

DOKUMENTATION

ZUM FACHTAG

„DATENSCHUTZ UND NEUE MEDIEN“

am 11. Februar 2003 in Frankfurt/M.



Deutscher Caritasverband e.V.
Basisdienste und
Besondere Lebenslagen
Postfach 420, 79004 Freiburg
Tel.: ++ 49(0)761 200-369
Fax: ++ 49(0)761 200-350
Renate.Walter-Hamann@caritas.de

Einleitung

In den Diensten und Einrichtungen der Caritas wird vielfach mit sensiblen personenbezogenen Daten gearbeitet. Datenschutzrechtliche Fragen haben in der Beratung, Behandlung und Betreuung der Caritas daher einen hohen Stellenwert. Das Vertrauensverhältnis zwischen Klient/in und Berater/in beruht wesentlich auch auf einem gesicherten Umgang mit personenbezogenen Daten und der Einhaltung des Datenschutzes.

Zusätzliche aktuelle Dynamik erhalten die Fragen des Datenschutzes durch den Einsatz neuer Möglichkeiten der edv- gestützten Datenübermittlung und der Vernetzung von Einrichtungen über Trägernetzwerke.

Was also – durchaus im Interesse der KlientInnen und MitarbeiterInnen – eine rasche Bearbeitung von Anfragen oder Anträgen ermöglicht, wirft gleichzeitig neue Fragen auf bzw. akzentuiert sie neu: Aspekte des Klientenschutzes und der Mitarbeiterrechte werden davon ebenso berührt wie die Klärung von Verfahrensabläufen und der Regelungsbedarf von erforderlichen Dienstvereinbarungen.

Da im vergangenen Jahr zahlreiche Anfragen zum Datenschutz im Kontext der edv- gestützten Datenweitergabe an das Fachreferat gerichtet worden sind, haben wir diese Fragen systematisiert und in Abstimmung mit mehreren Diözesan-Referenten-Konferenzen zur Grundlage eines fachbereichsübergreifenden Fachtages gemacht.

Der Fachtag hatte zum Ziel,

- die TeilnehmerInnen für die aktuellen datenschutzrechtlichen Fragen zu sensibilisieren
- die aktuelle Rechtslage zu zentralen datenschutzrechtlichen Fragekomplexen darzustellen
- Fragen der praktischen Umsetzung datenschutzrechtlicher Bestimmungen zu diskutieren.

Die Veranstaltung richtete sich an Referenten/innen der Diözesan-Caritasverbände in den Arbeitsfeldern des Referates Basisdienste und besondere Lebenslagen:

Allgemeine Sozialberatung, Rechtliche Betreuung, Schuldnerberatung, Suchthilfe, Straffälligen-hilfe und Wohnungslosenhilfe.

Als Referent konnte der kirchliche Datenschutzbeauftragte der Erzdiözese Freiburg und der Diözese Rottenburg-Stuttgart, Herr Dr. Siegfried Fachtet, gewonnen werden.

Die vorliegende Dokumentation behandelt die zentralen Themenschwerpunkte des Fachtages. Neben grundsätzlichen Ausführungen werden auch spezielle Fragestellungen aufgegriffen, die im Rahmen des Fachtages von den Teilnehmer/innen gestellt worden sind. Ergänzt wird die Dokumentation durch ein Glossar zentraler Fachbegriffe aus dem Rechts- und Verwaltungswesen.

Die Inhalte der Dokumentation gehen im Wesentlichen zurück auf die Ausführungen von Dr. Siegfried Fachtet im Rahmen der Veranstaltung und auf ergänzende Hinweise, die wir seinem Praxiskommentar zur Anordnung über den Kirchlichen Datenschutz (KDO), Luchterhand Verlag, entnommen haben.

Wir freuen uns, dass wir Ihnen dieses umfangreiche Datenmaterial zur Verfügung stellen können. Und wir hoffen, Ihnen damit eine Unterstützung für die praktischen Fragen in der Auseinandersetzung mit datenschutzrechtlichen Fragen, insbesondere im Kontext der edv-gestützten Datenweitergabe zu vermitteln.

Ich bedanke mich bei Herrn Dr. Facht und Frau Kirsten Schellack, Praktikantin im Referat BBL, die wesentlich zum Gelingen dieser Dokumentation beigetragen haben.

Wir freuen uns über Rückmeldungen, ob diese Materialien hilfreich für die Arbeit der Träger, Dienste und Einrichtungen vor Ort sind und welche Fragen möglicherweise noch aufgegriffen werden sollen.

Weitere Einzel-Exemplare können Sie im Referat Basisdienste und besondere Lebenslagen anfordern. Wir können Ihnen die Dokumentation auch als pdf- Datei übersenden.

Freiburg, den 25. April 2003

Renate Walter-Hamann
Referatsleiterin

Inhaltsverzeichnis

A1: Gründe für den Datenschutz
A2: Das informationelle Selbstbestimmungsrecht als Grundrecht
A3: Datenschutzrechtliche Anforderungen, die sich aus der Verfassung ableiten lassen
A4: Benennung der datenschutzrechtlichen Grundsätze
A5: Sozialdatenschutz

B1: Organisation der Beratung
B2: Verschiedene Einzelfragen
B3: Abgrenzung Berufsgeheimnis, besonderem Amtsgeheimnis,
Verschwiegenheit, Geheimhaltungsbestimmungen
B4: Der Arbeitsplatz
B5: Einzelfragen

C1: Zum Internet
C2: Die Nutzung der E-Mail am Arbeitsplatz
C3: Zum Intranet
C4: Das Netzwerk

Glossar und Begriffserklärungen zum Internet

Anhang

A1: Gründe für den Datenschutz

1. Persönlichkeitsrecht schützen:

- Der Datenschutz will das Persönlichkeitsrecht des einzelnen durch datenschutzrechtliche Regelungen schützen.
- Maßstab ist das informationelle Selbstbestimmungsrechts, das aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 des Grundgesetzes abgeleitet wird. In der Zwischenzeit geht die Literatur und die Rechtsprechung davon aus, dass es ein "verfassungsrechtlich gebotenes eigenständiges Grundrecht auf Datenschutz gibt".
- Die datenschutzrechtlichen Rechte haben aber auch den Zweck, Vorgaben zu formulieren, unter denen die Erhebung, Verarbeitung (einschließlich der Übermittlung) und die sonstige Nutzung personenbezogener Daten zulässig ist.
- Der Datenschutz will nicht nur kriminelle Handlungen verhindern, die unter Verwendung von Wissen über andere begangen werden, sondern er will auch die böswilligen, eigennützigen oder fahrlässig begangenen Manipulationen von Daten unterbinden (Schon die mangelnde Sorgfalt, die bloße Nachlässigkeit beim Umgang mit personenbezogenen Daten, kann für den Betroffenen weitreichende Folgen haben. Auch davor will der Datenschutz schützen.

2. Voraussetzungen für die Datenerhebung, Verarbeitung und Nutzung :

Das Datenschutzrecht dient auch dazu, im erlaubten Rahmen die ordnungsgemäße Erhebung, Verarbeitung, Verteilung bzw. Weiterleitung personenbezogener Daten und Informationen zu gewährleisten.

3. Rechte des Betroffenen stärken:

Das Datenschutzrecht räumt dem Betroffenen Rechte ein, die er gegenüber der datenverarbeitenden Stelle geltend machen kann.

A2: Das informationelle Selbstbestimmungsrecht als Grundrecht

1. Der Schutz der Persönlichkeitssphäre wird immer notwendiger:

Je leichter der Zugriff auf die Daten mittels elektronischer Datenverarbeitung ist, umso nachdrücklicher muss die Persönlichkeitssphäre des einzelnen geschützt werden. Allerdings hat die Persönlichkeitssphäre ebenfalls ihre Grenzen. Das *Bundesverfassungsgericht* hat in seiner bekannten Entscheidung zum Volkszählungsgesetz das Spannungsverhältnis zwischen den Rechten des einzelnen und den Rechten der Gemeinschaft beschrieben (BVerfGE 65, 1, NJW 1984, 419, Urteil vom 15. Dezember 1983).

2. Der Prüfungsmaßstab: Dazu sagt das *Bundesverfassungsgericht*: -

- Prüfungsmaßstab ist in erster Linie das durch Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG (Grundgesetz) geschützte allgemeine Persönlichkeitsrecht. Im Mittelpunkt der grundgesetzlichen Ordnung stehen Wert und Würde der Person, die in freier Selbstbestimmung als Glied einer freien Gesellschaft wirkt (a.a.O, S. 421 linke Spalte). Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen und zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wäre eine Gesellschaftsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß ...Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG umfasst...Dieses Recht auf "informationelle Selbstbestimmung" ist nicht schrankenlos gewährleistet. Der einzelne hat nicht ein Recht im Sinne einer absoluten, uneinschränk-baren Herrschaft über "seine" Daten; er ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit. Information, auch soweit sie personenbezogen ist, stellt ein Abbild sozialer Realität dar, das nicht ausschließlich dem Betroffenen allein zugeordnet werden kann. Das Grundgesetz hat, wie in der Rechtsprechung des BVerfG mehrfach hervorgehoben ist, die Spannung Individuum - Gemeinschaft im Sinne der Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person entschieden. Grundsätzlich muss daher der Einzelne Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnehmen" (a.a.O, S. 422 links).

3. Zu den Folgen des Urteils:

Dieses Urteil ist für die weitere Entwicklung des Datenschutzes sehr wichtig geworden. Das *Bundesverfassungsgericht* hat übrigens die verfassungsmäßige Zulässigkeit und Notwendigkeit einer Volkszählung bejaht und das vorgesehene Erhebungsprogramm als mit dem Grundgesetz vereinbar erklärt, zur Durchführung und Organisation aber einige zusätzliche verfahrensrechtliche Vorkehrungen gefordert. So wurden insb. der 1983 vorgesehene Melderegisterabgleich, der für die Gemeinden bei den bisherigen Volks-zählungen freilich immer von besonderem Nutzen war, sowie bestimmte Weiter-leitungsmöglichkeiten von Einzelangaben für verfassungswidrig erklärt.

- 4. Das Recht am gesprochenen Wort zählt zum Kern des Persönlichkeitsrechts:**
Das Recht am gesprochenen Wort schützt die Befugnis, selbst zu bestimmen, ob das Gesagte einzig dem Gesprächspartner, einem Kreis von Personen oder der Öffentlichkeit zugänglich sein soll und ob und von wem auf einen Tonträger aufgenommene Worte abgespielt werden dürfen. Das Recht am gesprochenen Wort schützt den Sprechenden auch davor, dass seine Äußerungen unbefugt außerhalb des von ihm selbst festgelegten Kreises von Zuhörern verwendet werden.
- 5. Das Recht am eigenen Bild zählt zum Kern des Persönlichkeitsrechts:**
Das Recht am eigenen Bild schützt das "Verfügungsrecht" über Darstellungen der Person, wonach jedermann grundsätzlich selbst und allein bestimmen darf, ob und inwieweit andere sein Lebensbild oder bestimmte Vorgänge aus seinem Leben darstellen dürfen.
- 6. Recht auf informationelle Selbstbestimmung:**
Das Recht auf informationelle Selbstbestimmung wurde erst zu Beginn der 80er Jahre vom *Bundesverfassungsgericht* unter Anwendung der Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG definiert. Dieses Recht beinhaltet die Befugnis, "grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen" (BVerfGE 54, 148, [153]; BVerfGE 72, 155, [170]; Recht der Datenverarbeitung, 1992, 208).
- 7. Das Recht auf kommunikative Selbstbestimmung:** In der Literatur wird ein "Recht auf kommunikative Selbstbestimmung" gefordert, da die moderne Fernmeldetechnik (ISDN) neue Risiken für die "Kommunikationskompetenz" bringt (Recht der Datenverarbeitung, 1992, 208).

A3: Datenschutzrechtliche Anforderungen, die sich aus der Verfassung ableiten lassen

1. Allgemeines Persönlichkeitsrecht:

Der Wert und die Würde der Person stehen im Mittelpunkt der grundgesetzlichen Ordnung. Ihrem Schutz dienen u. a. die in Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz gewährleisteten allgemeinen Persönlichkeitsrechte.

In Art. 1 Abs. 1 und Art. 2 Abs. 1 GG sind die Unantastbarkeit der Menschenwürde und das allgemeine Persönlichkeitsrecht verfassungsrechtlich verankert.

2. Das Persönlichkeitsrecht als "abgeleitete Befugnis" des Selbstbestimmungsrechts:

Das Persönlichkeitsrecht umfasst die aus dem Gedanken der Selbstbestimmung folgende Befugnis des einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen personenbezogene Lebenssachverhalte offenbart werden.

3. Gesellschaftsordnung und Datenschutz:

Die informationale Selbstbestimmung beinhaltet, dass der Bürger wissen können muss, wer was wann und bei welcher Gelegenheit über ihn weiß. Die Schaffung eines „gläsernen Menschen“ wäre mit der Verfassung nicht vereinbar.

4. Zum Individuum in der Gesellschaft:

Im Spannungsverhältnis Individuum - Gesellschaft muss der einzelne Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnehmen. Für den Bürger muss erkennbar sein, auf Grund welcher gesetzlichen Grundlagen sich die Voraussetzungen und der Umfang der Einschränkungen ergeben (Gebot der Normenklarheit).

5. Grundsatz der Verhältnismäßigkeit:

Dabei ist der Grundsatz der Verhältnismäßigkeit zu beachten. Dieser aus dem Rechtsstaatsprinzip gefolgerte Grundsatz gehört zur verfassungsmäßigen Ordnung und hat selbst Verfassungsrang. Er erklärt sich aus dem Wesen der Grundrechte selbst. Der allgemeine Freiheitsanspruch des Bürgers gegenüber dem Staat darf von der öffentlichen Gewalt nur soweit beschränkt werden, wie dies zum Schutz öffentlicher Interessen unerlässlich ist.

Der Grundsatz der Verhältnismäßigkeit besagt, dass eine an sich zulässige Maßnahme dann zu unterbleiben hat, wenn die mit ihr verbundenen Nachteile insgesamt die Vorteile überwiegen.

6. Datenschutzrechtliche Grundsätze:

Es gibt keine "belanglosen Daten" mehr. Das informationelle Selbstbestimmungsrecht hat Folgen nicht nur für die Erhebung von Daten, sondern auch für deren Nutzbarkeit und Verwendungsmöglichkeit (Zweckbestimmung, Kenntnis des Verwendungszusammenhangs).

A4: Benennung der datenschutzrechtlichen Grundsätze

1. Preisgabe und Verwendung von Daten:

Das Recht des einzelnen auf informationelle Selbstbestimmung gewährleistet die Befugnis, selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Der Bürger muss überschauen können, welche Daten über ihn gespeichert sind und weitergegeben werden.

2. Verbot mit Erlaubnisvorbehalt:

Einschränkungen in bezug auf "Preisgabe und Verwendung" sind nur auf verfassungs-mäßiger Grundlage zulässig.

- Dazu bedarf es im Verhältnis zum Staat eines Gesetzes, welches den Umfang der Datenerhebung und Nutzung näher regelt,
- im Rahmen der Privatautonomie vertraglicher oder freiwilliger Angaben (Einwilligung).

Die Datenschutzgesetze gehen von "einem Verbot der Datenerhebung, Datenverarbeitung und Datennutzung" aus, das nur bei Vorliegen eines "Erlaubnistatbestands" (gesetzliche Norm, im Bereich der Privatautonomie auch durch Vertrag oder Einwilligung) zulässig ist (Verbot mit Erlaubnisvorbehalt).

3. Zweckentfremdungs- und Verwertungsverbot:

Ein Schutz gegen Zweckentfremdung durch Weitergabe- und Verwertungsverbote ist erforderlich.

4. Keine Daten auf Vorrat:

Das Sammeln nicht anonymisierter Daten auf Vorrat zu unbestimmten Zwecken ist unzulässig. Es sind nur die Daten zu erheben, die zur Aufgabenerfüllung notwendig sind.

5. Keine Erstellung eines Persönlichkeitsbildes:

Das zulässige Zusammenführen verschiedener Daten ist dann nicht mehr erlaubt, wenn dies zur Erstellung eines Persönlichkeitsbildes führen könnte.

6. Grundsatz der Erforderlichkeit:

Es ist der Grundsatz der Erforderlichkeit zu beachten. Dies bedeutet, dass

- nur diejenigen personenbezogenen Daten des Betroffenen
- bei der Datenerhebung, Datenspeicherung, Datenveränderung und Datennutzung erfragt, aufgeschrieben oder in den Computer eingegeben usw. werden dürfen,
- die zur Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben erforderlich sind.

7. Zweckbindungsgrundsatz:

Außerdem ist auf den Grundsatz der Zweckbindung zu achten. Die Verwendung der personenbezogenen Daten ist grundsätzlich nur für den Zweck zulässig, für den sie erhoben worden sind.

8. Anforderungen der EU-Datenschutzrichtlinie:

Durch die EU-Datenschutzrichtlinie wurden neue wesentliche Strukturmerkmale europaweit vorgegeben. Neben der Einführung einer neuen Terminologie für verschiedene Begriffe

- erhielten bestimmte personenbezogene Daten den Status von „besonderen Arten personenbezogener Daten“ mit der Konsequenz, dass strengere Kriterien bei der Erhebung, Verarbeitung und Nutzung dieser Daten gelten,
- wurden Anforderungen für eine beabsichtigte Übermittlung von Daten ins Ausland formuliert, je nachdem, welcher Standard dort datenschutzrechtlich vorhanden ist,
- wurde die Meldepflicht bei automatisierter Verarbeitung an eine übergeordnete Instanz eingeführt, außer es wird ein betrieblicher Datenschutzbeauftragter bestellt, und

- wurde die Pflicht zur Vorabkontrolle festgeschrieben, wenn die automatisierte Verarbeitung besondere Risiken für die Rechte und Freiheiten der Betroffenen birgt. Diese Vorabkontrolle muss der betriebliche Datenschutzbeauftragte vornehmen.

9. Informationelle Gewaltenteilung:

Auch beim Datenaustausch (Weitergabe) zwischen verschiedenen Organisationseinheiten einer Verwaltungseinheit bzw. eines Trägers gilt der Grundsatz der informationellen Gewaltenteilung. Die Weitergabe von Daten ist nicht ohne weiteres möglich.

Vielmehr bedarf es hierzu nachvollziehbarer dienstlicher Erfordernisse.

Der hier anzuwendende Grundsatz der informationellen Gewaltenteilung besagt, dass personenbezogene Daten zweckgebunden grundsätzlich im Herrschaftsbereich der Stelle verbleiben müssen, die diese erhoben, gespeichert, verändert oder genutzt hat, um Aufgaben gemäß der eigenen Aufgabenstellung zu erfüllen.

- Eine Weitergabe ist nur unter Beachtung der Grundsätze der Erforderlichkeit, der Zweckbindung der Daten, der Aufsichts- und Kontrollbefugnisse, der Datenschutzkontrolle, der Datensicherung und insbesondere unter Berücksichtigung der Aufgabenstellung der abgebenden bzw. empfangenden Stelle möglich (vertikale informationelle Gewaltenteilung).
- Der Schutz des Beratungs- bzw. Privatgeheimnisses erfordert ebenfalls, den Informationsaustausch zwischen Berater und Dienstleitung an bestimmte Regeln und Voraussetzungen zu binden (horizontale informationelle Gewaltenteilung).

10. Schutzmaßnahmen:

Zum Schutz der personenbezogenen Daten sind verfahrensmäßige und organisatorische Schutzmaßnahmen zu treffen.

11. Übermaßverbot:

Bei ihrem Handeln ist die Verwaltung an die Grundsätze der Geeignetheit, der Erforderlichkeit und der Verhältnismäßigkeit gebunden (Übermaßverbot). Das Übermaßverbot erfordert "ein vernünftiges Verhältnis zwischen Anlass, Zweck und Ausmaß der Regelung". Dies wird aus dem zur verfassungsmäßigen Ordnung zählenden Rechtsstaatsprinzip gefolgert.

12. Datenschutzbeauftragter:

Die Einhaltung der Bestimmungen des Datenschutzes ist durch unabhängige Datenschutzbeauftragte sicherzustellen (*Bergmann / Möhrle / Herb*, Handkommentar zum Bundesdatenschutzgesetz, §1 Rd.-Nr. 13).

A5: Sozialdatenschutz

Sozialdaten sind personenbezogene Daten, die von einem Leistungsträger im Sinne des Sozialgesetzbuchs zur Erfüllung seiner Aufgaben nach dem SGB erhoben, verarbeitet oder genutzt werden. Dazu gehören

- Daten von Empfängern sozialer Leistungen,
- Daten von Versicherten der Sozialversicherung und deren Familienangehörigen,
- Daten von Arbeitgebern,
- Daten von Ärzten oder anderen Leistungserbringern.

Sozialdaten sind vorrangig beim Betroffenen zu erheben, unter bestimmten Voraussetzungen ist eine Datenerhebung bei dritten möglich. Die Stelle, die Auskunft möchte, hat darauf hinzuweisen, dass bzw. ob der Betroffene zur Auskunft verpflichtet ist.

Der Betroffene hat eine Mitwirkungspflicht, z.B. bei Geltendmachen von Leistungsansprüchen. Die Erklärung des Betroffenen, dass er mit Einholung von Daten einverstanden ist, muss klar und konkret abgefasst sein (Praxiskommentar KDO, Dr. Siegfried Facht, 1998, S.323).

B1: Organisation der Beratung

1. Rechtliche Einordnung der Beratung:

Der Schutz der Persönlichkeitsrechte zählt zu den Hauptpflichten bzw. Nebenpflichten des Beratungsvertrags, abhängig von der rechtlichen Ausgestaltung. Auch unabhängig von der rechtlichen Einordnung wird das Persönlichkeitsrecht des Ratsuchenden unmittelbar durch das verfassungsrechtlich aus Art. 2 Abs.1 i.V.m. Art. 1 Abs.1 Grundgesetz abgeleitete Recht auf informationelle Selbstbestimmung geschützt.

Da die kirchliche Datenschutzanordnung diese wesentlichen Wertentscheidungen der Verfassung übernimmt, rechtfertigt sich deren entsprechende Anwendung bei der Beratung bzw. der Aktenverwaltung.

Die Durchführung der Beratung überträgt der Rechtsträger regelmäßig seinen Mitarbeitern durch Arbeitsvertrag und Dienstanweisung. Bei fahrlässigem oder schuldhaftem Verhalten des Mitarbeiters (Erfüllungsgehilfen) haftet der Träger, ggf. auch der Mitarbeiter.

Vertragspartner des Ratsuchenden ist der Rechtsträger. Aus dieser Rechtsbeziehung ergeben sich Rechte und Pflichten. Wegen der Gesamtverantwortung stehen dem Rechtsträger und dessen Vertreter das Direktionsrecht zu.

2. Verschwiegenheit am Arbeitsplatz:

Vom ersten Kontakt an besteht die Pflicht des Beraters zur Verschwiegenheit, abgesehen von gesetzlich vorgeschriebenen Offenbarungspflichten. Die Pflicht zur Verschwiegenheit ergibt sich aus dem Arbeitsvertrag, aus den datenschutzrechtlichen Bestimmungen und für den in § 203 StGB angesprochenen Personenkreis aus der Pflicht, das Privatgeheimnis zu wahren. Für die Einhaltung ist der Träger mitverantwortlich.

3. Datenschutz:

Die Pflicht, vom ersten Kontakt an personenbezogene Daten des Ratsuchenden zu schützen, erfordert technische und organisatorische Maßnahmen:

angefangen beim Posteingang, über die Pflicht zur EDV-mäßigen Abschottung von Beratungsdaten bis zur sachgerechten und technischen Ausstattung der Dienststelle.

4. Schutz des Privatgeheimnisses:

Das Strafgesetzbuch ist ein für alle geltendes Gesetz. Geschütztes Rechtsgut des § 203 StGB ist das fremde Geheimnis, das dem Geheimhaltungspflichtigen aufgrund beruflicher oder amtlicher Stellung anvertraut oder sonst bekannt geworden ist.

Träger bzw. Dienstgeber müssen durch entsprechende technische und organisatorische Maßnahmen (Direktionsrecht) sicherstellen, dass das durch § 203 StGB geschützte Privatgeheimnis gewahrt werden kann

5. Zuordnung der Kompetenzen (u. a. Dienstaufsicht):

Die Festlegung des Umfangs übertragener Kompetenzen und die Sicherstellung des Datenschutzes i. w. S. (Aktenverwahrung, Zugangsregelung usw.) obliegen dem Dienstgeber (Rechtsträger).

Hinzu kommt die Pflicht, die Dienst- und Fachaufsicht sicherzustellen. Die Einsichtnahme des Trägers bzw. des Vorgesetzten in Akten des Beraters ist grundsätzlich möglich. Allerdings muss dort die Grenze gezogen werden, wo dies zu einem unbefugten Offenbaren von Privatgeheimnissen führen würde. Im Einzelfall muss geprüft werden, ob der Ratsuchende tatsächlich davon ausging, dass die Unterlagen auch durch einen in der Beratung qualifizierten Dienstvorgesetzten eingesehen werden. Die sich aus der Organisationsstruktur ergebenden Konsequenzen sind daher bereits in einem der ersten Gespräche mit dem Betroffenen zu klären bzw. festzulegen.

6. Kategorisierung des Datenmaterials:

In einer Beratungsstelle werden die unterschiedlichsten Daten erhoben, die, unternimmt man den Versuch einer Kategorisierung, in drei Gruppen eingeteilt werden können:

- **Erste Gruppe:**

Zum einen sind dies Daten, die für die Terminverwaltung nötig sind:

Name, Adresse, Telefonnummer des Klienten und die Zuordnung zu einem Berater einschließlich des Termins. Möglicherweise erfolgt noch die Zuordnung zu einem Beratungszimmer. Diese Daten sind zur Terminverwaltung nötig und damit im Prinzip all denen, die sie zur Terminvereinbarung mit den Klienten benötigen. Bei der Aufnahme dieser Daten muss in geeigneter Form dem Klienten klar gemacht werden, warum und zu welchem Zweck diese Daten erhoben werden. Regelmäßig wird ein kurzer Hinweis genügen. Werden diese Daten unmittelbar oder später in ein EDV-mäßige Terminplanungssystem aufgenommen, muss auch darüber eine Information an den Klienten ergehen. Dies gilt insbesondere dann, wenn der Termin telefonisch vereinbart wird.

- **Zweite Gruppe:**

Die zweite Gruppe von personenbezogenen Daten erfasst die Stammdaten des Klienten (Personaldatenblatt) und hiervon abgeleitet, die Statistikdaten.

Regelmäßig wird der sog. Klientenbogen EDV-mäßig erfasst. Diese Daten werden vom Berater aufgenommen und von der Verwaltung der Beratungsstelle (Sekretariat) EDV-mäßig aufbereitet. Der Klient wird regelmäßig davon ausgehen müssen, dass zur Betreuung und Abwicklung des Betreuungsverhältnisses (des privatrechtlich geschlossenen Beratungsvertrags) die Verwaltungsstelle und damit Beschäftigte der Beratungsstelle mit den Stammdaten befasst werden.

Daten für die Statistik sind zu anonymisieren und dürfen keinen Bezug zum Betroffenen aufweisen.

- **Dritte Gruppe:**

Als dritte Gruppe können die personenbezogenen Daten bezeichnet werden, die im Zusammenhang mit der Beratung entstehen.

Dies sind Informationen im Zusammenhang mit Beratungsinhalten:

Erstgesprächsprotokolle, Stundenprotokolle, Abschlussnotizen und Abschlussprotokolle.

Es bestehen Bedenken, solche Daten im Computer zu speichern. Soweit Sachverhalte diktiert oder geschrieben werden, sind diese Dateien dann zu löschen, sobald der zugrunde liegende Verwaltungsvorgang abgeschlossen ist, wenn also der Ausdruck erfolgt ist und das Schriftstück genehmigt wurde.

Ein unter datenschutzrechtlichen Gesichtspunkten nicht kalkulierbares Risiko entsteht, wenn solche Daten auf einem Computer gespeichert sind, der Internet-Zugang hat.

B2: Verschiedene Einzelfragen

1. Adressen von Teilnehmern (Selbsthilfegruppe):

Die Namen und Adressen (Teilnehmerlisten) von Personen, die an einer Veranstaltung oder Gruppenarbeit (Selbsthilfegruppen) teilnehmen, dürfen nicht vom Träger oder dessen Beauftragten weitergegeben werden.

Wünschen die Teilnehmer die Erfassung bzw. Weitergabe, so kann dies in Form eines Erhebungsbogens geschehen, in den jeder Teilnehmer - freiwillig und in Kenntnis des späteren Verwendungszwecks - personenbezogene Angaben macht. Der Erhebungsbogen sollte darauf hinweisen, zu welchen Zwecken die personenbezogenen Daten gewünscht werden.

2. Akten, Handakten:

In der Akte der Beratungsstelle werden nach dem vom Träger festgelegten Verfahren das Klientenstammblatt, Stundenprotokolle, Erstgesprächsprotokolle und/oder Abschlussprotokolle aufbewahrt.

Diese Akte ist nach einer bestimmten - festgelegten - Aufbewahrungsfrist ordnungsgemäß zu vernichten, wobei für Klientenstammbblätter und sonstige Unterlagen unterschiedliche Aufbewahrungsfristen festgelegt werden können.

In der Regel wird die Aufbewahrungsfrist 5 Jahre betragen, außer es bestünden "sonstige Aufbewahrungsgründe". Die Fristen für die Aufbewahrung sind auch der Kassationsordnung zu entnehmen, die auf Grund der diözesanen Archivanordnung erlassen wurde.

Ob eine Handakte zugelassen wird, hängt von der Trägerentscheidung und der Struktur des Beratungsdienstes ab.

Datenschutzrechtlich ist das Anlegen von Handakten äußerst problematisch. Darf der Berater neben der offiziellen Akte, eine zweite Notizenreihe führen, die niemand einsehen kann, entstehen verschiedene Probleme, u. a. die Frage der sicheren Verwahrung.

Auch hierfür trägt der Träger die Mitverantwortung. Die Handakten stehen im Eigentum der Dienststelle und verbleiben auch dort bei Ausscheiden des Mitarbeiters. Je nach Art der Handakten kann bei Ausscheiden des Mitarbeiters eine Vernichtung der Handakten angezeigt sein.

3. Aufbewahrungsfristen:

Die Aufbewahrungsfristen für Arbeitsunterlagen richten sich nach den gesetzlichen Bestimmungen, den vertraglichen Abmachungen oder nach den Erfordernissen des Verwaltungshandelns. Dabei sind verschiedene Gesichtspunkte zu berücksichtigen:

- gesetzliche Aufbewahrungsfristen,
- Dokumentationspflichten,
- Rechnungslegungspflicht,
- Datenschutz.

Die Frage, wie lange Akten und Aktennotizen nach Abschluss eines Betreuungsverhältnisses aufgehoben werden müssen, lässt sich nicht einheitlich beantworten. Bei der Suchtkrankenhilfe ist es Praxis, die Aktennotizen nach Beendigung eines Betreuungsverhältnisses 10 Jahre lang aufzuheben. Gleiches wird auch in den Einrichtungen der Psychiatrie praktiziert. Im Beratungswesen ist eine fünfjährige Aufbewahrung nach Abschluss der Beratung noch akzeptabel.

4. Auskünfte über Klienten:

Es ist nicht zulässig, ohne Rechtsgrund oder Einwilligung des Betroffenen Auskünfte über Ratsuchende zu geben.

Telefonische Auskunft auf Anfragen persönlich nicht bekannter Anfragender sollte überhaupt nicht gegeben werden; weder, wenn die Person bekannt, noch, wenn diese unbekannt ist oder sich gerade hier aufhält.

Lässt sich im Einzelfall nicht vermeiden, wegen einer Notsituation telefonisch Sachverhalte über Ratsuchende mitzuteilen, muss ggf. durch Rückruf bei der nachfragenden Stelle die Identität des Anrufenden geklärt werden. Es ist schon vorgekommen, dass sich Berater die Telefonnummer geben ließen, um einen Rückruf vorzunehmen, ohne zu klären, ob die genannte Telefonnummer wirklich zur angegebenen Stelle gehört. Die ISDN-Technik könnte dazu verführen, sich vom Anrufenden die Telefonnummer mitteilen zu lassen und diese mit der im Display angezeigten Nummer zu vergleichen. Auf diese Weise wird nur die Identität der Telefonnummern geklärt, nicht aber, ob z. B. das Vormundschaftsgericht wirklich unter der angegebenen Telefonnummer zu erreichen ist.

5. Datenerhebung:

Der Klient ist über den Umstand, dass seine personenbezogenen Daten erhoben werden, zu informieren.

Dies ist insbesondere dann zu beachten, wenn die Datenaufnahme telefonisch erfolgt (z. B. um ein erstes Beratungsgespräch zu vereinbaren). Der Klient ist auch über den "Erhebungszweck" zu informieren. Werden die personenbezogenen Daten in eine EDV-Anlage übernommen, ist der Klient auch hierüber zu informieren.

6. Einwilligung:

Wird die Einwilligung des Klienten benötigt, um z. B. die Weitergabe personenbezogener Daten im Rahmen der Teamarbeit oder der Supervision zu ermöglichen, ist dem Betroffenen ein echtes Wahlrecht einzuräumen. Dies kann bei der Einholung der schriftlichen Einwilligungserklärung (vgl. § 3 Abs. 2 KDO) in der Form geschehen, dass der Betroffene ankreuzt, ob er mit einer Datenweitergabe einverstanden ist.

7. Erlangung der Kenntnis von Strafdelikten:

In Gewissenskonflikt können Berater dann kommen, wenn ihnen z.B. offenbart wird, dass der Partner einer Ratsuchenden die eigenen Kinder sexuell missbraucht.

Soll bzw. kann Strafanzeige erstattet werden oder nicht?

In diesen emotional schwierigen Fällen muss das anvertraute Privatgeheimnis gewahrt werden. Bei einem unbefugten Offenbaren z. B. gegenüber staatlichen Stellen kann der Tatbestand des § 203 StGB verwirklicht werden. Eine gesetzliche Verpflichtung zur Weitergabe der Informationen besteht z. B. in den Fällen des § 138 StGB (Nichtanzeige geplanter Straftaten). Daraus wird sich allerdings nur in seltenen Fällen eine Offenbarungspflicht ableiten lassen, weil sich die Informationen typischerweise nicht auf eine in dieser Strafbestimmung genannte schwere Straftat beziehen.

Besteht eine gesetzliche Verpflichtung, Sachverhalte zu offenbaren (d. h. mitzuteilen oder anzuzeigen), ist typischerweise ebenfalls der Umfang der Daten, auf die sich die Mitteilungspflicht bezieht, angegeben.

Die Frage, ob ein unbefugtes Offenbaren eines Privatgeheimnisses ausnahmsweise von unserer Rechtsordnung gerechtfertigt ist, bedarf einer sorgfältigen Prüfung.

"Wer in einer gegenwärtigen, nicht anders abwendbaren Gefahr für Leben, Leib, Freiheit, Ehre, Eigentum oder ein anderes Rechtsgut eine Tat begeht, um die Gefahr von sich oder einem anderen abzuwenden, handelt nicht rechtswidrig, wenn bei Abwägung der widerstreitenden Interessen, namentlich der betroffenen Rechtsgüter und des Grades der ihnen drohenden Gefahren, das geschützte Interesse das beeinträchtigte wesentlich überwiegt. Dies gilt jedoch nur, soweit die Tat ein angemessenes Mittel ist, die Gefahr abzuwenden"

(§ 34 StGB, Rechtfertigender Notstand). Im o. a. Fall muss der Berater versuchen, durch weniger einschneidende Maßnahme, wie z. B. Rücksprache mit Fachdiensten, eine für die Beteiligten erträgliche Lösung zu finden. Hierzu zählt insbesondere die Beratung und Unterstützung der Ehefrau, durch konkrete Entscheidungen oder Maßnahmen, ggf. auch durch Hilfen zur vollziehenden räumlichen Trennung, Abhilfe zu schaffen.

Hinzuweisen ist auch auf strafrechtliche Konsequenzen für die Mutter selbst. Sie kann u. U. wegen Beihilfe zum sexuellen Missbrauch von Schutzbefohlenen belangt werden, weil sie unterlassen hat, die Tat zu verhindern (Unterlassungsdelikt). Die Mutter ist i. a. R. für die Tochter verantwortlich. Da die Belange der Tochter die der Mutter deutlich überwiegen, führt dies zu einer strafrechtlich relevanten "Garantenstellung" der Mutter gegenüber der Tochter, die für sie die Verpflichtung auslöst, die Tat zu verhindern (174 Abs. 1 Nr. 2, 27, 13 StGB).

8. Erlangung der Kenntnis von einer Straftat:

Der Berater kommt ebenfalls in eine schwierige Situation, wenn er darüber informiert wird, ein anderer sitze unschuldig im Gefängnis.

Es gelten die im Zusammenhang mit dem Sexualdelikt gemachten Aussagen.

Da kein Fall des § 138 StGB (Nichtanzeige geplanter Straftaten) vorliegt, besteht keine gesetzliche Verpflichtung, den Vorgang staatlichen Stellen zur Kenntnis zu bringen. Ein unbefugtes Offenbaren eines Privatgeheimnisses führt für den in § 203 StGB genannten Personenkreis zur Tatbestandsverwirklichung. Das unbefugte Offenbaren gegenüber staatlichen Stellen kann aber gerechtfertigt sein, wenn die Voraussetzungen des § 34 StGB vorliegen. Eine Wiederaufnahme zugunsten des Verurteilten ist nach § 359 StPO (Strafprozessordnung) u. a. zulässig, wenn neue Tatsachen oder Beweismittel beigebracht werden, die allein oder in Verbindung mit den früher erhobenen Beweisen die Freisprechung des Angeklagten oder in Anwendung eines milderen Strafgesetzes eine geringere Bestrafung oder eine wesentlich andere Entscheidung über eine Maßregel der Besserung und Sicherung zu begründen geeignet sind(359 Nr. 5 StPO).

9. Erstgespräch:

Im Erstgespräch ist der Ratsuchende auf die Erhebung, Verarbeitung und Löschung seiner Daten hinzuweisen, ebenso darauf, welche seiner Angaben auf freiwilliger Basis erhoben werden. Darüber hinaus ist der Ratsuchende darüber zu informieren, wer Zugang zu seinen Daten hat und wie sie verwendet werden. Diese Frage spielt im Zusammenhang mit Fallbesprechungen und Supervision eine Rolle.

10. Merkblatt der Beratungsstelle:

Es hat sich bewährt, die Klienten mit einem Merkblattes über die Arbeitsweise der Beratungsstelle zu informieren. Bei dieser Gelegenheit sollten auch darüber informiert werden, wer personenbezogene Daten aufnimmt, verarbeitet und speichert. Ein Hinweis auf die Datenschutzbestimmungen sollte nicht fehlen.

Folgende Formulierung kann auf dem Merkblatt aufgenommen werden:

- Angaben zu ihrer Person gegenüber der Beratungsstelle sind freiwillig.
- Der Umgang mit ihren Daten (auch EDV-mäßig) erfolgt entsprechend der kirchlichen Datenschutzanordnung.
- Ihre personenbezogenen Daten und Informationen über ihre Beratungsgespräche dürfen nur mit ihrer ausdrücklichen Einwilligung an Dritte außerhalb der Beratungsstelle weitergegeben werden.
- Kollegiale und fachliche Unterstützung und Supervision findet im Team der Beratungsstelle statt.
- Die Beratungsstelle erstellt - zum Nachweis gegenüber Träger, Zuschussgeber und Öffentlichkeit - ausschließlich eine anonymisierte Sammelstatistik (Anzahl der Ratsuchenden usw.)

11. Mitarbeiter der Beratungsstelle:

Ebenfalls bewährt hat sich, in der Dienststelle an geeigneter Stelle einen Hinweis auf die Mitarbeiter der Dienststelle zu geben. Aus dieser Liste soll hervorgehen, wer in der Beratungsstelle in welcher Funktion tätig ist.

12. Telefonverbindungserfassung durch die Telekom:

Durch die Digitalisierung des Telefonnetzes wird es möglich, Telefonverbindungsdaten umfassend zu speichern: die Rufnummer oder die Kennung des anrufenden und des angerufenen Anschlusses, den Beginn und das Ende der jeweiligen Verbindung, das Datum und die Uhrzeit. Der Inhaber des Telefonanschlusses kann sich über alle von seinem Anschluss geführten Telefongespräche informieren und erfährt die Telefonnummer des Anrufenden.

Diese technische Neuerung kann schwerwiegende Folgen für den gesamten Bereich der seelsorgerlichen und beratenden Arbeit der Kirchen haben (Pfarrämter, Beratungsstellen, Telefonseelsorge). Zwischenzeitlich wurden verschiedene Wege beschritten, um auch hier das Beratungsgeheimnis zu wahren.

13. Teamarbeit:

Der Ratsuchende ist davon in Kenntnis zu setzen, wer Zugang zu seinen Daten hat. Dies wird insb. bei der Teamarbeit und bei einer Supervision relevant. Allerdings ist auch im Team bzw. bei der Supervision zu empfehlen, keine Daten zu verwenden, die die Identifizierung eines Klienten ermöglichen. Die Besprechung von Problemfällen in anonymer Form erfüllt erfahrungsgemäß die Bedingungen einer Teamarbeit oder Supervision.

14. Telefonzentrale:

In modernen Telefonzentralen wird verstärkt die Elektronik eingesetzt, um verschiedene Daten zu speichern (gewählte Zielrufnummer, Datum, Uhrzeit und Dauer des Gesprächs, eine Kennzeichnung als Dienst- oder Privatgespräch, anfallende Gebühreneinheiten und Gebühr). Diese Erfassung tangiert das Persönlichkeitsrecht des einzelnen, insbesondere bei telefonischen Beratungsgesprächen mit angerufenen Ratsuchenden. Datenschutzrechtlich korrekte Lösungen müssen vor Ort umgesetzt werden

15. Transparenz der Datenerhebung:

Dem Ratsuchenden ist bereits am Telefon mitzuteilen, wenn seine Daten im Zusammenhang mit einer Terminvereinbarung aufgenommen werden ("Nun brauche ich noch einige Daten von ihnen...", "ich nehme ihre Daten auf..."). Werden Die Daten bereits bei der Anmeldung EDV-mäßig aufgenommen, ist auch dies dem Ratsuchenden mitzuteilen.

16. Terminkalender:

Der Terminkalender der Beratungsstelle ist den betroffenen Mitarbeitern allgemein zugänglich. Daher ist dieser - insbesondere bei Dienstschluss - sicher aufzubewahren.

17. Vertrauliches Wort in einer Arbeitsgruppe:

Soll in einer Selbsthilfegruppe über persönliche Probleme der Teilnehmer gesprochen werden, ist jeder vor Sitzungsbeginn auf die Vertraulichkeit hinzuweisen, ggf. unter Hinweis auf rechtliche Konsequenzen (Beleidigung, üble Nachrede, Schadensersatz, Unterlassungs-klage). Personen, die sich "an diese Spielregeln" nicht halten wollen, müssen ggf. von weiteren Sitzungen ausgeschlossen werden.

Allerdings muss den Teilnehmern auch klar sein, dass die maßgeblichen Ursachen, die zur Kenntnis persönlicher Sachverhalte führen, durch die Teilnehmer selbst gesetzt werden.

B3: Abgrenzung Berufsgeheimnis, besonderes Amtsgeheimnis, Verschwiegenheit, Geheimhaltungsbestimmungen

1. Abgrenzung:

Das Berufsgeheimnis und das besondere Amtsgeheimnis sind von anderen Verschwiegenheits- und Geheimhaltungsbestimmungen abzugrenzen.

Arbeitsrechtsrechtlich sind alle katholischen Mitarbeiter zur Verschwiegenheit verpflichtet (§ 9 BAT; § 5 AVR-Caritas; § 3 AVR). Berater sind auf die Wahrung des Beratungsgeheimnisses verpflichtet.

Strafrechtliche Konsequenzen werden in den § 203 ff StGB einem näher beschriebenen Personenkreis angedroht, wenn anvertraute oder sonst bekanntgewordene Privatgeheimnisse unbefugt offenbart werden. Die bei der Datenverarbeitung tätigen Personen haben das Datengeheimnis zu wahren

2. Berufs- und besondere Amtspflichten entstehen, wenn Personen auf Grund ihrer beruflichen Tätigkeit Informationen erhalten und zur Geheimhaltung der Daten verpflichtet sind.

Diese Pflicht zur gesteigerten Geheimhaltung ergibt sich aus staatlichen und kirchlichen Gesetzen. Allerdings fallen allgemeine dienst- und arbeitsrechtliche Verschwiegenheitspflichten nicht unter das Berufs- bzw. besondere Amtsgeheimnis. Auch das Datengeheimnis stellt kein besonderes Berufs- oder besonderes Amtsgeheimnis dar (*Bergmann/ Möhrle/Herb*, Handkommentar zum Bundesdatenschutzgesetz § 39 Rd.-Nr. 14).

- KDO und Berufsgeheimnis:

Die kirchliche Datenschutzordnung enthält keine spezielle Regelung, die die datenschutzrechtlichen Anforderungen zur Umsetzung des Berufs- bzw. Amtsgeheimnisses näher bestimmen. Diese Nichtübernahme von Regelungsinhalten zum Berufs- bzw. besonderen Amtsgeheimnis, die insb. in § 39 BDSG formuliert sind (Zweckbindung bei personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen), darf nicht zu der Annahme verleiten, das Berufs- oder besondere Amtsgeheimnis sei im Bereich der Katholischen Kirche weniger geschützt.

3. Zwei Fallgestaltungen sind gesondert zu untersuchen:

- Unter welchen Voraussetzungen dürfen personenbezogene Daten, die unter das Berufsgeheimnis bzw. besondere Amtsgeheimnis fallen, von den Personen weitergegeben oder übermittelt werden, die diese Daten erhoben haben?
- Wie kann sichergestellt werden, dass Sachverhalte, die unter das Berufsgeheimnis oder besondere Amtsgeheimnis fallen und übermittelt wurden, von der empfangenden Stelle nicht zweckwidrig weiterverwendet werden?

4. KDO 1977:

Bereits in der kirchlichen Datenschutzordnung aus dem Jahre 1977 wurden strenge Anforderungen formuliert. §10 Abs. 1 der kirchlichen Datenschutzordnung des Jahres 1977 lautete:

§ 10, Datenübermittlung innerhalb des kirchlichen Bereichs

(1 Die Übermittlung personenbezogener Daten an die in 1 Abs. 2 genannten Stellen ist zulässig, wenn sie zur Erfüllung des kirchlichen Auftrags erforderlich ist, der der übermittelnden Stelle oder dem Empfänger obliegt. Unterliegen die personenbezogenen Daten einem Berufs- oder besonderen Amtsgeheimnis und sind sie der zu übermittelnden Stelle von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht übermittelt worden, ist für die Zulässigkeit der Übermittlung ferner erforderlich, dass der Empfänger die Daten zur Erfüllung des gleichen Zweckes benötigt, zu dem sie die übermittelnde Stelle erhalten hat.

5. Bundesdatenschutzgesetz:

§ 39 BDSG führt für personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, eine besondere (strenge) Zweckbindung ein. Diese Bestimmung, die die zusätzlichen Anforderungen an die Zweckbindung personenbezogener Daten formuliert, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, lautet:

§ 39 BDSG, Zweckbindung bei personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen.

(1) Personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen und die von der zur Verschwiegenheit verpflichteten Stelle in Ausübung ihrer Berufs- oder Amtspflichten zur Verfügung gestellt worden sind, dürfen von der speichernden Stelle nur für die Zwecke verarbeitet oder genutzt werden, für den sie sie erhalten hat. In die Übermittlung an eine nicht-öffentliche Stelle muss die zur Verschwiegenheit verpflichtete Stelle einwilligen.

(2) Für einen anderen Zweck dürfen die Daten nur verarbeitet oder genutzt werden, wenn die Änderung des Zwecks durch besonderes Gesetz zugelassen ist.

6. **Entsprechende Anwendung der Regelungsinhalte:** Die datenschutzrechtlich korrekte Behandlung von solchen Sachverhalten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, erfordert strenge Anforderungen auch im kirchlichen Bereich. Dies führt bei der datenschutzrechtlichen Behandlung dieser Sachverhalte zur entsprechenden Anwendung von § 39 BDSG bzw. § 10 Abs. 1 KDO in der Fassung von 1977.

B4: Der Arbeitsplatz

1. Datensicherheit am Arbeitsplatz:

Jeder Arbeitsplatz ist in technischer und organisatorischer Hinsicht datenschutzrechtlich zu prüfen.

Der Rechtsträger hat in bezug auf den Arbeitsplatz u. a. folgende Fragen zu klären:

- Stehen personenbezogene Daten ausschließlich dem berechtigten bzw. befugten Mitarbeiter zur Verfügung (Transport, Zugang, Aufbewahrung usw.)?
- Kann der Mitarbeiter mit personenbezogenen Daten arbeiten, ohne dass Mitarbeiter oder Dritte (Publikumsverkehr) diese bewusst oder zufällig einsehen können?
- Wie werden die personenbezogenen Daten bei Abwesenheit des Mitarbeiters (z. B. Mittagszeit) geschützt?
- Besteht die Möglichkeit, vertrauliche Gespräche mit dem Klienten, Ratsuchenden usw. zu führen?
- Wie werden die personenbezogenen Daten nach Dienstschluss verwahrt?

2. Organisationsbefugnis und Direktionsrecht:

Die datenschutzrechtliche Sicherung ist nicht nur ein technisches, sondern vor allem ein organisatorisches Problem. Dieser Aufgabe muss sich der Arbeitgeber in Wahrnehmung seiner Organisationsbefugnis stellen und sie bewältigen.

B5: Einzelfragen

1. Abwesenheit im Büro:

Ist das Büro vorübergehend nicht besetzt, z. B. zur Mittagszeit, muss sichergestellt werden, dass Unbefugte diese Zeit nicht nutzen oder nutzen können, sich in den Besitz von Informationen zu bringen.

In noch größerem Maße stellt sich die Frage des unbefugten Zugangs bei Dienstschluss. Insbesondere bei Gleitzeitregelungen kann es vorkommen, dass Besucher unverschlossene Schreibtische und Schränke mit personenbezogenen Daten vorfinden.

Nicht zu unterschätzen ist die datenschutzrechtliche Gefährdungslage, die von Mitarbeitern des Putz-, Aufräum- bzw. Schlüsseldienstes ausgehen kann.

2. Briefe und Gutachten:

Arbeiten, die im Zusammenhang mit dem Posteingang anfallen (Befugnisse in Bezug auf das Öffnen und das Lesen der Post, Verteilen, Zuordnen, Transportieren usw.) müssen vom Rechtsträger oder dessen Beauftragten in datenschutzrechtlich korrekter Weise festgelegt werden.

3. Computer:

Die Entscheidung darüber, ob am Arbeitsplatz ein Computer eingesetzt werden soll, obliegt dem Rechtsträger. Die Diözesen haben Beschaffungsrichtlinien erlassen, um durch Schaffung von einheitlichen Rahmenbedingungen den kostengünstigen Einsatz bewährter Geräte und Software zu ermöglichen. Außerdem erleichtert dies die Wartung. Klar muss sein, dass durch die Anschaffung und den Einsatz von Computern ganz neue datenschutzrechtliche Fragestellungen auftreten.

4. Internetnutzung:

Berichte, Terminkalenderdaten, Abrechnungsvorgänge, Personalakten und andere sensible Dateninhalte haben auf Computern, die einen Internetzugang haben, grundsätzlich nichts zu suchen.

Es ist auch bei eingerichteter Firewall oder installiertem Virenschutzprogramm dauerhaft nicht zu gewährleisten, dass über diesen Internetzugang in das bestehende interne Daten-netz nicht eingedrungen wird.

5. Personalinformationssysteme:

Personalinformationssysteme stützen sich auf bestehende oder erst in der Entwicklung befindliche Teildatenbanksysteme, die in der Dienststelle verteilt sind und unterschiedlichen Zwecken dienen. Sie verknüpfen einzelne Informationsströme und verbinden unterschiedliche Funktionsbereiche. Die einzelnen Daten sind in Teildatenbanksystemen abgespeichert und werden durch das Personalinformationssystem technisch und organisatorisch verknüpft. Einer der Ziele des Systems ist es, die Arbeit in der Personal-abteilung zu rationalisieren. Durch die Verknüpfungsmöglichkeiten können nicht unerhebliche datenschutzrechtliche Probleme entstehen (gläserner Mensch).

Daher ist ggf. in Abstimmung mit dem Datenschutzbeauftragten zu klären, welche Maßnahmen zulässig sind. Die Zustimmung der Mitarbeitervertretung ist erforderlich bei Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Mitarbeiter zu überwachen (vgl. 36 MAVO).

6. Publikumsverkehr:

Bei Büros mit Publikumsverkehr ist sicherzustellen, dass Eintretende nicht fremde Akten, Aktennotizen, Listen, Bildschirmausschnitte usw. mitlesen können. Auch alle Arten von Terminplanungsunterlagen (Steckkasten, Terminkalender, Stechkarten usw.) sind nicht für die Augen Fremder bestimmt.

7. Überwachung:

Die Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Mitarbeiter zu überwachen ist eine zustimmungspflichtige Angelegenheit der Mitarbeitervertretung (vgl. § 36 MAVO).

8. **Unterlagen, Terminkalender mit Namen:**

Der Dienstgeber muss Regelungen in bezug auf die Ablage, Aufbewahrung, Sicherung und Aussonderung (Vernichtung) von Akten treffen.

Dienstliche Unterlagen im privaten Gebrauch sind nach Beendigung der Gebrauchsfähigkeit - im Einzelfall auch früher - an den Dienstgeber zurückzugeben, der über ihre Vernichtung entscheidet. So können dienstliche Terminkalender je nach Einschätzung des Dienstgebers vernichtet oder eine gewisse Zeit aufbewahrt werden.

9. **Zentrales Schreibbüro:**

Durch die Einrichtung eines zentralen Schreibdienstes außerhalb der originären Beratungsstelle ergeben sich neue datenschutzrechtliche Fragen:

- Dem Dienstgeber steht in bezug auf die Abwicklung der anfallenden Schreibarbeit ein umfassendes Organisationsrecht zu, welches sich aus seiner Direktionsbefugnis ergibt (Anweisungsrecht gegenüber den Mitarbeitern, Fürsorgepflicht, Pflicht zur sparsamen Verwendung von Haushaltsmitteln, Pflicht, Arbeitsabläufe rationell zu organisieren). Insoweit kann der Dienstgeber sich für die Einrichtung eines zentralen Schreibbüros aussprechen.
- Das Direktionsrecht des Dienstgebers wird beschränkt durch arbeitsrechtlich, arbeitsschutzrechtliche und insb. strafrechtliche Bestimmungen. Das Direktionsrecht wird ebenfalls beschränkt durch den datenschutzrechtlichen Grundsatz der informatio-nellen Gewaltenteilung. Dieser datenschutzrechtliche Grundsatz besagt, dass personen-bezogene Daten grundsätzlich zweckgebunden im Herrschaftsbereich der Stelle verblei-ben müssen. Dies gilt umso mehr, wenn es sich bei den erhobenen Daten um besonders sensible Angaben über persönliche oder familiäre Verhältnisse handelt.
- Im Laufe der Zeit hat sich in bezug auf die Frage, ob solche sensiblen Daten außerhalb der erhebenden Stelle verarbeitet und bearbeitet werden dürfen, gewisse Standards herausgebildet. § 90 a BBG (Bundesbeamtengesetz) schreibt vor, dass Beihilfeakten "stets" als Teilakte zu führen sind. "*Sie sollen in einer von der übrigen Personal-verwaltung getrennten Organisationseinheit bearbeitet werden, Zugang sollen nur Beschäftigte dieser Organisationseinheit haben*". Im Krankenhausbereich ist es unter-sagt, die Behandlungsunterlagen durch Fremdfirmen bearbeitet zu lassen, außer dieses würde ihrerseits durch ein Krankenhaus erfolgen. § 203 Abs. 3 Satz 2 StGB dehnt die Pflicht zur Wahrung des Privatgeheimnisses auf die berufsmäßig tätigen Gehilfen aus.
- Daraus ist zunächst zu folgern, dass eine Entscheidung des Dienstgebers, ein zentrales Schreibbüro zu schaffen, nicht automatisch mit datenschutzrechtlichen Standards in Einklang gebracht werden kann, sondern eine solche Entscheidung vielmehr regelmäßig gegen den datenschutzrechtlichen Grundsatz der "Zweckbindung von Daten", den "Grundsatz der Erforderlichkeit" und den "Grundsatz der Verhältnismäßigkeit" sowie und gegen Geheimhaltungsvorschriften verstößt.
- Die Erledigung dieser Arbeiten in einem zentralen Schreibbüro bedarf daher weiterer organisatorischer Maßnahmen:
 - Der Hin- und Hertransport von Unterlagen zur zentralen Schreibstelle muss besonders gesichert sind.
 - Die Zuständigkeit zur Erledigung dieser Arbeiten muss auf wenige Personen beschränkt bleiben.
 - Im zentralen Schreibbüro sind räumliche Trennungen durchzuführen, um eine unbefugte Kenntnisnahme zu verhindern.
 - Die elektronisch bearbeiteten Vorgänge müssen besonders gesichert werden und vor dem Zugriff anderer Personen besonders geschützt werden.

- Bei einer datenschutzrechtlich sachgerechten Umsetzung wird sich bald für den Dienstgeber die Frage stellen, ob es nicht sachgerechter bzw. angebrachter ist, wenn diese Arbeiten unmittelbar "vor Ort", also in jedem Fachdienst unmittelbar, erledigt werden (Grundsatz der Verhältnismäßigkeit). Ein Faltblatt, das den Klienten über die Datenerhebung, -verarbeitung und -nutzung informiert, muss auch auf das zentrale Schreibbüro hinweisen.

10. **Telefax**

Sensible personenbezogene Daten sollten nicht per Telefax versendet werden. Das Empfängergerät wird oft von auch von Personen genutzt, die mit dem versandten Vorgang nichts zu tun haben. Das versandte Dokument hat den Status einer Postkarte. Ein Geheimnisschutz der übermittelten Schriftstücke ist daher nicht gewährleistet. Sachverhalte, die auf dem Postweg nicht als „offene Karte“ übermittelt werden dürfen, dürfen nur in Ausnahmefällen und bei zusätzlichen Sicherungsmaßnahmen (z.B. Anruf mit der Information, dass das Fax abgeschickt wird, so dass der Empfänger es direkt annehmen kann) per Telefax übermittelt werden.

Grundsätzlich berechtigt eine Übermittlung von Sachverhalten nicht zu der Schlussfolgerung, dass auch die Antwort auf demselben Weg erfolgen dürfe.

Einige Diözesen haben Bestimmungen zur Nutzung von Telefaxgeräten erlassen, z.B.:

- Vor der Nutzung des Faxgerätes als Übermittlungsmittel prüfen, ob diese Methode wirklich adäquat ist.
- Keine Telefaxgeräte in Räumlichkeiten mit Publikumsverkehr. Der Standort des Geräts muss so gewählt werden, dass nur Befugte von den Faxvorgängen Kenntnis nehmen können.
- Fachabteilungen mit eigenen Fernkopierern müssen die eigene Telefax-Nummer angeben (Praxiskommentar KDO, Dr. Siegfried Facht, 1998, S. 338).

11. **Weitergabe/Übermittlung von Daten**

Die Weitergabe von personenbezogenen Daten zwischen verschiedenen Organisationseinheiten eines Trägers ist nicht ohne weiteres möglich. Grundsätzlich muss bei jeder Weitergabe von personenbezogenen Daten die Zulässigkeit geprüft werden. Zu prüfen ist auch, ob die Daten nicht, wie in der KDO formuliert, durch die entsprechenden Stellen beim Betroffenen selbst erhoben werden können.

12. Die Weitergabe bzw. Übermittlung von Daten an katholische und öffentliche Stellen

Datenschutz wird zwischen Abteilungen, Referaten, Diensten oder Einrichtungen statt (vertikale Gewaltenteilung) praktiziert, ebenso zwischen Rechtsträger und Abteilung bzw. Mitarbeiter (horizontale Gewaltenteilung).

Nur wenn die Datenübermittlung zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Empfängers liegenden Aufgaben erforderlich ist und die Voraussetzungen für die Nutzung nach § 10 KDO (Datenspeicherung, -veränderung und -nutzung) vorliegen, darf eine Übermittlung von Daten erfolgen.

13. Die Weitergabe/Übermittlung von Daten an nicht-kirchliche und nicht-öffentliche Stellen

Nach § 12 KDO ist eine Weitergabe/Übermittlung von Daten erlaubt, wenn

- sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist.
- Voraussetzungen vorliegen, die eine Nutzung nach §10 zulassen würden oder der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt.
- der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

Im zweiten Fall besteht für die übermittelnde Stelle die Pflicht, den Betroffenen über die Datenweitergabe zu informieren (Praxiskommentar KDO, Dr. Siegfried Fächet, 1998, S. 35).

C1: Zum Internet

- **Grundausrüstung** wird ein Computer, ein Modem und/oder eine Netzkarte und ein Telefonanschluß benötigt. Der Zugang zum "Netz der Netze" erfolgt über einen "Provider", zumeist ein kommerzielles Unternehmen, das den Internetzugang gegen eine monatliche Gebühr zur Verfügung stellt. Zu den monatlichen Gebühren des Providers kommen die eigenen Telefonkosten, wobei manche in Anspruch genommenen Dienste extra berechnet werden. Nicht zu unterschlagen sind – neben den Schulungskosten der Mitarbeiter – die Kosten für die Software-Produkte, einschließlich Kosten für den (ständig zu aktualisierenden) Sicherheitsstandard.
- **Gefährdungspotential:**
Beim Anschluss von Computern, insbesondere wenn diese innerhalb der Dienststelle vernetzt sind, entstehen Gefahren nicht nur in bezug auf die ordnungsgemäße Verwaltung personenbezogener Daten, sondern auch in bezug auf Ausspähung von Betriebsgeheimnissen oder der Beeinträchtigung der Hardware.
- **Sicherheitskonzept:**
Zur Vermeidung von Gefahren ist von der Stelle, die den Anschluss herstellen will, zunächst der individuelle Kommunikationsbedarf zu ermitteln und ein Sicherheitskonzept zu erarbeiten.
- **Firewall:**
Entschieden werden muss, ob jeder einzelne interne Computer geschützt oder ob ein zentraler Übergang (Anschluss) zwischen Netz und Internet geschaffen werden soll. Die am Markt erhältlichen Firewall-Produkte sind unterschiedlich leistungsfähig. Als Mindestanforderung werden im 17. Tätigkeitsbericht des Landesdatenschutzbeauftragten von Baden-Württemberg (1996, Landtagsdrucksache 12/750, S. 10 ff) genannt:
 - Prüfung der Zulässigkeit einzelner Datenverbindungen (z. B. Prüfung der Internet-Adresse der beteiligten Computer usw.).
 - Schutz von internen Computer-Adressen vor Ausforschung,
 - Protokollierung der Nutzung zugelassener Dienste einschließlich abgewiesener Verbindungsversuche, zurückgewiesener Datenpakete, erfolgreicher oder abgewiesener Versuche des Systemverwalterzugriffs auf Firewall-Komponenten, der Versuche, vom Internet aus Datenpakete durch die Firewall zu schleusen, die als Absenderangabe die Internet-Adresse eines internen Computers tragen (sog. IP-Spoofing-Attacke).
 - Benachrichtigung bei sicherheitsrelevanten Ereignissen.
- **Gefährdungspotential:**
Bei aller Vorsicht wird durch den Anschluss an das Internet/Intranet das Datenschutzrisiko für die im internen Netz befindlichen Daten erhöht. Die Gefahren für die eigenen Daten werden vielfach unterschätzt, wenn über Internet ein Programm genutzt wird, um z. B. eigene Berechnungen anzustellen. Da fast niemand garantieren kann, ob die auf den internen Computer geladenen (Rechen- oder Anwendungs-)Programme nicht weitere Anweisungen enthalten, die interne Daten manipulieren können, ist allergrößte Vorsicht geboten.

- **Risiken:**

Auf folgende datenschutzrechtlich relevanten Risiken weist der 17. Tätigkeitsbericht des Landesdatenschutzbeauftragten von Baden-Württemberg, (1996, Landtagsdrucksache 12/750) beim Anschluss dienstlicher Computer an das Internet hin (S. 12):

- Fehlen eines bzw. Vorliegen eines unvollständigen Sicherheitskonzept (insb. fehlende Dokumentation),
- Schutzmöglichkeiten der Paketfilter werden nicht oder nur unzureichend genutzt (insb. zu großzügig gewählte Filterregeln),
- Zulassung eines umfassenden Zugriff von Internet-Teilnehmer auf interne Daten des Dienstcomputers,
- Mängel bei der Administration der Firewall-Komponenten (insb. fehlende Terminalbeschränkung für Systemverwalter),
- Sicherstellung der ordnungsgemäßen Arbeitsweise des Paketfilters durch den Systemverwalter von einer definierten Stelle aus,
- Sonstiger Datenaustausch über frei anwählbare offene Telefonleitungen bei Umgehung der Firewall.

- **Homepage:**

Bei der Gestaltung der sog. Homepage sind in bezug auf personenbezogenen Daten die datenschutzrechtlichen Grundaussagen zu beachten, die - teilweise in unterschiedlichen Datenschutzgesetzen normiert sind.

Bei der Verwendung von personenbezogenen Daten, z. B. wer im Dienstbetrieb Ansprechpartner für bestimmte Fragen ist, kann nicht zwischen "personenbezogenen dienstlichen Daten" und "personenbezogenen Daten" unterschieden werden, da eine "Aufspaltung" der personenbezogenen Daten in "persönlichen" und einen "dienstlichen Bezug" nicht möglich ist. Die Berechtigung, die Namen der "zumindest wichtigen Personen" einer Diözese auf Webseiten anzugeben, wird sich als eine Nebenpflicht zum Arbeitsvertrag ergeben. Etwas anderes ergibt sich, wenn über Suchfunktion die Namen von Mitarbeitern auffindbar gemacht werden können.

Die Mitarbeitervertretung ist bezüglich des Internetauftritts einzubinden.

Eine Veröffentlichung von Mitarbeiter-Bildern darf allerdings nur mit ausdrücklicher Zustimmung der Betroffenen erfolgen. Übereinstimmung bestand auch darüber, dass das Recht auf Namensnennung nur bei berechtigter dienstlicher Notwendigkeit besteht.

- **Separater Computer:**

Von den kirchlichen Datenschutzbeauftragten wird empfohlen, den Internetzugang nur von einem unabhängig arbeitenden Computer aus zu ermöglichen, auf dem keine weiteren Daten der Dienststelle gespeichert sind.

Nur so lässt sich eindeutig verhindern, dass Angriffe "von außen" zu keinem Ausspähen führen. Wägt man den Schaden, der durch ein Eindringen Unbefugter in das interne Kommunikationsnetz mit den Anschaffungskosten eines für das Internet "zuständigen" Computers ab, ist die Antwort eindeutig: Der Zugang "zum Netz der Netze" ist von einer Dienststelle aus mit Hilfe eines Computers zu gewährleisten, der keine Vernetzung zu anderen Computern des Hauses hat und auf dem keine sensiblen Daten der Dienststelle gespeichert werden.

Die Konzentration auf einen "Internet-Computer" hat für den Dienstgeber auch den Vorteil, den Zugang zu Diensten des Internets "zentral" organisieren zu können. Das Laden von Spielen oder sonstiger Dienstleistungen aus dem Internet auf den Arbeitsplatz-PC wäre damit ausgeschlossen. Bei dieser Lösung entsteht allerdings das Problem, wie der E-Mail-Verkehr sinnvoll genutzt werden kann.

- **Verschlüsselung:**
 Mit einer Verschlüsselung von Daten wird versucht, Informationen nur den Berechtigten zukommen zu lassen. Personenbezogene Daten, die unverschlüsselt in Datennetzen fließen, sind offen lesbar wie Postkarten.
 Großer Beliebtheit erfreut sich zunehmend die asymmetrische Verschlüsselung.
 Dieser liegt folgendes Prinzip zugrunde: Jeder Kommunikationspartner erwirbt zwei "Schlüssel". Einer davon wird veröffentlicht, der dazugehörige verbleibt beim Datenempfänger und ist geheim. Zu einer relativen Datensicherheit kommt man, wenn die Nachricht an den Empfänger mit dessen öffentlichen Schlüssel verschlüsselt wird, weil eine Entschlüsselung der Nachricht nur durch den Empfänger mit dessen geheimen zweiten Schlüssel erfolgen kann.
 Diese Methode ermöglicht auch, die Echtheit der datenabsendenden Stelle nachzuweisen. Wer dem Empfänger eines Dokuments dessen Echtheit garantieren möchte, verschlüsselt es mit seinem geheimen Schlüssel und versendet es anschließend unter seinem Namen. Gelingt es dem Empfänger, das Dokument mit dem öffentlichen Schlüssel des Absenders zu entschlüsseln, ist die Authentizität nachgewiesen.

- **Laden von fremden Programmen:**
 Viele Angebote im Internet halten nicht nur Informationen in Form von Texten, Bildern und Querverweisen bereit, sondern sind auch in der Lage, Programme ablaufen zu lassen, z. B. Berechnungen durchzuführen (Baufinanzierung, Steuerbelastung usw.).
 Oft ist nicht klar, dass bei Nutzung solcher Angebote nicht nur Bilder und Texte auf den eigenen Computer geladen werden, sondern Ablaufprogramme.
 Diese starten ohne weiteres Zutun auf dem Computer des Internet-Teilnehmers, also dem eigenen Computer. Wer solche Programme ungeprüft übernimmt, weiß nicht, welche Programmabläufe auf den eigenen Computer geladen werden, ob Parameter des eigenen Computers verändert werden und welche Funktionen dann ablaufen. Der Nutzer liefert sich u. a. der Gefahr aus, dass interne Daten (z. B. Steuerdateien) manipuliert werden oder diese unberechtigt abgerufen werden können.

- **Paket- und Anwendungsfilter:**
 Die im Firewall-Produkt verwendeten "Paketfilter" vergleichen die Absender- und Empfängerdaten auf dem "elektronischen Umschlag" mit den hinterlegten Daten.
 Der Einsatz weiterer Sicherungskomponenten ist erforderlich, um die in der Literatur beschriebenen Manipulationsmöglichkeiten zu verhindern. Ein Anwendungsfilter z. B. greift auf die in den Paketen enthaltenen Daten, insb. auf Angaben über die Identität der Internet/Intranet-Nutzer und die von ihnen gewählten Dienste zu und kann damit auch darüber wachen, welche Personen welche Anwendungen nutzen können (17. Tätigkeitsbericht des Landesdatenschutzbeauftragten von Baden-Württemberg, 1996, Landtags-Drucksache 12/750, S. 11).

- **Abschottung sensibler Daten:**
 Personaldaten und sonstiges sensible Datenmaterial wie Finanzdaten sollten vom sonstigen innerbetrieblichen Datenaustausch abgeschottet werden.

C2: Die Nutzung des E-Mails am Arbeitsplatz

Im Zusammenhang mit der Nutzung des Internets erhalten Beschäftigte die Möglichkeit, E-Mails zu versenden und zu empfangen. Dabei ist zu beachten:

1. Gefährdungspotential

Das Versenden einer E-Mail über das Internet ist vergleichbar mit dem Versenden einer Postkarte, denn beide sind gleichermaßen vor unbefugten Zugriffen nicht geschützt. Während allerdings eine Postkarte „nur“ unbefugt gelesen werden kann, ist es möglich, eine E-Mail beliebig zu verändern, ohne dass der Empfänger dies feststellen kann. Und: Es ist für den Empfänger auch nicht unbedingt erkennbar, wer sich tatsächlich hinter einer E-Mail-Adresse verbirgt.

2. Verschlüsselung und Signatur

Um eine sichere Übertragung von Dokumenten zu gewährleisten, sollten diese verschlüsselt und digital signiert sein. Die Verschlüsselung gewährleistet die Vertraulichkeit der Nachricht, die digitale Signatur identifiziert den Absender eindeutig für den Empfänger. Der Mitarbeiter ist dahingehend zu schulen, diese Techniken einsetzen zu können. Die Computer sind mit (leicht bedienbarer, benutzerfreundlicher) Software auszustatten.

3. Geeignete technische Mittel

Bei der Nutzung von E-Mail sind personenbezogene Angaben auf das Mindestmaß zu beschränken (Grundsatz der Datenvermeidung und der Datensparsamkeit).

4. Bei dienstlicher Nutzung

Gestattet der Arbeitgeber die Nutzung von E-Mail und Internet ausschließlich zu dienstlichen Zwecken, ist dieser nicht Anbieter im Sinne des Telekommunikations- bzw. Teledienstrechts. Die Erhebung und Verarbeitung von Daten über das Nutzungsverhalten richtet sich nach den betrieblichen Nutzungsbestimmungen (Verordnungen/Erlassen) bzw. nach der kirchlichen Datenschutzanordnung (KDO). Der Arbeitgeber hat grundsätzlich das Recht, stichprobenartig zu prüfen, ob das Surfen bzw. E-Mail-Versenden der Beschäftigten dienstlicher Natur ist. Eine automatische Vollkontrolle durch den Arbeitgeber ist als schwerwiegender Eingriff in das Persönlichkeitsrecht des Beschäftigten nur bei konkretem Missbrauchsverdacht im Einzelfall zulässig. Auf mögliche Überwachungsmaßnahmen und in Betracht kommende Sanktionen sind die Beschäftigten hinzuweisen. Der Arbeitgeber darf die Nutzungs- und Verbindungsdaten nur insoweit kontrollieren, als dies im Einzelfall aus Gründen der Kostenkontrolle erforderlich ist. Wenn allerdings nur unerhebliche Kosten bei der Nutzung von Internet und E-Mail anfallen, ist eine Auswertung dieser Daten unverhältnismäßig.

5. Administrator

Wartungsarbeiten von Administratoren am EDV-Netz bzw. am Arbeitsplatz-Computer sind in erster Linie als Dienstleistung gegenüber dem Benutzer anzusehen und nicht als „Vollkontrolle der Nutzung durch den Arbeitgeber“. Daraus folgt: Die bei der Wartung durch den Administrator aufgedeckten Fälle missbräuchlicher Nutzung von Internet und E-Mail dürfen an den Arbeitgeber nur gemeldet werden, wenn das EDV-System bzw. der Computer im Zusammenhang mit der missbräuchlichen Nutzung beeinträchtigt wurde oder wenn der Administrator feststellt, dass ein schwerwiegender Verstoß gegen die Nutzungsbestimmungen des Arbeitgebers vorliegt (z.B. bei Aufruf pornographischer Seiten). Protokollierungsdaten dürfen nur zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherung des ordnungsgemäßen Betriebs genutzt werden, nicht zur Kontrolle des Verhaltens oder der Leistung des Beschäftigten. Aus Gründen der Datensicherheit dürfen Teilinhalte oder Anlagen von E-Mails unterdrückt werden, die gefährliche oder verdächtige ausführbare Codes enthalten (Dateien mit den Erweiterungen *.exe, *.bat, *.zip, *.arj usw.).

6. Dienstliche Belange

Von ein- und ausgehenden dienstlichen E-Mails darf der Arbeitgeber im selben Maße Kenntnis nehmen wie von dienstlichem Schriftverkehr.

7. Anvertrauen von Privatgeheimnissen

Bei Mitarbeitern, denen in ihrer Tätigkeit persönliche Geheimnisse anvertraut werden und die deshalb in einem besonderen Vertrauensverhältnis zu den betroffenen Personen stehen (z.B. Ärzte, Sozialarbeiter/-pädagogen, Psychologen) muss gewährleistet werden, dass der Arbeitgeber- soweit es sich um diesen Personenkreis handelt- keine Rückschlüsse auf die betroffenen Personen (Klienten) nehmen kann.

8. Private Nutzung von E-Mail und Internet

Der Arbeitgeber ist nicht verpflichtet, den Beschäftigten die private Nutzung von E-Mail und Internet zu gestatten. Lässt er die private Nutzung zu, ist er den Mitarbeitern gegenüber Telekommunikations- bzw. Teledienst-Anbieter. Eine zugelassene private Nutzung kann vom Arbeitgeber an Beschränkungen und Kontrollbefugnisse geknüpft werden.

9. Dienstvereinbarungen

Die kirchlichen Datenschutzbeauftragten empfehlen, über die Nutzung von E-Mail und Internet eine Dienstvereinbarung mit der Mitarbeitervertretung abzuschließen, da die Protokollierung, die Auswertung und die Durchführung von Kontrollen geeignet sein können, das Verhalten und die Leistung der Mitarbeiter zu kontrollieren.

10. Zusammenfassung

Personenbezogene Daten dürfen per E-Mail nur dann übermittelt werden, wenn sie verschlüsselt und mit einer Signatur versehen sind.

Weitere Informationen zur Nutzung von E-Mails usw. sind u.a. auf der Internetseite des Landesdatenschutzbeauftragten des Landes Brandenburg abrufbar:

www.lda.brandenburg.de

C3: Zum Intranet

1. Intranet:

Die Diözesen und Caritasverbände bauen gegenwärtig sog. Intranetze auf.

Dies sind Verbindungen zu einem zentralen Rechner der Diözese oder des Caritasverbands, der nur von berechtigten und mit einem Passwort ausgestatteten Benutzer genutzt werden kann. Über den zentralen Rechner besteht die Möglichkeit, ins Internet zu kommen.

Diese Intranetze haben den Vorteil, dass die Anwahl über die relativ sicheren öffentlichen Telefonleitungen (z. B. von Verbindungsknoten zu Verbindungsknoten der Telekom) zum zentralen Rechner erfolgt und die elektronische Post (E-Mails) beim zentralen Rechner für den Abruf, der wiederum über die relativ sicheren öffentlichen Telefonleitungen erfolgt, geschieht. Ein weiterer Vorteil liegt darin, dass die zentralen Rechner über aktualisierte und hochmoderne (und deshalb relativ teure) Sicherheitseinrichtungen verfügt, so dass elektronische Angriffe aus dem Internet besser abgewehrt werden können. Auf einem Computer dürfen aus Sicherheitsgründen nicht die Zugangsberechtigungen zum Intranetz und zu sonstigen Internetanbietern liegen.

C4: Das Netzwerk

1. Netzwerk:

Auch die Vernetzung der verschiedenen Computer einer Dienststelle stellt datenschutzrechtliche Anforderungen, die kurz mit der Frage beschrieben werden können: "Wer hat Zugriff auf die Daten, wer verwaltet die Daten?". Auch hier ist ein Sicherheitskonzept erforderlich, insb. bezüglich der Administratoren-Rechte. Die Nutzung bestimmter Daten kann auf bestimmte Arbeitsplätze beschränkt werden. Die Protokollierung der Zugriffe ist zwingend nötig. Es muss zwischen, "Nur-Lese-Rechte" und "Lese- und Bearbeitungs-rechte" unterschieden werden. Ein besonderes Augenmerk ist auf die Datensicherung zu legen.

2. Errichtungskontrolle:

Jedes Dokument soll mit einer Zugangskontrolle versehen sein, welches die Personen oder Personengruppen benennt, die das Dokument "errichtet hat", es lesen darf und wer Daten – „unter Benennung der Verantwortlichkeit" anfügen darf. Übernahme von Daten darf nur erlaubt sein, wenn derjenige, der sie errichtet hat, zustimmt. Die Zugangsberechtigung zu verschiedenen Datengruppen ist zu beschränken.

3. Sicherheitskonzept für das Netzwerk:

Zugriffsrechte sind auf Grund von Zugangskontrolllisten innerhalb der festgelegten spezifischen Berechtigungen zu erteilen. Die Vertraulichkeit kann nur durch "starke kryptographische Verfahren" gewährleistet werden, die Dokumentensicherheit durch "starke Integritätssicherungs-mechanismen", um Verfälschungen zu verhindern. Hierzu zählt auch, die Anwendersoftware selbst vor Verfälschung zu schützen, damit diese die geforderte "Funktionalität" behält. Die "Prüfung von Integritätsverletzungen" soll automatisch bei jedem erneuten Aufruf der jeweiligen Anwendungssoftware erfolgen.

Die Herkunft der Datei ist normalerweise nicht sicher nachzuweisen. Daher: Die Herkunft des Dokuments durch digitale Signaturen sichern. Passwörter sind möglicherweise nicht sicher genug. Es kann auf chipkartengestützte Verfahren, auf kryptographische Mechanismen oder biometrische Authentifizierungsverfahren zurückgegriffen werden. Es muss sichergestellt sein, dass das "Absenden" und das "Empfangen" nicht abgestritten werden kann.

Jeder Aufruf ist zu protokollieren (nach Benutzer, nach Zugangsart, nach Zugangsdatum und Zeit). Damit wird die Rekonstruierbarkeit einer Datei für jeden beliebigen Zeitpunkt gewährleistet. Das Recht auf Einsicht muss geregelt sein.

4. Passwort-Weitergabe

Das Passwort für die im Computer gespeicherte Klientendatei darf vom jeweiligen Mitarbeiter an niemanden weitergegeben werden. Wenn der Mitarbeiter durch längere Abwesenheit, z.B. bedingt durch Krankheit, seiner Arbeitsstelle fern bleiben muss, sollte

das Passwort dem jeweiligen Administrator mitgeteilt und von ihm verwaltet werden. Der Mitarbeiter hat jedoch nicht das Recht, die Passwortweitergabe grundsätzlich zu verweigern. Bei längerer Abwesenheit des Mitarbeiters und der damit zusammenhängenden Passwortweitergabe für Klientendateien an den Administrator muss von den Klienten keine entsprechende Einverständniserklärung eingeholt werden. Der Beratungsvertrag legt diese Regelung fest.

Die Geschäftsführung kann nicht über das Passwort Einsicht in Klientendateien nehmen, aber eine anonyme oder verschlüsselte Übermittlung von Daten verlangen, um sich über die Leistungen des Mitarbeiters zu informieren.

(VABS- Rechtsfragen, Kapitel II, 1994)

Glossar

Datei, automatisierte

Eine automatisierte Datei ist:

Eine Datensammlung, die durch ein automatisiertes Verfahren ausgewertet werden kann, wobei die Auswertung nach bestimmten Merkmalen erfolgt, z.B. Adressverwaltungsprogramme.

Gewaltenteilung

- Informationelle: ein aus datenschutzrechtlichen Grundsätzen entwickelter Begriff, der die Notwendigkeit beschreibt, personenbezogene Daten technisch und organisatorisch auf den Ort ihrer Erhebung, Verarbeitung, Nutzung zu beschränken.
Personenbezogene Daten müssen grundsätzlich zweckgebunden bei der Stelle (Abteilung, Referat, Dienst, Einrichtung usw.) verbleiben, die diese erhoben, gespeichert, verändert oder genutzt hat. Eine Weitergabe der Daten ist unter Beachtung der Grundsätze der Erforderlichkeit, der Zweckbindung, der Aufsichts- und Kontrollbefugnisse, der Datenschutzkontrolle und -sicherung möglich. Hierbei müssen die Aufgabenstellungen der datenabgebenden bzw. -empfangenden Stelle berücksichtigt werden.
- Vertikale: Daten werden in zulässiger Weise nur zwischen Abteilungen, Referaten, Diensten und Einrichtungen ect. eines Trägers weitergegeben.
- Horizontale: Daten dürfen trotz der Direktionsbefugnis der Rechtsträger von den Abteilungen bzw. den Mitarbeitern nur dann weiter gegeben werden, wenn es rechtlich zulässig ist.

Handakte

Ansammlung von Papieren, Notizen, Kopien, die sich ein Mitarbeiter im Zusammenhang mit der Bearbeitung eines Vorgangs macht.

Informationelles Selbstbestimmungsrecht

Besondere Ausprägung des verfassungsrechtlich garantierten Persönlichkeitsrechts. Der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner Daten. Der Einzelne muss Einschränkungen seines informationellen Selbstbestimmungsrechts hinnehmen, wenn überwiegendes Allgemeininteresse vorherrscht.

Personenbezogene Daten

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

Personenbezogene Daten, besondere Arten

Besondere Arten persönlicher Daten sind nach EU-Datenschutzrichtlinie z.B. Daten, die sich auf die Gewerkschaftszugehörigkeit, die geschlechtliche Bestimmung (z.B. Homosexualität) und ethnische Zugehörigkeit beziehen.

Begriffserklärungen zum Internet

- **Browser** ist das Programm, mit dem man durch das "WWW" surfen kann. Ein Browser ist notwendig, um überhaupt WWW-Seiten ansehen zu können.
- **Cookies** (engl. cookie = Keks) sind kleine Datenmengen, die zusammen mit den eigentlich angeforderten Daten aus dem Internet an den Computer des Benutzers übermittelt werden. Dort werden diese Daten gespeichert und für einen späteren Abruf bereitgehalten. Dadurch wird im einfachsten Fall ein wiederholter Zugriff eines bestimmten Benutzers (exakt: des Browsers auf dem Computer, den er verwendet), auf das Internet-Angebot erkennbar. Vor allem benützen Cookies, um Kundenprofile zu erstellen oder ein persönliches Angebot zusammenzustellen. Man kann einstellen (z. B. InternetExplorer 3.0: Menü, Ansicht/Optionen/Erweitert), ob der Computer Cookies akzeptieren kann.
- **Domain** ist eine weltweit erreichbare (elektronische) Adresse, die der Computer braucht, um Nachrichten zustellen zu können.
- **FTP** steht für File Transfer Protocol und dient dem Übertragen von Dateien zwischen Rechnern mit Hilfe eines normierten Befehlssatzes. Auf dem eigenen Rechner läuft der FTP-Client, der die Befehle an den entfernten FTP-Server weiterleitet. Dort werden oftmals Programme, Texte, Grafiken oder Tondateien zur Nutzung vorgehalten (sog. Anonymous FTP).
- **HTML** ist die Sprache, in der die Webseiten geschrieben werden. Erst der Browser ermöglicht die graphische Umsetzung der HTML-Befehle (Abk. für Hypertext Markup Language).
- **HTTP** ist quasi die technische Grundlage für das WWW. Dem Computer wird mitgeteilt, dass die Daten aus HTML-Code bestehen, deshalb beginnen WWW-Adressen mit http://, neuere Browser-Programme ermöglichen das Ansehen der Webseiten auch ohne diese Voranstellung.
- **IP-Adresse** ist die "Adressen" des Computers, bestehend aus einer Zahlenkombination.
- **Link** ist der englische Ausdruck für Verbindung und bezeichnet die (anklickbaren) Verweise von einer WWW-Seite.
- **Mailbox** ist im Internet das persönliche Postfach, in dem Nachrichten gespeichert werden. Manchmal wird der Begriff "Mailbox" auch für den "Mailbox-Computer" verwendet, der nicht nur die persönliche Post des Nutzers aufbewahrt, sondern auch andere Dienste.
- **Online** bedeutet, dass man eine "offene Telefonleitung" zu einem Rechner besteht.
- **PGP** ist ein Verschlüsselungsprogramm für e-Mails. Das Programm kann sowohl E-Mails verschlüsseln als auch elektronische Unterschriften leisten (Pretty Good Privacy).
- **PoP** bedeutet "point of Presence" und gleichbedeutend mit Provider bzw. Einwahlknoten.
- **Provider** ist ein Internetanbieter und ermöglicht den Zugang zum Internet.
- **Proxy-Server** ist ein Rechner, der nicht jede Anfrage einer Internetadresse in das Netz weitergibt sondern erst nachschaut, ob jemand die Seite schon angefordert hat, die er – zur Entlastung der Leitungen – zwischengespeichert hat. Proxy-Server werden vor allem auch bei Intranetzen, die ans Internet angeschlossen sind, verwendet, um Verbindungskosten zu sparen und die Arbeitsgeschwindigkeit zu erhöhen.
- **Server:** Ein WWW-Server ist ein "Informationstechnik"-System ("IT-System), das über eine Informationsdatenbank dem Browser (auch WWW-Client genannt) Dateien zur Verfügung stellt. Der Browser zeigt die Informationen des WWW-Servers auf dem Benutzerrechner an.
- **URL** ist eine exakte Adressenangabe für Dateien im Internet (Universal Resource Locator).

Anhang

Literatur

Fachet, Dr., Siegfried
Datenschutz in der katholischen Kirche
Praxiskommentar zur Anordnung über den kirchlichen Datenschutz (KDO)
Neuwied 1998

Fachet, Dr., Siegfried
Damit's die Spatzen nicht von den Dächern pfeifen
Artikel zum Datenschutz in „neue Caritas“, Heft 20, November 2000, S.36-40

Abdruck der Kirchlichen Datenschutzanordnung (KDO) in „neue Caritas“, Heft 6, 2001, S. 32-39

VABS- Rechtsfragen
Papier zur rechtlichen Klärung von Datenschutzfragen Juli 1994

Adressen

Dr. Siegfried Fachet
Datenschutzbeauftragter der Erzdiözese Freiburg und
der Diözese Rottenburg- Stuttgart
Katholisches Büro Stuttgart
Staffenbergstraße 14
70184 Stuttgart

VABS
Verband ambulanter Behandlungsstellen für Suchtkranke/Drogenabhängige e.V.
Stefan Bürkle, Geschäftsführer
Karlstr. 40
79104 Freiburg