrsdaten der Personalvertretung, der Schwerbehindertenvertretung sowie der Frauen- bzw. Gleichstellungsbeauftragten u.ä. nur insoweit kontrollieren, als dies im Einzelfall aus Gründen der Kostenkontrolle erforderlich ist. Soweit allerdings nur unerhebliche Kosten bei der Nutzung von Internet und E-Mail anfallen – was überwiegend der Fall sein wird –, ist eine Auswertung dieser Daten unzulässig.
- e. Eine Betriebs- oder Dienstvereinbarung kann nur dann als besondere Rechtsvorschrift angesehen werden, wenn die Datenerhebung, -verarbeitung und -nutzung ausreichend und präzise innerhalb des Erlaubnisumfangs gesetzlicher Bestimmungen geregelt wird und sie das gesetzliche Schutzniveau nicht unterschreitet.
- f. Im Regelfall sollte darauf verzichtet werden, die Verarbeitung von Protokolldaten auf die Einwilligung der Beschäftigten zu stützen, da sie aufgrund des Abhängigkeitsverhältnisses zum Arbeitgeber nicht immer freiwillig entscheiden können. Nur ausnahmsweise ist auch die Einwilligung der Beschäftigten in eine Verarbeitung der Protokolldaten über die unter a. genannten Vorschriften hinaus möglich. Die Beschäftigten können z. B. die Verwertung ihrer Protokolldaten verlangen, um den Verdacht einer unbefugten Internetnutzung auszuräumen.
- g. Soweit die Nutzung von E-Mail und Internet zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherung des ordnungsgemäßen Betriebs der Verfahren protokolliert wird, dürfen diese Daten nach dem BDSG, den Landesdatenschutzgesetzen und dem Beamtenrecht des Bundes und der Länder auch nur zu diesen Zwecken genutzt werden, nicht aber zur Verhaltens- und Leistungskontrolle der Beschäftigten.
- h. Von ein- und ausgehenden dienstlichen E-Mails seiner Beschäftigten darf der Arbeitgeber im selben Maße Kenntnis nehmen wie von deren übrigen dienstlichen Schriftverkehr. Beispielsweise könnte der Vorgesetzte verfügen, dass ihm seine Mitarbeiter jede ein- oder ausgehende E-Mail einzeln zur Kenntnis zuleiten.
- i. Aus Gründen der Datensicherheit dürfen Teilinhalte oder Anlagen von E-Mails unterdrückt werden, wenn sie ein Format aufweisen, das zu Sicherheitsrisiken auf Rechnern oder im Netzwerk führen kann.

III. Private Nutzung

1. Allgemeines

- a. Wenn ein Arbeitgeber den Beschäftigten die private Nutzung von Internet oder E-Mail erlaubt, ist er ihnen gegenüber TK- bzw. Telemediendienste-Anbieter.
- b. Vom Arbeitgeber beauftragte Zugangsanbieter (Access Provider) sind zwar diesem gegenüber TK- bzw. Telemediendienste-Anbieter, gegenüber den privat nutzenden Beschäftigten sind die Provider aber lediglich Auftragnehmer des dann als Anbieter zu qualifizierenden Arbeitgebers.
- c. Der Arbeitgeber ist gegenüber den Beschäftigten und den Absendern zur Einhaltung des Fernmeldegeheimnisses verpflichtet. Daher gelten die gleichen Bedingungen wie beim privaten Telefonieren.
- d. Es gelten die Regelungen der Telekommunikationsgesetzes, des Telemediengesetzes bzw. des Rundfunkstaatsvertrages.
- e. Der Arbeitgeber ist nicht verpflichtet, den Beschäftigten die private Nutzung des Internet zu erlauben. Entschließt er sich jedoch dazu, muss es ihm grundsätzlich möglich sein, diese Erlaubnis an einschränkende Voraussetzungen zu knüpfen (z. B. eine angemessene Art der Kontrolle durchzuführen). Beschäftigte, die diese Beschränkungen nicht akzeptieren wollen, können ihre Einwilligung ohne jeden dienstlichen Nachteil verweigern.
- f. Der Umfang der privaten Nutzung, ihre Bedingungen sowie Art und Umfang der Kontrolle, ob diese Bedingungen eingehalten werden, müssen – am sinnvollsten durch Dienstvereinbarung oder -anweisung – unter Beteiligung des Personalrats eindeutig geregelt werden.
- g. Eine Protokollierung darf ohne Einwilligung erfolgen, wenn sie zu Zwecken der Datenschutzkontrolle, der Datensicherung, zur Sicherung des ordnungsgemäßen Betriebs der Verfahren oder zu Abrechnungszwecken erforderlich ist.

2. Besonderheiten bei E-Mail

- a. 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.
- b. Der Arbeitgeber sollte vor dem Hintergrund des von ihm zu wahrenen Fernmeldegeheimnisses entweder für die Beschäftigten separate E-Mail-Adressen zur privaten Nutzung einrichten oder – falls privates Surfen erlaubt ist – sie auf die Nutzung eines Web-Mail-Dienstes verweisen.

- c. Wie bei der dienstlichen Nutzung (s. II.i.) dürfen aus Gründen der Datensicherheit eingegangene private E-Mails oder deren Anhänge unterdrückt werden, wenn sie ein Format aufweisen, das zu Sicherheitsrisiken führen kann. Die Verfahrensweise ist den Beschäftigten zuvor bekannt zu geben. Generell sind die Beschäftigten darüber zu unterrichten, wenn an sie gerichtete oder von ihnen abgesendete E-Mails ganz oder teilweise unterdrückt werden oder virenverseucht sind. Eine Untersuchung von virenverseuchten E-Mails mit Kenntnisnahme des Inhalts, etwa durch den Systemadministrator, ist nur unter Einbeziehung der betreffenden Beschäftigten zulässig.
- d. Eine zentrale Spam-Filterung, bei der automatisch auf den Header oder Inhalte zugegriffen wird, darf nur mit Einwilligung des Empfängers erfolgen, da die Reichweite des Fernmeldegeheimnisses erst endet, wenn die E-Mail in seine vollständige Verfügungsgewalt gelangt ist. Auch dies ist als einschränkende Voraussetzung für die Erlaubnis zur privaten Nutzung (s. o., III.1.e) anzusehen und damit Bestandteil der Einwilligung. Die Einwilligung kann pauschal vorab erfolgen. Die Beschäftigten sind über die Art und Weise der Spam-Filterung, insbesondere über die dabei stattfindende Verarbeitung personenbezogener Daten, zu informieren.
- e. Eine darüber hinaus gehende inhaltliche Kontrolle ist nicht zulässig.