

von Rechtsanwalt **Max-Lion Keller**, LL.M. (IT-Recht)

Rechtliche Ausgestaltung einer IT-Betriebsvereinbarung

Es sollte mittlerweile für jedes Unternehmen eine Selbstverständlichkeit darstellen, den Angestellten in verbindlicher Art und Weise vorzugeben, in welcher Form die betriebseigenen Telekommunikationseinrichtungen (wie z.B. e-Mail, Internet, Telefon etc.) genutzt werden dürfen.

Dies ist jedoch meist keineswegs der Fall – wie die Beratungspraxis der IT-Recht Kanzlei zeigt. Stattdessen scheinen viele Geschäftsführer den Umstand schlicht zu ignorieren, dass es mittlerweile fast schon ein gesetzliches „Muss!“ darstellt, den Angestellten eine rechtlich verbindliche „Handlungsanleitung“ hinsichtlich des Umgangs mit unternehmenssensiblen Systemen vorzugeben.

Nur auf diese Weise ist es beispielsweise möglich,

- unter Berücksichtigung des geltenden Datenschutzrechtes die gesetzlichen Verpflichtungen hinsichtlich der revisionssicheren E-Mail Archivierung zu erfüllen,
- sicherheitsrelevante Risiken frühzeitig zu erkennen und wirkungsvoll zu begegnen. So werden heutzutage alle wesentlichen Funktionen und Aufgaben eines Unternehmens maßgeblich durch die Informationstechnik (IT) unterstützt. Ein Ausfall von IT-Systemen muss insgesamt kurzfristig kompensiert werden können – wofür auch die Einbeziehung der Mitarbeiterschaft gehört. Diese gilt es bezüglich der Themen „IT-Security“, Datenschutz und Risikoprävention zu sensibilisieren und ihr nicht zuletzt dadurch Rechtssicherheit zu verschaffen.

I. Das Gesetz ernst nehmen!

Die vorgenannten Punkte sollte auch jeder Geschäftsführer ernst nehmen, da das Gesetz seine persönliche Haftung für den Fall vorsieht, dass er Entwicklungen, die zukünftig ein Risiko für das Unternehmen darstellen könnten (dazu gehört eben auch die unterlassene Speicherung geschäfts- oder steuerrechtlich relevanter Mails), nicht durch ein Risikomanagement überwacht und durch geeignete Maßnahmen vorbeugt. Dies gilt sowohl für die persönliche Haftung

- des Vorstands einer AG (§ 91 Abs. 2 und § 93 Abs. 2 AktG),

- des Geschäftsführers einer GmbH, der die "Sorgfalt eines ordentlichen Geschäftsmannes" aufzubringen hat (§ 43 Abs. 1 GmbHG), als auch für

- anderer Gesellschaftsformen, wie etwa der Offene Handelsgesellschaft oder der Kommanditgesellschaft. Diese sind den Kapitalgesellschaften hinsichtlich der Rechtspflichten zur IT-Sicherheit dann gleichgestellt, wenn sie keine natürliche Person als persönlich haftende Gesellschafter haben (vgl. dazu das Kapitalgesellschaften und Co-Richtlinie-Gesetz, "KapCoRiLiG").

II. Rechtliche „Handlungsanleitung“ in Form einer Betriebsvereinbarung (oder auch einer „Mitarbeiterrichtlinie“)

Ziel einer jeden rechtlichen „IT-Handlungsanleitung“ sollte sein, allgemeine Richtlinien der Ausgestaltung und Entwicklung für das Arbeiten mit IT-Systemen aufzustellen, die Qualität der Arbeit zu fördern sowie die Mitarbeiter vor unzulässigen Verhaltens- und Leistungskontrollen und vor Eingriffen in das allgemeine Persönlichkeitsrecht zu schützen.

Im Folgenden werden nun die wichtigsten Regeln zur Nutzung der unternehmenseigenen „IT-Infrastruktur“ dargestellt, wie sie etwa auch im Rahmen einer Mitarbeiterrichtlinie (bzw. Betriebsvereinbarung) Eingang finden könnten. Dabei wird unter dem Begriff „IT-Infrastruktur“ die Gesamtheit aller Gebäude, Kommunikationsdienste (Netzwerk), Maschinen (Hardware) und Programme (Software) eines Unternehmens verstanden.

1. Regelungsbedarf: Infrastruktur (Gebäude etc.)

An erster Stelle einer jeden IT-Betriebsvereinbarung sollten sich konkret gefasste Vorgaben befinden, die die Sicherheit unternehmenseigener Gebäude, Räume, Fahrzeuge etc. zum Gegenstand haben. Dementsprechend könnte etwa geregelt werden,

- wie sich die Mitarbeiter den Zugang zum Gebäude verschaffen dürfen (etwa durch den Einsatz einer elektronischen Schließanlage und von Transponder-Systemen).

- wie die Zugangsrechte bezüglich besonders sensibler Räume geregelt sind.
- dass etwa darauf zu achten ist, dass alle sicherheitsrelevanten Zugänge, wie Gebäude- oder Bürozugänge in Zeiten, in denen ein Raum nicht besetzt ist, verschlossen sind. Dies bezieht, neben Türen, auch die Fenster im Erdgeschoss ein. wie man bei Verlust oder Diebstahl von Transpondern bzw. Schlüsseln zu reagieren hat.
- wie Alarmanlagen zu behandeln sind.
- was bei einem frühen Eintreffen oder auch spätem Verlassen des Gebäudes zu beachten ist – etwa wenn eine Sicherheitsfirma oder auch ein Hausmeister existent ist.
- wie sich Besucher anzumelden und beim Verlassen wieder abzumelden haben (Stichwort: Besucherausweis, Registrierung etc.).
- etc. etc.

2. Regelungsbedarf: Arbeitsplatz

Des Weiteren sollte die IT-Betriebsvereinbarung den Mitarbeitern deutlich vor Augen führen, dass gerade sie es sind, die für den Schutz der IT-Systeme vor unbefugter, unsachgemäßer und missbräuchlicher Benutzung Sorge zu tragen haben. Hierfür ist etwa unabdingbar, dass bestimmte Regeln am Arbeitsplatz eingehalten werden, wie z.B.

- die PC-Sperrung beim Verlassen des Arbeitsplatzes. Zudem sollte der Arbeitsplatz in einer Art und Weise verlassen werden, dass keine schutzbedürftigen Unterlagen zurückgelassen werden.
- der sensible Umgang mit Passwörtern.
- die Abmeldung des Dialogs bei servergestützten Anwendungen bei längerer Abwesenheit bzw. bei längerem Nichtgebrauch.
- dass bei Diensten der PC ordnungsgemäß auszuschalten und beispielsweise sämtliche Ausdrucke aus dem Drucker zu entfernen wären.

Anmerkung: Abhängig von der unternehmenseigenen IT-Infrastruktur empfiehlt die IT-Recht Kanzlei, dass besonders sensible bzw. unternehmenskritische Daten nicht auf der Festplatte des Arbeitsplatz-PCs gespeichert werden dürfen (da dort meist gespeicherte Daten nicht gesichert werden.) Vielmehr sollten Daten dieser Art stets und ausschließlich auf dem Netzlaufwerk gespeichert werden.

3. Regelungsbedarf: Telefon, Internet und E-Mail

Was viele nicht wissen: Nach einem Urteil des [Bundesarbeitsgerichts aus dem Jahr 2005 \(07.07.2005, Az. 2 AZR 581/04\)](#) ist die Benutzung betrieblicher Kommunikationseinrichtungen zu privaten Zwecken unzulässig und dies auch in den Fällen, dass keine ausdrücklichen betrieblichen Verbote zur privaten Nutzung existieren! Hier mag allenfalls eine äußerst kurzfristige private Nutzung des Internets während der Arbeitszeit allgemein gerade noch als hinnehmbar angesehen werden.

Vor dem Hintergrund greift auch das Argument der sog. „betrieblichen Übung“ in den Fällen nicht, dass der Arbeitgeber schlicht den Umgang mit betriebsinternen Telekommunikationssystemen bisher nicht geregelt hat. Hier gilt im Grundsatz, dass auch in diesem Fall den Mitarbeitern verwehrt ist, etwa das Internet zu privaten Zwecken in nicht nur geringfügiger Form zu nutzen.

Im Folgenden wird dargestellt, wie etwa die nur eingeschränkte private Nutzung der betriebsinternen Telekommunikationseinrichtungen rechtlich umgesetzt werden könnte.

3a. Nutzung des Telefons

Klargestellt muss zu Beginn sein, dass die private Nutzung von Telefondiensten nur im geringfügigen Umfang zulässig ist und das auch nur, soweit die betriebliche Aufgabenerfüllung sowie die Verfügbarkeit der Telekommunikationsanlagen für betriebliche Zwecke nicht beeinträchtigt werden. Der Begriff „geringfügiger Umfang“ ist nun natürlich äußerst dehnbar und sollte unbedingt konkretisiert werden - etwa dergestalt, dass dem Arbeitnehmer am Tag 2-3 kurze Telefonate während der Arbeitspausen gestattet werden könnten, die insgesamt auch nicht länger als etwa 5 min dauern dürften. Des Weiteren sollte unbedingt geregelt werden, dass

- insbesondere das Abrufen kostenpflichtiger Informationen bzw. das Anwählen von Servicenummern für den Privatgebrauch nicht gestattet ist.
- mittels privaten Telefonanrufen keine kommerziellen oder gar geschäftlichen Zwecke verfolgt werden dürfen.
- die Privatnutzung des betriebseigenen Telefons jederzeit ohne Angabe von Gründen widerrufen werden kann.
- aus Kostengründen Telefonate aus dem Festnetztelefon stets dem Mobiltelefon vorzuziehen sind.
- etc. etc.

Anmerkung: Zuletzt sollte der Arbeitnehmer auch noch deutlich darauf hingewiesen werden, dass zur Überprüfung der rechtlichen Vorgaben regelmäßige, nicht personenbezogene Stichproben durchgeführt werden – im Rahmen der geltenden datenschutzrechtlichen Bestimmungen.

3b. Nutzung des Internets und von E-Mail Systemen

Hier empfiehlt sich regelungstechnisch, zwischen der Nutzung der Systeme zu dienstlichen sowie zu privaten Zwecken zu unterscheiden.

3bi. Nutzung zu dienstlichen Zwecken

Zweck des Internets und der E-Mail ist es, den Mitarbeitern als Arbeitsmittel im Rahmen der Aufgabenerfüllung zur Verfügung zu stehen und damit auch insbesondere der Verbesserung der internen und externen Kommunikation, der Erzielung einer höheren Effizienz und der Beschleunigung der Informationsbeschaffung und der Arbeitsprozesse zu dienen.

Da jedoch per E-Mail abgegebene und eingegangenen Erklärungen grundsätzlich die gleiche rechtliche Bedeutung wie Brief- oder Faxsendungen zukommt, erfordert insoweit das Auftreten der Mitarbeiter im Internet zu dienstlichen Zwecken die Einhaltung bestimmter Regeln („Internet -Etikette“), wie etwa,

- dass Daten eines E-Mailkontos des Unternehmens nicht durch eine automatische Weiterleitung an externe E-Mailkonten, beispielsweise an Freemail-Konten wie GMX, WEB.DE etc. versendet werden dürfen.

- bei längere Abwesenheit im Postfach eine Abwesenheitsmeldung mit vordefiniertem Inhalt eingerichtet werden muss.
- bei einer geschäftlichen E-Mail es verpflichtend ist, dass am Ende der E-Mail eine Signatur angegeben wird.
- etc. etc.

3bii. Nutzung zu privaten Zwecken

Den Mitarbeitern sollte im Einzelnen vorgeschrieben werden, auf welche Art und Weise mittels E-Mails privat über die firmeninterne IT-Infrastruktur in geringfügigen Umfang (!) kommuniziert werden kann. Folgende Lösungen bieten sich hierzu an:

- Zeitliche Ausnahmeregelung ("Nutzung in Pausen und außerhalb der Arbeitszeit" oder "nur zwischen xx Uhr und yy Uhr") definieren, in der auf einen Freemail-Account (wie web.de) zugegriffen werden darf.
- Den Mitarbeitern kann neben einer geschäftlichen E-Mailadresse auch eine privat (und als solche gekennzeichnete) E-Mailadresse zur Verfügung gestellt werden - verbunden mit der Auflage, dass nur Letztere zu privaten Zwecken genutzt werden darf. Damit würde eine zentrale sowie effiziente Archivierung ermöglicht werden, da auf diese Weise eine Vermischung privater und dienstlicher E-Mail ausgeschlossen 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 aus-reichend, wenn technische Maßnahmen dazu geeignet sein könnten, den Arbeitnehmer zu überwachen - was naturgemäß gerade für Telekommunikationssysteme gilt.
- 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.)

Unbedingt zu regeln wäre zudem noch, dass etwa die

- Privatnutzung nicht zur Verfolgung gewerblicher oder geschäftsmäßiger Interessen erfolgen darf.
- Privatnutzung nicht zu Zwecken erfolgen darf, die die Interessen oder das Ansehen des Unternehmens beeinträchtigen können - wie etwa das Abrufen, Verbreiten oder Speichern von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, sexistischen, gewaltverherrlichenden oder pornografischen Äußerungen oder Abbildungen.
- Privatnutzung von E-Mails eine freiwillige Leistung des Unternehmens darstellt und jederzeit widerrufen werden kann.
- etc. etc.

Hinweis: Eine professionelle Mitarbeiterrichtlinie (oder auch Betriebsvereinbarung) würde des Weiteren

- Regelungen zum Schutz der IT-Systeme „Internet und E-Mail“ vorsehen,
- eine Handlungsanweisung bei Virenbefall vorgeben und
- klare Regelungen zum Thema „Kontrolle der Mitarbeiter“ enthalten.

4. Regelungsbedarf: Externe Datenträger

Als externe Datenträger werden z.B. CDs, DVDs, USB-Sticks, Speicher-Chips, Disketten, Speicher von Digitalkameras etc. bezeichnet. Insbesondere sie bergen ein großes Risiko, Viren in die IT-Systeme einzuschleusen. Aus diesem Grund sollten auch alle eventuell benötigten Daten und Programme auf externen Datenträgern von der IT-Abteilung (eigenständiges Kopieren ist zu untersagen) in das Netz eingespielt werden, die diese vorher auf Viren untersucht. Auch weitere rechtliche Vorgaben sind erforderlich, etwa dass der Zugriff auf externe Datenträger nur in Ausnahmefällen erlaubt sein sollte.

5. Regelungsbedarf: Passwortgebrauch, mobile Geräte und Home Office

Zum weiteren Regelungsumfang einer Betriebsvereinbarung könnte etwa noch der Umgang mit sensiblen Passwörtern, mobilen Geräten wie etwa Handys, PDAs und Laptops und auch die Nutzung und Gestaltung des häuslichen Arbeitsplatzes sein.

III. Fazit

Über kurz oder lang sollte in jedem Unternehmen verbindlich geklärt werden, in welcher Art und Weise die Mitarbeiter etwa zur Nutzung sensibler betriebsinterner Kommunikationseinrichtungen befugt sind. Hierzu bietet sich etwa eine IT-Betriebsvereinbarung oder auch eine sog. IT-Mitarbeiterrichtlinie (als ausgestaltetes Weisungsrecht des Arbeitgebers) an – am besten noch flankiert durch Einwilligungserklärungen der Mitarbeiter.

Autor:

RA Max-Lion Keller, LL.M. (IT-Recht)
Rechtsanwalt