Datenschutz in der Katholischen Kirche

Sicherheit und Ordnungsgemäßheit kirchlicher Datenverarbeitung

Arbeitshilfe Nr. 601 Stand: März 2006

Mitarbeitervertretung und Datenschutz

Der Diözesandatenschutzbeauftragte
des Erzbistums Hamburg,
der Bistümer Hildesheim, Osnabrück
und des Bischöflich Münsterschen Offizialats in Vechta i.O.

DATENSCHUTZ
IN DER KATHOLISCHEN KIRCHE

Mitarbeitervertretung und Datenschutz

Inhalt

Anlage

Herausgeber:
Der Diözesandatenschutzbeauftragte der norddeutschen Bistümer
Schwachhauser Heerstraße 67 • 28211 Bremen • ☏ 0421 / 16 30 19 25
Internet: http://www.datenschutz-kirche.de
E-Mail: info@datenschutz-katholisch-nord.de

Erscheinungsdatum:
März 2006

Kapitel 1 Rechtsgrundlagen

1. Eigenständigkeit kirchlichen Datenschutzes

Das Bundesdatenschutzgesetz gilt nicht für Dienststellen und Einrichtungen der öffentlich-rechtlichen Religionsgesellschaften. Das ergibt sich aus § 2 Abs. 2 BDSG, der die Vorschrift ausdrücklich nur auf öffentliche Stellen des Bundes und der Länder, soweit sie Bundesrecht ausführen und nichtöffentliche Stellen der Privatwirtschaft erstreckt. Auch die jeweiligen Landesdatenschutzgesetze beziehen kirchliche Einrichtungen nicht mit ein. Sie gelten nur für die öffentlichen Stellen der Länder. Der Grund hierfür liegt in dem verfassungsrechtlich garantierten Selbstverwaltungsrecht der Kirchen (Art. 140 GG i.V.m. Art. 137 III WRV). Dort heißt es:

> *"Jede Religionsgesellschaft ordnet und verwaltet ihre Angelegenheiten selbständig innerhalb der Schranken des für alle geltenden Gesetzes. Sie verleiht ihre Ämter ohne Mitwirkung des Staates oder der bürgerlichen Gemeinde."*

Nach Auffassung des Bundesverfassungsgerichts (Goch-Beschluß) gilt diese Befugnis auch für Einrichtungen der Kirche in privater Rechtsform. Grundlegend war dabei die Überlegung, dass nur die Kirche selbst bestimmen könne, welche Einrichtungen, die mit ihrer Hilfe oder Zustimmung geschaffen worden sind, auch an ihrem Sendungsauftrag teilhaben und daher zur Kirche gehören. Darüber hinaus dürfe die Kirche auch frei wählen, welcher Rechtsform sie sich dabei bediene (Recht der Formwahl). Eine verfassungskonforme Auslegung des BDSG muss daher dazu führen, das auch Einrichtungen der Kirche in privater Rechtsform (z.B. Stiftungen, Vereine etc.) nicht dem Bundesdatenschutzgesetz unterliegen. Diese Rechtsauffassung wird von den staatlichen Stellen auch geteilt. Vereinzelte Stimmen in der juristischen Fachliteratur fordern jedoch eine Anwendung des dritten Abschnitts des BDSG auf kirchliche Einrichtungen in privater Rechtsform.

Geht man mit der herrschenden Meinung davon aus, dass das Bundesdatenschutzgesetz insgesamt auf alle kirchlichen Einrichtungen unanwendbar ist, so bedeutet das freilich nicht, dass die Kirche ein datenschutzfreier Raum ist. Der Bundesgesetzgeber hat schon vor Schaffung des ersten Bundesdatenschutzgesetzes von 1977 die Erwartung geäußert, dass die Kirchen von ihrem Recht auf Selbstverwaltung auch tatsächlich Gebrauch machen und eine eigenständige Regelung schaffen würden. In § 15 Abs. 4 BDSG ist dies unmittelbar zum Ausdruck gekommen:

> *„Für die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgesellschaften gelten die Absätze 1 bis 3 entsprechend, sofern sichergestellt ist, dass bei diesen ausreichende Datenschutzmaßnahmen getroffen werden.“*

Eine eigenständige kirchliche Regelung muss sowohl dem Grundgedanken des Datenschutzes, wie auch den besonderen Verhältnissen der Kirche als Communio (Gemeinschaft aller Gläubigen in Christus) und dem Gedanken der Dienstgemeinschaft gerecht werden. Insoweit

ist die Situation dem Mitarbeitervertretungsrecht vergleichbar. Die Kirche hat auch im Datenschutz das Recht auf den "Dritten Weg".

Um ein einheitliches Recht in allen deutschen Diözesen zu gewährleisten, hat die Vollversammlung der Deutschen Bischofskonferenz, nach Vorarbeit durch die Kommission für Meldewesen und Datenschutz beim Verband der Diözesen Deutschlands (VDD) allen Bischöfen empfohlen, für den Bereich ihres Sprengels die „Anordnung über den kirchlichen Datenschutz – KDO“ in Kraft zu setzen. Für das Erzbistum Hamburg ist dies mit Veröffentlichung im Kirchlichen Amtsblatt vom 15.11.2003, Art. 129, Seite 149 geschehen.

2. Fundamentalrecht auf Schutz der Intimsphäre

Im Dezember 1983 hat das Bundesverfassungsgericht in seinen Beschlüssen zur Verfassungsmäßigkeit des Volkszählungsgesetzes erstmalig ein Grundrecht auf informationelle Selbstbestimmung erkannt. Im gleichen Jahr – einige Monate zuvor – hat Papst Johannes Paul II das neue Kirchenrecht, den Codex Iuris Canonici promulgiert. Mit ihm wurden erstmalig Fundamentalrechte für den kirchlichen Bereich geschaffen. In can. 220 CIC wurde dabei ausdrücklich auch die Verpflichtung zum Datenschutz festgeschrieben:

> *"Niemandem ist es erlaubt, den guten Ruf, den jemand hat, rechtswidrig zu schädigen und das Recht irgendeiner Person auf Schutz der eigenen Intimsphäre zu verletzen."*

Die Verpflichtung zum Schutz der Intimsphäre hat dabei nicht nur juristische, sondern vor allem theologische Bedeutung. Sie ist Teil des christlichen Menschenbildes, der von Gott verliehenen Würde der Person und seiner Befugnis, nach eigenem Gewissen zu handeln und zu entscheiden. Der Schutz des Beicht– und Seelsorgegeheimnisses, den die Kirche schon lange kennt, ist in unserer hochtechnisierten Welt allein nicht mehr ausreichend, um die von Gott gewollte Freiheit des Einzelnen zu erhalten. Andererseits ist auch die Kirche auf die Datenverarbeitung zur Erfüllung ihrer Aufgaben angewiesen. Daher gibt can. 223 CIC dem Ortsbischof die Befugnis, die Ausübung dieses Rechts zu regeln:

> *"§ 1. Bei der Ausübung ihrer Rechte müssen die Christgläubigen sowohl als Einzelne wie auch zusammengefasst in Vereinigungen das Gemeinwohl der Kirche sowie die Rechte anderer und ihre Pflichten gegenüber anderen beachten.*
>
> *§ 2. Der kirchlichen Autorität steht es zu, im Hinblick auf das Gemeinwohl die Ausübung der den Christgläubigen eigenen Rechte zu regeln."*

Die deutschen Bischöfe haben durch Schaffung einer für den Bereich der DBK einheitlichen "Anordnung über den kirchlichen Datenschutz – KDO -" von dieser Möglichkeit Gebrauch gemacht und zugleich im Rahmen des Selbstverwaltungsrechts eine dem staatlichen Recht vergleichbare Regelung geschaffen.

3. Anordnung über den kirchlichen Datenschutz

Die KDO gilt für alle Einrichtungen, die nach kirchlichem Selbstverständnis zur Kirche gehören. In § 1 Abs. 2 KDO werden die kirchlichen Rechtsträger enumerativ aufgeführt. Ziffer 1 nennt die lineare Struktur der verfassten Kirche, Ziffer 2 den wichtigen Bereich der Caritas, der überwiegend als eingetragener Verein organisiert ist. § 1 Abs. 2 Zi. 3 KDO bezieht schließlich alle weiteren kirchlichen Rechtsträger, ausdrücklich ohne Rücksicht auf ihre Rechtsform in den Geltungsbereich der KDO mit ein. Einrichtungen, die sich im Hinblick auf das Mitbestimmungsrecht auf ihre Kirchlichkeit berufen, kirchliche Tarife anwenden und somit den "Dritten Weg" in Anspruch nehmen, unterliegen daher auch dem kirchlichen Datenschutz.

Wie das Bundesdatenschutzgesetz auch, ist die KDO ein Auffanggesetz. Sie gilt überall dort, wo spezielle gesetzliche Regelungen fehlen. Die Mitarbeitervertretungsordnung ist beispielsweise eine Vorschrift, die der KDO als "lex specialis" im Range vorgeht. Die KDO bleibt aber anwendbar, wo die MAVO schweigt.

Weitere, von der katholischen Kirche erlassene datenschutzrechtliche Bestimmungen sind:

- Anordnung über das kirchliche Meldewesen (KMAO)
- Anordnung zum Schutz personenbezogener Daten in katholischen Schulen in freier Trägerschaft
- Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern
- Ordnung zum Schutz von personenbezogenen Daten bei Friedhöfen in kirchlicher Trägerschaft
- Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche
- Anordnung über den Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft
- Richtlinie zum Einsatz von Arbeitsplatzcomputern
- Datenschutz bei der Übermittlung personenbezogener Daten über Telefaxgeräte

Das kirchliche Selbstverwaltungsrecht gilt nur im Rahmen, der für alle geltenden Gesetze. Daher sind staatliche Gesetze, die allgemeine Regeln für bestimmte Lebens-. und Wirtschaftsbereiche aufstellen, auch von der Kirche zu beachten. Hierunter fallen zum Beispiel:

- das Teledienstegesetz (TDG) und das Teledienstedatenschutzgesetz (TDDG)
- das Telekommunikationsgesetz (TKG) und die Telekommunikations-Datenschutzverordnung (TDSV)
- das Strafgesetzbuch, insbesondere die Vorschriften zum Schutz des persönlichen Lebens- und Geheimbereichs (§§ 201 bis 205 StGB und zur Computerkriminalität (§§ 263a, 268, 269, 270, 271, 273, 274 Abs. 1 Nr. 2, 303a, 303b StGB)

Kapitel 2 Die Grundlagen des Datenschutzes

1. Notwendigkeit gesetzlicher Regelungen

Seit der Anerkennung eines Grundrechts auf informationelle Selbstbestimmung durch das Bundesverfassungsgericht, stellt sich jede Erhebung und Verarbeitung personenbezogener Daten als Grundrechtseingriff dar. Solche Grundrechtseingriffe sind nach unserer Verfassung jedoch nur durch Gesetz oder aufgrund eines Gesetzes zulässig (Art. 19 GG), das Art und Ausmaß der Freiheitseinschränkungen der Bürger regelt. Das Volkszählungsurteil hat daher zu einer völlig veränderten Sichtweise des Datenschutzes geführt.

Nach dem BDSG 1977 war die Verarbeitung personenbezogener Daten **grundsätzlich erlaubt** (Freiheit der Datenverarbeitung). Im Interesse der Betroffenen waren lediglich Vorkehrungen gegen den Missbrauch dieser Daten zu treffen. Aufgabe der Datenschutzbestimmungen war es, die Freiheit der Daten verarbeitenden Stellen im notwendigen Umfang einzuschränken.

Die nachfolgenden Regelungen erklärten die Datenverarbeitung **grundsätzlich** für **verboten**. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten darf danach nur erfolgen, wenn ein Gesetz oder das BDSG sie zulassen oder der Betroffene eingewilligt hat (Verbot mit Erlaubnisvorbehalt). Die KDO ist diesem Ansatz gefolgt. § 3 I KDO bestimmt:

> *„(1) Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ist nur zulässig, soweit*
> *1. diese Anordnung oder eine andere kirchliche oder eine staatliche Rechtsvorschrift sie erlaubt oder anordnet oder*
> *2. der Betroffene eingewilligt hat.“*

Für den Umgang mit Daten der Personen, die kirchliche Einrichtungen in Anspruch nehmen, stehen eine Reihe spezialgesetzlicher Regelungen zur Verfügung. Das gilt für Gemeindemitglieder (KMAO) und in einigen Bistümern auch für Kindergartenkinder und deren Sorgeberechtigten (KiTaO), Schüler und deren Eltern (SchulDO), Patienten kirchlicher Krankenhäuser (KrhsDSO), Käufer von Grabstellen (FrhDSO), etc.. Für die Verarbeitung von Personaldaten sind bisher keine speziellen Vorschriften erlassen worden. Die Rechtsgrundlagen für ihre Verarbeitung finden sich daher §§ 9, 10 KDO:

> ***„§ 9 Datenerhebung***
>
> *(1) Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der verantwortlichen Stellen erforderlich ist.*
>
> ***§ 10 Datenspeicherung, -veränderung und -nutzung***
>
> *(1) Das Speichern, Verändern oder Nutzen personenbezogener Daten ist zulässig, wenn es zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich ist und es für die Zwecke erfolgt für die die Daten erhoben worden sind. Ist keine*

Erhebung vorausgegangen, dürfen die Daten nur für die Zwecke geändert oder genutzt werden, für die sie gespeichert worden sind.“

2. Datenvermeidung und Datensparsamkeit

Die Befugnis zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten erstreckt sich nur auf solche Informationen, deren Kenntnis für die Erfüllung der Aufgaben der Dienststelle erforderlich ist. Nicht zulässig ist somit das Anlegen umfangreicher Datensammlungen, ohne unmittelbaren Bezug zur dienstlichen Tätigkeit. Hierin liegt zugleich die Forderung nach einer "schlanken Verwaltung", die sowohl Kosten reduzieren, wie auch den "gläsernen Christen" verhindern will. Es ist daher genau zu hinterfragen, wofür die gespeicherten Informationen benötigt werden. Sind sie nicht erforderlich, so sind sie zu löschen.

Am einfachsten ist diese Forderung dann zu gewährleisten, wenn die bei der Datenverarbeitung eingesetzten technischen Systeme eine übermäßige Sammlung von Daten, deren systematische Auswertung und Weitergabe gar nicht erst ermöglichen. Daher verlangt § 2a KDO, dass die Gestaltung und Auswahl von Datenverarbeitungssystemen an dem Ziel auszurichten habe, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Ist der Personenbezug nicht erforderlich, so sind die Daten zum frühest möglichen Zeitpunkt zu anonymisieren oder pseudonymisieren.

3. Unmittelbarkeit der Datenerhebung

Eine wesentliche Forderung aus dem Volkszählungsurteil bestand darin, dem Betroffenen jederzeit die Möglichkeit zu geben, zu erkennen, was über ihn gewusst wird. Benötigt eine Dienststelle Informationen über Mitarbeiter, so sind diese daher selbst nach ihren Verhältnissen zu befragen. § 9 II KDO bestimmt:

„(2) Personenbezogene Daten sind beim Betroffenen zu erheben. Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn
1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder
2. a) die zu erfüllende Aufgabe ihrer Art nach eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder
b) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.“

Die in § 9 KDO genannten Ausnahmetatbestände treffen auf Personaldaten in der Regel nicht zu. Sollen sie ausnahmsweise dennoch zum Tragen kommen, bedarf es einer genauen Überprüfung der Voraussetzungen.

Oft wird auch übersehen, dass darüber hinaus noch eine Güterabwägung zwischen den schutzwürdigen Belangen des Mitarbeiters und dem dienstlichen Interesse der Daten verarbeitenden Stelle erforderlich ist. Nur bei wirklich **zwingender** Notwendigkeit kann dem dienstlichen Interesse der Vorrang eingeräumt werden.

4. Strenge Zweckbindung

Eine weitere zentrale Forderung des Datenschutzes liegt in der Zweckgebundenheit des Datenbestandes. Das Bundesverfassungsgericht hatte ausdrücklich verlangt, das jeder Betroffene die Möglichkeit behalten müsse, zu erkennen, was, wann, von wem und bei welcher Gelegenheit über ihn gewusst wird. Dieses Ziel lässt sich aber nur dann erreichen, wenn seine Daten ausschließlich zu dem Zweck genutzt werden, für den sie erhoben worden sind. Das gilt in besonderem Maße für sensible Daten, wie Personaldaten. Die Datenerhebung und ihr Verwendungszweck muss für den Betroffenen auch erkennbar sein. Das gilt besonders für Überwachungsanlagen. Sie sind nur zulässig, wenn auf ihre Existenz und den Grund ihrer Installation deutlich hingewiesen wird.

5. Technisch-organisatorische Absicherung

Die vorbezeichneten Ziele lassen sich selbstverständlich nur erreichen, wenn ausreichende Maßnahmen zum Schutz der Daten getroffen werden. § 6 KDO bestimmt daher:

> ***„§ 6 Technische und organisatorische Maßnahmen***
> *Kirchliche Stellen im Geltungsbereich des § 1 Abs. 2, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieser Anordnung, insbesondere die in der Anlage zu dieser Anordnung genannten Anforderungen zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht."*

Die Verpflichtung trifft die Daten verarbeitenden Stellen selbst, ihre Verwaltungsleiter und EDV-Verantwortlichen. Der Datenschutzbeauftragte wacht lediglich darüber, dass die Maßnahmen ausreichend sind.

Aus der generellen Verpflichtung zum Schutz der Daten ist für die elektronische Datenverarbeitung ein konkreter Anforderungskatalog entwickelt worden, der in einer Anlage zu § 6 KDO benannt wird. Die Umsetzung dieser acht Gebote ist in der Praxis oft nicht ganz einfach. Die neue KDO hat jedoch in den §§ 18a, 18b die Möglichkeit geschaffen, einen Betrieblichen Beauftragten für den Datenschutz zu bestellen. Je nach Umfang der Datenverarbeitung und der Sensibilität des Datenbestandes, sollte von dieser Möglichkeit auch Gebrauch gemacht werden. Die Organisation der EDV allein dem Systemverwalter oder gar dem Lieferanten der Hard- und Software zu überlassen, ist jedenfalls bei komplexen Strukturen nicht ausreichend.

6. Rechte der Betroffenen (Mitarbeiter)

Die Einhaltung der Datenschutzvorschriften kann nicht besser kontrolliert werden, als durch die Betroffenen selbst. Zudem sollen Vertrauen und Offenheit den Umgang der Daten verarbeitenden Stellen mit den Betroffenen kennzeichnen. Gerade kirchliche Einrichtungen sind

zur Erfüllung ihrer Aufgaben hierauf angewiesen. Meist wird von ihnen sogar mehr erwartet, als von staatlichen oder gar gewerblichen Einrichtungen. Daher war es von Anfang an Ziel des Datenschutzes, die Rechte derer zu stärken, die gezwungen sind, Informationen über sich preiszugeben.

Was schon für den Einzelnen gilt, der der Dienststelle als Dritter gegenübertritt, gilt selbstverständlich auch für die Mitarbeiter. Die sich aus dem Dienstvertrag ergebende Fürsorgepflicht des Dienstherrn gebietet einen offenen und fairen Umgang mit seinen Rechten. Welche Ansprüche dem Mitarbeiter gegenüber der Daten verarbeitenden Stelle zustehen, ist zur Wahrung der Übersichtlichkeit in einer Tabelle im Anhang aufgelistet.

Tabelle: Rechte der Betroffenen (Mitarbeiter)

Gefahren aus Sicht der Betroffenen	Rechte, um diesen Gefahren zu begegnen	Vorschriften der KDO
Personenbezogene Daten sollen in einer Datenverarbeitung verarbeitet werden	Einwilligungserfordernis, Aufklärung über die Zwecke der Datenverarbeitung	§ 3 I, II
Unkenntnis über die gespeicherten Daten	Recht auf unentgeltliche Auskunft	§ 13
Erhebung ohne Kenntnis des Betroffenen	Recht auf Benachrichtigung	§ 13a
Die Daten sind unrichtig.	Recht auf Berichtigung	§ 14 I
Speicherung der Daten ist unzulässig oder nicht mehr erforderlich.	Recht auf Löschung Recht auf Sperrung	§ 14 II Zi. 1, 2 § 14 III
Streit über die Richtigkeit der Daten	Recht auf Sperrung der Daten	§ 14 IV
Erhebung, Verarbeitung oder Nutzung der Daten verletzt das schutzwürdige Interesse der Person auf Grund seiner besonderen, persönlichen Situation	Widerspruchsrecht, Recht auf Unterlassung	§ 14 V
Übermittlung unrichtiger oder bestrittener Daten an Dritte	Recht auf Benachrichtigung der Datenempfänger	§ 14 VIII
Unzulässige Weitergabe	Recht auf Unterlassung	§ 823 BGB
Rechte auf Auskunft, Unterlassung oder Löschung werden von der Dienststelle übergangen	Beschwerde an den Diözesandatenschutzbeauftragten ohne Einhaltung des Dienstweges	§ 15
Versuch, den Betroffenen zum Verzicht auf seine Rechte zu bewegen (z.B. durch Dienstvertrag).	Verzicht auf die Rechte aus §§ 13, 14 ist unwirksam	§ 5 I
Dem Betroffenen entsteht Schaden durch unrichtige Datenverarbeitung	Recht auf Schadensersatz in unbegrenzter Höhe	§ 823 BGB

Kapitel 3 Mitwirkung der Mitarbeitervertretung bei Personalangelegenheiten

1. Personalakten

Die Personalaktenführung ist Sache des Dienstgebers. Nach § 36 I Zi. 5 MAVO bedarf der Inhalt des Personalfragebogens der Zustimmung der Mitarbeitervertretung. Hier kann im Sinne der Datenvermeidung und Datensparsamkeit mit darauf geachtet werden, dass von den Mitarbeitern nur solche personenbezogene Daten erhoben werden, die von der Dienststelle auch tatsächlich zur Durchführung des Dienstverhältnisses benötigt werden.

Bei vielen Personalentscheidungen (Kündigungen, Höhergruppierungen etc.) ist die MAV zu beteiligen. In vielen Fällen wird es dabei zweckmäßig sein, die Personalakte des betroffenen Mitarbeiters einzusehen. Aufgrund der besonderen Sensibilität von Personaldaten ist dies jedoch **nur mit ausdrücklicher Zustimmung** des Mitarbeiters möglich. Damit die Personalabteilung vor Herausgabe der Unterlagen ausreichend rechtlich abgesichert ist, **ist die Zustimmung in jedem Fall schriftlich zu erteilen** (§ 26 II S. 2 MAVO). Bestehen mehrere Akten (z.B. Haupt– und Nebenakten), so muss in der Zustimmungserklärung auch genau angegeben werden, ob die gesamte Akte oder nur bestimmte Teilakten eingesehen werden dürfen.

Bei Führung der Personalakten in elektronischer Form, besteht Anspruch auf einen vollständigen Ausdruck des aktuellen Datenbestandes. Ein Verweis auf die Einsichtnahme am Bildschirm, würde die Arbeit der MAV unzumutbar erschweren und liegt regelmäßig auch nicht im Interesse der Betroffenen. Nach Abschluss der Angelegenheit sind sie datenschutzgerecht (z.B. durch Reißwolf) zu vernichten.

Auch Arbeitszeitkarten fallen unter den Begriff der Personalakte und sind wie diese zu behandeln. Einsichtnahme durch die MAV ist daher nur mit Zustimmung des Mitarbeiters möglich.

Personalakten werden der MAV in der Regel zur Einsichtnahme ausgehändigt. Damit verbunden ist das Recht, sich Notizen hieraus anzufertigen. Kopien oder vollständige Ablichtungen der Personalakte sind jedoch nur mit **ausdrücklicher Genehmigung** des Betroffenen zulässig. Auch sie sind nach Ende der Angelegenheit datenschutzgerecht zu vernichten.

2. Informationsrecht bei Einstellungen

Neueinstellungen von Mitarbeitern, die nicht nur geringfügig beschäftigt werden sollen, und auch nicht im pastoralen Dienst tätig sind, sind nur mit Zustimmung der Mitarbeitervertretung möglich (§ 34 I MAVO). Die MAV hat jedoch nur ein eingeschränktes Prüfungsrecht, das sich aus § 34 II MAVO ergibt. Ihre Zustimmung darf sie nur bei Gesetzesverstößen oder bei einer zu erwartenden Störung des Arbeitsfriedens verweigern.

Die Auswahl unter mehreren, gleich geeigneten Bewerbern unterliegt allein dem Dienstgeber. Im Hinblick auf den Grundsatz der Datenvermeidung und Notwendigkeit der Datenübermittlung (§ 11 I KDO) ließe sich daher auch an ein eingeschränktes Informationsrecht der MAV denken.

Da es jedoch eine große Zahl von Möglichkeiten gibt, aus denen sich Zustimmungsverweigerungsgründe ergeben könnten, darf das Informationsrecht der MAV nicht zu eng gefasst werden. So können sich beispielsweise Anhaltspunkte für eine Störung des Arbeitsfriedens auch aus Arbeitszeugnissen früherer Tätigkeiten ergeben. § 34 III MAVO verpflichtet den Dienstgeber daher die MAV über die Person des Bewerbers, also über seine fachliche und menschliche Qualifikation zu unterrichten. Sind dem Dienstgeber Gründe bekannt, die auf bestimmte Verhaltensweisen, Berufsauffassungen oder Probleme an früheren Arbeitsstellen hindeuten, so sind sie der MAV ebenfalls mitzuteilen.

Um das Mitwirkungsrecht abzusichern, ist der MAV auf Verlangen auch die gesamte Bewerbungsakte zur Einsichtnahme zur Verfügung zu stellen. Auch hier sind wie bei der Personalakte keine Kopien oder gar die Anlage von Zweitakten zulässig.

Gegenüber den Datenübermittlungsvorschriften der KDO ist die MAVO das speziellere Recht, so dass § 11 KDO hier nicht zur Anwendung kommt.

3. Gehaltslisten

Grundsätzlich hat die MAV kein Einsichts- und Informationsrecht bezüglich der Gehaltszahlungen an Mitarbeiter. Andererseits ist es nach § 26 I MAVO ihre Aufgabe, darauf zu achten, dass alle Mitarbeiter nach Recht und Billigkeit behandelt werden. Um dieser Aufgabe gerecht werden zu können, sind ihr auch alle Unterlagen vorzulegen, die zur Beurteilung des Sachverhaltes erforderlich sind. Besteht also tatsächlich der durch konkrete Umstände begründete Verdacht, dass Mitarbeiter gegen Recht und Billigkeit unterschiedlich behandelt werden, so muss der MAV ein Recht auf Einsichtnahme der Bruttolohn- und Gehaltslisten zugestanden werden. Ein Anspruch auf Aushändigung oder Anfertigung von Kopien dieser Listen besteht wegen der damit verbunden Missbrauchsgefahr jedoch nicht.

4. Stellenplan

Nach § 27 II MAVO hat die Mitarbeitervertretung Anspruch auf Vorlage des Ist-Stellenplans. Sie ist als über die tatsächlich vorhandenen und besetzten Stellen zu unterrichten. Ob der MAV auch der Soll- Stellenplan bekannt zu geben ist, ist streitig (bejahend Bleistein/Thiel, Kommentar zur Rahmenordnung einer Mitarbeitervertretungsordnung, 4. Aufl. 2004, § 26 Anm. 37, § 27 Anm. 19), braucht aus datenschutzrechtlicher Sicht jedoch nicht entschieden zu werden, da dieser keine, über den Ist-Stellenplan hinausgehenden personenbezogenen Informationen enthält.

Die Frage, welchen Inhalt der Stellenplan haben darf, der der MAV zu übermitteln ist, wird durch die MAVO nicht geregelt. Hier ist also auf § 11 KDO zurückzugreifen:

> ***„§ 11 Datenübermittlung an kirchliche und öffentliche Stellen***
> *(1) Die Übermittlung personenbezogener Daten an Stellen im Geltungsbereich des § 1 ist zulässig, wenn*
> *1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Empfängers liegenden Aufgaben erforderlich ist und*
> *2. die Voraussetzungen vorliegen, die eine Nutzung nach § 10 zulassen würden.*
> *(2) ...*
> *(3) Der Empfänger. darf die übermittelten Daten für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nur unter den Voraussetzungen des § 10 Abs. 2 zulässig.*

Hieraus folgt, dass die Angaben, die zur Erfüllung der Aufgaben der MAV notwendig sind, auch übermittelt werden dürfen. Im Hinblick auf die Aufgaben nach §§ 34, 35 MAVO bestehen aus datenschutzrechtlicher Sicht keine Bedenken, wenn folgende Informationen weitergegeben werden:

- Kostenstelle
- Einzelstellen innerhalb der Kostenstellen
- Vor- und Zuname der Stelleninhaber
- Vergütungsgruppen
- Umfang des Beschäftigungsverhältnisses (Vollzeit/Teilzeit)
- freie Mitarbeiter

Für weitere personenbezogene Informationen besteht allerdings kein Raum. Kein Anspruch besteht insbesondere auf Angaben zum Alter, Familienstand, Kinderzahl, etc.

5. Schweigepflicht

Die Schweigepflicht der Mitarbeitervertreter ist in § 20 MAVO ausdrücklich geregelt. Verstöße hiergegen können nach Entscheidung der Schlichtungsstelle zum Ausschluss aus der MAV führen, § 13c Nr. 5 MAVO. Außerdem kann die Verletzung der Schweigepflicht eine fristlose Kündigung rechtfertigen, wenn die Fortsetzung des Dienstverhältnisses wegen des Vertrauensverlustes nicht mehr zumutbar ist.

Ergänzend gilt auch für Mitarbeitervertreter das Datengeheimnis nach § 4 KDO. Die KDO wird in diesem Falle nicht von der MAVO als dem spezielleren Recht verdrängt, da die Wahrung des Datengeheimnisses einem anderen Schutzzweck dient.

> ***„§ 4 Datengeheimnis***
> *Den bei der Datenverarbeitung tätigen Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis schriftlich zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.“*

§ 4 KDO schließt die Erhebung, Verarbeitung und Nutzung von Daten in den Schutzzweck mit ein und bezieht sich somit auf alle Phasen der Datenverarbeitung. Gegen das Datengeheimnis verstößt demgemäß auch derjenige, der sich Informationen in unbefugter Weise verschafft oder für eigene Zwecke ausnutzt. Mitglieder der MAV, die dienstlich personenbezogene Daten verarbeiten, haben daher auch die Verpflichtungserklärung nach § 4 KDO zu unterschreiben.

Sind MAV-Mitglieder in der Datenverarbeitung beschäftigt, so darf das auf keinen Fall dazu führen, dass über die Informationsrechte der MAV hinaus, Daten an die Mitarbeitervertretung weitergegeben werden.

6. Namensschilder im kirchlichen Dienst

Durch eine Anordnung von Dienstvorgesetzten an Mitarbeiterinnen und Mitarbeiter, Namensschilder zu tragen, werden diese veranlasst, ihren Namen dienststellenintern und auch gegenüber Dritten preiszugeben. Dies stellt eine der öffentlichen Stelle zuzurechnende Verarbeitung von Beschäftigtendaten dar, deren Zulässigkeit sich grundsätzlich nach § 12 I KDO beurteilt. Sollen Beschäftigte Namensschilder tragen, auf denen Vor- und Zuname und evtl. der Zuständigkeitsbereich und Stellung ausgewiesen sind, sollte die Einwilligung der Betroffenen eingeholt werden. Wünschenswert ist dieses Vorgehen bereits deshalb, weil damit die Akzeptanz der Beschäftigten erreicht wird.

Ist ein Vorgehen auf freiwilliger Basis nicht möglich, beurteilt sich die datenschutzrechtliche Zulässigkeit im Einzelfall danach, ob Publikumsverkehr oder sonst ein direkter Kontakt zu Besuchern der Einrichtung fester Bestandteil der Aufgabe der Beschäftigten ist. Namensschilder erleichtern Außenstehenden die Kontaktaufnahme. Mitarbeiter sind als solche erkennbar, signalisieren ihre Gesprächsbereitschaft und sind als Person ansprechbar. Es ist jedoch sicher zu stellen, dass die Beschäftigten die Möglichkeit besitzen, ausnahmsweise vorliegende besondere Umstände geltend zu machen, die in ihrem individuellen Fall gegen das Tragen von Namensschildern sprechen.

Eine Geheimhaltung der Identität von Mitarbeitern ist aus Fürsorgegründen dann erforderlich, wenn Leben und Gesundheit von Beschäftigten gefährdet oder sonstige schwerwiegende Belästigungen zu befürchten sind. Werden diese Grundsätze beachtet, bestehen gegen die Anordnung des Dienstherrn, Namensschilder zu tragen, unter den genannten Voraussetzungen keine datenschutzrechtlichen Bedenken.

7. Weitergabe von Personaldaten an Dritte

Die Weitergabe personenbezogener Daten an Dritte ist nach §§ 11, 12 KDO zu beurteilen. Dritter in diesem Sinne ist jede andere selbständige Einrichtung. Grundsätzlich ist danach die Datenweitergabe von personenbezogenen Daten, die im Rahmen eines Dienstverhältnisses erhoben und gespeichert wurden, nur zulässig, wenn dies zur Durchführung des Vertragsverhältnisses erforderlich ist.

Die Übermittlung von Mitarbeiterdaten zum Zwecke der Werbung, wird nicht vom Vertragszweck eines Arbeitsvertrages gedeckt. Das gilt auch für kirchliche Publikationen, wie die Kirchenzeitung oder die Angebote des Weltbild Verlages. Ebenso ist es unzulässig, Mitarbeiterdaten an Gewerkschaften zu übermitteln, damit diese etwa ihre Beiträge besser berechnen können.

Kapitel 4 Mitwirkung der MAV bei technischen Änderungen

1. Datenschutz durch Technik

Der moderne Datenschutz ist nicht auf dem Stand des Volkszählungsurteils des Bundesverfassungsgerichts stehen geblieben. Moderne technische Möglichkeiten, vor allem die Nutzung des Internets, haben immer stärker den Ruf nach Sicherheit und Schutz des persönlichen Lebensbereiches laut werden lassen. Wer will sich schon an Homebanking oder Homeshopping beteiligen, wenn er damit rechnen muss, dass seine Kreditkarten- und Geheimnummern von jedem mitgelesen werden und zu seinem Schaden benutzt werden können? Ziel moderner Betriebssystem- und Programmentwicklungen ist daher die Schaffung einer datenschutzgerechten Infrastruktur. Dieses Bemühen sollte von den Anwendern dadurch unterstützt werden, dass sie sich beim Kauf von EDV- und Telefonanlagen bewusst für sichere Technologien entscheiden. In den Datenschutzgesetzen des Bundes und der Länder wird die Möglichkeit vorgesehen, Programme und Verfahren aus datenschutzrechtlicher Sicht zertifizieren und mit einem Gütesiegel versehen zu lassen. Allerdings hat bisher lediglich Schleswig-Holstein entsprechende Ausführungsvorschriften erlassen. Für die Zukunft ist mit einer Ausweitung dieser Möglichkeit zu rechnen. Künftig sollten dann nur noch zertifizierte Programme eingesetzt werden.

Nach § 29 I Nr. 14, 15 MAVO ist die Mitarbeitervertretung im Wege der Anhörung und Mitberatung zu beteiligen, wenn grundlegende Änderungen der Arbeitsmethoden oder Maßnahmen zu Hebung der Arbeitsleistung erfolgen sollen. Der Einsatz technischer Hilfsmittel, wie EDV-Anlagen kann ebenso hierunter fallen, wie der Einsatz neuer Programme, die Bildung von Arbeitsgruppen bei der EDV-Nutzung, etc. Der Dienstgeber ist gem. § 6 KDO verpflichtet, solche Änderungen in datenschutzgerechter Weise vorzunehmen. Aufgabe der MAV ist es, hierauf hinzuweisen und gegebenenfalls im Wege der Betriebsvereinbarung mit der Einrichtung die Arbeitsmethoden festzulegen. Das gilt insbesondere bei Einführung von Personalinformationssystemen.

2. Offenheit gegenüber den Mitarbeitern

Die Mitarbeitervertretung ist immer dann besonders gefordert, wenn Maßnahmen zur Kontrolle der Mitarbeiter durchgeführt werden sollen. Daher besteht hier auch eine Zustimmungspflicht nach § 36 I Nr. 9 MAVO. Der Datenschutz will die Einführung von Kontrollsystemen grundsätzlich nicht verhindern. Jeder Dienstgeber ist berechtigt, seine Mitarbeiter hinsichtlich ihrer Arbeitsleistung, Einhaltung der Arbeitszeiten, etc. zu kontrollieren. Fragen nach dem Sinn solcher Einrichtungen für Arbeitsleistung und Betriebsklima sind vom Datenschutz

aus nicht zu beantworten. Hier handelt es sich um politische Fragen, die von der MAV mit dem Dienstgeber geklärt werden müssen.

Wichtig ist jedoch, dass alle durchgeführten Maßnahmen den Mitarbeitern vorher bekannt gegeben werden. Es ist in geeigneter Form auf das Bestehen der Überwachungseinrichtung, ihren Zweck und die beabsichtigten Auswertungen hinzuweisen. So muss beispielsweise klar sein, ob ein Zeiterfassungssystem nur zum Zwecke der Abrechnung der geleisteten Arbeitsstunden oder auch zur Kontrolle der Einhaltung der Dienstzeiten verwendet werden soll. Erinnern wir uns: Die Nutzung der Daten ist immer nur für den Zweck gestattet, für die sie erhoben worden sind (strenge Zweckbindung). Der Zweck muss also **vor der Erhebung** festgelegt und bekannt gegeben werden. Die Zwecke einer solchen Datenerhebung sollten schriftlich, möglichst im Wege einer Betriebsvereinbarung festgelegt werden

Völlig datenschutzwidrig ist die Durchführung geheimer Überwachungsmaßnahmen. Ausnahmen hiervon können nur dort bestehen, wo es um die Aufdeckung von Straftaten geht, wenn der Täter anders nicht zu ermitteln ist.

3. Telefondatenerfassung und -abrechnung

Die Rechtmäßigkeit der Aufzeichnung der Verbindungsdaten dienstlich geführter Telefongespräche ist nicht zweifelhaft. Sie muss jedoch der Zweckbestimmung des Vertragsverhältnisses dienen. Grundsätzlich ist die Möglichkeit, mit der Telekommunikationsanlage Gebührenabrechnungen zu erstellen, ein Hilfsmittel zur Gebührenabrechnung und nicht ein Kontrollinstrument zur Überwachung der Telefonpraxis der Mitarbeiterinnen und Mitarbeiter. Da die Verwaltungsleitung darüber zu wachen hat, dass mit den zur Verfügung stehenden Geldern wirtschaftlich und sparsam umgegangen wird, ist sie auch befugt, das Führen von Dienstgesprächen zu überprüfen. Dafür ist es zulässig, die Zielrufnummer vollständig zu erfassen. Jeder Arbeitnehmer und jede Arbeitnehmerin ist seiner beziehungsweise ihrer Firma zur Rechenschaft über die Führung der **dienstlich** veranlassten Gespräche verpflichtet. Im Rahmen von Stichproben und bei einem begründeten Verdacht, dass unbefugt Privatgespräche auf Kosten des Unternehmens geführt werden, kann eine diesbezügliche Überprüfung der Telefondaten zulässig sein. Eine regelmäßige Auswertung der Telefondaten zur Überprüfung des allgemeinen Arbeitsverhaltens der Beschäftigten ist sowohl aus datenschutzrechtlicher Sicht als auch nach der Rechtsprechung der Arbeitsgerichte unzulässig.

Einschränkungen gelten dort, wo Mitarbeiter nach § 203 StGB zu besonderer beruflicher Verschwiegenheit verpflichtet sind. Da die ausgewiesene Telefonnummer auf die angerufene Person schließen lässt, ist von einer Speicherung der vollständigen Rufnummer abzusehen. Eine Speicherung unter Verkürzung der Nummer um die letzten drei Stellen, bleibt jedoch zulässig.

Wird auch eine private Telefonnutzung zugelassen, wird der Dienstgeber zum Telekommunikationsdiensteanbieter und hat insbesondere das Fernmeldegeheimnis nach Maßgabe des § 85 Telekommunikationsgesetz (TKG) zu wahren. Eine Aufzeichnung der Kommunikationsdaten privater Telefonate der Beschäftigten ist der Dienststelle daher ausschließlich zu Ab-

rechnungszwecken erlaubt. Unterliegt die private Nutzung besonderen Einschränkungen, etwa im Hinblick auf mögliche Beeinträchtigungen des Dienstbetriebes (z.B. zeitliche Beschränkung auf Pausen o.ä.), müssen die Beschäftigten sich ausdrücklich mit diesen Nutzungsbedingungen einverstanden erklären. Nur wenn diese Einwilligung vorliegt, ist die Dienststelle in begründeten Verdachtsfällen berechtigt, die sich aus der Abrechnung insgesamt ergebende Zeitdauer privater Telefongespräche auf die Vereinbarkeit mit arbeitsvertraglichen Pflichten hin zu überprüfen. Daneben ist bei der Erfassung von Daten der von den Beschäftigten geführten Telefongespräche gem. § 36 I Nr. 9 MAVO die Zustimmung der MAV erforderlich.

Werden die Gesprächsnachweise über private Telefongespräche zur Abrechnung an die Beschäftigten übersandt, hat dies in verschlossenen, persönlich adressierten Umschlägen zu geschehen. Die Speicherung der erfassten Telefondaten ist auf den Zeitraum zu beschränken, in dem in der Regel abrechnungstechnische Fragen geklärt werden können, üblicherweise genügt hierzu eine Speicherung von drei Monaten.

4. Mithören dienstlich veranlasster Telefongespräche

Sollen dienstlich veranlasste Telefongespräche mitgehört werden, so ist hierbei das Recht am eigenen Wort der Beschäftigten zu beachten. Das in Art. 2 I i.V.m. Art. 1 I GG verfassungsrechtlich gewährleistete Persönlichkeitsrecht ist auch im Privatrechtsverkehr und damit im beruflichen Bereich zu beachten (BAG NJW 1986, 341). Dieses Recht umfasst die Befugnis des Menschen selbst zu bestimmen, ob seine Worte einzig seinem Gesprächspartner, einem bestimmten Kreis oder der Öffentlichkeit zugänglich sein sollen (BVerfGE 54, 148 [155]). Der dienstliche oder rein geschäftliche Charakter eines Telefongesprächs beseitigt diese Bestimmungsbefugnis nicht ohne weiteres (BVerfG in CR 1992, 498 [499]). Dementsprechend unterliegen auch dienstliche Telefonate dem Schutz des allgemeinen Persönlichkeitsrechts. Dies gilt selbst dann, wenn eine Mithörmöglichkeit bekannt ist. Ein Mithören dienstlicher Telefongespräche ist regelmäßig nur dann mit dem allgemeinen Persönlichkeitsrecht vereinbar, wenn der Umstand des Mithörens signalisiert wird und überwiegende Firmeninteressen das Mithören rechtfertigen oder wenn das Personal wirksam eingewilligt hat (vgl. auch BAG NJW 1998, 1331 ff.).

Weiterhin ist zu beachten, dass es sich bei dem Mithören von Telefongesprächen regelmäßig um eine Maßnahme zur Überwachung des Verhaltens und der Leistung der Beschäftigten mittels einer technischen Einrichtung handelt. Die Einführung und Anwendung derartiger technischer Einrichtungen unterliegt gemäß § 36 I Nr. 9 MAVO der Zustimmung der MAV. Dabei ist es Aufgabe der MAV, auf eine Betriebsvereinbarung hinzuwirken, durch die der Katalog der Daten und die Auswertungen in so engen Grenzen gehalten werden wie möglich. Durch eine solche Betriebsvereinbarung wird innerbetriebliches Datenschutzrecht geschaffen. Letztlich bleibt festzustellen, dass Mitarbeiter und Mitarbeiterinnen keineswegs einem permanenten Kontrolldruck ausgesetzt sein dürfen. Kontrollen sind grundsätzlich nur nach Maßgabe des Verhältnismäßigkeitsgrundsatzes zulässig. Demzufolge müssen die Beschäftigten Kontrollen ihres Arbeitsverhaltens nur dann hinnehmen, wenn diese geeignet und erforderlich sind, um den Zweck des Beschäftigungsverhältnisses zu erreichen.

Bei der datenschutzrechtlichen Beurteilung der Frage des Mithörens von Telefongesprächen sind neben den Persönlichkeitsrechten der Beschäftigten auch diejenigen der anrufenden Kundinnen und Kunden zu berücksichtigen. Deshalb sind derartige Abhörmaßnahmen durch den Arbeitgeber gegenüber der Kundin oder dem Kunden transparent zu machen. Aus diesem Grund ist eine vorherige Unterrichtung – etwa durch eine kurze Ansage – geboten und auf Wunsch ein nicht abgehörtes Gespräch zu ermöglichen

5. E-Mail und Internet am Arbeitsplatz

Der Themenkreis der Nutzung von E-Mail und Internet am Arbeitsplatz wirft eine Reihe datenschutzrechtlicher Fragen auf. Grundsätzlich empfiehlt es sich, die Nutzung von E-Mail und Internet für die Dienststelle im Rahmen einer Betriebsvereinbarung schriftlich und verbindlich unter Einbeziehung der Mitarbeiter und Mitarbeiterinnen zu regeln (siehe Anhang).

Wesentliches Unterscheidungskriterium für die rechtliche Beurteilung möglicher Zugriffsrechte auf den E-Mail-Verkehr der Mitarbeiter ist die Frage der Zulassung **dienstlicher** und **privater** Nutzung. In einer Dienststelle kann die Nutzung von E-Mail und Internet auf dienstliche Zwecke beschränkt sein. Eine Einrichtung ist nicht verpflichtet, private E-Mail-Nutzung zuzulassen. Der Schriftverkehr mit E-Mails zu dienstlichen Zwecken unterliegt gegenüber der Verwaltungsleitung ebenso wenig wie dienstliche Briefpost dem Fernmeldegeheimnis, da die Mitarbeiter im Rahmen ihrer dienstlichen Aufgaben für das Unternehmen tätig werden. Wie bei herkömmlicher Briefpost können Vorgesetzte sich daher dienstliche E-Mails vorlegen lassen bzw. sich einen Zugang hierzu einräumen lassen. Darüber hinaus dürfen Firmen auch aus Sicherheitsgründen ein- und ausgehende E-Mails geschäftlicher und privater Natur auf Virenbefall kontrollieren, wenn die Kontrolle automatisch erfolgt. Die zu diesem Zweck gespeicherten Daten dürfen allerdings auch nur zu dem genannten Zweck verwendet werden, eine Kontrolle beispielsweise des Arbeits- und Leistungsverhaltens der Mitarbeiter und Mitarbeiterinnen ist unzulässig. Darüber hinaus darf die Geschäftsleitung von ein- und ausgehenden E-Mails der Beschäftigten im selben Maße Kenntnis nehmen, wie von deren sonstigem dienstlichen Schriftverkehr. Das Gebot der Transparenz der Datenverarbeitung beinhaltet in diesem Zusammenhang allerdings die Verpflichtung des Unternehmens, die Mitarbeiterinnen und Mitarbeiter über diesen Umstand zu informieren.

Die Kommunikation der Beschäftigten mit der MAV bzw. mit dem Betriebsarzt oder der Betriebsärztin per E-Mail stellt im Rahmen des dienstlichen E-Mail-Verkehrs einen Sonderfall dar. Die Einrichtung hat sicherzustellen, dass diese Kommunikation vertraulich möglich ist. Es empfiehlt sich daher, für diesen Personenkreis einen gesonderten E-Mail-Anschluss zur Verfügung zu stellen, der nicht den üblichen Zugriffen im Betrieb ausgesetzt ist, bzw. den Mitarbeiterinnen und Mitarbeitern die Möglichkeit zu geben, E-Mails zu verschlüsseln. Unter welchen Voraussetzungen in begründeten Ausnahmefällen auch der E-Mail-Verkehr mit der MAV kontrolliert werden kann, ist in einer Betriebsvereinbarung zu regeln. Diese kann zum Beispiel Stichprobenkontrollen vorsehen, wenn der Verdacht besteht, dass strafrechtlich relevante Inhalte oder Computerviren auf diesem Wege verbreitet werden. Sollte es nicht möglich sein, die entsprechenden technischen Voraussetzungen für eine vertrauliche Kommunikation per E-Mail mit der MAV zu schaffen, sind die Betriebsangehörigen hierüber mit Hin-

weis auf die Konsequenzen zu unterrichten. Für Betriebsärzte und Betriebsärztinnen, die aufgrund ihres Berufes einer besonderen Verschwiegenheitspflicht unterliegen und aufgrund ihrer Tätigkeit Kenntnis von sensiblen personenbezogenen Daten erhalten, bestehen grundsätzliche datenschutzrechtliche Vorbehalte gegen die Nutzung von E-Mail zum Zwecke des Austausches vertraulicher Informationen.

Private Nutzung von E-Mail und Internet kann eine Dienstelle erlauben. Wegen der bestehenden technischen Schwierigkeiten, dienstliche und private Post bei der Nutzung einer E-Mail-Adresse voneinander zu trennen, ist es notwendig, bei der Zulassung privater Nutzung jedem Mitarbeiter und jeder Mitarbeiterin eine eigene E-Mail-Adresse für private Post zuzuweisen. Lässt eine Einrichtung die private Nutzung von E-Mail am Arbeitsplatz zu, wird es im Sinne des Teledienstedatenschutzgesetzes (TDDG) Diensteanbieter und ist damit zur Wahrung des Fernmeldegeheimnisses verpflichtet. Es darf die Verbindungsdaten nicht dauerhaft speichern, das TDDG erlaubt eine Speicherung nur zu Abrechnungszwecken. Auch zur Sicherung der Dienstleistung bzw. für die Fehlersuche und Behebung darf eine Protokollierung erfolgen.

Im Regelfall unterliegt die Zulassung der privaten Nutzung speziellen Einschränkungen, beispielsweise im Hinblick auf Empfängerkreis oder auf eine mögliche Beeinträchtigungen des Dienstbetriebes (z.B. zeitliche Beschränkung auf Pausen o.ä.). Bestehen solche Nutzungsbeschränkungen, müssen die Beschäftigten, die die private E-Mail-Nutzung wünschen, sich ausdrücklich mit den Nutzungsbedingungen einverstanden erklären. Dies kann nicht im Rahmen einer Vereinbarung mit der MAV erfolgen, sondern muss individuell mit jedem Mitarbeiter schriftlich vereinbart werden, d.h. jeder Beschäftigte muss eine schriftliche Vereinbarung über die Bedingungen der Nutzung der E-Mail für private Zwecke abschließen und die Möglichkeit erhalten, im Zweifelsfall auf die private Nutzung zu verzichten. In der Nutzungsordnung, die einer privaten Nutzung der E-Mail-Funktion zugrunde liegt, muss auch festgelegt werden, welche Überprüfungsrechte von der Administration oder von der Personalverwaltung wahrgenommen werden. Dabei ist die Kontrolle so zu gestalten, dass bereits im Ansatz so wenig personenbezogene Daten wie möglich verarbeitet werden. Das gebietet der Grundsatz der Datenvermeidung und Datensparsamkeit.

In der Regel nimmt die Administration die Auswertung der Protokolldaten für das Unternehmen vor. Es ist üblich und zulässig, dass die Administration auch beauftragt wird, die Beachtung der Einschränkungen für die private Nutzung zu überprüfen. Eine Verletzung des Fernmeldegeheimnisses besteht nicht bereits dann, wenn die Geschäftsleitung über Verstöße gegen die Nutzungsbedingungen des privaten E-Mail-Verkehrs informiert wird, beispielsweise bei übermäßiger zeitlicher Inanspruchnahme. In der Nutzungsvereinbarung ist festzulegen, wann und in welchen Fällen die Administration verpflichtet ist, die Geschäftsleitung bzw. die handelnde Personalstelle über missbräuchliche Nutzung der E-Mail-Funktion zu informieren. Weiterhin sollte in der Nutzungsvereinbarung eindeutig geregelt werden, dass auch im Rahmen einer Missbrauchskontrolle grundsätzlich vom Inhalt privater E-Mails nicht Kenntnis genommen werden darf.

6. Fotos von Mitarbeitern im Internet

Die Veröffentlichung von Fotos der Mitarbeiter im Internet begegnet grundsätzlichen datenschutzrechtlichen Bedenken. Fotos von Beschäftigten in das Internet einzustellen, ist nur mit der ausdrücklichen Einwilligung der abzubildenden Personen zulässig. Auch hier gilt das Recht am eigenen Bild. Die Einwilligung der Beschäftigten muss in schriftlicher Form erfolgen und den Betroffenen deutlich machen, worin eingewilligt werden soll. Auch sollte darauf hingewiesen werden, dass die erteilte Einwilligung jederzeit widerrufen werden kann. Dass einzelne Beschäftigte die Anfertigung von Fotos dulden, kann nicht bereits als Einwilligung in die Veröffentlichung des Bildes im Internet gewertet werden. Auch die Zustimmung zur Veröffentlichung in Printmedien kann nicht als Zustimmung zur Veröffentlichung im Internet gewertet werden.

Wird eine Veröffentlichung von Beschäftigtenfotos im Internet angestrebt, sollte unbedingt eine Vereinbarung mit der MAV über die Rahmenbedingungen getroffen werden. Ziel der Vereinbarung muss es sein, die Einwirkungsmöglichkeiten der Beschäftigten zu sichern und klare Regelungen darüber zu treffen, welche Beschäftigtengruppen von der Veröffentlichung betroffen sein sollen und wie die Veröffentlichung technisch realisiert wird.

7. Arbeitszeiterfassung

Die regelmäßige monatliche Information der Beschäftigten über den Stand ihres Arbeitszeitkontos ist unbedenklich. Nicht zulässig ist jedoch die Versendung in einem offenen Sammelumschlag nach Kontrolle durch die Personalabteilung. Diese Form der Datenweitergabe, die den Zugriff Dritter, beispielsweise den von Vorgesetzten, auf die Daten ermöglicht, ist datenschutzrechtlich ebenso unzulässig wie die generelle Arbeitszeitkontrolle durch die Personalabteilung. Die Information von Vorgesetzten über die Arbeitszeitkonten der Beschäftigten ist nur dann zulässig, wenn sie für die Zwecke der Personalplanung und des Personaleinsatzes. erforderlich ist, also die konkrete Aufgabe in der Vorgesetztenfunktion ohne die Kenntnis dieser Daten nicht sachgerecht erfüllbar wäre.

Die laufende Unterrichtung von Vorgesetzten über den Stand des Arbeitszeitkontos von Mitarbeitern ist unter dem Aspekt des Datenschutzes nur unbedenklich, wenn in Einzelfällen das Zeitdefizit oder Zeitguthaben von Beschäftigten geeignet ist, den Dienstablauf zu beeinträchtigen. Eine generelle regelmäßige Information der vorgesetzten Personen ist nicht verhältnismäßig.

8. Multifunktions- und Chipkarten für Mitarbeiter

Chipkartenausweise können neben dem Identitätsnachweis über vielfältige Zusatzfunktionen verfügen, wie etwa Zutrittsberechtigung zu Gebäuden, Arbeitszeiterfassung, Authentifikation gegenüber Servern oder als Zahlungsmittel für die Kantine. Auch als Instrument für digitale Signatur und Verschlüsselung kommen Chipkarten in Betracht. Es liegt auf der Hand, dass die Kontrollmöglichkeiten des Dienstherrn durch den Einsatz von Chipkarten erleichtert werden, was insbesondere bei der Verknüpfung unterschiedlicher Funktionen unter dem Ge-

sichtspunkt des Mitarbeiterdatenschutzes problematisch werden kann. So könnte sich der Dienstherr etwa mittels Zeiterfassungs- und Zutrittsdaten ein Bewegungsprofil seiner Mitarbeiter erstellen. Wegen der **Möglichkeit** der Mitarbeiterkontrolle, ist vor Einführung mobiler personenbezogener Speicher- und Verarbeitungsmedien die Zustimmung der MAV erforderlich. Da es sich in der Regel um komplexe Datenverarbeitungssysteme handelt, ist der Abschluss einer Betriebsvereinbarung, der den Einsatz dieser Systeme, die berechtigten Auswertungsmöglichkeiten und die zu ihrem Schutz zu treffenden Maßnahmen festlegt, sinnvoll Eine solche Vereinbarung muss mindestens die Anforderungen von § 5b KDO erfüllen:.

> ***„§ 5b Mobile personenbezogene Speicher- und Verarbeitungsmedien***
> *(1) Die Stelle, die ein mobiles personenbezogenes Speicher- und Verarbeitungsmedium ausgibt oder ein Verfahren zur automatisierten Verarbeitung personenbezogener Daten, das ganz oder teilweise auf einem solchen Medium abläuft, auf das Medium aufbringt, ändert oder hierzu bereithält, muss den Betroffenen*
> *1. über ihre Identität und Anschrift,*
> *2. in allgemein verständlicher Form über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten,*
> *3. darüber, wie er seine Rechte nach den §§ 13 und 14 ausüben kann und über die bei Verlust oder Zerstörung des Mediums zu treffenden Maßnahmen unterrichten, soweit der Betroffene nicht bereits Kenntnis erlangt hat.*
> *(2) Die nach Absatz 1 verpflichtete Stelle hat dafür Sorge zu tragen, dass die zur Wahrnehmung des Auskunftsrechts erforderlichen Geräte oder Einrichtungen in angemessenem Umfang zum unentgeltlichen Gebrauch zur Verfügung stehen.*
> *(3) Kommunikationsvorgänge, die auf dem Medium eine Datenverarbeitung auslösen, müssen für den Betroffenen eindeutig erkennbar sein.“*

9. Videoüberwachung am Arbeitsplatz

Für die Überwachung öffentlicher Räume, die von einer unbestimmten Vielzahl von Personen benutzt werden können, mit Videokameras stellt § 5a KDO eine Rechtsgrundlage bereit.

> ***„§ 5a Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen***
> *(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie*
> *1. zur Aufgabenerfüllung oder zur Wahrnehmung des Hausrechts oder*

2. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

(2) Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen.

(3) Die Verarbeitung oder Nutzung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über eine Verarbeitung oder Nutzung entsprechend § 13 a zu benachrichtigen.

(5) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen."

Probleme aus datenschutzrechtlicher Sicht bestehen vor allem dann, wenn bei der Überwachung von Eingangsbereichen zugleich die dort tätigen Mitarbeiter beobachtet werden können. Eine generelle Überwachung des Arbeitsverhaltens von Mitarbeitern „rund um die Uhr" verletzt den Grundsatz der Menschenwürde und deren Persönlichkeitsrecht. Sie kann nur ausnahmsweise gestattet sein, wenn Anhaltspunkte dafür vorliegen, dass der Mitarbeiter schwerwiegende Straftaten begeht und eine Aufklärung anders nicht möglich ist. In diesen selten vorkommenden Fällen, ist die MAV entsprechend zu beteiligen. Auch Fälle, in denen eine Videoüberwachung zum Schutz der Mitarbeiter erforderlich ist (z.B. Kassenhalle), sind denkbar und sollten zuvor mit der MAV vereinbart werden. In allen anderen Fällen sind Videokameras so zu installieren, dass der Arbeitsbereich der Mitarbeiter nicht erfasst wird.

Der Aufbewahrungszeitraum für Videobänder ist auf das unbedingt erforderliche Maß zu reduzieren. In der Regel reicht es aus, wenn das Band innerhalb von 24 Stunden überschrieben wird. Bei Vorliegen besonderer Vorkommnisse kann das Band gesichert und solange aufbewahrt werden, wie es zur Durchsetzung der eigenen Ansprüche erforderlich ist. Berücksichtigt werden sollte auch, das Videobänder im Zivil- und Strafprozess nur als Augenscheinsobjekte zugelassen sind. Ihr Beweiswert hängt daher wesentlich von den Zeugenaussagen über die Erstellung des Bandes ab. Das Verfahren der Videoüberwachung, insbesondere die Verantwortlichkeiten für das Einlegen und Entnehmen des Bandes und seine anschließende Aufbewahrung sollte daher genau dokumentiert sein.

Eine ausschließlich zur Kontrolle der Beschäftigten eingesetzte Videoüberwachung ist nach ständiger Rechtsprechung der Arbeitsgerichte unzulässig und als Verstoß gegen das Persönlichkeitsrecht der Betroffenen anzusehen. Ausnahmen hiervon sind in den gleichen Fällen, wie oben möglich.

Dienstvereinbarung
zwischen
dem ……
und
der Mitarbeitervertretung im ……
über die Nutzung elektronischer Kommunikationssysteme am Arbeitsplatz

Das ……. und die Mitarbeitervertretung im …….
schließen nach § 38 Mitarbeitervertretungsordnung die folgende Dienstvereinbarung über die Nutzung elektronischer Kommunikationssysteme am Arbeitsplatz:

§ 1 Gegenstand und Geltungsbereich

Diese Vereinbarung regelt die Grundsätze für den Zugang und die Nutzung der Internetdienste im ……. und gilt für alle Mitarbeiter, deren Arbeitsplätze über einen Internetzugang verfügen.

§ 2 Zielsetzung

Ziel dieser Vereinbarung ist es, die Nutzungsbedingungen sowie die Maßnahmen zur Protokollierung und Kontrolle transparent zu machen, die Persönlichkeitsrechte der Mitarbeiter zu sichern und den Schutz ihrer personenbezogenen Daten zu gewährleisten.

§ 3 Nutzung

(1) Der Internet-Zugang steht den Mitarbeitern als Arbeitsmittel im Rahmen der Aufgabenerfüllung zur Verfügung und dient insbesondere der Verbesserung der internen und externen Kommunikation, der Erzielung einer höheren Effizienz und der Beschleunigung der Informationsbeschaffung und der Arbeitsprozesse.

(2) Die private Nutzung im geringfügigen Umfang ist zulässig, soweit die dienstliche Aufgabenerfüllung sowie die Verfügbarkeit des IT-Systems für dienstliche Zwecke nicht beeinträchtigt werden und fiskalische Grundsätze dem nicht entgegenstehen. Privater E-Mail-Verkehr darf nur über die kostenlosen Web-Mail-Dienste abgewickelt werden. Das Abrufen von kostenpflichtigen Informationen für den Privatgebrauch ist unzulässig. Im Rahmen der privaten Nutzung dürfen keine kommerziellen oder sonstigen geschäftlichen Zwecke verfolgt werden.

(3) Eine Unterscheidung von dienstlicher und privater Nutzung auf technischem Weg erfolgt nicht. Die Protokollierung und Kontrolle gemäß §§ 6 und 7 dieser Vereinbarung erstrecken sich auch auf den Bereich der privaten Nutzung des Internetzugangs.

(4) Durch die private Nutzung des Internetzugangs erklärt der Mitarbeiter seine Einwilligung in die Protokollierung und Kontrolle gemäß §§ 6 und 7 dieser Vereinbarung für den Bereich der privaten Nutzung.

§ 4 Verhaltensgrundsätze

(1) Grundsätzlich gelten die Regelungen der „Dienstanweisung für die Nutzung des IT-Systems im ……..

(2) Unzulässig ist jede absichtliche oder wissentliche Nutzung des Internet, die geeignet ist, den Interessen der Dienststelle oder deren Ansehen in der Öffentlichkeit zu schaden, die Sicherheit des Behördennetzes zu beeinträchtigen oder die gegen geltende Rechtsvorschriften und die Dienstanweisung für die Nutzung des IT-Systems gemäß Absatz 1 verstößt. Dies gilt vor allem für

- das Abrufen oder Verbreiten von Inhalten, die gegen persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstoßen,
- das Abrufen oder Verbreiten von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, sexistischen, gewaltverherrlichenden oder pornografischen Äußerungen oder Abbildungen.

(3) Zur Überprüfung der Einhaltung der Regelungen dieser Vereinbarung werden regelmäßige nicht-personenbezogene Stichproben in den Protokolldateien durchgeführt (vgl. § 6 Abs. 3). Ergänzend wird eine Übersicht über das jeweilige Gesamtvolumen des ein- und ausgehenden Datenverkehrs erstellt.

(4) Die bei der Nutzung der Internetdienste anfallenden personenbezogenen Daten werden nicht zur Leistungs- und Verhaltenskontrolle verwendet. Sie unterliegen der Zweckbindung dieser Vereinbarung und den einschlägigen datenschutzrechtlichen Vorschriften.

§ 5 Information und Schulung der Beschäftigten

Die Beschäftigten werden durch die Dienststelle über die besonderen Datensicherheitsprobleme bei der Nutzung der elektronischen Kommunikationssysteme unterrichtet. Sie werden für den sicheren und wirtschaftlichen Umgang mit diesen Systemen qualifiziert und über die einschlägigen Rechtsvorschriften informiert.

§ 6 Protokollierung und Kontrolle

(1) Die Verbindungsdaten für den Internet-Zugang werden mit Angaben von

- Datum / Uhrzeit,
- Adressen von Absender und Empfänger und
- übertragener Datenmenge

protokolliert.

(2) Die Protokolle nach Absatz 1 werden ausschließlich zu Zwecken der

- Analyse und Korrektur technischer Fehler
- Gewährleitung der Systemsicherheit
- Optimierung des Netzes
- statistischen Feststellung des Gesamtnutzungsvolumens
- Stichprobenkontrollen gemäß Absatz 3 und
- Auswertungen gemäß § 7 dieser Vereinbarung (Missbrauchskontrolle)

verwendet.

(3) Die Protokolle werden durch einen von der Einrichtungsleitung schriftlich beauftragten Mitarbeiter regelmäßig stichprobenhaft hinsichtlich der aufgerufenen Websites, aber nicht personenbezogen gesichtet und ausgewertet. Die Auswertung der Übersicht des Gesamtdatenvolumens erfolgt monatlich ebenfalls durch diesen Mitarbeiter. Der betriebliche Datenschutzbeauftragte wird beteiligt, wenn er dies wünscht.

(4) Der Zugriff auf die Protokolldateien für die Zwecke der Erstellung der Übersicht, der Durchführung der nicht-personenbezogenen Stichproben und der jeweiligen Auswertung ist auf den von der Einrichtungsleitung beauftragten Mitarbeiter begrenzt. Dieser hat eine entsprechende Verpflichtungserklärung zum Datenschutz unterschrieben. Darüber hinaus ist er hinsichtlich der Einhaltung des Fernmeldegeheimnisses und des Datenschutzes auf die strafrechtlichen Konsequenzen bei Verstößen hingewiesen worden.

(5) Die Protokolldaten werden nach einer Woche automatisch gelöscht.

§ 7 Maßnahmen bei Verstößen / Missbrauchsregelung

(1) Bei Verdacht auf missbräuchliche / unerlaubte Nutzung des Internetzugangs gemäß §§ 3 und 4 dieser Vereinbarung durch einen Mitarbeiter erfolgt unter Beteiligung des betrieblichen Datenschutzbeauftragten eine Überprüfung durch eine von der Einrichtungsleitung einzusetzende Untersuchungsgruppe, der auch der nach § 6 Abs. 3 beauftragte Mitarbeiter angehört. Sie veranlasst gegebenenfalls weitere Untersuchungsmaßnahmen (z.B. Offenlegung der IP-Adresse des benutzten PC's oder weitere Überprüfungen). Auf der Basis dieser Untersuchung erstellt sie einen Bericht, der dem Betroffenen ausgehändigt wird. Dieser ist anschließend dazu zu hören.

(2) Im Übrigen gelten die einschlägigen Regelungen des Disziplinar- bzw. Tarifrechts.

(3) Ist aufgrund der stichprobenhaften nicht-personenbezogenen Kontrollen bzw. der Auswertung der Übersicht des Datenvolumens eine nicht mehr tolerierbare Häufung von offensichtlich privater Nutzung des Internetzugangs zu erkennen, so werden innerhalb von einer zu setzenden Frist von 2 Wochen die Stichproben weiterhin nichtpersonenbezogen durchgeführt. Ergeben diese Stichproben bzw. die Auswertung der Übersicht des Datenvolumens keine Änderung im Nutzungsverhalten, so werden die Protokolle der folgenden 2 Wochen durch eine Untersuchungsgruppe stichprobenhaft personenbezogen ausgewertet. Hierbei wird wie im Falle des Verdachts einer missbräuchlichen Nutzung (Abs. 1) vorgegangen. Zu den Verfahren nach Satz 1 und Satz 2 erfolgt eine entsprechende vorherige schriftliche Mitteilung an alle Beschäftigten.

(4) Ein Verstoß gegen diese Dienstvereinbarung kann neben den dienst- und arbeitsrechtlichen Folgen auch strafrechtliche Konsequenzen haben.

(5) Die Dienststellenleitung behält sich vor, bei Verstößen gegen diese Vereinbarung die private Nutzung des Internetzugangs im Einzelfall zu untersagen.

§ 8 Änderungen und Erweiterungen

(1) Geplante Änderungen und Erweiterungen an den elektronischen Kommunikationssystemen werden der Mitarbeitervertretung und dem betrieblichen Beauftragten für den Datenschutz mitgeteilt. Es wird dann geprüft, ob und inwieweit sie sich auf die Regelungen dieser Vereinbarung auswirken. Notwendige Änderungen oder Erweiterungen zu dieser Vereinbarung können im Einvernehmen in einer ergänzenden Regelung vorgenommen werden.

(2) Zur Evaluierung dieser Dienstvereinbarung ist nach Ablauf von zwei Jahren ein Erfahrungsbericht vorzulegen.

§ 9 Schlussbestimmungen

(1) Diese Vereinbarung tritt mit ihrer Unterzeichnung in Kraft. Sie kann mit einer Frist von drei Monaten zum Monatsende, frühestens jedoch zum _____ gekündigt werden. Im Falle einer Kündigung bleibt sie bis zum Abschluss einer neuen Vereinbarung gültig.

(2) Jeder Mitarbeiter bestätigt schriftlich die Kenntnisnahme. Ein Abdruck der Vereinbarung wird ihm zusammen mit einer Kopie der Bestätigung ausgehändigt.