von Rechtsanwalt **Patrick Prestel**

Welche Lösungsmöglichkeiten gibt es für den Konflikt zwischen E-Mail-Archivierung und Fernmeldegeheimnis/Datenschutz? Die FAQ zur E-Mail-Archivierung Teil 4

In den letzten 25 Fragen der FAQ der IT-Recht Kanzlei zur E-Mail-Archivierung geht es um Lösungsmöglichkeiten und deren jeweilige Ausgestaltung sowie das Recht des Arbeitgebers zur Kontrolle seiner Mitarbeiter.

61. Kann im Rahmen des Bundesdatenschutzgesetzes in die E-Mail Archivierung eingewilligt werden?

Individuelle Einwilligungen sind möglich. Diese müssten nach § 4a BDSG schriftlich und freiwillig abgegeben werden. Die Freiwilligkeit kann aufgrund des unterschiedlichen Kräfteverhältnisses zwischen Arbeitgeber und Arbeitnehmer, insbesondere vor dem Abschluss des Arbeitsvertrages, nicht vorliegen. Diesbezüglich bedarf es aber immer einer Einzelfallbetrachtung. Weiterhin darf die Einwilligung in nicht allgemeinegehaltene Erklärungen formuliert werden. Nicht ausreichend sind danach Formulierungen wie „Der Arbeitnehmer gestattet dem Arbeitgeber jede Nutzung persönlicher Daten, die im Arbeitsverhältnis anfallen." Vielmehr bedarf es einer detaillierten Formulierung. Schließlich muss der Arbeitgeber den Arbeitnehmer rechtzeitig und umfassend über Zweck, Art und Umfang der beabsichtigten Datennutzung informieren.

Neben dem Aufwand die Einwilligung einzuholen, besteht die praktische Gefahr, dass einzelne Mitarbeiter die Einwilligung nicht erteilen, sodass keine umfassende und automatisierte Archivierung möglich ist. Zudem ist die Einwilligung jederzeit widerruflich.

62. Kann hierbei die E-Mail-Archivierung auch in einer Betriebsvereinbarung geregelt werden?

Auch kann über die Datenerhebung und –verarbeitung eine Betriebsvereinbarung geschlossen werden, da eine solche eine „andere Rechtsvorschrift" im Sinne des § 4 BDSG ist. Dabei ist die Mitwirkung des Betriebsrats nach § 87 I Nr. 6 BetrVG nötig.

63. Gibt es hierbei für den Arbeitgeber noch eine gesetzliche Lösung?

Für die Emailarchivierung kommt innerhalb eines Betriebes § 32 BDSG als gesetzliche Rechtfertigung zur Anwendung. Dieser erlaubt die Erhebung, Verarbeitung und Nutzung personenbezogener Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist.

Erforderlich ist die Verwendung personenbezogener Daten dann, wenn keine objektiv zumutbare Alternative existiert. Die Erforderlichkeit ist anzunehmen, wenn die berechtigten Interessen des Arbeitgebers auf andere Weise nicht oder nicht angemessen gewahrt werden können. Es ist eine Interessensabwägung zwischen dem Datenschutz des Arbeitnehmers (Art. 2 I GG i.V.m. Art.1 I GG) und dem Schutz des eingerichteten und ausgeübten Gewerbebetriebes des Arbeitgebers (Art. 14 I GG) vorzunehmen.

Bei der Archivierung ist zu berücksichtigen, dass sich für den Arbeitgeber aus den zahlreichen gesetzlichen Vorschriften nicht nur ein Interesse, sondern eine Pflicht zur Archivierung ergibt. Deshalb kann die Erforderlichkeit im Sinne des § 32 BDSG unseres Erachtens nur zu bejahen sein. Allerdings sollte der Arbeitgeber seiner Pflicht aus § 4 III BDSG den Arbeitnehmer über die Archivierung zur Informieren nachkommen.

64. Welche Lösungsmöglichkeiten gibt es für den Konflikt zwischen E-Mail-Archivierung und Fernmeldegeheimnis/Datenschutz?

1. Möglichkeit = Totalverbot des Einsatzes von E-Mails zu privaten Zwecken im Unternehmen
2. Möglichkeit = Zulassung mitarbeitereigener Mobilgeräte
3. Möglichkeit = Vorbehaltslose Erlaubnis des Einsatzes von E-Mails zu privaten Zwecken
4. Möglichkeit = Die Zwischenlösungen

a. Zugriff auf Web-Accounts
b. Zuweisung einer privaten neben der geschäftlichen E-Mailadresse
c. Kennzeichnung der privaten E-Mails.
d. Anlegen eines Ordners mit privaten E-Mails
e. Gesonderte Surfstationen für Arbeitnehmer
f. Einwilligung in die Archivierung der privaten E-Mails
g. privates Surfen über einen eigenen Proxyserver

65. Wie ist die Situation bei einem Totalverbot der privaten Nutzung?

Zumindest aus rechtlicher Sicht scheint diese Lösung die ideale: das Unternehmen wird nicht zum Telekommunikationsanbieter so dass das Fernmeldegeheimnis nicht gilt. Und auch kann datenschutzrechtlich die Archivierung gerechtfertigt werden. So können Rechtsunsicherheiten für den Arbeitgeber und den Arbeitnehmer vermieden und SPAM-Filter, Vertretungszugriffe, Archivierung und Kontrollen einer missbräuchlichen Nutzung ermöglicht werden. Das Unternehmen hat dann das Recht, beliebig und unbegrenzt auf die E-Mails der jeweiligen Mitarbeiter zu archivieren.

66. Was ist bei der Aufstellung eines solchen Verbots zu beachten?

Das Verbot sollte im Unternehmen kommuniziert und schriftlich niedergelegt werden. Daneben muss es kontrolliert und durchgesetzt werden.

67. Warum sollte das Verbot kommuniziert werden?

Das Verbot sollte im Unternehmen aus Rechtssicherheitsgründen unbedingt kommuniziert werden. Zwar kann ein Arbeitnehmer laut dem Bundesarbeitsgericht nicht von der Erlaubnis der privaten Nutzung ausgehen, wenn keine Regelung vorliegt oder diese nicht kommuniziert wurde. Denn der Arbeitgeber allein bestimmt die Art der Verwendung der betrieblichen Mittel. Die Bereitstellung eines Internetzugangs bedeutet nicht, dass der Arbeitgeber auch stillschweigend die private Nutzung gestattet. Der Arbeitnehmer muss grundsätzlich davon ausgehen, dass er die betrieblichen Mittel nur zu betrieblichen Zwecken einsetzen darf. Aber für die Rechtssicherheit aller Beteiligten ist die Klarstellung sehr zu empfehlen.

68. Warum sollte das Verbot schriftlich niedergelegt werden?

Zu beachten wäre, dass das E-Mail Verbot aus Beweisgründen in jedem Fall schriftlich fixiert werden sollte, etwa durch

- entsprechende Richtlinien betreffend der Nutzung der firmeneigenen IT-Infrastruktur,
- Betriebsvereinbarungen,
- Einverständniserklärungen der Belegschaft oder gar
- den individuellen Anstellungsvertrag.

69. Warum muss das Verbot in der Praxis durchgesetzt werden?

Das Verbot ist auch in der Praxis durchzusetzen. Untersagt nämlich ein Arbeitgeber die private Nutzung von E-Mails, ohne dies dann regelmäßig zu kontrollieren und zu unterbinden, kann sich das Verbot in eine Duldung "umwandeln".

Der Arbeitnehmer hat nach einer Weile der Duldung (sog. betriebliche Übung) einen Anspruch auf die Leistung, hier die Privatnutzung. Der Annahme einer Duldung durch den Arbeitgeber steht zudem nicht entgegen, dass er bei Duldung seinen Archivierungspflichten ohne Verstoß gegen das Fernmeldegeheimnis nicht nachkommen kann. Denn wenn er Kenntnis von der privaten Nutzung hat und nicht dagegen vorgeht, dann kann zu Recht angenommen werden, dass er seine eigenen Pflichten billigend verletzt. Regelmäßig wird darüber gestritten, ob der Arbeitgeber wirklich Kenntnis von der Nutzung hatte und in welchem Umfang er die Nutzung duldete. Um dem vorzubeugen, sind regelmäßig Kontrollen vorzunehmen und auch für den Fall von Verstößen Sanktionen vorzusehen, die in besonderen Fällen bis zu einer (verhaltensbedingten) Kündigung reichen können.

70. Wie ist die Situation bei der Zulassung mitarbeitereigener Mobilgeräte?

Solche Mobilgeräte sind mitarbeitereigene (private) Handys und Laptops. Über viele Handys kann man mittlerweile ins Internet gehen. Bei Laptops kann über einen USB-Surf-Stick die Internetverbindung hergestellt werden. In beiden Fällen wird der Internetzugang durch den Vertragspartner des Arbeitnehmers (Handyvertrag oder Surf-Stick-Vertrag) bereitgestellt. Dann ist nicht der Arbeitgeber Anbieter nach dem TKG, sondern der Vertragspartner des Internetzugangs des Mitarbeiters. Zudem werden die privaten E-Mails nicht durch den Arbeitgeber archiviert. Und die privaten Daten des E-Mailaustausches werden auch nicht gebackupt, sodass kein Konflikt mit dem BDSG entstehen kann.

Es sollte jedoch hierbei unbedingt eine IT-Vereinbarung getroffen werden, welche die Nutzung der mitarbeitereigenen Mobilgeräte regelt. Dabei sollten die Nutzungszeiten auf die Pausen beschränkt oder auf die Arbeitszeiten angerechnet werden. Weiter sollte es ein Verbot der Übertragung von betrieblichen Daten auf die mitarbeitereigenen Mobilgeräte und umgekehrt sowie ein Verbot der Verbindung der mitarbeitereigener Mobilgeräte mit dem betrieblichen Kommunikationssystem geben. Schließlich sollte es eine Pflicht zur Deaktivierung der Foto- und Webcam-Funktion geben, um insbesondere Betriebsgeheimnisse zu schützen.

71. Wie ist die Situation bei vorbehaltsloser Erlaubnis des Einsatzes von E-Mails zu privaten Zwecken?

Diese Alternative ist aus rechtlicher Sicht alles andere als ideal. Dem Arbeitgeber ist es verwehrt, den privaten E-Mailverkehr seiner Mitarbeiter zu lesen, ja geschweige denn zu archivieren, da das Fernmeldegeheimnis nach § 88 III TKG gilt. Konsequenz: Dem Arbeitergeber bleibt nichts anderes übrig, als sich, in der Regel sehr aufwendigen und damit kostenintensiven technischen Lösungen zu bedienen, die in der Lage sind, private Mails von dienstlichen zu trennen. Von manchen Juristen wird vertreten, dass es in diesem Fall dem Arbeitgeber nicht verwehrt werden dürfe, immerhin den Betreff der jeweiligen E-Mail zu öffnen bzw. sichtbar zu machen.

Dies ist jedoch abzulehnen, da jeglicher Inhalt der privaten Mail, also auch der Betreff, vom Fernmeldegeheimnis geschützt ist. Können private Mails von den betrieblichen Mails nicht unterschieden werden, ist dem Arbeitgeber auch der Zugriff auf die geschäftlichen Emails versagt.

Anders ist es nur hinsichtlich der Verkehrsdaten nach § 100 III TKG.

Der Zugriff auf den Inhalt der Emails kann für den Arbeitgeber zu einer Strafbarkeit nach §§ 206 und 202a StGB führen.

Theoretisch ist es möglich, dass der Arbeitgeber mit den Mitarbeitern Individualvereinbarungen trifft, in denen die Mitarbeiter in die Emailarchivierung einwilligen. Diese Einwilligung muss in Anlehnung an das BDSG freiwillig abgegeben werden. In der Praxis wird es jedoch nur schwer möglich sein, von allen Arbeitnehmern eine Einwilligung zu erhalten.

In dieser Konstellation ergibt sich eine Pflichtenkollision des Arbeitgebers. Er verletzt entweder die Straftatbestände nach §§ 206, 202a StGB (Datenschutz, Fernmeldegeheimnis) oder nach 238b StGB (Buchführungspflicht). Da es nun an einer Norm wie § 32 BDSG fehlt, welche die Datenerhebung an das Kriterium der Erforderlichkeit knüpft, wäre es denkbar über den rechtfertigenden Notstand nach § 34 StGB zu lösen. Dieser knüpft auch an eine Abwägung an. Ob die Einhaltung der Buchführungspflicht dem Interesse an Datenschutz und Fernmeldegeheimnis wie von § 34 StGB verlangt wesentlich überwiegt, ist Ansichtssache. Da es hierzu allerdings keine Rechtsprechung gibt, kann von dieser Lösung nur abgeraten werden.

72. Wie ist die Situation bei der Erlaubnis des Zugriffs auf Web-Accounts?

Der Arbeitgeber erlaubt den Zugriff auf eine private E-Mailadresse des Arbeitnehmers in einem Freemail-Account wie gmx.de, yahoo.de, web.de etc. und verbietet den privaten E-Mailverkehr über die geschäftliche E-Mailadresse. Dadurch bleibt die geschäftliche E-Mailadresse von privaten Inhalten frei und kann ohne Konflikt mit dem Fernmeldegeheimnis archiviert werden. Ein Verstoß dagegen ist ein Verstoß des Arbeitgebers gegen seine Treuepflicht, sodass er nicht mehr schutzwürdig ist.

Durch das Erlauben der privaten Nutzung wird der Arbeitgeber nun wieder Anbieter der

Telekommunikation. Wie oben dargelegt, darf dann der Arbeitgeber weder vom Inhalt noch von den Verbindungsdaten der Telekommunikation Kenntnis nehmen. Deshalb ist zu beachten, dass ein Firmennetzwerkrouter nicht die Webanfragen protokollieren darf. Ebenso darf dies nicht durch Proxy-Router geschehen. Denn auch diese schreiben normalerweise die Webanfragen mit. Eine Webanfrage ist der Aufruf einer (Web-) Seite über einen Browser.

Weiter sollte das private Surfen zeitlich beschränkt werden, also zum Beispiel auf die Zeiten von 08:00 Uhr bis 09:30 Uhr, von 12:00 Uhr bis 13:00 Uhr. Denn damit ist der Arbeitgeber nur in diesen Zeiträumen Anbieter nach dem TKG. Somit bleibt ihm in der übrigen Zeit die Möglichkeit die Arbeitnehmer zu überwachen (dazu mehr im 7.Teil der Serie „Überwachung und Kontrolle“).

73. Wie ist die Situation bei der Zuweisung einer privaten E-Mail-Adresse neben der geschäftlichen?

Den Mitarbeitern kann neben einer geschäftlichen E-Mailadresse auch eine privat und als solche gekennzeichnete E-Mailadresse (z.B. Max.Muster.Privat@Firmenname.de) zur Verfügung gestellt werden - verbunden mit der Auflage, dass nur letztere zu privaten Zwecken genutzt werden darf. Der Arbeitgeber würde dann nur die E-Mails der geschäftlichen E-Mailadresse archivieren. Damit würde eine zentrale, sowie effiziente Archivierung ermöglicht werden, da auf diese Weise eine Vermischung privater wie auch dienstlicher E-Mail ausgeschlossen sein würde. Nicht zuletzt würde man damit auch etwaigen Konflikten mit Betriebsräten aus dem Weg gehen können, die ansonsten bei betrieblichen Vereinbarungen zur E-Mailnutzung hinzugezogen werden müssten. So wird etwa das Mitbestimmungsrecht von Betriebsräten seitens der Rechtsprechung recht weit gefasst. Es sei demnach ausreichend, wenn technische Maßnahmen dazu geeignet sein könnten, den Arbeitnehmer zu überwachen - was naturgemäß gerade für Telekommunikationssysteme gilt.

Nicht ausreichend ist es, wenn im Rahmen der geschäftlichen E-Mailadresse nur zwei verschiedene (Unter-) Folder eingerichtet werden und einer für betriebliche E-Mails und der andere für geschäftliche E-Mails verwendet wird. Denn, wie im 4. Teil der Serie unter VII.2.c. beschrieben, werden die E-Mails bereits und sofort beim Eingang auf dem Server des Arbeitgebers archiviert. Somit wäre eine private E-Mail schon archiviert und die Trennung von den betrieblichen E-Mails käme zu spät.

Was passiert jedoch, wenn der Arbeitnehmer versehentlich (oder auch nicht) ein private E-Mail vom Account der geschäftlichen E-Mail-Adresse versendet? Dann kann sich unseres Erachtens der Arbeitgeber gegenüber dem Arbeitnehmer auf dessen Arbeitnehmertreupflicht berufen. Der Arbeitnehmer hat diese verletzt und ist nicht schutzwürdig, vor allem deswegen, weil der Arbeitgeber ausreichend tätig geworden ist, um dem Arbeitnehmer eine sichere Möglichkeit zur privaten Nutzung zu ermöglich.

74. Wie ist die Situation bei der Pflicht zur Kennzeichnung der privaten E-Mails?

Auch könnte man an Regelungen denken, die dem Mitarbeiter vorschreiben würden, private E-Mails auch im Header deutlich als "privat" zu kennzeichnen. (So wird es zum Teil auch von Behörden praktiziert.) Von manchen Juristen wird vertreten, dass es in diesem Fall dem Arbeitgeber nicht verwehrt werden dürfe, immerhin den Betreff der jeweiligen E-Mail zu öffnen bzw. sichtbar zu machen. Dies ist jedoch abzulehnen, da jeglicher Inhalt der privaten Mail, also auch der Betreff, vom Fernmeldegeheimnis geschützt ist. Können private Mails von den betrieblichen Mails nicht unterschieden werden, ist dem Arbeitgeber auch der Zugriff auf die geschäftlichen Emails versagt. Anders ist es nur hinsichtlich der Verkehrsdaten nach § 100 III TKG.

Praktisch schwierig wird es hierbei zudem, wenn jemand eine private E-Mail an den Arbeitnehmer schickt und nicht weiß, dass diese mit „privat“ gekennzeichnet sein muss. Dann kann diese Lösung versagen. Ob man hierbei noch einen Treuepflichtverstoß des Arbeitnehmers begründen kann, ist eine Entscheidung im Einzelfall.

75. Wie ist die Situation, wenn die Arbeitnehmer einen Ordner mit privaten E-Mails anlegen?

Hier liegt der Arbeitnehmer in seinem E-Mail-Programm einen (Unter-) Ordner an, der mit Privat gekennzeichnet wird und nicht bei der Archivierung erfasst wird. In diesen Ordner verschiebt er seine privaten E-Mails, bevor die Archivierung durchgeführt wird. Dazu darf allerdings nicht sofort beim Ein- und Ausgang der E-Mails auf dem Firmenserver archiviert werden. Sondern es muss ein bestimmter Zeitpunkt festgelegt werden bis zu welchem der Arbeitnehmer alle privaten E-Mails vom Posteingang und Postausgang in den Ordner Privat verschieben kann. Zum Beispiel könnte man festlegen, dass der Arbeitnehmer dies bis zum x-ten Tag eines jeden Monats zu tun hat.

Problematisch hierbei ist aber, dass nicht oder nur schwer verhindert werden kann, dass kurz vor der Archivierung noch eine private E-Mail eingeht.

76. Wie ist die Situation, wenn gesonderte Surfstationen eingerichtet sind?

Der Arbeitgeber kann seinen Arbeitnehmern gesonderte Rechner zur Verfügung stellen, von welchen aus die Arbeitnehmer auf das Internet und ggf. einen Drucker zugreifen können. Diese Rechner stehen auf einem zentralen Platz und dienen mehreren Arbeitnehmer zugleich, z.B. pro Abteilung oder pro Stockwerk ein Rechner.

Die Arbeitnehmer können von dort auf ihre Freemail-Accounts wie gmx.de, yahoo.de, web.de etc. zugreifen, sonstige Seiten ansurfen, Dateien herunterladen, Dateien drucken etc.. Dieser PC wird weder gebackupt, noch archiviert oder überwacht. Wenn ein Arbeitnehmer den Rechner verlässt, kann er den

Rechner herunterfahren bzw. neustarten. Der Rechner ist so konfiguriert, dass er bei jedem Herunterfahren ein komplettes Reset durchführt. Damit werden z.B. alle heruntergeladenen Daten des Arbeitgebers oder der Verlauf des Browsers gelöscht, sodass jeder nachfolgend nutzende Arbeitnehmer nicht auf die Daten seines Vorgängers sehen kann.

77. Wie ist die Situation, wenn die Arbeitnehmer in die E-Mail-Archivierung einwilligen?

Teilweise wird die Ansicht vertreten, dass der Arbeitnehmer in die Archivierung der privaten E-Mails einwilligen kann. Damit kann der Arbeitgeber dem Arbeitnehmer die private E-Mail-Nutzung gewähren, wenn der Arbeitnehmer vorher die Einwilligung abgibt. Andernfalls erteilt er ihm ein Verbot zur privaten Nutzung.
Begründet wird die Auffassung damit, dass der Arbeitnehmer auf den, ihm gesetzlich gewährten Schutz des Fernmeldegeheimnisses verzichten kann.

Die Gegenauffassung hält den Verzicht deshalb nicht möglich, da das Fernmeldegeheimnis auch für den Kommunikationspartner des Arbeitnehmers gilt. Für den Kommunikationspartner kann der Arbeitnehmer jedoch nicht „mitverzichten“.

Hiergegen wird zwar teilweise vertreten, dass das Fernmeldegeheimnis nur für den Arbeitnehmer gelte, da der Arbeitgeber nur gegenüber diesem Anbieter nach dem TKG werde. Dies ist unserer Meinung aber nicht richtig. Das Fernmeldegeheimnis gilt unserer Auffassung auch für den jeweiligen Kommunikationspartner. Demzufolge führt diese Lösung nicht zu einer Möglichkeit die private E-Mailnutzung und die Archivierung zu vereinen.

78. Wie ist die Situation, wenn das private Surfen über einen eigenen Proxyserver läuft?

Der Arbeitgeber richtet einen eigenen Proxyserver ein, über den ausschließlich das private Surfen der Arbeitnehmer läuft. Zudem ist auf allen lokalen Rechner eine Software installiert, über die der Arbeitnehmer bestimmen kann, ob er gerade privat oder dienstlich surft. Damit kann das private Surfen von dienstlichen getrennt werden. Die Arbeitnehmer dürfen die dienstliche E-Mailadresse nicht zu privaten Zwecken benutzen. Aber sie können jederzeit auf ihre Web-Accounts zugreifen.
Hinsichtlich der Daten, die auf dem Proxyserver für das private Surfen anfallen, ist der Arbeitgeber Diensteanbieter nach dem TKG, Damit hat er für diesen Server nur die beschränkten Zugriffsrechte, die ihm das TKG einräumt. Hinsichtlich der anderen Server, über die das dienstliche Surfen und E-Mailen läuft, ist der Arbeitgeber kein Diensteanbieter und damit kann er auf diese Server zugreifen. Somit ist die E-Mail-Archivierung möglich.

79. Sollte ein Arbeitgeber seine Arbeitnehmer kontrollieren?

Ja. Um zum Beispiel die Weitergabe von Betriebsgeheimnissen, eine unerlaubte private Nutzung des E-Mail-Systems, oder die Begehung von Straftaten durch den Arbeitnehmer aufzudecken und zu unterbinden, möchte und muss der Arbeitgeber den Arbeitnehmers kontrollieren und überwachen. Technisch gesehen greift der Arbeitgeber dabei auf den E-Mail-Server zu oder setzt einen Sniffer ein.

80. Inwieweit darf ein Arbeitgeber seine Arbeitnehmer kontrollieren?

Aber auch die Frage inwieweit der Arbeitgeber den Arbeitnehmer überwachen darf, sprich einzelne Mails lesen und das Abrufen von Internetseiten nachvollziehen darf, hängt vom TKG und dem BDSG ab.

81. Kann der Arbeitgeber kontrollieren, wenn die private Nutzung verboten ist?

Das TKG gilt in diesem Falle nicht, da der Arbeitgeber kein Dienstanbieter im Sinne des TKGs ist. Aber dann gilt das BDSG. Gemäß § 4 BDSG dürfen personenbezogene Daten nur erhoben oder genutzt werden, wenn dies durch den Betroffenen oder durch Gesetz oder eine andere Rechtsvorschrift gestattet ist.

Für die Überwachung kommt innerhalb eines Betriebes § 32 BDSG als gesetzliche Gestattung im Sinne des § 4 BDSG zur Anwendung. Dieser erlaubt nach Abs.1 S.1 die Erhebung, Verarbeitung und Nutzung personenbezogener Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist.

Erforderlich ist die Verwendung personenbezogener Daten dann, wenn keine objektiv zumutbare Alternative existiert. Die Erforderlichkeit ist anzunehmen, wenn die berechtigten Interessen des Arbeitgebers auf andere Weise nicht oder nicht angemessen gewahrt werden können. Es ist eine Interessensabwägung zwischen dem Datenschutz des Arbeitnehmers (Art. 2 I GG i.V.m. Art.1 I GG) und dem Schutz des eingerichteten und ausgeübten Gewerbebetriebes (Art. 14 I GG) vorzunehmen.

Im Rahmen der Überwachung eines Arbeitnehmers wird beim E-Mailverkehr zwischen den Verbindungsdaten (Datum, Uhrzeit, Datenvolumen und wohl auch E-Mail-Adressen) und dem E-Mail-Inhalten differenziert. Während erstere nach der Rechtsprechung gespeichert werden können, ist dies bei Letzteren umstritten.
Denn zum Teil werden die Grundsätze zur Telefonüberwachung als Vergleichsmaßstab heran gezogen. Danach ist eine Überwachung der -Mail nicht möglich, da die Inhalte eines Telefonats durch den Arbeitgeber weder mitgeschnitten noch mitgehört werden dürfen.

Teilweise wird die E-Mail jedoch mit dem Geschäftsbrief gleichgesetzt wird. Danach kann der Inhalt einer E-Mail problemlos, ebenso wie der Inhalt eines Geschäftsbriefes, gelesen werden. Diese Ansicht ist unserer Auffassung auch richtig, da die E-Mail wie ein Geschäftsbrief später für Dritte abrufbar ist und dies dem Arbeitnehmer beim Verfassen bewusst ist. Die Flüchtigkeit des gesprochenen Worts wie bei einem Telefonat ist bei der E-Mail nicht gegeben.

82. Wie kann der Arbeitgeber kontrollieren, wenn die private Nutzung verboten ist?

Hierbei ist jedoch auch zu beachten, dass die Kontrolle abgestuft im vorgenommen werden muss, um nicht unverhältnismäßig zu sein. Zunächst darf nur auf die Verbindungsdaten Zugriff genommen werden. Ist schon daran (z.B. an der Betreffzeile oder der Emailempfängeradresse) zu erkennen, dass ein Missbrauch vorliegt, ist eine Kenntnisnahme des Inhalts nicht mehr nötig.

Eine Überwachung, insbesondere eine Compliance-Überwachung, ist hier also zulässig.
Schließlich bleibt jedoch eine systematische und lückenlose Überwachung des E-Mail-Verkehrs und der Internetnutzung ein unzulässiger Verstoß gegen das allgemeine Persönlichkeitsrecht nach Art. 2 I, 1 I GG, da diese nicht erforderlich ist. Denn regelmäßig wird der Arbeitgeber die Missbrauch auch durch eine stichprobenartige Kontrolle feststellen können.

Allerdings verlangt § 32 I 2 BDSG für die Datennutzung zur Aufdeckung einer Straftat engere Voraussetzungen. Dafür müssen zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat. Weiter muss die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich sein und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung darf nicht überwiegen.

83. Wie kann der Arbeitgeber kontrollieren, wenn die private Nutzung erlaubt ist?

Mails nicht unterschieden werden, ist dem Arbeitgeber auch der Zugriff auf die geschäftlichen Emails versagt. Die Überwachung des privaten E-Mail-Verkehrs ist sowohl hinsichtlich der Verbindungsdaten als auch des Inhalts der E-Mails unzulässig. Denn dann gilt als spezielles Gesetz das TKG. In diesem gibt es keinerlei Rechtfertigungsgründe für das Lesen der Emails. Vielmehr kann das Lesen einer E-Mail durch den Arbeitgeber selbst eine Straftat nach § 206 StGB sein. Von der Unzulässigkeit des Lesens kann nur in ganz seltenen Fällen zur Missbrauchskontrolle (z.B. Verrat von Geschäftsgeheimnissen oder Begehung einer Straftat) und nur bei Vorliegen von konkreten Anhaltspunkten eine Ausnahme zugelassen werden. Folglich kann es auch hier zu einer Pflichtenkollision für den Arbeitgeber kommen: er darf nicht seine Compliancepflicht und ebenso den Datenschutz nicht verletzen.

Die einzige Ausnahme hierbei ist der Fall einer rechtswidrigen Inanspruchnahme der Telekommunikationsanlage. Dann darf der Arbeitgeber dann gemäß § 100 III TKG Verkehrsdaten erheben und verwenden. Allerdings gilt dies erst, wenn dem Arbeitgeber zu dokumentierende,

tatsächliche Anhaltspunkte für einen derartigen Missbrauch vorliegen.

84. Kann der Arbeitgeber einen Beweis, den er durch eine Kontrolle erlangt hat, in einem Gerichtsprozess verwenden?

Weiterhin ist fraglich, ob der Arbeitgeber, der durch eine Kontrolle einen Beweis für einen Missbrauch erlangt hat, diesen Beweis auch im Prozess verwenden darf. Denn im Prozessrecht gibt es bestimmte Beweisverwertungsverbote. Die herrschende Meinung differenziert danach, ob ein Beweismittel unter unverhältnismäßiger Verletzung von Grundrechten des Betroffenen erlangt wurde.

Bei der Missbrauchskontrolle von Internetnutzung ist das Wahrheitsermittlungsbedürfnis gegen das allgemeine Persönlichkeitsrecht des Arbeitnehmers abzuwägen. Das allgemeine Persönlichkeitsrecht wurde aber bereits bei der Prüfung der Rechtmäßigkeit der Kontrollmaßnahme im Rahmen des TKGs oder des BDSG berücksichtigt. Somit ergibt sich, dass ein Beweis, der rechtmäßig nach dem TKG oder dem BDSG erhoben wurde, auch verwertbar ist.

85. Können die Festplatten der lokalen Rechner der Mitarbeiter durch Backup gesichert werden?

Neben der E-Mailarchivierung und dem Backup der E-Mailordner werden in einem Unternehmen in aller Regel auch Backups der Festplatten der lokalen Rechner der einzelnen Mitarbeiter erstellt.

Auf der lokalen Festplatte können private Dateien des Arbeitnehmers (Fotos, Textdokumente etc.) gespeichert sein. Die Dateien kann der Arbeitnehmer auf dem Rechner originär erstellt, von einem externen Datenträger auf ihn übertragen oder durch Herunterladen aus dem Internet oder aus einer E-Mail auf ihm gespeichert haben.

Sollte die Datei aus einer privaten E-Mail heruntergeladen worden sein, zählt sie zwar zum Inhalt einer Fernkommunikation, jedoch unterliegt sie nicht mehr dem Fernmeldegeheimnis, da dieses endet, wenn die Übermittlung der Kommunikation beendet ist. Dies ist hier der Fall. Die Datei ist nun im alleinigen Herrschaftsbereich des Arbeitnehmers. Dies gilt unabhängig davon, ob die E-Mail samt Datei noch auf einem Server des Arbeitgebers liegt. Denn die E-Mail und Datei auf dem Server des Arbeitgebers ist immer noch vom Fernmeldegeheimnis geschützt.

Für die privaten Dateien, die der Arbeitnehmer auf seinem Rechner gespeichert hat, gilt dann das Bundesdatenschutzgesetz. Dann können wiederum individuelle Einwilligungen eingeholt oder eine Betriebsvereinbarung über das Backup geschlossen werden.

Schließlich kann das Backup auch durch § 32 BDSG gerechtfertigt werden, wenn das Backup ein für die

Durchführung des Arbeitsverhältnisses erforderliche Maßnahme ist. Erforderlich ist die Verwendung personenbezogener Daten dann, wenn keine objektiv zumutbare Alternative existiert. Die Erforderlichkeit ist anzunehmen, wenn die berechtigten Interessen des Arbeitgebers auf andere Weise nicht oder nicht angemessen gewahrt werden können. Es ist eine Interessensabwägung zwischen dem

Datenschutz des Arbeitnehmers (Art. 2 I GG i.V.m. Art.1 I GG) und dem Schutz des eingerichteten und ausgeübten Gewerbebetriebes (Art. 14 I GG) vorzunehmen.

Der Arbeitgeber hat ein berechtigtes Interesse daran, die Festplatten zu backupen, da dort wichtige Dokumente der Arbeit (wie Verträge, Vereinbarungen, Präsentationen, Fotos, Memos usw.) liegen, die nicht verloren gehen dürfen oder sollen. Die Abwägung fällt dahingehend aus, dass der Datenschutz zurücktreten muss. Ihm kann aber ausreichend Raum geschaffen werden, indem auf der Festplatte eines jeden lokalen Rechners ein Ordner „Privat“ eingerichtet wird, der nicht gebackupt wird. Speichert ein Arbeitnehmer eine Datei dann nicht im Ordner „Privat“, verstößt er gegen seine Arbeitnehmertreuepflicht und ist nicht mehr schutzwürdig.

86. Welche Punkte sollten in einer IT-Richtlinie in einem Unternehmen geregelt werden, um die Nutzung der gesamten Telekommunikation rechtsicher zu gestalten.

Die E-Mailarchivierung ist zwar ein zentraler Punkt, jedoch sollten bei der Erstellung einer IT-Richtlinie noch einige Punkte mehr beachtet werden. Im Folgenden werden diese aufgelistet und kurz beschrieben, Sie sind unseres Erachtens unbedingt regelungsbedürftig.

1. Ziel und Zweck der Richtlinie
2. Geltungsbereich / Verantwortlichkeit

2.1. Geltungsbereich der Richtlinie: für welche Beschäftigten, für welche Betriebsteile, für mobile Arbeit, auch außerhalb der Geschäftsräume?

2.2. Wer trägt die Verantwortlichkeit für die Richtlinie?

3. Arbeitsplatz

3.1. Allgemeine Regeln am Arbeitsplatz

beispielsweise: unbeaufsichtigte Rechner für Dritte nicht frei zugänglich lassen; Verhalten bei geplanter Abwesenheit (z. B. längere Besprechungen, über Nacht/ das Wochenende, Dienstreisen, Urlaub, Fortbildungsveranstaltungen)

3.2. Nutzung der betriebseigenen Hard- und Software

3.2.1. Nutzungsbedingungen, Pflege, Störungsmeldung

unter anderem: (Un-) Zulässigkeit der Verwendung von Instant-Messaging-Programmen, alternativen Browsern oder alternativen E-Mail Clients

3.2.2. Verbote

zum Beispiel: Benutzung betriebsfremder Hardware oder Software ohne die gültige Lizenz zu installieren, zu speichern oder in irgendeiner Form zu nutzen

4. Daten

4.1. Speicherung und Datenhaltung

beispielsweise: Datenspeicherung auf Netzwerklaufwerken oder lokalen Laufwerken

4.2. Datensicherheit

unter anderem: Schutz vor unerlaubtem bzw. unbeabsichtigtem Zugriff oder Möglichkeit des Zugriffs auf

die Daten durch einen Vertreter (bei Abwesenheiten, Krankheit etc.)

4.3. Datensicherung

zum Beispiel: Besondere Regelung für besonders wichtige Backups

5. Telefondienste

Umfasst sind Endgeräte (Festnetztelefone, Mobilteile, das Telefaxgerät), die hausinterne Telefonanlage samt Anschlüsse sowie die Mobiltelefone

5.1. Nutzung

5.1.1. Allgemeines

5.1.2. Mobiltelefon

dauerhaftes Mobiltelefon, ausgeliehenes Mobiltelefon

5.1.3. Private Nutzung

Unter anderem: Umfang, Tageseiten, Zulassung der privaten Nutzung ist eine freiwillige Leistung des Arbeitgebers

5.2. Kontrolle

5.2.1. Nicht personenbezogene Stichproben

5.2.2. Keine Leistungs- und Verhaltenskontrolle

5.2.3. Mobilfunk

Dokumentation über den Einzelgebührennachweis durch den Netzbetreiber

6. E-Mail und Internet

6.1. Nutzung zu dienstlichen Zwecken

6.1.1. Nutzungsvorgaben zum IT-System „E-Mail“

Beispielsweise: mehrmals tägliches Überprüfen des Postfachs; Zugang zu den E-Mails für einen Vertreter bei urlaubs- oder krankheitsbedingter und unerwarteter Abwesenheit; Verpflichtende Angabe einer standardisierten Signatur am Ende der E-Mail

6.1.2. In der Regel nur dienstlich veranlasste Nutzung von Internet- und E-Mail

6.2. Nutzung zu privaten Zwecken

6.2.1. Verbote private Nutzung

Vollständiges oder teilweises Verbot der privaten Nutzung

6.2.2. Gestattete private Nutzung

Mittel (Extra-Postfach für private E-Mails oder Browsernutzung für ein Webbasiertes Postfach); Umfang und Tageszeiten; Zulassung privater Nutzung stellt eine freiwillige Leistung des Unternehmens dar.

6.3. Verhaltensgrundsätze

Keine Nutzung der IT-Systeme „Internet“ und „E-Mail“ zu Zwecken, die die Interessen, das Ansehen oder die Sicherheit des Unternehmens beeinträchtigen oder die gegen geltende Rechtsvorschriften verstoßen.

6.3.1. Verbote

Unter anderem: Versand unternehmensrelevanter Daten ohne dienstliche Notwendigkeit an externe E-Mailkonten; Abrufen, Verbreiten oder Speichern von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, sexistischen, gewaltverherrlichenden oder pornografischen Äußerungen oder Abbildungen

6.3.2. Download von Software nur durch hierzu autorisierte Mitarbeiter
6.3.3. Blockierte Internetseiten

6.4. Kontrolle
6.4.1. Erhebung von Protokollen
Zweck, Umfang, Inhalt
6.4.2. Löschung von Protokollen
6.5. Technische Schutzeinrichtungen der IT-Systeme „E-Mail und Internet“
Unter anderem: E-Mail-Firewall, „Junk-E-Mail“-Ordnern, Anti-Virensoftware, keine Übermittlung von eingehenden E-Mails mit Anhängen, deren Umfang mehr als 20 MB beträgt
6.6. Gefährdung durch Schadprogramme
6.6.1. Präventive Maßnahmen
Zum Beispiel: Virenschutz-Software wie auch der lokalen Firewall beherrschen; Vermeidung nicht vertrauenswürdiger Websites, Beschränkung auf dienstliche Notwendigkeit
6.6.2. Anzeichen von Infektion durch Computer-Schadprogramme
6.6.3. Maßnahmen bei Verdacht auf Infektion durch Schadprogramme

7. Mobile Geräte und externe Datenträger
Zum Bereich mobiler Geräte gehören insbesondere Firmen-Handys, PDAs, Notebooks. Als externe Datenträger werden z.B. CDs, DVDs, USB-Sticks, mobile Festplatten, sonstige Speicher-Chips, Disketten etc. bezeichnet.
7.1. Allgemeine Richtlinien für den Umgang mit mobilen Geräten
Unter anderem: PIN bzw. ein Kennwort als Minimalschutz für den Start der Geräte; persönlich zugeteilte Firmennotebooks ggf. komplett verschlüsseln
7.2. Herausgabepflicht zum Ende des Arbeitsverhältnisses

8. Nutzung von Funknetzen (WLAN/WiFi, Bluetooth etc.)

9. Allgemeine IT-Sicherheitsbestimmungen
9.1. Verbote
Beispielsweise: Verwendung von Cracker- oder Hackermethoden ;Kein Vordringen in Bereiche des Netzwerkes oder einzelner Systeme, die nicht für den Arbeitnehmer selbst und sein Aufgabengebiet freigegeben oder vorgesehen sind
9.2. Kennwortgebrauch
9.2.1. Allgemeine Richtlinien für den Umgang mit Kennwörtern
Zum Beispiel: nur „komplexe“ Kennwörter vergeben; vertraulich behandeln; Änderung aus Sicherheitsgründen nach Ablauf eines bestimmten Zeitraumes (derzeit ca. 1 Jahr)
9.2.2. Herausgabepflicht zum Ende des Arbeitsverhältnisses

10. Missbrauchskontrolle / Maßnahmen bei Verstößen
Gezielte personenbezogene Auswertung bei begründetem Verdacht auf missbräuchliche/ unerlaubte Nutzung

11. Ständige Verbesserung der Sicherheitsstandards

12. Inkrafttreten

Zurück zu den[anderen Teilen der FAQ.](/faq-email-archivierung.html)

Autor:
RA Patrick Prestel