von Rechtsanwalt **Patrick Prestel**

Regelungsbedürftige Punkte: für die Nutzung der Telekommunikationsanlagen (E-Mail, Telefon etc.) (9. Teil der neuen Serie der IT-Recht Kanzlei zu den Themen E-Mailarchivierung und IT-Richtlinie)

Der 9. Teil der Serie zeigt die nicht nur möglichen, sondern vielmehr notwendigen Punkten auf, die in einer IT-Richtlinie geregelt werden sollten, um die Nutzung der gesamten Telekommunikation in einem Unternehmen 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

Autor:
RA Patrick Prestel