

Der Eidgenössische
Datenschutzbeauf-
tragte informiert

Leitfaden über Internet- und E-Mail- Überwachung am Arbeitsplatz

Für öffentliche Verwaltungen und Privatwirtschaft

Inhaltsverzeichnis

Einleitung: Das Surfen und die Überwachung.....	3
1. Die wichtigsten netzbasierten Anwendungen.....	4
1.1 Anwendungen ohne inhaltliche Speicherung.....	4
1.2 Anwendungen mit inhaltlicher Speicherung.....	4
2. Tangierte Interessen des Arbeitgebers.....	6
3. Technische Schutzmassnahmen.....	9
4. Hinterlassene Spuren beim Surfen.....	11
5. Die Nutzungsregelung über privates Surfen und Mailen.....	13
6. Gesetzliche Grundlagen der Überwachung.....	16
7. Voraussetzungen für die Überwachung der Internet- und E-Mail-Nutzung.....	18
7.1 Die vorherige Information.....	18
7.2 Die Feststellung eines Missbrauches.....	19
8. Phasen der Überwachung.....	20
8.1 Erste Phase: Anonyme Kontrolle der Sicherheit und der Einhaltung der Nutzungsregelung.....	20
8.2 Zweite Phase: Feststellung von Auffälligkeiten.....	21
8.2.1 Weder Missbrauch noch technische Störung.....	21
8.2.2 Kein Missbrauch, aber technische Störung.....	22
8.2.3 Missbrauch, aber keine technische Störung.....	22
Spezialfall E-Mail.....	23
Spezialfall Straftat.....	24
8.2.4 Sowohl Missbrauch als auch technische Störung.....	26
9. Besondere Fälle des E-Mail-Missbrauches.....	27
10. Leistungsüberwachung und Geschäftskontrolle.....	28
11. Sanktionen bei Missbrauch.....	30
12. Ansprüche des Arbeitnehmers bei unzulässiger Überwachung.....	32
13. Weitere Bestimmungen des Datenschutzgesetzes.....	33
Fazit: Technische Schutzmassnahmen statt Überwachung.....	34
Anhang 1: Voraussetzungen und Ablauf.....	35
Anhang 2: Checkliste.....	36
Anhang 3: Fussnoten.....	39

Einleitung: Das Surfen und die Überwachung

Der Einzug der neuen Technologien in die Arbeitswelt hat Produktivität und Qualität eines Unternehmens gesteigert, brachte aber gleichzeitig weniger erfreuliche Phänomene mit sich: Unerlaubtes Surfen und E-Mails während der Arbeitszeit schadet den Unternehmen nicht nur finanziell, sondern kann auch den ganzen Datenverkehr eines Betriebs lahm legen oder die Speicherkapazität überfordern. Darüber hinaus kann das Besuchen illegaler Internetseiten für das Unternehmen nicht nur rufschädigend sein, sondern auch rechtliche Konsequenzen haben.

Die Schutzmassnahmen, die der Arbeitgeber gegen Missbräuche des Internets oder des E-Mails einsetzt, sind oft nicht weniger zweifelhaft. Spionprogramme und ständige Auswertungen der Internetspuren sind verbotene Beschneüfungen der Angestellten.

Ein Umdenken ist gefordert: Der Arbeitgeber hat seine Bemühungen auf die technische Prävention zu konzentrieren. Statt die Angestellten zu überwachen soll er technische Schutzmassnahmen einsetzen, die verbotenes Surfen verhindern und das Unternehmen vor technischem Schaden schützen. Nur wenn ein Missbrauch so nicht verhindert werden kann, darf er Internetspuren personenbezogen auswerten.

Der Arbeitgeber muss sich aber auch die Frage stellen, ob und in welchem Umfang ein Internetzugang für jeden Angestellten notwendig ist.

Dieser Leitfaden setzt sich zunächst mit den wichtigsten netzbasierten Anwendungen, deren Spuren sowie den tangierten Interessen des Arbeitgebers und den entsprechenden technischen Schutzmassnahmen auseinander. Anschliessend werden die gesetzlichen Grundlagen, die Voraussetzungen und der Ablauf der Internet- und E-Mail-Überwachung erörtert. Zum Schluss wird auf die Folgen missbräuchlicher Internetnutzungen und -überwachungen hingewiesen. Ein Ablaufschema im Anhang sowie eine Checkliste stellen die wichtigsten Punkte übersichtlich dar.

1. Die wichtigsten netzbasierten Anwendungen

Das Internet bietet eine Vielzahl von Anwendungen, die allgemein Internetdienste genannt werden, jedoch auch firmeninterne Netzdienste (Intranet) umfassen. Diese sogenannten netzbasierten Anwendungen können in zwei grössere Kategorien unterteilt werden, diejenigen ohne und diejenigen mit inhaltlicher Speicherung auf einem Datenträger des Arbeitgebers.

1.1 Anwendungen ohne inhaltliche Speicherung

Unter Anwendungen ohne inhaltliche Speicherung auf einem Datenträger des Arbeitgebers fällt zunächst das **klassische Surfen auf dem World Wide Web**, d. h. das Sichten von Webseiten, die auf unterschiedlichen Rechnern (Web Server) abgelegt sind und über eine eigene Adresse direkt abgerufen werden können. Spezielle Suchmaschinen wie Altavista oder Google ermöglichen eine Art Volltextsuche in einer weltweiten Datenbank nach benutzerdefinierten Kriterien. Von **multimedialem Surfen** spricht man dann, wenn Audio- und Videoquellen sowie die Telephonie netzbasiert sind.

Die sogenannten **Newsgroups** stellen öffentliche Diskussionsforen dar. Sie beruhen auf dem Prinzip des "Schwarzen Bretts" und werden daher als elektronische Pinnwand bezeichnet. Alle Teilnehmenden einer Newsgroup können Einsendungen abgeben, die dann von allen Internetnutzern abgerufen und gelesen werden können.

Beim **Internet Relay Chat (IRC)** findet über die Tastatur des Computers ein gesprächsartiger Meinungs-austausch in Echtzeit statt. Allen Teilnehmenden des Chat wird ein Name, meistens ein Pseudonym, zugewiesen, der es ermöglicht zu erkennen, von wem die Beiträge stammen.

1.2 Anwendungen mit inhaltlicher Speicherung

Bei Anwendungen mit inhaltlicher Speicherung auf einem Datenträger des Arbeitgebers geht es hauptsächlich um das **Herunter- und/oder Hinaufladen** von Dateien (Download/Upload) mittels Protokollen wie HTTP oder FTP. Klas-

Klassische Beispiele hierfür sind Anwendungsprogramme wie Freeware, Shareware, Spiele oder Musikdateien.

In diese Kategorie gehört zudem das Empfangen und Versenden von Nachrichten mit elektronischer Post, dem sogenannten **E-Mail**. Auf diese Weise können reine Textdokumente, gegebenenfalls mit angehängten Dateien aller Art, gezielt an andere Netzteilnehmende übermittelt werden. Das E-Mail entspricht damit funktionell weitgehend der herkömmlichen Post. Falls keine Verschlüsselung vorhanden ist, ist die Vertraulichkeit eines E-Mails mit derjenigen einer Postkarte vergleichbar.

Eine weitere Variante der elektronischen Post ist webbasiert. Ist diese verschlüsselt (Protokoll HTTPS/SSL), entgeht sie einer inhaltlichen Kontrolle durch den Arbeitgeber und gehört zu den Anwendungen ohne inhaltliche Speicherung beim Arbeitgeber.

2. Tangierte Interessen des Arbeitgebers

Durch Benutzung des vernetzten Computers am Arbeitsplatz können bestimmte Interessen und technische Einrichtungen des Arbeitgebers beeinträchtigt werden. Dies betrifft folgende Bereiche:

- Speicherkapazität und Netzwerkbandbreite, durch übermässige Internet- und E-Mail-Nutzung;
- Daten- und Anwendungssicherheit (Verfügbarkeit, Integrität, Vertraulichkeit), durch Einfuhr von Viren, Würmern, Trojanischen Pferden oder Installation von fremden Programmen;
- Arbeitszeit und andere finanzielle Interessen (Produktivitätsverluste, Kostensteigerung für zusätzliche Mittel und/oder Leistungen, Netzkosten, usw.);
- weitere rechtlich geschützte Interessen des Arbeitgebers, wie Ruf, Fabrikations- und Geschäftsgeheimnisse oder Datenschutz.

Die **Speicherkapazität** wird hauptsächlich durch heruntergeladene Dateien oder E-Mails beansprucht (vgl. Kapitel 1). Die beim Surfen oder Chatten abgerufenen Informationen werden vom System meist nur temporär auf der lokalen Festplatte gespeichert. Diese temporäre Speicherung wird nicht vom Benutzer ausgelöst, sondern ist systembedingt. Sowohl diese temporäre Dateien als auch die entsprechenden Randdaten (Verlauf/History) können vom Benutzer gelöscht werden, um einen persönlichen Beitrag zum Schutz der Privatsphäre zu leisten.

Die **Netzwerkbandbreite** wird hingegen sowohl bei den Anwendungen mit als auch bei denen ohne inhaltliche Speicherung beansprucht.

Eingehende E-Mails verbleiben in einem elektronischen Postfach eines Firmenservers, wo sie der Adressat entweder speichern oder löschen kann, nachdem er sie gelesen hat. Die Speicherung betrifft einerseits Randdaten wie Absender, Empfänger, Betreffzeile oder Datum, andererseits den Inhalt des E-Mails. Durch angehängte Dokumente wird die Speicherkapazität der Firma zusätzlich belastet.

Durch Installation fremder Programme wie Bildschirmschoner können berufliche Anwendungen unzugänglich gemacht (Verfügbarkeit) oder gefälscht (Integrität/Vertraulichkeit) werden. Die Hauptkategorien von Computerinfektionen sind Viren, Würmer und Trojanische Pferde.

Ein **Virus** ist ein Programmstück im Maschinencode, das sich vervielfacht, in andere Programme hineinkopiert und zugleich schädliche Funktionen in einem Rechnersystem ausführen kann¹. Viren werden von externen Quellen wie E-Mails, Disketten, Spiele oder Freeware eingeführt. Bestimmte Virenarten zerstören beispielsweise die Integrität einer Datei, indem sie Buchstaben ändern, andere können die gesamte Datei zerstören.

Ein **Wurm** ist ein eigenständiges Programm, das sich selbst durch Kopieren von einem System zum nächsten fortpflanzt, üblicherweise über ein Netzwerk. Ein Wurm kann, wie ein Virus, Daten direkt zerstören oder die Systemleistung heruntersetzen. Im weiteren schaden Würmer typischerweise, indem sie Trojanische Pferde übertragen.

Mit Hilfe dieser **Trojanischen Pferde** können z.B. Passwörter gestohlen werden, die es dann ermöglichen, Dateien unerlaubterweise anzusehen, zu verändern und zu löschen. Ein Trojanisches Pferd ist ein eigenständiges Programm, das vordergründig eine vorgesehene Aufgabe verrichtet, zusätzlich jedoch eine oder mehrere verborgene Funktionen enthält.² Wenn ein Benutzer das Programm aufruft, führt das Trojanische Pferd zusätzlich eine ungewollte sicherheitskritische Aktion aus. Die verbotene Funktion wird dabei mit den Privilegien des Benutzers ausgeführt, der das Programm aufgerufen hat.

Die Benutzung des Computernetzes verursacht in unterschiedlicher Weise **Kosten**, entweder pauschal oder zeit- und/oder volumenabhängig. Im Falle der Pauschaltariflösung spielt es für die effektiven Kosten keine Rolle, wie lange jemand surft, wohl aber im Zusammenhang mit der **verlorenen Arbeitszeit**. Werden hingegen zeit- und/oder distanzabhängige Kosten verrechnet, so kann die effektive Dauer des Surfens – neben der verlorenen Arbeitszeit – ins

Arbeitszeit – ins Gewicht fallen. In beiden Fällen kann eine erhöhte Bandbreitenkapazität erforderlich sein.

Weitere Kosten für den Arbeitgeber können durch die Nutzung von kostenpflichtigen Web-Angeboten entstehen, wenn der Zugriff in dessen Namen bzw. mit dessen Kreditkarte erfolgt. Arbeitnehmer können auch bewusst oder unbewusst im Namen der Firma im Internet Rechtsgeschäfte abschliessen und den Arbeitgeber dadurch verantwortlich machen.

Fabrikations- und Geschäftsgeheimnisse sowie **Datenschutzinteressen** der Firma können auch gefährdet werden, z. B. wenn vertrauliche Informationen per E-Mail an Unberechtigte versendet werden. Diese Gefahr wird erhöht durch den zunehmenden Einsatz von portablen Arbeitsinstrumenten wie Laptops, Personal Digital Assistants oder Handys. Die nachstehend erwähnten technischen Schutzmassnahmen finden bei diesen Geräten nur beschränkte Anwendung.³ Zusätzlich besteht die Gefahr, Geschäftsgeheimnisse zu verlieren, da Laptops leicht vergessen oder gestohlen werden können.

3. Technische Schutzmassnahmen

Es gibt keine absolute technische Sicherheit. Technische Schutzmassnahmen können jedoch die Risiken im Zusammenhang mit der Internet- und E-Mail-Nutzung reduzieren.

Durch den Einsatz von solchen Schutzmassnahmen erkennt der Arbeitgeber frühzeitig mögliche Gefahren für die Sicherheit und Funktionstüchtigkeit des elektronischen Systems. Die präventive Wirkung dieser Massnahmen soll den Einsatz repressiver Mittel wie die personenbezogene Überwachung weitgehend ersetzen (vgl. Kap. 8). Zu den wichtigsten technischen Schutzmassnahmen gehören Antivirus- und Diskquotaprogramme, Backups (Datensicherungen) und Firewalls. Zusätzlich sollen die Surf- und Mailprogramme nach dem letzten Stand der Technik⁴ installiert und in einer sicherheitsmässigen Form konfiguriert werden.⁵

Antivirusprogramme ermöglichen, Viren aufzuspüren und in der Regel auch zu entfernen. Sie müssen den aktuellen Virendatenbanken der neusten Softwareversion entsprechen und auf jedem Arbeitsplatz aktiv sein. Wenn es technisch nicht möglich ist, einen Virus zu entfernen, gestattet die regelmässige Datensicherung auf Backups die Wiederherstellung virenfreier Dateien.

Diskquotas sind Programme, welche im Betriebssystem installiert sind und die Speicherkapazität jedes Benutzers begrenzen. Dies führt zu einer Selbstbeschränkung, da eine Erweiterung des Speicherraumes begründet werden muss. Durch Diskquotas werden unnötige Überlastungen der Speicherkapazität vermieden, womit eine Intervention des Arbeitgebers in diesen persönlichen Räumen nicht mehr notwendig ist. Im Gegensatz zu Diskquotas eignet sich die Sperrung von E-Mails mit einer bestimmten Grösse als technische Schutzmassnahme nicht, da sie durch Aufteilen der betreffenden E-Mails leicht umgangen werden kann.

Firewalls schützen die eigenen Daten vor externen Angriffen⁶ und verhindern, dass Netzwerkbandbreite und Arbeitszeit übermässig beansprucht werden. Sie werden meist auf Netzebene zwischen Internet, Intranet und gegebenen-

gegebenenfalls Extranet⁷ eingesetzt und filtern den Datenverkehr in beide Richtungen nach USERID, IP-Adresse oder Applikationsprotokolle⁸. Die Firewall kann mit einer sogenannten Sperrliste erweitert werden. Diese enthält unerwünschte, vom Hersteller oder vom Arbeitgeber definierte URLs⁹. Eine andere Möglichkeit besteht in einer Positivliste, die diejenigen Internet-Adressen elektronisch freigibt, die notwendig sind, um die Aufgaben für die Firma zu erfüllen.

Firewalls können jedoch umgangen werden, indem ein Modem bei der lokalen Arbeitsstation eingesetzt wird.

Für die **Filetransferprotokolle** wie FTP und HTTP kann sich die Sperrung auch auf bestimmte Dateiformate (exe, mp3, usw.) beziehen. Eine ähnliche Sperrung kann auch für E-Mail-Anhänge erfolgen. Die Wirksamkeit solcher Sperrungen muss jedoch relativiert werden, da gewisse Formate, wie z. B. die komprimierte Archivdatei zip, in der Regel selber nicht gesperrt sind, aber gesperrte Dateiformate enthalten können. Die absolute Inhaltssicherheit (Content Security) ist also nicht möglich. Aus diesem Grund ist es auch nicht sinnvoll, auf die Chiffrierung zu verzichten, da diese dasselbe Problem für die Inhaltssicherheit darstellt wie zip-Dateien.

Als Ergänzung zu den Hardware-Netzfirewalls werden heute auch bei den einzelnen Arbeitsstationen Firewalls in Softwareform installiert, sogenannte Personal Firewalls.

Da diese technischen Schutzmassnahmen eine absolute Sicherheit nicht gewährleisten können, werden oft sogenannte **Intrusion Detection Systems** sowohl auf Netz- als auch auf Client-Ebene eingesetzt. Der Einsatz eines solchen Systems unterstützt die Aufdeckung von Missbräuchen.

Durch den Einsatz angemessener technischer Schutzmassnahmen sollten nur selten konkrete technische Störungen vorkommen.

4. Hinterlassene Spuren beim Surfen

Die Spuren, die bei der Benutzung netzbasierter Anwendungen hinterlassen werden, bestehen in der Regel nur aus den Randdaten "wer, was, wann". Unter einer Protokollierung versteht man eine fortlaufende Aufzeichnung dieser Randdaten. Ob Protokollierungen eingesetzt werden und wer darauf Zugriff hat, muss nach den Kriterien der Zweck- und Verhältnismässigkeit entschieden werden. Wenn z. B. präventive Massnahmen den Schutz sensibler Personendaten nicht gewährleisten, können Protokollierungen notwendig sein (Art. 10 Verordnung zum Bundesgesetz über den Datenschutz, VDSG, SR 235.11).

Die für die Überwachung am Arbeitsplatz relevanten Protokollierungen können an drei verschiedenen Stellen stattfinden: Auf den Netzkopplungselementen¹⁰, auf den Intranet-Servern¹¹ und auf dem Computer des Benutzers.

Auf der Ebene der **Netzkopplungselemente** können Protokollierungen, bestehend aus der IP-Adresse („wer“), der Zeitangabe („wann“¹²) und der abgerufenen URL („was“), generiert werden. Obschon die URL ein Randdatum ist, kann der abgerufene Inhalt in der Regel nachträglich wiederhergestellt werden. Es besteht auch die Möglichkeit einer Sperrung gewisser Datenflüsse. Versuche, diese Sperrungen zu durchdringen, werden ihrerseits protokolliert.

Im Logon auf **Intranet-Ebene** hingegen besteht die Protokollierung aus dem Benutzernamen (USERID, „wer“), gegebenenfalls mit der IP-Adresse, wenn letztere dynamisch vergeben wurde¹³. Die Zeitangabe („wann“) wird ebenfalls protokolliert, sowie der Gegenstand („was“) wie Ein- und Ausloggen, Ausdrucken, Applikationsabruf, usw.

In den E-Mail-Servern (Schnittstelle Intra-/Internet) werden Absender- und Empfängeradresse, Zeitangabe und Betreffzeile der E-Mails protokolliert sowie der Zeitpunkt, wann ein E-Mail gelesen bzw. versandt wurde.

Auf dem **Computer des Benutzers** können durch den unzulässigen Einsatz von sogenannten Spionprogrammen (vgl. Kapitel 6) sämtliche Aktivitäten festgehalten werden.

Sogenannte **Sniffer** können eingesetzt werden, um eine detaillierte Protokollierung der übertragenen Datenpakete, sowohl der Randdaten als auch der Inhalte, zu erstellen.

Sicherheitskopien von Dateien (Backups) stellen eine Protokollierung dar und sollten somit nur mit Vorsicht ausgewertet werden.

Zudem gestatten mehrere Surfprogramme (Browser) während einer bestimm- baren Zeit die Protokollierung aller Internet-Zugriffe auf der Festplatte des Computers (Verlauf/History). Diese Surfprogramme erstellen sogar temporäre Dateien der Inhalte (Cache) und permanente Spuren-Dateien (Cookies) über die besuchten Seiten.

Abgerufene Internet-Seiten können Gegenstand einer Zwischenspeicherung in einem sogenannten Proxy-Server im Intranet sein. Jeder andere Zugriff auf diese Seite durch andere Arbeitnehmer derselben Firma erfolgt direkt beim Proxy-Server. Somit erübrigt sich einen neuen Zugriff auf das Internet.

5. Die Nutzungsregelung über privates Surfen und Mailen

Ob Angestellte das Recht haben, privat Internet und E-Mail zu nutzen, hängt in erster Linie vom Willen des Arbeitgebers ab. Ähnlich wie in anderen Bereichen des Arbeitsverhältnisses, hat er ein Weisungsrecht (Art. 321d Obligationenrecht, OR, SR 220). Wichtig ist, dass der Arbeitgeber die effektiven beruflichen Bedürfnisse seiner Angestellten differenziert überprüft, bevor er ihnen den Internetzugang gewährt. Durch spezifische Schulung sollen die Angestellten auf die Sicherheitsgefahren bei der Benutzung netzbasierter Anwendungen sensibilisiert werden.

Für den Arbeitgeber ist es ratsam, eine schriftliche Weisung über die Nutzung netzbasierter Anwendungen zu erlassen, obschon dies nicht obligatorisch ist. Eine solche Nutzungsregelung schafft Transparenz und Rechtssicherheit in den Beziehungen zwischen Arbeitgeber und Arbeitnehmer. Jeder Arbeitnehmer sollte daher am besten schriftlich über die Regelung informiert werden. Eine nur mündlich kommunizierte Nutzungsregelung ist zwar ebenfalls verbindlich, kann aber im Streitfall zu Nachweisschwierigkeiten führen. Deshalb ist allen Angestellten ein schriftliches Exemplar auszuhändigen, dessen Empfang sie quittieren.

Die private Benutzung der netzbasierten Anwendungen wird je nach Nutzungsregelung entweder zugelassen, eingeschränkt oder ganz verboten.

Eine Einschränkung kann auf unterschiedliche Weise erfolgen. Die zeitliche Begrenzung privater Surftouren, z. B. 15 Minuten pro Tag, ist aus zwei Gründen nicht empfehlenswert: Einerseits ist nicht feststellbar, ob sie eingehalten wird, da der Zeitpunkt, wann eine Internet-Seite verlassen wird, in der Regel nicht protokolliert wird. Andererseits würde eine Protokollierung der Nutzungsdauer kaum zuverlässige Rückschlüsse auf die effektive zeitliche Beanspruchung ermöglichen, da die abgerufene Internet-Seite hinter einer anderen Applikation (z. B. dem Textverarbeitungsprogramm) offen bleiben kann, ohne dass sie jedoch tatsächlich benutzt wird. Erst die Protokollierung einer Reihe aufeinanderfolgender Internet-Zugriffe vom selben Computer aus innerhalb

innerhalb einer bestimmten Zeitspanne könnte Rückschlüsse auf die tatsächliche Benutzungsdauer ermöglichen, wenn die einzelnen Zugriffe in kurzen Zeitabständen voneinander erfolgt sind. Eine 100%-ig richtige Aussage über die Dauer der Benutzung netzbasierter Anwendungen lässt sich aber auch in solchen Fällen nicht machen.

Eine Einschränkung kann erfolgen durch Sperrung unerwünschter Internetangebote (Börse, elektronische Stellenanzeiger, E-Commerce-Seiten, pornographische oder rassistische Texte oder Bilder, usw.), durch Festsetzung einer bestimmten, beanspruchbaren Speicherkapazität des Servers (vgl. Kapitel 3) oder eines Zeitpunktes, ab welchem eine private Benutzung erlaubt ist (z. B. ab 18 Uhr).

Die Einschränkung oder das Verbot der privaten Benutzung netzbasierter Anwendungen kann auch durch Umschreibung der zugelassenen Internetangebote erfolgen, mit einer Positivliste, die z. B. nur die Informationsbeschaffung auf Internet-Seiten offizieller Behörden erlaubt (vgl. Kapitel 3). Im Allgemeinen ist eine Surf tour zulässig, wenn sie beruflichen Zwecken dient.

Falls die Internetnutzung eingeschränkt ist, könnte es eine Lösung sein, wenn der Arbeitgeber – ähnlich wie beim Telefon – ein unüberwachtes, von den Benutzern zu zahlendes Internet-Terminal zur Verfügung stellt.

Wenn keine Nutzungsregelung besteht, können die Angestellten davon ausgehen, dass die private Internetnutzung erlaubt ist, auch wenn privates Telefonieren verboten sein sollte.¹⁴ Die Interessen und Mittel des Arbeitgebers müssen aber gewährleistet bleiben. Letzteres hängt mit der Sorgfalts- und Treuepflicht (Art. 321a OR) zusammen, die den Arbeitnehmer verpflichtet, die Interessen des Arbeitgebers zu wahren. Was dies im Zusammenhang mit der Internetnutzung bedeutet, hängt von den konkreten Umständen im Einzelfall ab. Die Gefahr besteht, dass der Arbeitgeber falsch beurteilt, ob eine Surf tour zulässig ist.

Aus diesen Gründen ist es empfehlenswert, eine schriftliche Nutzungsregelung zu erlassen. Je konkreter und klarer diese ist, desto unmissverständlicher sind die Grenzen der erlaubten privaten Internetnutzung am Arbeitsplatz.

Viele Arbeitgeber stellen ihren Angestellten tragbare Arbeitsinstrumente zur Verfügung. Diese sind auch von der Überwachung betroffen, was ein besonderes Problem darstellt, da diese Geräte oft auch privat benutzt werden.

6. Gesetzliche Grundlagen der Überwachung

Die Gefahr der dauerhaften Verhaltensüberwachung der Arbeitnehmer am Arbeitsplatz war 1984 Auslöser einer parlamentarischen Motion¹⁵ über den Persönlichkeitsschutz von Angestellten. Infolge dieser Motion erliess der Bundesrat eine Verordnung, welche die gezielte Verhaltensüberwachung am Arbeitsplatz verbietet (Art. 26 Abs. 1 Verordnung 3 zum Arbeitsgesetz, ArGV 3, SR 822.113). Sind Überwachungs- und Kontrollsysteme aus anderen Gründen erforderlich, müssen sie so gestaltet und angeordnet sein, dass sie die Gesundheit und die Bewegungsfreiheit der Arbeitnehmer nicht beeinträchtigen (Art. 26 Abs. 2 ArGV 3). Geschützt werden soll in erster Linie die Gesundheit und die Persönlichkeit der Arbeitnehmer vor ständiger, gezielter Verhaltensüberwachung durch Einsatz eines Überwachungssystems.¹⁶ Die Verhaltensüberwachung ohne Überwachungssystem fällt nicht in den Anwendungsbereich von Art. 26 ArGV 3.

Im Zusammenhang mit der Nutzung von Internet und E-Mail am Arbeitsplatz bedeutet dies, dass ständige, personenbezogene Überwachungen der Internetnutzung durch Auswertung der Protokollierungen nicht zulässig sind. Aus diesem Grund dürfen auch Spionprogramme¹⁷ nicht eingesetzt werden. Letztere werden überdies meist unangekündigt gebraucht.

Gestattet sind stichprobenartige, anonyme Kontrollen der Protokollierungen, um zu überprüfen, ob die Nutzungsregelung eingehalten wird.

Sowohl der Einsatz technischer Schutzmassnahmen als auch die Kontrolle der Einhaltung der Nutzungsregelung sind im Grunde genommen nichts anderes als anonyme Verhaltensüberwachungen. Wenn diese Massnahmen einen konkreten Missbrauch aufzeigen – und die Belegschaft vorher entsprechend informiert wurde – kann dies zu einer personenbezogenen Verhaltensüberwachung führen, indem die Protokollierungen ausgewertet werden. Solche Auswertungen dienen dazu, Beweise zu erheben, um Missbräuche sanktionieren zu können, die durch fehlende oder mangelhafte technische Schutzmassnah-

technische Schutzmassnahmen nicht verhindert werden konnten (z. B. Zugriffe auf Internetseiten, die nicht auf die Sperrliste der Firewall figurieren, vgl. Kapitel 8, b2 und b4).

Das Verbot der Verhaltensüberwachung gemäss Art. 26 ArGV3 gilt also nicht absolut. Es geht vielmehr darum, den Persönlichkeitsschutz der Arbeitnehmer und die Interessen des Arbeitgebers (vgl. Kapitel 2) gegeneinander abzuwägen. In Einzelfällen, wenn Missbräuche festgestellt werden und die entsprechende vorherige Information besteht, dürfen personenbezogene Verhaltensüberwachungen vorgenommen werden. Werden keine Missbräuche festgestellt, müssen sowohl die Gewährleistung der Sicherheit als auch die Kontrollen der Einhaltung der Nutzungsregelung anonym bleiben.¹⁸

Deswegen ist es empfehlenswert, die Korrespondenzliste der Benutzernamen mit den IP-Adressen und die Protokollierungen der besuchten Internetseiten separat aufzubewahren. Diese Protokollierungen dürfen nur bei einem Missbrauch und vorheriger Information der Arbeitnehmer (vgl. Kapitel 7) mit der Korrespondenzliste verknüpft werden. Sind Benutzername und Protokollierung nicht trennbar, z. B. in der Proxy-Firewall, empfiehlt es sich, erstere zu pseudonymisieren.

Es ist aber zu bedenken, dass weder getrennte Listen noch Pseudonymisierung der Benutzernamen eine anonyme Überwachung garantieren, wenn die IP-Adressen der einzelnen Arbeitsstationen allgemein bekannt sind.

Die berufliche Leistung darf vom Arbeitgeber überwacht werden, was im Kapitel 10 behandelt ist.

Neben Art. 26 ArGV 3 schützen auch das Datenschutzgesetz sowie Art. 328 und 328b OR die Persönlichkeit des Arbeitnehmers. Diese Bestimmungen sehen auch vor, dass der Arbeitgeber Personendaten nur unter Einhaltung des Zweck- und Verhältnismässigkeitsprinzips bearbeiten darf.

7. Voraussetzungen für die Überwachung der Internet- und E-Mail-Nutzung

Um eine personenbezogene Überwachung einleiten zu dürfen, muss der Arbeitgeber die Belegschaft vorher informieren und einen Missbrauch festgestellt haben. Im Detail gelten folgende Regeln.

7.1 Die vorherige Information

Anders als bei der Nutzungsregelung, die nicht obligatorisch ist, hat der Arbeitgeber die Pflicht, eine Überwachungsregelung zu erlassen, da die Überwachung einen Eingriff in die Privatsphäre des Arbeitnehmers darstellen kann (Prinzip von Treu und Glauben, Art. 4 Abs. 2 DSG). Ein solcher Eingriff ist dann gegeben, wenn Protokollierungen privater Surftouren personenbezogen ausgewertet werden.

Der Arbeitgeber muss darüber informieren, dass die Möglichkeit der personenbezogenen Auswertung der Protokollierungen besteht und dass die Auswertungsergebnisse an die Vorgesetzten weitergegeben werden, falls ein Missbrauch festgestellt wird. Sieht die Überwachungsregelung diese Information nicht vor, so muss dies nachgeholt werden, bevor Protokollierungen personenbezogen ausgewertet werden.

Empfehlenswert ist auch darüber zu informieren, wer für die personenbezogenen Auswertung der Protokollierungen zuständig ist, welche konkreten arbeitsrechtlichen Sanktionen ergriffen werden können und wie bei Verdacht auf eine Straftat vorgegangen wird. Ratsam ist ferner die Information über die eingesetzten Protokollierungen, deren Zweck, Inhalt und Aufbewahrungsdauer.

Über die anonymen Kontrollen muss der Arbeitgeber seine Belegschaft nicht zwingend informieren, aus Transparenzgründen ist jedoch auch dies empfehlenswert.

Die Kenntnis, dass eine Überwachung möglich ist, kann eine abschreckende Wirkung auf das Surfverhalten der Angestellten haben.

7.2 Die Feststellung eines Missbrauches

Ein Missbrauch liegt vor, wenn die Nutzungsregelung verletzt worden ist. Missbräuchlich ist je nach Nutzungsregelung z. B. das Surfen auf Web-Seiten, die keine berufliche Relevanz aufweisen, oder das private Surfen tout court, wenn es ausdrücklich verboten wurde. Der Versuch, auf Internetseiten zuzugreifen, die durch technische Schutzmassnahmen gesperrt wurden, stellt hingegen keinen Missbrauch dar.

Fehlt eine Nutzungsregelung, so können die Treuepflicht oder das Zweck- und Verhältnismässigkeitsprinzip trotzdem verletzt werden. Ist dies der Fall, dann spricht man auch von einem Missbrauch (vgl. Kapitel 5).

Der Arbeitgeber muss daran denken, dass die IP-Adresse (vgl. Kapitel 4) und somit die Identität des fehlbaren Arbeitnehmers bewusst vertuscht werden kann, z. B. indem jemand den PC eines anderen Mitarbeiters fürs private Surfen verwendet. Arbeitsrechtliche Sanktionen dürfen nur bei 100%-iger Sicherheit über die Identität des fehlbaren Arbeitnehmers getroffen werden.

8. Phasen der Überwachung

Um eine Übersicht über die verschiedenen Phasen zu bekommen, kann das Ablaufschema im Anhang 1 konsultiert werden. Im Folgenden werden die einzelnen Schritte der Überwachung genauer kommentiert.

8.1 Erste Phase: Anonyme Kontrolle der Sicherheit und der Einhaltung der Nutzungsregelung

Eine Aufgabe der Informatikdienste oder Sicherheitsbeauftragten eines Unternehmens besteht in der Gewährleistung der Sicherheit und Funktionstüchtigkeit der technischen Mittel. In Kleinbetrieben ist der Vorgesetzte dafür selber zuständig. Die Gewährleistung der Sicherheit erfolgt laufend, meistens durch den Einsatz von technischen Schutzmassnahmen (z. B. Intrusion Detection System). Die Abwehr von internen oder externen Angriffen wird weitgehend diesen Massnahmen überlassen.

Der Arbeitgeber hat dafür zu sorgen, dass die technischen Schutzmassnahmen regelmässig dem neuesten Stand der Technik angepasst werden.

Sofern keine sicherheitsrelevanten Gefahren oder Angriffe verzeichnet werden, spielen die Protokollierungen bei der Gewährleistung der Sicherheit und Funktionstüchtigkeit keine Rolle. Demzufolge dürfen sie auch nicht personenbezogen ausgewertet werden. Erst wenn eine technische Störung vorliegt, können die Protokollierungen beigezogen werden, um deren Ursache zu klären. In dieser Phase der Überwachung kommt zum Ausdruck, dass der technische Schutz der Ressourcen Vorrang vor jeglicher personenbezogenen Kontrolle hat.

Unter der Voraussetzung, dass die Angestellten vorgängig darüber informiert wurden, darf der Arbeitgeber mit Hilfe der Protokollierungen kontrollieren, ob das Verbot bzw. die Einschränkung der privaten Internet- und E-Mail-Nutzung eingehalten wurde. Die Aufgabe kann vom Sicherheits- oder vom Datenschutzbeauftragten wahrgenommen werden. Die Person, die für die Kontroll-

Kontrollaufgabe zuständig ist, muss über ihre Verantwortung klar informiert werden, besonders im Zusammenhang mit personenbezogenen Auswertungen.

Die Kontrollen der Einhaltung der Nutzungsregelung dürfen nur stichprobenartig, nach einem bestimmten Zeitplan (z. B. einmal pro Monat) erfolgen und nur eine beschränkte Benutzungsdauer (z. B. die letzten 5 Tage des Monats) decken. Die Überwachung der gesamten Zeitspanne seit der letzten Stichprobe käme einer ständigen Verhaltensüberwachung gleich, welche gemäss Art. 26 ArGV 3 nicht zulässig ist.¹⁹ Die Kontrolle erfolgt in dieser Phase anonym, da mit einem Missbrauch nicht a priori zu rechnen ist.

Die Protokollierungen der E-Mail-Nutzung betreffen die Adressierungselemente (darunter vor allem die Absender- und Empfängeradresse), weswegen diese Kontrolle von der Technik her immer personenbezogen erfolgt. Der Arbeitgeber muss deswegen den Sicherheitsbeauftragten darauf aufmerksam machen, dass diese Daten vertraulich sind und dass eine ständige Überwachung des E-Mail-Verkehrs nicht erlaubt ist.

8.2 Zweite Phase: Feststellung von Auffälligkeiten

Bei einer Gewährleistung der Sicherheit bzw. der anonymen Kontrolle der Einhaltung der Nutzungsregelung, oder durch andere Hinweise, die nicht auf einer personenbezogenen Auswertung der Protokollierungen beruhen, können vier verschiedene Szenarien eintreffen:

- Weder Missbrauch noch technische Störung
- Kein Missbrauch, aber technische Störung
- Missbrauch, aber keine technische Störung
- Sowohl Missbrauch als auch technische Störung

8.2.1 Weder Missbrauch noch technische Störung

Wird kein Missbrauch festgestellt, hat der Arbeitgeber die technischen Schutzmassnahmen und/oder die Nutzungsregelung nur an den technischen

Fortschritt anzupassen, z. B. durch die Beschaffung eines neuen, effizienteren Antivirusprogramms oder durch die Erweiterung der Firewall mit einer überarbeiteten Sperrliste. Eine personenbezogene Auswertung der Protokollierungen ist nicht erlaubt.

8.2.2 Kein Missbrauch, aber technische Störung

Beispiele für eine technische Störung ohne Missbrauch sind eine Lahmlegung des betrieblichen Datenverkehrs, weil die Netzwerkbandbreite überfordert wurde, oder ein Computerabsturz, nachdem der Informatikdienst ein Programm fehlerhaft installiert hat oder weil ein Virus – beim beruflichen Surfen – eingeschleppt wurde.

Die technischen Schutzmassnahmen werden angepasst, um diese konkreten technischen Störungen in Zukunft zu vermeiden. Auch in diesem Szenario ist eine personenbezogene Auswertung der Protokollierungen nicht erlaubt, da kein Missbrauch vorliegt.

Durch den Einsatz angemessener technischer Schutzmassnahmen sollten konkrete technische Störungen kaum vorkommen.

8.2.3 Missbrauch, aber keine technische Störung

Verschiedene Anzeichen können auf einen Verstoss gegen das Verbot des privaten Surfens während der Arbeitszeit hinweisen: Anhaltspunkte können sich bei einer anonymen Kontrolle der Protokollierungen ergeben, wenn übermässige Netzkosten festgestellt werden oder wenn offensichtlich privat ausgedrucktes Material vorgefunden wird. Der Arbeitgeber passt daraufhin die technischen Schutzmassnahmen sowie, wenn nötig, die Nutzungsregelung an. Da der festgestellte Missbrauch keine technische Störung hervorgerufen hat, informiert der Arbeitgeber zuerst die gesamte Belegschaft über den Missbrauch sowie über die Möglichkeit personenbezogener Auswertungen der Protokollierungen, wenn weitere Missbräuche festgestellt werden sollten. Ob der fehlbare Arbeitnehmer sofort oder erst bei einer Wiederholung eines Missbrauchs identifiziert werden soll, entscheidet der Arbeitgeber aufgrund der Schwere des ersten Missbrauchs.

Die Identifikation erfolgt durch Vergleich der Internet-Protokollierungen (IP-Adresse) mit dem entsprechenden Benutzernamen (USERID). Der Benutzername befindet sich im Falle der statisch vergebenen IP-Adresse (vgl. Kapitel 4) auf einer vom Intranet-Administrator verwalteten Korrespondenztabelle. Bei der dynamischen Vergabe der IP-Adresse ist die Korrespondenz in den Intranet-Logon-Protokollierungen zu finden. Im besonderen Fall der Proxy-Firewall (vgl. Kap. 6) befinden sich IP-Adresse und Benutzername sogar in der gleichen Protokollierung.

Die Auswertung der Protokollierung geht an den Vorgesetzten, der die passenden arbeitsrechtlichen Massnahmen, die in der Nutzungsregelung vorgesehen sind, gegen den fehlbaren Arbeitnehmer treffen kann (vgl. Kapitel 11).

Spezialfall E-Mail

Die Kontrolle der Einhaltung des Verbotes bzw. der Einschränkung der privaten E-Mail-Nutzung am Arbeitsplatz geschieht aufgrund der Adressierungselemente. Der Arbeitgeber darf keine Einsicht in den Inhalt privater E-Mails haben (für die geschäftlichen E-Mails vgl. Kapitel 10).

In der Praxis stellt sich das Problem, dass E-Mails aufgrund der Adressierungselemente nur selten oder gar nicht deutlich als privat bzw. beruflich eingestuft werden können. Der Sicherheitsbeauftragte muss sich in solchen Fällen an den betroffenen Arbeitnehmer wenden, um die Natur eines fraglichen E-Mails zu klären. Stellt sich heraus, dass das E-Mail privater Natur ist, kann der Sicherheitsbeauftragte den Vorfall dem Vorgesetzten melden, ohne dabei in den Inhalt Einsicht genommen zu haben.

Die Unterscheidung zwischen privaten und beruflichen E-Mails erleichtern könnte ein Vermerk „privat“ oder „persönlich“. Die Angabe „vertraulich“ ist ungeeignet, da sie sich auch auf geschäftliche E-Mails beziehen kann.

Eine weitere Möglichkeit, den Inhalt privater E-Mails zu schützen, besteht darin, einen verschlüsselten E-Mail-Dienst zu gebrauchen.²⁰ Ohne Verschlüs-

Verschlüsselung entspricht die Vertraulichkeit eines E-Mails derjenigen einer Postkarte.

Ob internetbasierte, verschlüsselte E-Mail-Dienste überhaupt benutzt werden dürfen, hängt von der Nutzungsregelung ab. Ist die Internetnutzung verboten, geht der Arbeitnehmer das Risiko ein, wegen privaten Surfens am Arbeitsplatz sanktioniert zu werden. Der Einsatz eines firmenweiten Drittschlüssels²¹, der es dem Arbeitgeber ermöglicht auch verschlüsselte E-Mails zu lesen, muss in der Nutzungsregelung mitgeteilt und gebührend begründet werden.

Für den privaten E-Mail-Gebrauch am Arbeitsplatz gilt also folgende Regel: Lässt die Nutzungsregelung die private E-Mail-Nutzung zu, so empfiehlt sich die Verschlüsselung. Ist die private E-Mail-Nutzung am Arbeitsplatz untersagt, verzichtet man am besten darauf. Eine vollständige Verhinderung eingehender privater E-Mails ist hingegen nicht möglich. Der Arbeitgeber muss sich bewusst sein, dass er den Arbeitnehmer nicht für den Eingang aller privater E-Mails verantwortlich machen kann.

Spezialfall Straftat

Wenn der Arbeitgeber im Rahmen einer anonymen Kontrolle den konkreten Verdacht schöpft, dass eine Straftat per Internet oder E-Mail begangen wurde, so kann er die entsprechenden Beweise, bestehend aus den Protokollierungen und eventuellen Backups, sichern. Da die Beweissicherung technisch komplex ist, sollte sie durch einen Spezialisten (forensic computing scientist) durchgeführt werden.

Aufgrund der Protokollierungen oder durch Beschwerde von betroffenen Arbeitnehmern oder Dritten kann der Verdacht auf ein Verhalten entstehen, das nicht nur gegen Arbeitsvertrag oder Nutzungsregelung verstösst, sondern einen Straftatbestand erfüllt, wie

- Rufschädigung (Art. 173ff StGB)
- sexuelle Belästigung am Arbeitsplatz (Art. 198 StGB)

- Verbreitung von rassistischem oder pornographischen Material (Art. 261^{bis} und 197 StGB)
- „Sabotage per Internet“ oder „Betriebsspionage“ (vgl. insb. Art. 143, 143^{bis}, 144^{bis}, 147 StGB)
- usw.

Der Entscheid, ob Anzeige erstattet wird oder nicht, liegt beim Vorgesetzten, nicht beim Sicherheitsbeauftragten. Es besteht keine Anzeigepflicht, ist jedoch empfehlenswert, zumindest im Zusammenhang mit Officialdelikten, Anzeige zu erstatten, um die Gefahr der Mittäterschaft zu verhindern.

Nur wenn der Missbrauch zugleich eine technische Störung hervorgerufen hat, kann der Arbeitgeber bei Verdacht auf eine Straftat selber die Identität der betroffenen Person ausfindig machen und Anzeige gegen diese Person erstatten. Die Identifikation der fehlbaren Person erfolgt hauptsächlich wegen der technischen Störung und der daraus folgenden arbeitsrechtlichen Sanktionierung.

Da die Identifikation bei Straftatverdacht ohne technische Störung des Systems nur in ganz bestimmten Fällen zulässig ist (vgl. erster Abschnitt im Kap. 8.2.3), darf der Arbeitgeber die Protokollierungen nicht sofort auswerten. Nur in Spezialfällen oder wenn der Verdacht auf eine grobe Straftat besteht, ist die personenbezogene Auswertung zulässig. In diesem Fall kann der Arbeitgeber Anzeige gegen eine identifizierte Person erstatten. Ansonsten erstattet der Arbeitgeber Anzeige gegen Unbekannt und die Auswertungen werden von der Strafjustiz vorgenommen. Das weitere Vorgehen ist in jedem Fall Sache der zuständigen Strafjustizbehörden.

Wenn eine Straftat begangen wird, stehen in der Regel überwiegende öffentliche Interessen auf dem Spiel. Deswegen ist eine weitere Überwachung des Internetverhaltens – falls zur Erhärtung des Verdachtes nötig – ausnahmsweise gestattet. Wegen des schweren Eingriffs in die Persönlichkeit, kann jedoch nur die zuständige Strafjustizbehörde eine solche Überwachung anordnen.

anordnen. Vom Arbeitgeber selber durchgeführte, weitere Verhaltensüberwachungen, nachdem ein Verdacht entstanden ist, können als unzulässige Beweismittel im Rahmen eines Strafverfahrens betrachtet werden. Zudem können sie auch rechtliche Folgen für den Arbeitgeber nach sich ziehen (vgl. Kapitel 12).

Der Arbeitgeber muss das Resultat der Ermittlungen gegenüber Dritten, insbesondere gegenüber den anderen Angestellten, vertraulich behandeln.

Vorbehalten bleiben auch bei einer Straftat die arbeitsrechtlichen Sanktionen wegen Verletzung der Nutzungsregelung (vgl. Kapitel 11).

8.2.4 Sowohl Missbrauch als auch technische Störung

Beruflich nicht erklärbare Überlastung der Speicherkapazität, Lahmlegung des betrieblichen Datenverkehrs oder Absturz des Computers sind nur einige der konkreten technischen Störungen, die auf einem Missbrauch der netzbasierten Anwendungen beruhen können. Die Ursachen dafür sind oft das Herunterladen und Speichern fremder Dateien, die übermässige private Nutzung des E-Mails mit grossen Anhängen oder das Einschleppen von Viren sowie fehlende, ungenügende oder nicht funktionierende technische Schutzmassnahmen.

Da in solchen Fällen die Interessen und Ressourcen des Arbeitgebers in messbarer Weise tangiert werden, darf der Sicherheitsbeauftragte die Protokollierungen der netzbasierten Anwendungen sofort personenbezogen auswerten und die Resultate an den Vorgesetzten zur Sanktionierung weiterleiten, sofern die Arbeitnehmer in der Überwachungsregelung vorgängig darüber informiert wurden. Zudem müssen die technischen Schutzmassnahmen und gegebenenfalls die Nutzungsregelung angepasst werden.

Für den Fall der E-Mail-Überwachung und dem Verdacht auf eine Straftat gelten die Ausführungen im vorhergehenden Kapitel.

9. Besondere Fälle des E-Mail-Missbrauches

Darf der Arbeitgeber einen Mitarbeiter identifizieren, dem z. B. Persönlichkeitsverletzungen oder Mobbing durch anonyme E-Mails vorgeworfen werden?

Die mögliche Persönlichkeitsverletzung eines Arbeitnehmers ist ausschliesslich Sache der betroffenen Person und der Ziviljustiz. Der Arbeitgeber hat jedoch das Recht, selber die Identität der fehlbaren Person herauszufinden, wenn die anonymen E-Mails die Treuepflicht und damit die Interessen des Arbeitgebers tangieren, z. B. durch Kränkung eines Mitarbeiters und daraus folgendem Leistungseinbruch oder durch negativen Einfluss auf das Arbeitsklima. Die Identifikation ist ebenfalls erlaubt, wenn private E-Mails in der Nutzungsregelung verboten sind. Der Rechtfertigungsgrund für die Identifikation der fehlbaren Person ist in einem solchen Fall die Verletzung der Nutzungsregelung resp. der Treuepflicht, nicht die vermeintliche Persönlichkeitsverletzung.

Wenn dem Vorgesetzten zu Ohren kommt, dass über ihn persönlichkeitsverletzende E-Mails kursieren, so hat er zuerst das Gespräch mit den Arbeitnehmern zu suchen, um die Angelegenheit wenn möglich auf diese Weise zu klären. Auch wenn diese Gespräche zu keinem Resultat führen, d. h. wenn die E-Mails weiter kursieren, so darf der Vorgesetzte die entsprechenden E-Mail-Protokollierungen nicht personenbezogen auswerten, da der Persönlichkeitschutz der Arbeitnehmer gegenüber seiner – vermeintlich – verletzten Persönlichkeit überwiegt. Ausserdem würde dadurch auch die Meinungsäusserungsfreiheit der Arbeitnehmer tangiert. Möglich ist die Anrufung des Zivil- oder Arbeitsrichters, wenn er die fehlbare Person identifizieren lassen und gegen sie gerichtlich vorgehen will.

10. Leistungsüberwachung und Geschäftskontrolle

Mit Leistungsüberwachung wird die systematische, qualitative und/oder quantitative Produktionserfassung gemeint. Sie darf nur für eine beschränkte Dauer durchgeführt werden. Die Angestellten müssen zudem über die in Frage kommende Überwachungsperiode vorgängig informiert werden. Im Zusammenhang mit netzbasierten Anwendungen ist z. B. dann von Leistungsüberwachung die Rede, wenn Arbeit per E-Mail verrichtet wird. Dies ist beispielsweise im Direct-Marketing-Bereich der Fall.

Eingehende geschäftliche E-Mails, wie z. B. Anfragen von Kunden, dürfen aus Geschäftskontrollgründen vom Arbeitgeber eingesehen werden. Deswegen ist er berechtigt, in den E-Mail-Briefkasten abwesender Arbeitnehmer Einsicht zu nehmen. Wenn der Arbeitgeber die per E-Mail verrichtete Arbeit und/oder die eingehenden geschäftlichen E-Mails zu kontrollieren gedenkt, so hat er die Arbeitnehmer darüber vorgängig in einer Überwachungsregelung zu informieren.

Auch in diesem Zusammenhang stellt sich das Problem der Unterscheidung zwischen geschützten privaten und kontrollierbaren beruflichen E-Mails (vgl. Kapitel 8.2.3).

Wenn kein Unterscheidungsvermerk zwischen privaten und beruflichen E-Mails besteht und die private Natur eines E-Mails aufgrund der Adressierungselemente nicht erkennbar und nicht anzunehmen ist, darf der Arbeitgeber – analog den klassischen Postsendungen – davon ausgehen, dass das E-Mail beruflich ist. Bestehen berechtigte Zweifel an der Natur eines E-Mails, so hat der Arbeitgeber dies mit dem Arbeitnehmer abzuklären. Die Einsicht in den Inhalt des fraglichen E-Mails ist in diesem Fall nicht gestattet, unabhängig davon, ob private E-Mails erlaubt sind oder nicht. Solche Unterscheidungsschwierigkeiten bei Abwesenheit eines Angestellten lassen sich z. B. dadurch verhindern, dass die eingehenden geschäftlichen E-Mails automatisch an einen anderen geschäftlichen E-Mail-Briefkasten weitergeleitet werden.

Stellt der Arbeitgeber im Rahmen der Leistungsüberwachung fest, dass der E-Mail-Dienst unerlaubterweise privat genutzt wird, so kann er die entsprechenden Sanktionen aussprechen (vgl. Kapitel 11). Verletzt der Arbeitgeber die obigen Überwachungsregeln, so stehen dem Arbeitnehmer die Rechtsansprüche gemäss Kapitel 12 zu.

Die gleichen Regeln gelten auch für den Fall, dass ein einziger, gemeinsamer E-Mail-Briefkasten für mehrere Arbeitnehmer besteht.

11. Sanktionen bei Missbrauch

Wenn die Voraussetzungen und die Regeln der Überwachung eingehalten worden sind, kann der Arbeitgeber im Falle eines erwiesenen Missbrauchs arbeitsrechtliche Sanktionen gegen den fehlbaren Arbeitnehmer aussprechen. Der Arbeitnehmer haftet für den Schaden, den er absichtlich oder fahrlässig dem Arbeitgeber zufügt (Art. 321e OR).

In Frage kommen z. B. Abmahnungen, Sperrungen des Internetzugriffs, Schadenersatzforderungen, Lohnkürzungen oder Versetzungen. In extremen Fällen, wie bei wiederholtem Missbrauch mit technischer Störung trotz Abmahnung oder bei erwiesenen Straftaten kann der Arbeitgeber sogar die Entlassung aussprechen (Art. 335 OR). Die fristlose Entlassung eines Arbeitnehmers kann nur ausgesprochen werden, wenn dem Arbeitgeber nach Treu und Glauben die Fortsetzung des Arbeitsverhältnisses nicht mehr zugemutet werden kann (Art. 337 OR).

Für das Aussprechen von Sanktionen ist nur der Vorgesetzte des fehlbaren Arbeitnehmers zuständig. Wenn es in der Überwachungsregelung vorgesehen und der Missbrauch mit 100%-iger Sicherheit erwiesen ist, dürfen die Informatikdienste oder Sicherheitsbeauftragten selber Abmahnungen aussprechen sowie Zugriffsbeschränkungen oder Löschungen vornehmen. Die Löschung missbräuchlich heruntergeladener Dateien sollte in der Regel nur bei fehlenden Diskquotas nötig sein. Vor einer Löschung müssen die betroffenen Arbeitnehmer informiert werden und, sofern es technisch zumutbar ist, soll ihnen die Möglichkeit gegeben werden, die betreffenden Dateien, z. B. E-Mails, auf privaten Datenträgern zu speichern.

Die Sanktionen müssen der Schwere des jeweiligen Missbrauches angepasst und in ihrem Umfang bereits in der Überwachungsregelung bestimmt oder bestimmbar sein.

Ein Missbrauch muss nicht immer auf bösem Willen des Arbeitnehmers basieren. Oft stecken dahinter Neugierde und fehlende Information über die damit

damit verbundenen Sicherheitsgefahren durch den Arbeitgeber. Dieser trägt in solchen Fällen ein Teil der Verantwortung.

Wenn in der Nutzungsregelung auf die Gefahren von Viren hingewiesen wird und die Arbeitnehmer verpflichtet sind, die installierten Virenschutzprogramme einzusetzen, so führt ein Verstoss gegen diese Anweisung und die daraus folgende Infektion eines Rechners zu einer Schadenersatzpflicht der fehlbaren Person. Einen wesentlichen Teil der Verantwortung für die Infektion eines Rechners trägt der Arbeitgeber selber, wenn er kein oder kein geeignetes Antivirusprogramm installiert hat. Auch für sonstige mangelnde Sicherheitsvorkehrungen trägt der Arbeitgeber einen Teil der Verantwortung.

Wenn keine Nutzungsregelung mit klar definierten Unterscheidungskriterien zwischen zulässiger beruflicher Informationsbeschaffung und unzulässiger privater Surfing vorhanden ist, wird es in der Praxis nicht leicht sein, eine Internetnutzung für erlaubt oder unerlaubt zu erklären. In solchen Fällen dürfen Sanktionen gegen einen Arbeitnehmer nur dann ergriffen werden, wenn ein klarer Missbrauch vorliegt.

Bei Mangel einer Nutzungsregelung haftet der Arbeitnehmer nur für vorsätzlich oder grobfahrlässig herbeigeführten Schäden.

Vorbehalten bleibt die strafrechtliche Verfolgung durch die zuständige Behörde, wenn ein Straftatbestand vorliegt.

12. Ansprüche des Arbeitnehmers bei unzulässiger Überwachung

Wenn der Arbeitgeber die einschlägigen Voraussetzungen und Regeln bei der Überwachungen der Internet- und E-Mail-Aktivitäten der Arbeitnehmer nicht einhält, so kann dies als widerrechtliche Persönlichkeitsverletzung gerichtlich angefochten werden (Art. 15 und 25 DSG). Der betroffene Arbeitnehmer kann seine Ansprüche (Feststellung der Widerrechtlichkeit, Schadenersatz, usw.) zuerst beim Arbeitgeber geltend machen. Geht dieser nicht auf die Forderungen des Arbeitnehmers ein, so kann der Arbeitsrichter angerufen werden. Dieser wendet in der Regel ein rasches und kostenloses Verfahren an. Auch die arbeitsrechtlichen Sanktionen, die der Arbeitgeber aufgrund einer missbräuchlichen Überwachung ausgesprochen hat, können angefochten werden (z. B. missbräuchliche Kündigung, Art. 336 OR).

Dem Arbeitgeber können im Falle einer missbräuchlichen Überwachung auch strafrechtliche Folgen drohen, z. B. infolge einer Verletzung des Geheim- oder Privatbereiches durch Aufnahmegeräte (Art. 179^{quater} StGB) oder bei unbefugtem Beschaffen von Personendaten (Art. 179^{novies} StGB).

Zu den unzulässigen Überwachungen gehören insbesondere die personenbezogene Auswertung der Protokollierungen ohne vorherige Information der Arbeitnehmer und/oder ohne Feststellung eines Missbrauchs sowie der Einsatz von Spionprogrammen.

13. Weitere Bestimmungen des Datenschutzgesetzes

Sowohl die Informatikdienste bzw. die Sicherheitsbeauftragten als auch die Vorgesetzten haben die Personendaten (hauptsächlich die Protokollierungen und deren Auswertungen), die sie im Zusammenhang mit einer Überwachung bearbeiten, durch angemessene technische Schutzmassnahmen gegen unbefugte Zugriffe zu schützen (Art. 7 Abs. 1 DSG).²² Sie sorgen insbesondere für die Vertraulichkeit, die Verfügbarkeit und die Integrität der Personendaten (Art. 8 Abs. 1 der Verordnung zum DSG, VDSG, SR 235.11).

Der Arbeitnehmer darf vom Arbeitgeber jederzeit Auskunft darüber verlangen, ob Daten über ihn bearbeitet werden (Art. 8 Abs. 1 DSG). Dies kann sogar eine überwachungshemmende Wirkung auf den Arbeitgeber haben.

Personendaten dürfen nicht ohne Einwilligung der betroffenen Personen oder einen anderen überwiegenden Rechtfertigungsgrund an unberechtigte Dritte bekannt gegeben werden (Art. 12 und 13 DSG). Die Arbeitskollegen der betroffenen Person gelten in Bezug auf den Datenschutz als Dritte.

Dem Arbeitgeber obliegt keine gesetzliche Aufbewahrungspflicht im Zusammenhang mit Protokollierungen. Zu Beweissicherungszwecken dürfen die Protokollierungen für eine beschränkte Zeit, in der Regel nicht länger als vier Wochen, aufbewahrt werden. Die Aufbewahrungsdauer hängt vom Zweck der Protokollierung ab (vgl. Kapitel 4). Im Rahmen von Sanktionsverfahren oder Strafverfolgungen dürfen sie bis zum Ablauf der entsprechenden Rechtsmittelfristen aufbewahrt werden.

Fazit: Technische Schutzmassnahmen statt Überwachung

Die Arbeitgeber und ihre Angestellten sind gegenseitig voneinander abhängig. Während der Arbeitgeber auf die zuverlässige Arbeit seiner Belegschaft angewiesen ist, so muss sich diese darauf verlassen können, dass sie von ihrem Arbeitgeber korrekt behandelt werden. Im Fall der Internet- und E-Mail-Nutzung am Arbeitsplatz bedeutet dies, dass Angestellte sich selber beschränken müssen, während der Arbeitgeber die Persönlichkeit seiner Belegschaft mit allen Mitteln schützen muss. Deswegen muss er das Schwergewicht auf die technischen Schutzmassnahmen legen, die nur noch ein Surfen im Sinne der Unternehmung ermöglichen.

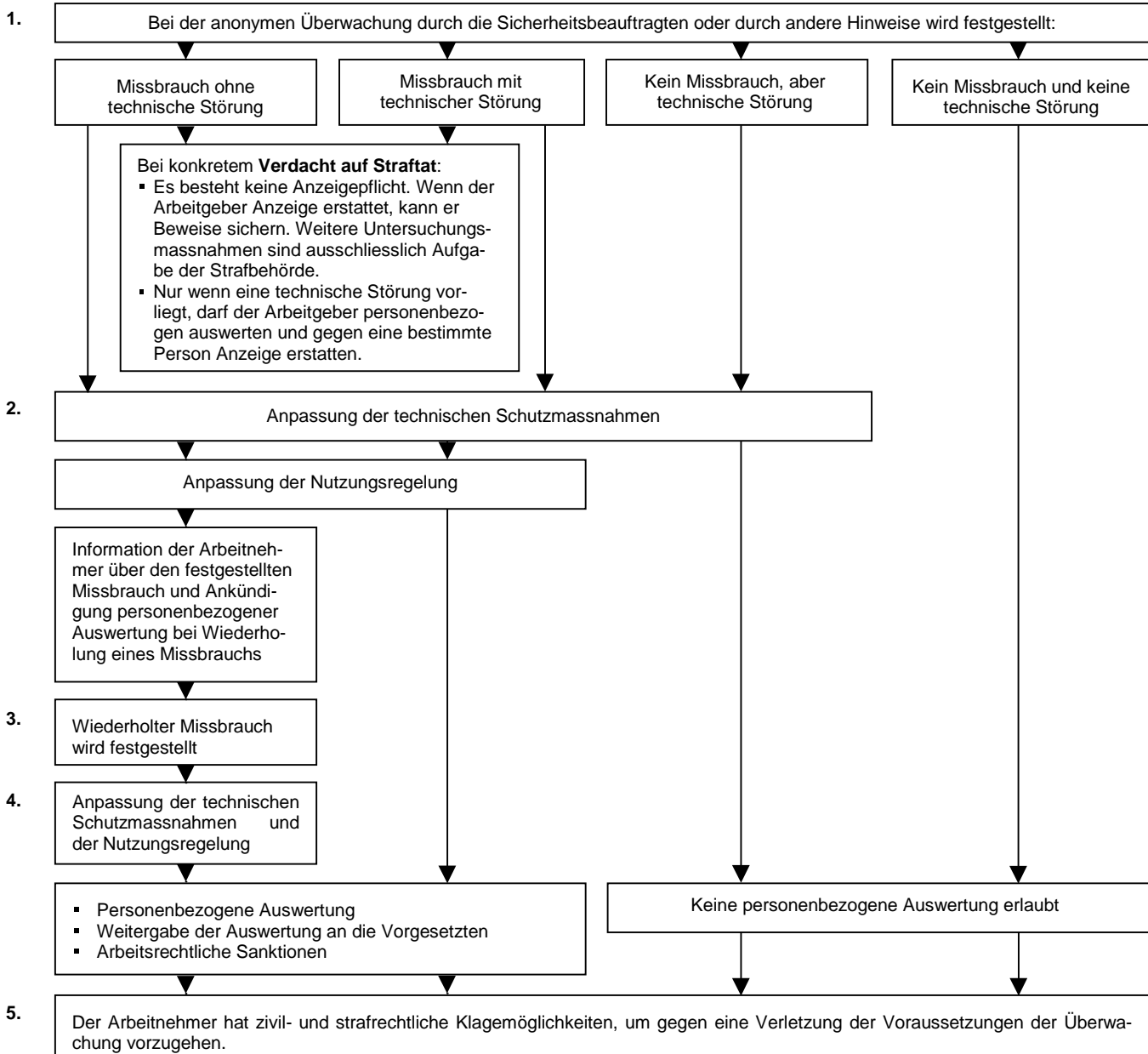
Da aber nicht alle Missbräuche durch technische Vorsorge verhindert werden können, so muss der Arbeitgeber klare Richtlinien verfassen, was zulässig ist und was nicht, und was wie überwacht und ausgewertet wird. Präzise Regelungen verschaffen Klarheit im Umgang mit Internet am Arbeitsplatz und verhindern unnötige Rechtsstreitigkeiten.

Anhang 1: Voraussetzungen und Ablauf

A. DIE VORAUSSETZUNGEN DER ÜBERWACHUNG

1. Der Arbeitgeber setzt technische Schutzmassnahmen wie Antivirusprogramme, Firewalls, Diskquotas, Backups usw. ein. Der Einsatz von sogenannten Spionprogrammen beim Benutzer ist verboten. Der Arbeitgeber bestimmt die einzusetzenden Protokollierungen und sorgt dafür, dass einzig der Sicherheitsbeauftragte bei Bedarf darauf Zugriff hat.
2. Der Arbeitgeber informiert die Arbeitnehmerschaft über folgende Punkte:
 - Eingesetzte **technische Schutzmassnahmen** und bestehende Protokollierungen
 - **Nutzungsregelung**
Dies ist eine schriftliche Weisung, die besagt, ob und wie die Benutzung von E-Mail und Internet erlaubt ist. Eine solche Regelung ist empfehlenswert, da sie Klarheit schafft.
 - **Überwachung**
Die Sicherheitsbeauftragten führen laufend anonyme Überwachungen der technischen Ressourcen (intrusion and abuse detection) durch und können die Einhaltung der Nutzungsregelung stichprobenweise anonym überprüfen. Ein Missbrauch muss jedoch festgestellt werden, bevor der Arbeitgeber die Protokollierungen personenbezogen auswerten darf. Ein solcher liegt dann vor, wenn gegen die Nutzungsregelung oder gegen die Treuepflicht bzw. gegen die Verhältnismässigkeit verstossen wird. Damit personenbezogen ausgewertet werden darf, ist zudem ein schriftliches Überwachungsreglement zwingend. Darin sind auch die Bekanntgabe der Auswertungen an die Vorgesetzten und die Sanktionen geregelt.
N.B. - Die Überwachung des E-Mail-Gebrauchs ist von der Technik her immer personenbezogen und nur aufgrund der Vertraulichkeitsangaben (privat, persönlich, vertraulich) oder der Adressierungselemente erlaubt. Wenn die Natur des E-Mails unklar bleibt, muss die betroffene Person gefragt werden.
- Die Protokollierung der durch die technischen Schutzmassnahmen verhinderten Operationen werden nicht personenbezogen ausgewertet.

B. DER ABLAUF DER ÜBERWACHUNG



Anhang 2: Checkliste

1. Haben Sie die Risiken identifiziert und die Arbeitnehmer entsprechend geschult?
2. Haben Sie folgende technische Schutzmassnahmen eingesetzt?
 - Backups
 - Antivirusprogramm
 - Diskquotas
 - Firewall mit Sperr- bzw. Positivliste (ev. mit Intrusion Detection System)
3. Werden die technischen Schutzmassnahmen dem neuesten Stand der Technik regelmässig angepasst?
4. Entsprechen die bestehenden Protokollierungen einer erwiesenen Notwendigkeit und wurde ihr Zweck, Inhalt und Zugriffsberechtigung in der Überwachungsregelung festgehalten?
5. Haben Sie auf den Einsatz gesetzlich verbotener Spionprogramme verzichtet?
6. Haben Sie eine Nutzungsregelung mit klaren Grenzen zwischen zulässiger und unzulässiger Internet- und E-Mail-Nutzung erlassen?
7. Falls Sie die Internet- und E-Mail-Aktivitäten Ihrer Angestellten überwachen, müssen Sie sich an folgende Regeln halten:
 - Die stichprobenartigen Kontrollen der Einhaltung der Nutzungsregelung erfolgen anonym. Personenbezogene Auswertungen der Protokollierungen finden nur bei Feststellung eines Missbrauches statt.
 - Die Arbeitnehmer müssen über die Möglichkeit der personenbezogenen Auswertung der Protokollierungen nach Feststellung eines Missbrauches informiert werden.
8. Empfehlenswert sind auch die Informationen über:
 - Eingesetzte Protokollierungen, ihren Zweck, Inhalt und Aufbewahrungsdauer;

- Die Zuständigkeit für die personenbezogene Auswertung der Protokollierungen;
 - Die Vorgehensweise bei Verdacht auf eine Straftat;
 - Die Weitergabe der Auswertungsergebnisse an die Vorgesetzten;
 - Die konkreten arbeitsrechtlichen Sanktionen.
9. Steht jedem Mitarbeiter ein Exemplar der Nutzungs- und Überwachungsregelung auf Papier zur Verfügung?
10. Haben Sie sich bei der Sanktionierung eines Missbrauchs über die Identität des fehlbaren Mitarbeiters vergewissert?
11. Haben Sie die technischen Schutzmassnahmen bei jeder Feststellung einer technischen Störung angepasst?
12. Haben Sie bei Vorliegen eines Verdachtes auf Straftat die zuständige Behörde eingeschaltet?
13. Sind die Informatikdienste oder Sicherheitsbeauftragten auf die Vertraulichkeit der bearbeiteten Daten aufmerksam gemacht worden?

Falls Sie weitere Fragen haben, wenden Sie sich bitte an folgende Adresse:

Eidgenössischer Datenschutzbeauftragter

3003 Bern

Tel. 031 322 43 95

Fax 031 325 99 96

E-Mail info@edsb.ch

April 2001

Anhang 3: Fussnoten

- ¹ Duden Informatik, 2. Auflage, Mannheim, Leipzig, Zürich, Wien, 1993.
- ² Z. B. das Programm Stripes.exe bei MS-DOS.
- ³ Vgl. dazu Leitfaden des Eidg. Datenschutzbeauftragten über die technischen und organisatorischen Massnahmen.
- ⁴ Service Pack, Service Release, Hotfixes, Patches, usw.
- ⁵ Z. B. Cookies ablehnen oder Javascript ausschalten, um E-Mail-Wiretaps (Abhörung) zu verhindern.
- ⁶ Die Firewall kann mit der sogenannten Network Address Translation NAT die persönlichen IP-Adressen durch eine öffentliche Firmen-IP-Adresse ersetzen, und somit einen Hackerangriff von aussen verhindern.
- ⁷ Demilitarisierte Zone (DMZ), wo sich die Internet-Firmenserver befinden.
- ⁸ Http, ftp, telnet, nntp, smtp, etc.
- ⁹ URL: Uniform Resource Locator wie z. B. <http://www.unerwuenscht.ch>.
- ¹⁰ Router, Paketfilter, Firewalls, usw.
- ¹¹ Logon, File-, Print-, E-Mail-, Proxy-Server, usw.
- ¹² Diese beschränkt sich auf den Zeitpunkt des Abrufs einer Internetdatei, nicht auf deren Dauer.
- ¹³ Durch ein sogenanntes DHCP-Protokoll kann die IP-Adresse dynamisch erteilt werden, d. h. derselbe Benutzer bekommt nicht immer die gleiche Adresse.
- ¹⁴ Gewisse Kreise vertreten die Auffassung, dass das Verbot privaten Telefonierens auf die private Internetnutzung analog anwendbar sei.
- ¹⁵ Motion Fritz Reimann vom 12. Dezember 1984 betreffend Persönlichkeitsschutz des Arbeitnehmers.
- ¹⁶ Vgl. auch schriftliche Beantwortung der Motion durch den Nationalrat am 20. Februar 1985 sowie Bemerkungen des Wegleitungsentwurfes zu Art. 26 ArGV 3.
- ¹⁷ Ghost Keylogger, WinWhatWhere Investigator, PC Activity Monitor, usw.
- ¹⁸ Auch die Entstehungsarbeiten zu Art. 26 ArGV 3 wiesen im Zusammenhang mit der Telefonüberwachung zu Recht darauf hin, dass erst bei einem konkreten Missbrauch die vollständigen Randdaten des Telefonverkehrs personenbezogen ausgewertet werden dürfen.
- ¹⁹ Der Leistungseinbruch eines Arbeitnehmers rechtfertigt eine Kontrolle der Protokollierungen nicht, da dem Arbeitgeber die Feststellung des Leistungseinbruches genügt, um die entsprechenden arbeitsrechtlichen Schritte gegen die betroffene Person einzuleiten.
- ²⁰ Die Verschlüsselung kann bspw. durch Benutzung von PGP-Software (Pretty Good Privacy) oder webbasierter E-Mail-Dienste wie Hushmail.com gewährleistet werden, wobei ein vollständiger Schutz nur erreicht wird, wenn sowohl Absender wie auch Empfänger einen verschlüsselten E-Mail-Dienst benutzen.
- ²¹ Additional decryption key, Corporate Message Recovery Key, Recovery Agent, usw.
- ²² Vgl. dazu Leitfaden des Eidg. Datenschutzbeauftragten über die technischen und organisatorischen Massnahmen.