



KERSTIN BLOSSEY

Private Nutzung von E-Mail- und Internetdiensten am Arbeitsplatz

Schwierigkeitsgrad:



Heikles Thema für alle Arbeitgeber! In vielen Fällen sind gelegentliche private E-Mails oder kurze private Ausflüge ins Internet am Arbeitsplatz gängige Praxis.

Hadte einer unserer Professoren noch im Jahr 2001 seine ernsthaften Zweifel gelehrt, dass sich das Internet etablieren könnte, ist es heute mit seinen vielfältigen Diensten und Möglichkeiten beinahe so normal wie Telefon, Fernseher und Automobil.

Neue Techniken, neue Chancen, neue Wege, Barrierefreiheit bezüglich sprachlicher und geografischer Grenzen – bei aller Freiheit und Vielfalt gibt es auch für diesen Bereich Regeln, die zum Ziel haben, die Privatsphäre und Selbstbestimmung des Einzelnen Benutzers schützen zu helfen, wo er oder sie es nicht ausreichend selbst kann. Die private Nutzung von E-Mail und Internet am Arbeitsplatz ist hier ein spannender Grenzfall, denn eine rechtlich einwandfreie Lösung ist derzeit noch nicht gefunden. Trotzdem – oder gerade deshalb – ist es wichtig, dass Arbeitgeber genauso wie die Beschäftigten über die Gefahren, das Haftungsrisiko und wie man diese wirksam vermeiden kann, Bescheid wissen.

Ausgangssituation

Man denke an einen durchschnittlichen Betrieb im Mittelstand. Es werden personenbezogene Daten verarbeitet, daher ist die Firma verpflichtet, mit entsprechenden Maßnahmen ein angemessenes Datenschutzniveau zu leben. Den Beschäftigten des Unternehmens – oder einer anderen Einrichtung (Der Einfachheit halber wird der Begriff *Unternehmen* pseudonym verwendet für alle Stellen, die auf Grund der automatisierten

Verarbeitung personenbezogener Daten zum Datenschutz nach Bundesdatenschutzgesetz (BDSG) verpflichtet sind.) – wird der Zugang zum Internet und ein personalisierter geschäftlicher E-Mail-Account als Arbeitsmittel zur Verfügung gestellt. Bisher ist die private Nutzung von E-Mail und Internet am Arbeitsplatz nach Aussagen von Mitarbeitern geduldet, d. h. es wurde weder ein Verbot ausgesprochen, noch ist die generelle Erlaubnis dazu in irgendeiner formellen Weise klar definiert.

Ziel ist es, eine einheitliche Regelung der privaten Nutzung dieser elektronischen Kommunikationsdienste festzuschreiben. Warum dies dringend erforderlich ist, wird dieser Artikel im Weiteren darlegen.

Wir gehen bei der weiteren Betrachtung von zwei Prämissen aus:

- Für die gelegentliche private elektronische Korrespondenz benutzt der Mitarbeiter das geschäftliche auf den Namen des Mitarbeiters benannte E-Mail-Konto und das zugehörige Postfach, das zu seinem Arbeitsplatz gehört;
- Personalisierte E-Mails enthalten personenbezogene Daten bzw. sind das per se.

(Rechts)Grundlagen zum Thema

Der Schlüssel für das Bedürfnis, eine vertragsähnliche Regelung der Privatnutzung zu schaffen, entspringt unter anderem folgenden Überlegungen aus dem Gesetz.

IN DIESEM ARTIKEL ERFAHREN SIE...

warum jedes Unternehmen die private E-Mail- und Internetnutzung regeln muss;

drei Modelle, die sich für eine praktikable Umsetzung eignen;

wie Sie das Thema in Ihrem Unternehmen angehen können.

WAS SIE VORHER WISSEN/KÖNNEN SOLLTEN...

keine spezifischen Vorkenntnisse erforderlich.

Personenbezogene Daten in E-Mail- und Internetnutzung

Generell gibt es einige interessante Aspekte, wenn man genauer hinsieht, hier die wichtigsten:

- Die Tatsache der Bereitstellung von Internetdiensten und der Online-Verbindung macht den Arbeitgeber zum Teledienste- bzw. Telekommunikationsdienstleister. Je nach der konkreten Ausgestaltung der Nutzungsmöglichkeiten sind die Vorschriften des Telemediengesetzes (TMG) für den inhaltlichen, des Telekommunikationsgesetzes (TKG) für den technischen Schwerpunkt sowie generell des Bundesdatenschutzgesetzes (BDSG) zu beachten. Bei der Beurteilung, ob und inwieweit der Arbeitgeber die Beschäftigten anhand der Verbindungs- und Nutzungsdaten kontrollieren und überwachen darf, ist es von Bedeutung, ob den Angestellten 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;
- Die Behandlung personalisierter Werbefortschriften (Spam) ist ein weiterer spannender Punkt, da personalisierte E-Mails an den Adressaten ausgeliefert werden müssen. Man muss bei der Spamabwehr als Arbeitgeber daher sehr genau hinsehen, an welcher Stelle man die elektronische Werbeflut beeinflusst. Da viele Lösungen, die man hierfür kaufen kann, nicht die Anforderungen des gesetzlichen Datenschutzes berücksichtigt haben, sollte man bei einer Anschaffung in jedem Fall genauer hinsehen.

Diese beiden eben genannten Punkte sind für sich einen eigenen Artikel wert und werden der Übersicht halber in diesem Artikel nicht weiter berücksichtigt. Wir wenden uns den (noch) schwerwiegenden Punkten zu, der privaten E-Mail-Nutzung am Arbeitsplatz, wie unter 1. bei den Prämissen schon genauer erläutert.

Beurteilung in der Literatur

Private E-Mails unterliegen dem Fernmeldegeheimnis, bei gestatteter privater Nutzung gilt der Arbeitgeber als Diensteanbieter im Sinne des § 2 I Nr. 1 TMG (*Nachrichtenmittler*) und muss sich vor allem an die Vorgaben aus § 88 ff. Telekommunikationsgesetz (TKG) i.V.m. Art. 10 Grundgesetz (GG) halten. Nicht nur die Inhalte privater elektronischer Nachrichten gelten als Bestandteil des Fernmeldegeheimnisses, sondern auch die zugehörigen Rahmen-daten eines Fernmeldevorgangs, z. B. die Verbindungsdaten. In diesem Zusammenhang sei auch nochmals auf die Entscheidung, dass IP-Adressen als personenbezogenes Datum zu werten und entsprechend zu behandeln sind, hingewiesen.

Der Schutz des Fernmeldegeheimnisses endet zu dem Zeitpunkt, wenn die Nachricht beim Empfänger angekommen ist. Der Übertragungsvorgang ist beendet, E-Mails sind nicht weiter der theoretischen Zugriffsmöglichkeit Dritter ausgesetzt, der Empfänger schließlich hat ab diesem Zeitpunkt die Möglichkeit, die E-Mail zu verarbeiten oder zu löschen. Hier beginnt schließlich das Hoheitsgebiet des BDSG. Verstöße gegen das Fernmeldegeheimnis können als Straftatbestand nach § 206 StGB geahndet werden, Verstöße gegen den Datenschutz mit bis zu 250.000 Euro sowie bis zu 2 Jahren Haft (pro Fall).

Um den Internetdienst technisch zu ermöglichen, darf der Arbeitgeber 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 Arbeitgeber sich vor dem Verrat von Firmengeheimnissen schützen müsse sowie insbesondere Zugriffe der Beschäftigten auf illegale Inhalte und deren Kopie auf den Firmenrechner verhindern wolle. Schließlich hat der Arbeitgeber 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. Eine Zulässigkeit der Datenverwendung ist jedoch nur gegeben, soweit für die Erbringung der Dienste und ihre Abrechnung erforderlich sowie zur Beseitigung von technischen Störungen und Missbräuchen. In der Regel sind Nutzungsdaten wie z.B. serverseitige Protokollierungen somit nach Beendigung der Verbindung unverzüglich zu löschen (§ 88 ff. TKG, § 11 ff. TMG). Zur Verfolgung strafrechtlicher Interessen muss ein konkreter Verdachtsfall vorliegen, erst dann ist eine zeitlich begrenzte Erfassung, Speicherung und Auswertung weiterer Daten möglich – jedoch nach den arbeits- und datenschutzrechtlichen Normen, z.B. Miteinbeziehung des Betriebsrats und des DSB. Der Arbeitgeber unterliegt hier also generell einem weitgehenden Kontrollverbot.

Personenbezogene Daten...

...sind alle Angaben über persönliche und/oder sachliche Verhältnisse eines lebenden Menschen (*natürliche Person*). Dies beginnt bereits mit seinem Namen, seiner Adresse, Rufnummern und Durchwahlen (auch dienstlich), sein Kfz-Kennzeichen, seine Krankengeschichte, Bewerbungsunterlagen, Identifikationsausweise (Dienstausweis, Reisepass etc.) und geht bis hin zu seiner finanziellen Situation, seiner Meinung, Herkunft oder persönlichen Überzeugung.

Betriebliche Übung...

...bezeichnet die Tatsache, dass der Arbeitgeber bestimmte Verhaltensweisen regelmäßig wiederholt zulässt, aus der die Arbeitnehmer schließen können, dass ihnen die aufgrund dieser Verhaltensweisen gewährten Leistungen oder Vergünstigungen auch künftig auf Dauer gewährt werden sollen. Dabei kommt es ausschließlich auf die gleichartige wiederholte Praktizierung eines Verhaltens des Arbeitgebers an. Wie lange ein Arbeitgeber eine Duldung durchführt, bis sie zum Rechtsanspruch führt, ist nicht festgelegt, daher sind bisher dazu keine Urteile bekannt. In der Literatur werden Zeiträume zwischen 4 bis 12 Monaten genannt.

Im Falle der ausschließlich dienstlichen Nutzung besteht zwischen dem Unternehmen und den Beschäftigten kein Anbieter-Nutzer-Verhältnis, da es sich bei der Bereitstellung der Dienste nicht um ein Angebot von Telekommunikations- und Telediensten im Sinne des TKG bzw. des TMG handelt. Die Rechtmäßigkeit einer Verarbeitung personenbezogener Daten richtet sich dann 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 Arbeitgeber das Recht des Beschäftigten auf informationelle Selbstbestimmung tangieren, d.h. einen Eingriff in die Grundrechte des Beschäftigten darstellen. Auch wenn sich der Beschäftigte dem Direktionsrecht seines Arbeitgebers unterwirft, kann er

sich doch auf seine Grundrechtspositionen berufen. Dies geht so weit, dass unter Umständen das E-Mail-Postfach eines plötzlich nicht mehr verfügbaren Mitarbeiters nicht geöffnet werden darf aus Geschäftsinteressen heraus, wenn nicht ausgeschlossen werden kann, dass doch eine private E-Mail enthalten sein könnte. Dies wurde durch die eine oder andere Aufsichtsbehörde in der Vergangenheit bereits so praktiziert.

Seit 2006 zählen geschäftliche E-Mails zur Geschäftskorrespondenz (s. auch § 257 II HGB) und sind in der Regel sechs Jahre aufbewahrungspflichtig. Sie sind elektronisch in unveränderbarer Form vorzuhalten, ein Ausdruck auf Papier ist nicht ausreichend. Vor diesem Hintergrund sollte der Arbeitgeber eine strikte physikalische Trennung privater und geschäftlicher E-Mail-Konten anstreben, da sonst eine Archivierung schwer bis nahezu unmöglich werden kann. Zugleich ist die Privatsphäre der Mitarbeiter durch eine solche Lösung

besser geschützt als über die private Nutzung des geschäftlichen E-Mail-Accounts. Ist eine solche Trennung nicht realisierbar, sind alle E-Mails zu archivieren und die gesamte dienstliche und private E-Mail-Korrespondenz der Arbeitnehmer darf nicht durch den Arbeitgeber eingesehen oder gar kontrolliert werden – sofern nicht schwerwiegende Sonderfälle wie z.B. die Verletzung von Straftatbeständen vorliegen. Dieses weitgehende Kontrollverbot haben die verschiedenen Aufsichtsbehörden für den Datenschutz bis heute ebenfalls in ihren Berichten bestätigt.

Datenschutzkonforme Lösungsmöglichkeiten

Generell gibt es zwei Möglichkeiten der sinnvollen betrieblichen Lösung: entweder eine genau definierte Erlaubnis (in unterschiedlichen Ausprägungen) oder ein generelles – und eindeutig formuliertes – Verbot, abhängig davon, wie die private Nutzung von E-Mail und Internet am Arbeitsplatz bisher geregelt und in der Praxis umgesetzt wurde. Die auf bestimmte Zeiten oder Leistungsvolumina begrenzte Erlaubnis kann sicherlich nicht als praktikabel empfohlen werden, da die Problematik der privaten E-Mail-Korrespondenz und dem Schutz des Fernmeldegeheimnisses nicht behoben wird.

Die geregelte Erlaubnis

Die private Nutzung des betrieblichen Internet- und E-Mail-Zugangs ist zulässig, soweit eine ausdrückliche und klar definierte Gestattung des Arbeitgebers erfolgt ist. Diese kann mündlich, im Rahmen des Arbeitsvertrages, durch eine Zusatzvereinbarung oder aber auch durch eine entsprechende Betriebsvereinbarung erfolgen.

Diese Vereinbarung muss zu folgenden Punkten eine Regelung treffen – hier sind ein paar Aspekte über das BDSG hinaus zu beachten:

- Erfolgt eine erlaubte private E-Mail-Nutzung auf dem Firmenaccount oder über ein externes Mailkonto (z.B. über einen Webmail-Dienst im Internet), d.h. außerhalb des Zugriffs des Arbeitgebers;
- Ist die private Nutzung generell, innerhalb oder außerhalb der Arbeitszeit gestattet?

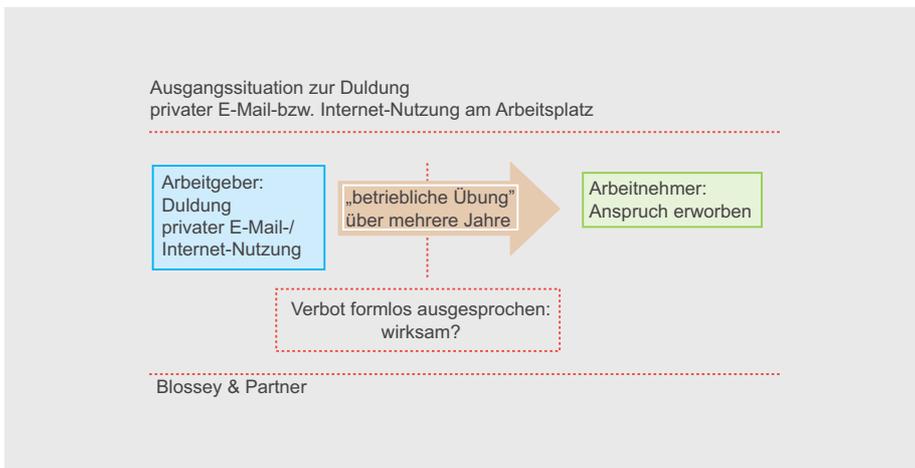


Abbildung 1. Internet-Nutzung am Arbeitsplatz

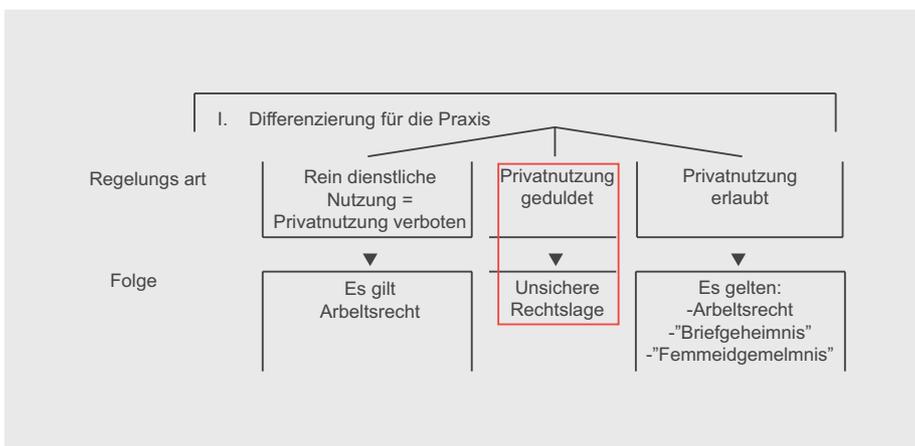


Abbildung 2. Quelle: Kramer, 2007

- Wie groß ist der maximale zeitliche Umfang der privaten Nutzung pro Tag/ Woche/Monat?
- Wer trägt etwa entstehende Kosten? Wie werden sie abgerechnet?
- Wo sollen private Dateien abgespeichert werden? Wo dürfen sie nicht abgespeichert werden?
- Welchen maximalen Umfang dürfen private Dateien haben?
- Auf welchen Internetseiten ist der Zugang untersagt (Filterung)?
- Ist das Abspeichern aus dem Internet geholter Dateien auf der Festplatte und/oder auf dem Server sowie die Verwendung mobiler Datenträger gestattet?
- Welche Begrenzung existiert für das "Downloaden" von Dateien?
- Willigt der Mitarbeiter bei der privaten Nutzung des Geschäfts-E-Mail-Accounts ein, dass sein geschäftlicher E-Mail-Account geöffnet werden darf, wenn der Mitarbeiter kurzfristig nicht verfügbar ist und dürfen Stellvertreterregelungen getroffen werden?
- Ist der Arbeitgeber berechtigt, private Dateien zu löschen? Unter welchen Voraussetzungen?
- Bei der Nutzung des geschäftlichen E-Mail-Accounts ist der Mitarbeiter mit der Archivierung seiner privaten E-Mails einverstanden?
- Ist die Eröffnung der privaten Nutzung davon abhängig, dass der Mitarbeiterinnen und Mitarbeiter zuvor sein Einverständnis mit bestimmten regelmäßigen Kontrollen durch den Arbeitgeber erklärt?

Für die geregelte Erlaubnis haben sich in der Praxis zwei Modelle durchgesetzt:

- die pauschale Genehmigung;
- die Bereitstellung von speziellen *Privatsurfplätzen*.

Die pauschale Genehmigung

Die pauschale Genehmigung erfolgt unter der Prämisse, dass ein Arbeitnehmer sich auch bei der privaten Nutzung mit dem Medium auseinandersetzt und seine Kenntnisse und Fähigkeiten verbessert. Die Nutzung wird als permanente Weiterbildung verstanden. Damit wird allerdings der Arbeitgeber zum Telediensteanbieter an

die Vorgaben Fernmeldegeheimnisses, der Zugangsfreiheit nach TMG und, sofern die private Nutzung des geschäftlichen E-Mail-Accounts erlaubt ist, an die allgemeinen Informationspflichten, sprich Anbieterkennzeichnung, gebunden.

Das heißt in der Praxis, dass der Arbeitgeber weder den Internet- noch den E-Mailverkehr in dem Sinne überwachen darf, wie es zum vollumfänglichen Schutz des betriebsinternen Netzes notwendig wäre. Hat der Arbeitnehmer die Kosten der privaten Nutzung zu tragen, dürfen nach § 15 TMG alle Daten erhoben werden, die zur Abrechnung erforderlich sind. Diese sind jedoch ebenso nach TMG sofort wieder zu löschen, sobald sie zum Zwecke der Abrechnung nicht mehr benötigt werden.

Tipp: Das Einholen einer Einwilligung der Arbeitnehmer in die Protokollierung und Kontrolle erleichtert den Umgang an dieser Stelle. Diese Einwilligung kann Bestandteil des einzelnen Arbeitsvertrages sein. Es kann aber auch im Rahmen einer Betriebsvereinbarung festgelegt werden, dass der Arbeitnehmer seine Einwilligung mit der privaten Nutzung konkludent erklärt.

Wie jedoch oben bereits erwähnt, ist eine vorliegende Einwilligung kein Garant dafür, dass Sie im Zweifelsfall tatsächlich zugreifen dürfen.

Privatsurfplätze

Die Alternative ist die Bereitstellung definierten Sammelarbeitsplätze (*Privatsurfplätze*) zum privaten Surfen und zur

privaten E-Mail-Nutzung. Dabei kann die Nutzung von normalen Arbeitsplätzen hinsichtlich der Art des Datenverkehrs kontrolliert werden, die Nutzung der Privatsurfplätze dagegen nicht. Mit einer solchen Vorgehensweise kann eine Gefährdung der Funktionsfähigkeit des Netzwerkes durch Viren und eine Beeinträchtigung der Produktivität verringert werden und je nach Situation die Akzeptanz der Mitarbeiterinnen und Mitarbeiter gesteigert werden.

Tipp: Aktivitäten dieser Privatsurfplätze können und dürfen nicht überwacht werden. Verbunden damit ist ein stark erhöhtes Sicherheitsrisiko für Mitarbeiter wie Arbeitgeber und im Falle rechtlich unzulässiger Aktivitäten an den PCs ggf. ein erhöhtes Haftungsrisiko des Arbeitgebers. Hinzu kommt, dass entsprechende Terminals zusätzliche Ressourcen fressen (Bandbreite, Hardware, Zeit zum Aufsuchen, technische Installation und Pflege). Diese Lösung eignet sich aus Datenschutzsicht daher nur bedingt für die Praxis.

Exkurs: Stillschweigende Duldung

Hier ist besondere Vorsicht geboten. Viele Arbeitgeber dulden die Nutzung des dienstlichen Internet- und E-Mail-Zuganges für private Zwecke. Hierdurch kann und wird in den meisten Fällen eine „betriebliche Übung“ entstehen. Eine solche betriebliche Übung kann einen Rechtsanspruch des Personals auf Privatnutzung ergeben und damit die ausdrückliche Genehmigung des Arbeitgebers quasi ersetzen.

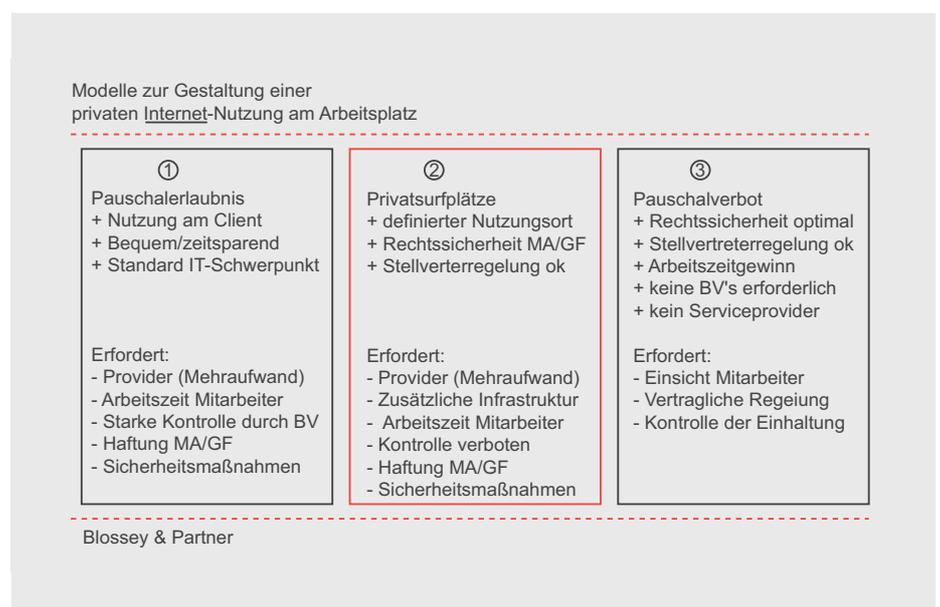


Abbildung 3. Modelle zur Gestaltung einer privaten Internet-Nutzung am Arbeitsplatz

Wurde also in einem Betrieb eine gewisse Zeit lang die private Nutzung des dienstlichen Internet- und E-Mail-Zugangs geduldet, und ist bei den Arbeitnehmern der Eindruck entstanden, dass dies auch weiterhin so sein wird, haben die Arbeitnehmer unter Umständen einen Anspruch auf die Privatnutzung erworben. Eine somit erfolgte Gestattung der Privatnutzung des dienstlichen Internet- und E-Mail-Zugangs kann vom Arbeitgeber grundsätzlich nicht *einseitig* rückgängig gemacht oder eingeschränkt werden. Der entstandene Anspruch des Personals auf private Nutzung kann nur mit Einwilligung des Arbeitnehmers eingeschränkt werden. Verweigert der Arbeitnehmer seine Zustimmung, bleibt dem Arbeitgeber nur der unschöne Weg, die Vertragsänderung im Wege der Änderungskündigung des Arbeitsverhältnisses zu erzwingen (Abbildung 1).

Tip: *Der ungeregelte Zustand der Duldung ist für alle Beteiligten eine rechtlich kritische Grauzone, die weder dem Mitarbeiter noch dem Arbeitgeber irgendeine Form von Sicherheit bringt,*

jedoch viele rechtliche Unwägbarkeiten enthält, die auch die Privatsphäre der Mitarbeiter einschränken kann. Daher sollte möglichst schnell eine eindeutige Regelung getroffen werden.

Grundsätzliches Verbot

Das grundsätzliche Verbot versetzt den Arbeitgeber in die scheinbar einfachste Situation: Er ist kein Telediensteanbieter im Sinne des TMG und nur in beschränktem Umfang an die Vorgaben des § 88 TKG (Fernmeldegeheimnis) gebunden. Das heißt, in der Praxis darf er zum Zweck der Datensicherheit und des stabilen Netzbetriebes den Datenverkehr z.B. an der Firewall überwachen, das Herunterladen von Daten aus dem Netz mittels Filter überprüfen bzw. verhindern und z.B. in besonderen Situationen auch den Inhalt von E-Mails lesen. Diese sind per Definition rein dienstlicher Natur. E-Mails, die an Mitarbeiterinnen und Mitarbeiter gesendet werden, werden dabei bis zum Erkennen eines privaten Inhalts als dienstlich behandelt. Dieser Fall tritt zum Beispiel im Falle einer

Vertretung im Abwesenheitsfall einer Mitarbeiterin oder eines Mitarbeiters ein. Empfehlenswert ist hier jedoch die Genehmigung durch den Arbeitnehmer zum Zugang zu seinem E-Mail-Account.

Tip: *auch bei einem generellen Verbot fallen bei der Nutzung des Geschäfts-E-Mail-Accounts personenbezogene Daten im Sinne des BDSG an, die entsprechend zu schützen sind. Ein Verbot ist also kein Freibrief für eine willkürliche Datenerfassung und -verwendung.*

Zulässigkeit von Kontrollen aus Datenschutzsicht

Die Kontrolle der Internet- und E-Mail-Nutzung befindet sich – unabhängig von der Frage, ob es sich um dienstliche oder private Nutzung handelt – immer im Spannungsfeld zwischen den berechtigten Interessen des Arbeitgebers, seine Mitarbeiter zu kontrollieren, und den Interessen des Personals an der Beachtung ihres allgemeinen Persönlichkeitsrechts. Diese widerstreitenden Interessen finden Ausdruck in der Begrenzung der Kontrollmöglichkeiten des Arbeitgebers im Wesentlichen durch das Verfassungsrecht (*allgemeines Persönlichkeitsrecht*) und die datenschutzrechtlichen und bereichsspezifischen Vorschriften.

Eine missbräuchliche Nutzung kann bei einer unerlaubten oder übermäßigen privaten Nutzung, unerlaubtem Downloaden, strafrechtlich relevantem Verhalten eventuell auch beim Aufrufen von Internetangeboten mit pornographischen oder ähnlichen Inhalten vorliegen. In solchen Fällen ist die Zulässigkeit der Überwachung anhand der Regelungen des BDSG und unter Beachtung des allgemeinen Persönlichkeitsrechtes herauszuarbeiten (Abbildung 2).

Hieraus ergeben sich folgende Grundsätze:

- Besteht ein konkreter Missbrauchsverdacht, darf der Arbeitgeber Datum, Uhrzeit, Dauer der Verbindung und die aufgerufenen Webseiten temporär im 4-Augen-Prinzip (unter Miteinbeziehung des Datenschutzbeauftragten und des Betriebsrats) kontrollieren;
- Bei dem Verdacht auf Missbrauch kann der Arbeitgeber lediglich anhand der aufgerufenen Webseite überprüfen, ob

Wochenrückblick zu den Datenschutz-Schlagzeilen in der Online-Presse

Das Redaktionsteam von Blosssey & Partner stellt jede Woche neu die Schwerpunktthemen rund um Datenschutz für Sie zusammen unter <http://www.blosssey-partner.de> (News, unten rechts). Gucken Sie doch mal rein, das Archiv reicht bis 2004 zurück und bietet sogar eine einfache Suchfunktion. Viel Spaß beim Stöbern.

Ausblick aufs nächste Heft:

Eine ganze Reihe von Pflichten und Rechten rund um das Datenschutzgesetz führen zu diversen Kennzeichnungs- und Informationsbedürfnissen. Wir beschäftigen uns mit unterschiedlichen Bereichen und wie man sie nutzbringend gestalten kann.

Textreste:

Jegliche Verwendung geschäftlicher E-Mails ist daher abhängig von der – freiwilligen – Einwilligung aller betroffenen Mitarbeiter oder das Vorliegen einer gesetzlichen Erlaubnis bzw. Verpflichtung zur Verwendung. Natürlich gehören private E-Mails auch an sich zu den personenbezogenen Daten nach BDSG und unterliegen von daher einem datenschutzrechtlichen Schutzbedarf.

Info:

Aus Datenschutzsicht ist das Thema *private E-Mail-Nutzung am Arbeitsplatz* im Bezug auf *personenbezogene Daten* nach § 4 I BDSG ebenfalls mehrfach zu beachten, nämlich:

- in Form der gesetzlich vorgeschriebenen Archivierung (Geschäftskorrespondenz, vgl. Handelsgesetzbuch) als Speicherung eine Unterform des Verarbeitens nach § 3 IV BDSG sowie der;
- in Form des Zugriffs auf archivierte Mails als Nutzen nach § 3 V BDSG.

es sich um private oder dienstliche Nutzung handelt;

· Eine Kontrolle *just for fun*, d.h. ohne konkrete Verdachtsmomente, ist unzulässig.

Eine inhaltliche Kontrolle ist nur in Ausnahmefällen zulässig. Ein solcher kann vorliegen, wenn der Arbeitnehmer unerlaubt pornografische Seiten (eventuell gar mit strafrechtlichem Inhalt) auf die Festplatte gespeichert hat. Möglich und zulässig ist auch die Installierung einer Filter-Software. Mit einer solchen Software können bestimmte Seiten des Internets bereits vorab für die Nutzung der Mitarbeiterinnen und Mitarbeiter gesperrt werden.

Fazit

Die derzeitige Praxis im Unternehmen, vor allem die Diskrepanz zwischen schriftlich vorgeschriebener und gelebter Form, lässt Handlungsalternativen offen, die keine ganz eindeutige Rechtslage ergeben. Dies erschwert sowohl die Systemkontrolle aus unternehmensökonomischen Gesichtspunkten als auch alltagsbezogene Themen wie die Stellvertreterregelung bezüglich der Mitarbeiter-E-Mail-Accounts und deren Archivierung, die jedoch erforderlich wäre. Es bedarf insofern einer offiziellen klaren Regelung, die für den gesamten Personalstamm mit Internet-/E-Mail-Zugriff im Unternehmen gültig und vor allem bindend umzusetzen ist. Dabei ist zwischen rechtlichen Verpflichtungen, die aus dem gewünschten Modell entstehen können und der Praktikabilität im Unternehmen sorgfältig abzuwägen.

Die folgende Grafik fasst gängige Modelle zur Gestaltung der Internetnutzung zusammen (Abbildung 3).

Dringend empfehlenswert aus Sicht des Datenschutzes ist die Trennung des privaten E-Mail-Verkehrs vom Geschäfts-E-Mail-Account durch eine strikte Auslagerung auf ein Mailkonto bei einem externen Webmail-Anbieter.

Diese Empfehlung dient vor allem vor allem dem Schutz der Privatsphäre der Mitarbeiter, ermöglicht aber zugleich die unkomplizierte Handhabung von Stellvertreterregelungen, Archivierung und Einsichtnahme in das dienstliche Postfach im Notfall erleichtert. Die Nutzung des

Internets zu den Pausenzeiten ist praktikabel, muss dann allerdings auch stichprobenartig kontrolliert werden. Dies gehört i.d.R. auch zu den Aufgaben des DSB.

Optimaler Weise ist eine solche Umsetzung in Form einer Betriebsvereinbarung festzuhalten, um diese für alle Beteiligten verbindlich und nachvollziehbar zu gestalten. Diese ist ausdrücklich zusammen mit dem Betriebsrat und der DSB umzusetzen.

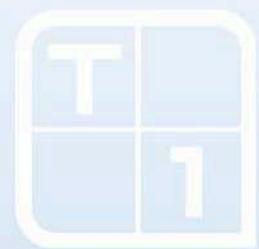
Die Modelle zeigen, dass eine praktikable Lösung dieser Thematik geradezu trivial einfach zu realisieren sein kann. Vor dem Hintergrund der Flut von Schlagzeilen zu erfolgten Datenschutzpanne in den letzten Monaten sollte man gerade bei einem so heiklen Thema kein unnötiges Risiko mehr eingehen.

Anmerkung zu diesem Artikel: Als Sekundärliteratur kamen das BDSG, das TMG, das TKG, das GG in der jeweils aktuell gültigen Fassung, verschiedene Kommentare zum BDSG von Gola/Schomerus, Simitis, Bergmann/Möhrle/Herb, diverse Vortragsunterlagen, die im Einzelnen nicht mehr zuordenbar sind sowie diverse Tätigkeitsberichte der Aufsichtsbehörden zum Einsatz. Der Punkt 4 entstammt im Wesentlichen Ausführungen von P. Kramer, Rechtsanwalt und Dozent.

Dieser Artikel hat seinen Ursprung in einer unsortierten privaten Zusammenfassung aus sehr vielen Quellen, die jetzt gar nicht mehr nachvollziehbar sind. Da Quellenangaben damals nicht erforderlich waren, können diese jetzt nicht mehr im Einzelnen benannt werden. Die Autorin bittet um Nachsicht.

Kerstin Blossey

Die Autorin ist Dipl. Informations-Wirtin (FH) und Gründerin von Blossey & Partner, einem aufstrebenden Unternehmen, das sich inzwischen ausschließlich auf den betrieblichen/behördlichen Datenschutz spezialisiert hat. Zum Kundenkreis zählen deutsche ebenso wie international angesiedelte mittelständische Unternehmen und Einrichtungen aus so unterschiedlichen Branchen wie Medien, Softwareindustrie, produzierendes Gewerbe, Wirtschaft, Gesundheitswesen, Tourismus und die öffentliche Hand.



Think-1st Ltd.

**Network and
Security consulting
at its best, available
across Europe**

**Hacking Trainings
on demand.**

**See
www.think-1st.de
for details.**

**Office Germany:
Think1ST Ltd. & Co. KG**

**Fon: +49 (30) 935 544 92
Fax: +49 (30) 935 544 93**

**E-Mail: sales@think-1st.de
Internet: www.think-1st.de**