Datenschutz in der Katholischen Kirche

Sicherheit und Ordnungsgemäßheit kirchlicher Datenverarbeitung

Arbeitshilfe Nr. 200 Stand: Dezember 2015

Datenschutz im Pfarrbüro

Eine Arbeitshilfe für kirchliche Einrichtungen

2. Auflage

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

DATENSCHUTZ
IN DER KATHOLISCHEN KIRCHE

Datenschutz im Pfarrbüro

Eine Arbeitshilfe für kirchliche Einrichtungen

Inhalt

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:
2. Auflage, Dezember 2015
Februar 2013

I. Die Meldedaten (Gemeindemitgliederverzeichnis)

Das Gemeindemitgliederverzeichnis ist die wirksame und gleichzeitig notwendige Grundlage für eine ordnungsgemäße pastorale Versorgung in den Kirchengemeinden. Sein möglichst vollständiger und richtiger Inhalt ist für kirchliches Handeln daher von entscheidender Bedeutung. Nach deutschem Recht erhalten wir diese Daten durch staatliche Übermittlung. Geregelt ist dies durch das Bundesmeldegesetz (BMG) vom 03. Mai 2013, zuletzt geändert am 20.10.2015 und in Kraft getreten am 01.11.2015.

Nach § 42 Abs. 1 BMG hat die katholische Kirche, als öffentliche Religionsgesellschaft gegenüber den Einwohnermeldeämtern Anspruch auf Übermittlung der Daten ihrer Mitglieder. Zudem dürfen ihr nach § 42 Abs. 3 BMG ein Teil der Meldedaten von Familienmitgliedern, die einer anderen oder gar keiner Kirche angehören ebenfalls übermittelt werden (Familienverbund). Allerdings haben die Betroffenen in diesem Fall das Recht, einer Übermittlung zu widersprechen und sind hierauf bereits bei der Anmeldung sowie einmal jährlich durch öffentliche Bekanntmachung hinzuweisen.

Die Datenübermittlung erfolgt durch die Meldebehörden (kommunaler Datensatz). Dabei müssen jedoch gesetzlich zwei wesentliche Voraussetzungen vorliegen.

a) Nach § 42 Abs. 1 BMG dürfen den öffentlichen Religionsgesellschaften die Daten ihrer Mitglieder **zur Erfüllung ihrer Aufgaben, nicht jedoch zu arbeitsrechtlichen Zwecken** übermittelt werden.
b) Nach § 42 Abs. 5 BMG ist die Übermittlung "… nur zulässig, wenn sichergestellt ist, dass bei dem Datenempfänger **ausreichende Maßnahmen zum Datenschutz** getroffen sind". Die Feststellung hierüber trifft eine durch Landesrecht zu bestimmende Behörde.

Zur ersten Voraussetzung nehmen hier die Ausführungen zu Ziffer II Stellung, ausreichende Datenschutzmaßnahmen werden unter Ziffer III erläutert. Eine Veröffentlichung der Daten ist nur in eingeschränkten Umfange möglich und wird unter Ziffer IV dargelegt.

Bevor wir hierzu kommen, wollen wir uns erst einmal den Inhalt der Pfarrdatei anschauen.

1. Der kommunale Datensatz

Von den Mitgliedern bekommen wir folgende Daten:

Familiennamen, frühere Namen, Vornamen, Doktorgrad, Ordensname, Künstlername, Tag und Ort der Geburt, Geschlecht, Staatsangehörigkeiten, gegenwärtige und letzte frühere Anschrift, Haupt- und Nebenwohnung, bei Zuzug aus dem Ausland auch die letzte frühere Anschrift im Inland, Tag des Ein- und Auszugs, Familienstand, beschränkt auf die Angabe, ob verheiratet oder eine Lebenspartnerschaft führend oder nicht; zusätzlich bei Verheirateten oder Lebenspartnern: Tag der Eheschließung oder

der Begründung der Lebenspartnerschaft, Zahl der minderjährigen Kinder, Übermittlungssperren, Sterbetag und -ort.

Von den Familienmitgliedern erhalten wir (falls nicht widersprochen wird):

Familiennamen, Vornamen, Tag und Ort der Geburt, Geschlecht, Zugehörigkeit zu einer öffentlich-rechtlichen Religionsgesellschaft, derzeitige und letzte frühere Anschrift Auskunftssperren nach § 51, Sterbedatum.

§ 55 Abs. 2 BMG gibt den Ländern die Befugnis, durch Landesrecht den Religionsgesellschaften weitere Daten zu übermitteln.

Die Datenübermittlung erfolgt an die Meldestelle im Generalvikariat / Ordinariat. Von dort aus werden sie in einem kirchlichen Rechenzentrum verarbeitet und als Gemeindemitgliederverzeichnis den Pfarrgemeinden zur Verfügung gestellt.

2. Kirchliche Amtshandlungsdaten

Ergänzt wird das Gemeindemitgliederverzeichnis durch kirchliche Amtshandlungsdaten, wie Taufe, Erstkommunion, Firmung, Eheschließung, Weihe, Profess, sowie Aufnahme und Wiederaufnahme von Kirchenmitgliedern (§ 5 Abs. 3 KMAO). Diese Matrikeldaten sind neben den Meldedaten wesentliche Voraussetzung für kirchliches Wirken, da Sakramente nur einmalig gespendet werden dürfen und darauf hinzuwirken ist, dass die Mitglieder der katholischen Kirche diese möglichst vollständig empfangen.

Aus der in § 5 Abs. 3 Satz 2 KMAO gewählten Formulierung, dass das Gemeindemitgliederverzeichnis "insbesondere" die oben genannten Amtshandlungsdaten enthält, lässt sich der Schluss ziehen, dass auch noch weitere Informationen über die Mitglieder hinzugefügt werden können. Dabei ist jedoch zu bedenken, dass nur Daten, die auch erforderlich sind, eingetragen werden dürfen (§ 5 Abs. 3 Satz 1 KMAO). Private Kenntnisse, wie etwa die über Alkoholprobleme einzelner Mitglieder oder der Umstand, dass ein Familienmitglied aus der Kirche ausgetreten ist, sind **nicht** eintragungsfähig. Die Übernahme bestimmter Aufgaben in der Gemeinde (Kirchenvorstand, Pfarrgemeinderat, Pastoralrat, usw.) können eingetragen werden, wenn diese regelmäßige schriftliche Informationen oder Unterlagen über das Bistum oder die Pfarrgemeinde erhalten sollen.

3. Die Behandlung von Sperrvermerken

Nach § 9 Ziffer 5 des Bundesmeldegesetzes (BMG) hat jeder Bürger gegenüber der Meldebehörde ein Recht auf die unentgeltliche Speicherung von Übermittlungssperren. Eine Verarbeitung oder Nutzung dieser Daten ist nach § 41 BMG für die Datenempfänger nur zulässig, wenn eine Beeinträchtigung schutzwürdiger Interessen der betroffenen Person ausgeschlossen werden kann.

a. Übermittlungssperre gemäß § 42 Abs. 3 Satz 2 BMG:

Familienangehörige der Mitglieder (Ehegatten, minderjährige Kinder und die Eltern minderjähriger Kinder), die nicht derselben oder keiner öffentlich-rechtlichen Religionsgesellschaft angehören, können verlangen, dass ihre Daten nicht übermittelt werden und sind darauf bei der Anmeldung hinzuweisen. Sie sind daher im Gemeindemitgliederverzeichnis nicht enthalten und dürfen auch nicht nachträglich, etwa bei privater Kenntnis des Pfarrers von den Familienverhältnissen hinzugefügt werden.

b. Auskunftssperren gemäß §§ 51 BMG:

- § 51 Abs. 1 Auskunftssperre bei Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnlichen schutzwürdigen Interessen. Die Auskunftssperre wird auf Antrag oder von Amts wegen eingetragen. Ihre Eintragungsdauer ist nach Absatz 4 auf zwei Jahre befristet, kann jedoch auf Antrag verlängert werden.
- § 51 Abs. 5 Geschützt wird auch das Offenbarungs- und Ausforschungsverbot bei Adoptionsverhältnissen wie es in § 1758 BGB und § 63 Abs. 1 PStG festgelegt ist.
  Eine Sperre besteht auch in Fällen, in denen nach § 63 Abs. 2 PStG der Vorname und das Geschlecht des Betroffenen nach dem Transsexuellengesetz geändert worden ist.

Die Auskunftssperre bewirkt, dass eine Melderegisterauskunft unzulässig ist. Diese Verpflichtung trifft auch die Pfarrgemeinden. Das gilt für Einzelauskünfte und besonders natürlich auch für Veröffentlichungen. So ist beispielsweise eine Bekanntgabe von Alters- und Ehejubiläen im Pfarrbrief in diesen Fällen nicht statthaft! Die Betroffenen brauchen hierzu auch nicht erneut zu widersprechen.

II. Nutzung des Gemeindemitgliederverzeichnisses

Sowohl das staatliche Recht (§ 42 Abs. 1 BMG), wie auch das kirchliche Recht (§ 5 Abs. 3 Satz 1 KMAO) beschränken die Nutzung der Daten auf die Erfüllung der, in der Zuständigkeit der Gemeinde liegenden Aufgaben. Hierzu gehören beispielsweise

- Einladungen von Kirchenmitgliedern zu Sakramentsspendungen (Erstkommunion, Firmung),
- Einladungen bestimmter Altersgruppen zu Veranstaltungen (Beispiel: Teilnahme an Jugendangeboten, Seniorentagen, usw.),
- die Vorbereitung des Besuchs von Gemeindemitgliedern, auch durch Gemeindehelfer,
- Zustellung des Pfarrbriefs,
- Erstellung von Wählerverzeichnissen,
- Anschreiben an die Gemeinde oder einzelne Mitglieder mit Bitte um Unterstützung für besondere Projekte (Fundraising).

Nicht hierzu gehört die Nutzung der Daten zur Information an Dritte außerhalb der Gemeinde. Eine Weitergabe ist hier nur mit schriftlicher Einwilligung der Betroffenen möglich. Hierzu zählen beispielsweise:

- die Weitergabe von Daten an die lokale Presse
- die Weitergabe an Banken
- die Weitergabe von Daten an Einzelhandelsgeschäfte

Die Daten dürfen auch, nach ausdrücklicher Bestimmung in § 42 BMG nicht für arbeitsrechtliche Zwecke verwendet werden. Der Bundesgesetzgeber hat diese Einschränkung erstmalig mit aufgenommen, aus der Sorge heraus, dass Daten über bestehende Lebenspartnerschaften zu Beeinträchtigung der Betroffenen insbesondere in kirchlichen Arbeitsverhältnissen führen könnten. Die gesetzliche Formulierung ist jedoch so gefasst, dass auch in anderen Fällen, eine Auskunftserteilung an eine Bewerbungsstelle oder ein Personalbüro zu unterbleiben hat. Die Bestätigung, dass ein Bewerber als Mitglied der Katholischen Kirche in ihrem Gemeindemitgliedsverzeichnis eingetragen ist, ist unzulässig. Alle Informationen, die ein Arbeitgeber zur Durchführung eines Bewerbungsverfahrens braucht müssen also durch unmittelbare Befragung des Bewerbers sowie die Vorlage geeigneter Urkunden durch ihn ermittelt werden![1]

1. Information von Kirchenvorstand / Pastoralrat

Der Kirchenvorstand / Pastoralrat ist das gesetzliche Vertretungsorgan der Gemeinde. Er verwaltet das Vermögen und hat dabei über alle finanzwirksamen Maßnahmen der Pfarrei zu entscheiden. Dieser Aufgabe kann er nur gerecht werden, wenn er über alle in seinen Zu-

[1] Dies hat das Kirchenrechtliche Institut der Evangelischen Kirche in Deutschland durch eine Stellungnahme von Prof. Heinig vom 16.10.2015 für den Bereich der EKD festgestellt.

ständigkeitsbereich fallenden Angelegenheiten umfassend unterrichtet wird. Unter haftungsrechtlichen Gesichtspunkten besteht unter Umständen sogar eine Verpflichtung der Vorstandsmitglieder, sich zu informieren. Hierzu kann er z. B. Akten einsehen und Betroffene anhören. Demgegenüber besteht nach dem Kirchenvermögensverwaltungsgesetz (§ 8 IV KVVG) eine besondere Pflicht zur Amtsverschwiegenheit. Sitzungen und Protokolle in Personalangelegenheiten sind nicht öffentlich.

Grenzen bestehen allerdings dort, wo Dritte nicht offenbarungspflichtig sind oder sich durch die Preisgabe von Informationen strafbar machen würden (Beispiel: Verletzung von Privatgeheimnissen, § 203 StGB).

2. Erstellung von Teilnehmerlisten / Telefonlisten

In vielen Bereichen ist die Verteilung von Teilnehmerlisten durchaus angebracht. So werden Mütter von Kindergartenkindern in Stand gesetzt, untereinander Kontakt zu halten und wichtige Änderungen kurzfristig zu übermitteln. Auch für Pfarrgemeinderäte, Kirchenvorstände, Kommunion- und Firmvorbereitungskreise, Jugendgruppen und viele andere Bereiche ist eine Telefonliste wesentliche Voraussetzung für den Kontakt untereinander.

Datenschutzrechtlich ist eine solche Weitergabe von Privatdaten aber nur dann zulässig, wenn eine Rechtsvorschrift sie vorsieht oder die Betroffenen eingewilligt haben (§ 3 Abs. 1 KDO). Für diese Fälle besteht eine solche Vorschrift nicht, so dass Telefonlisten nur weitergegeben werden dürfen, wenn die Teilnehmer einverstanden sind. In der Regel geschieht das, in dem eine vorbereitete leere Liste ausgelegt wird, in der jeder sich eintragen kann, wenn er diese Kontaktmöglichkeiten wünscht. Auch die Erstellung einer vollständig vorbereiten Telefonliste ist möglich, wenn den Betroffenen vor ihrer Verteilung die Möglichkeit gegeben wird, sich durch Schwärzung auszutragen. Weiterhin ist mit den beteiligten Personen abzusprechen, welchen inhaltlichen Umfang die Liste haben soll. Soll außer dem jeweiligen Namen nur die Telefonnummer oder auch die Adresse und evtl. weitere Informationen hierin aufgenommen werden?

3. Weitergabe von Daten an ehrenamtliche Gemeindehelfer

Eine Weitergabe von Daten an Gemeindehelfer, die beispielsweise neu zugezogene und ältere Gemeindemitglieder besuchen, ist als Erfüllung eines kirchlichen Auftrages dann unbedenklich, wenn es sich um Daten handelt, die die Helfer für ihre Arbeit benötigen und die Helfer die Datenschutzverpflichtungserklärung gemäß § 4 KDO unterschrieben haben Gleiches gilt für Sammelaktionen, die für z. B. karitative Zwecke durchgeführt werden. Die Daten sind nach Gebrauch an die Kirchengemeinde zurückzugeben. Die Anfertigung von Abschriften oder Ablichtungen ist unzulässig.

4. Umgang mit Wählerlisten

Für die Wahlen zum Kirchenvorstand und zum Pfarrgemeinderat werden, unter Beachtung der jeweils gültigen Wahlordnungen, Wählerlisten erstellt. Die dort eingetragenen Personen können sich zum Nachweis ihres Wahlrechts hierauf berufen. Deshalb ist in einem bestimmten Zeitraum vor der Wahl den Wahlberechtigten die Möglichkeit eröffnet, sich davon zu überzeugen, ob sie tatsächlich in der Wählerliste stehen. In den Wahlordnungen wird das Verfahren dazu festgelegt. Früher war es üblich, die Wählerlisten zu bestimmten Zeiten im Pfarrbüro offen auszulegen, so dass jedermann Einsicht nehmen konnte. Diese Verfahrensweise entspricht nicht mehr den datenschutzrechtlichen Anforderungen. Sie führt letztlich dazu, dass Auskunfts- und Übermittlungssperren leicht umgangen werden können. Prinzipiell sind zum Schutz der Personen, die eine Auskunftssperre eingetragen haben, zwei Verfahrensweisen denkbar:

1. Es werden zwei getrennte Wählerlisten für Wahlberechtigte mit und ohne Auskunftssperre erstellt. Die allgemeine Liste kann dann weiter zur Einsichtnahme bereitgehalten werden, während die Liste mit den schützenswerten Daten unter Verschluss bleibt.

2. Es wird eine einheitliche Liste für alle Wahlberechtigten erstellt, die jedoch nicht mehr öffentlich ausliegt. Die Gemeindemitglieder haben in diesem Fall jedoch Anspruch auf Auskunft darüber, ob sie selbst ordnungsgemäß eingetragen sind. Weitere Auskünfte sind unzulässig.

Die jeweilige Verfahrensweise steht nicht im Belieben der Pfarrgemeinden, sondern richtet sich nach der jeweils gültigen Wahlordnung. Inzwischen haben sich alle norddeutschen Diözesen für die zweite Lösung entschieden. Die nachfolgende Tabelle gibt einen Überblick über die zurzeit gültigen Regelungen.

Übersicht über die bestehenden Regelungen in den norddeutschen Diözesen		
Erzbistum Berlin	§ 1 Abs. 4 WO zur Wahl der Kirchenvorstandsmitglieder im Erzbistum Berlin vom 01.05.2011	§ 1 Ziff. 3 und § 3 Wahlordnung der Pfarrgemeinderäte im Erzbistum Berlin in der Fassung vom 01.05.2011
Erzbistum Hamburg	§ 6 WO für Kirchenvorstände in der Erzdiözese Hamburg (KVWahlO)	§ 6 WO für Pfarrgemeinderäte in der Erzdiözese Hamburg (PGRWahlO)
Bistum Hildesheim	§ 6 WO für die Kirchenvorstände in der Diözese Hildesheim i.d.F. vom 1.1.2006	§ 6 WO für die Pfarrgemeinderäte in der Diözese Hildesheim
Bistum Magdeburg	§ 8 WO für die Wahl des Kirchenvorstandes (WOKV) vom 01.02.2004	§ 10 WO für die Pfarrgemeinderäte im Bistum Magdeburg vom 01.02.2004
Bistum Osnabrück	§ 6 WO für die Kirchenvorstände in der Diözese Osnabrück (i.d.F. v. 6.12.2005)	§ 6 WO für die Pfarrgemeinderäte in der Diözese Osnabrück (i.d.F. v. 6.12.2005)
Offizialat Vechta	§ 6 WO für die Kirchenausschüsse im Oldenburgischen Teil der Diözese Münster vom 25.01.2006	

5. Umgang mit dem Personalschematismus

Der Personalschematismus wird nur für den dienstlichen Gebrauch herausgegeben. Eine Weitergabe an Dritte ist nicht zulässig. Der Bezug über örtliche Buchhandlungen ist nicht möglich. Anfragen zur Überlassung des Personalschematismus seitens Dritter sind negativ zu beantworten oder in Zweifelsfällen an das Generalvikariat bzw. Bischöfliche Offizialat weiterzuleiten.

6. Verwaltung der Kirchenbücher

Für die Verwaltung der Kirchenbücher mit den Matrikeldaten und die Urkundensammlung der Pfarrei gilt can. 535 CIC sowie die hierzu erlassenen Partikularnormen der Bischofskonferenz und des Diözesanbischofs. Ältere Bücher sind gemäß der Regelungen zum Archivwesen der katholischen Kirche sorgfältig aufzubewahren. Diese Vorschriften sind als bereichsspezifische Normen der KDO vorrangig (§ 1 Abs. 3 KDO).

7. Fundraising / Spendenaufrufe

Fundraising ist der moderne Begriff für das Sammeln von Spenden. Damit verbindet sich eine systematische Erhebung der anzusprechenden Geber (Wer kommt als Spender in Frage?) sowie ein ordnungsgemäße Planung der durchzuführenden Maßnahmen und eine verantwortungsvolle Verwaltung und Nutzung der erhaltenen Gelder. Im heutigen Verständnis ist Fundraising ein "Geben und Nehmen" zwischen den angesprochenen Personen und der Gemeinschaft, die um ihre Hilfe bittet. So kann der Spender regelmäßig mit der Pfarrei in besonderer Weise verbunden werden, etwa durch persönliche Einladungen zu Festen oder bestimmten Veranstaltungen in Bezug auf die Spende. Beispielsweise eine gemeinsame Besichtigung des Glockenturms, wenn hierfür Geld gesammelt wurde. Auch kleinere Geschenke, wie eine Miniaturnachbildung einer Heiligenfigur kommen infrage, wenn für ihre Restaurierung Geld gegeben wurde. Hier sind große Teile der Fantasie und das Einfühlungsvermögen der Fund Raiser gefordert.

Die Frage stellt sich natürlich, ob hierfür auch Daten aus dem Gemeindemitgliederverzeichnis verwendet werden dürfen. Gehört also Fundraising zu den Aufgaben der Kirche, für die ihr die Meldedaten übermittelt werden? Dabei ist zu berücksichtigen, dass die katholische Kirche schon immer weitgehend von Spenden gelebt hat. So wurden zum Beispiel die großen Kathedralen des Mittelalters sowohl durch unentgeltliche Arbeitsleistungen der Stadtbewohner, wie auch durch Sach- oder Geldspenden reicher Bürger des Ortes finanziert. Insbesondere soziale Leistungen sind dort, wo keine staatlichen Beihilfen bestehen, ohne Spendenbeiträge oft nicht finanzierbar. Das Sammeln von Finanzhilfen für Zwecke die heute steuerrechtlich als gemeinnützig anerkannt sind und auch hierfür verwendet werden, gehört zu den elementaren Aufgaben der Kirche. Das Bistum Hildesheim hat in § 1 Abs. 1 seiner Fundraisingordnung dementsprechend bestimmt:

> *(1) Die in § 1 Abs. 2 KDO genannten diözesanen Stellen sind berechtigt, zum Zwecke der Finanzierung ihrer rechtmäßigen Aufgaben, Fundraising-Maßnahmen im räumlichen Bereich ihrer Tätigkeit durchzuführen. Zu diesem Zweck dürfen personenbezogene Daten aus den Gemeindemitgliederverzeichnissen genutzt werden.*

In den anderen Bistümern fehlt zwar eine ausdrückliche Bestimmung dieser Art, jedoch wird auch dort die Vereinbarkeit mit den rechtmäßigen Aufgaben der Kirche angenommen. Aus datenschutzrechtlicher Sicht ist jedoch dabei eine Reihe von Punkten zu beachten:

1. Es muss sich um die Finanzierung rechtmäßiger Aufgaben aus den Bereichen der Verkündigung, Seelsorge oder der Nächstenliebe handeln.
2. Die Zwecke müssen als gemeinnützig (§ 52 Abgabenordnung), mildtätig (§ 53 Abgabenordnung) oder zur Förderung kirchlicher Zwecke (§ 54 Abgabenordnung) anerkannt sein.
3. Die Verwendung der Mittel muss selbstlos sein und dürfen abzüglich der Kosten der Maßnahme nur für die erklärten Zwecke ausgegeben werden.
4. Menschen, die ausdrücklich erklärt haben, keine Spendenaufforderungen erhalten zu wollen, dürfen nicht angeschrieben werden (sog. "Robinsonliste").
5. Der Spendenaufruf muss von dem Vertreter der erhebenden Körperschaft unterzeichnet sein, also im Falle der Pfarrgemeinde durch den Kirchenvorstand, dieser vertreten durch den Pfarrer und ein weiteres KV-Mitglied.
6. Wird die damit verbundene Datenverarbeitung einer dritten Stelle übertragen, liegt eine Auftragsdatenverarbeitung vor, die nur in Anwendung von § 8 KDO statthaft ist. Danach ist der Auftrag schriftlich zu erteilen, wobei auch die Bedingungen der Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten festzulegen sind. Ebenso ist in der Vereinbarung festzulegen, durch welche technisch-organisatorischen Maßnahmen die Daten geschützt werden. **Die Verantwortung für die Datenverarbeitung verbleibt beim Auftraggeber!** Die Betroffenen können ihre Rechte nach § 8 Abs. 1 Satz 2 KDO nur ihm gegenüber geltend machen.
7. **Keine Weitergabe der Daten an andere Fundraisingorganisationen**, die Spendenzwecke außerhalb der Pfarrgemeinde verfolgen. Das Bistum selbst verfügt insoweit über ein eigenes Register nach § 5 Abs. 6 KMAO. Eine Weitergabe von Spenderdaten an Stellen außerhalb des Bistums sind mangels Rechtsgrundlage unzulässig und können daher nur mit ausdrücklicher, schriftlicher Einwilligung der Betroffenen erfolgen (§ 3 Abs. 1, 2 KDO). Lediglich im Bistum Hildesheim ist durch § 3 Fundraisingordnung geregelt, dass der Generalvikar, für eine Datenübermittlung an Stellen außerhalb des Bistums ausnahmsweise eine Genehmigung erteilen kann.
8. Soweit das jeweilige Bistum bereichsspezifische Vorschriften zur Durchführung von Fundraisingmaßnahmen erlassen hat, sind diese unbedingt zu beachten. Bisher ist das nur in Hildesheim geschehen durch die "Anordnung zum Schutz personenbezogener Daten bei der Durchführung von Fundraising-Maßnahmen im Bistum Hildesheim – FundrO". Weitere Bistümer planen den Erlass einer solchen Bestimmung.

8. Datenaustausch mit der Militärseelsorge

Katholische Gemeindemitglieder, die zur Bundeswehr eingezogen werden, mögen durch die Kirchengemeinden an die zuständigen Standortpfarrer gemeldet werden.

Laut Artikel 4 der Päpstlichen Statuten für die Seelsorge in der Deutschen Bundeswehr unterstehen dem Jurisdiktionsbereich des Militärbischofs alle katholischen Soldaten und jene katholischen Zivilisten, die nach den jeweils gehenden Gesetzen in die Streitkräfte integriert sind; desgleichen die katholischen Familienmitglieder der Berufssoldaten, der Soldaten auf Zeit und der oben genannten Zivilisten, auch wenn der Familienvater nicht katholisch ist. Die Ortsgeistlichen übermitteln dem zuständigen Standortpfarrer die entsprechenden kirchlichen Amtshandlungsdaten. Die Eintragung in die Matrikel der Standortpfarrei erfolgt ohne Nummer. Es handelt sich um Taufen, Konversionen, Trauungen und Begräbnisse.

9. Weitergabe im Rahmen der Krankenhausseelsorge

Gemäß Art. 140 des Grundgesetzes i. V. m. Art. 141 der Verfassung des Deutschen Reiches vom 11. August 1919 sind die Religionsgesellschaften zur Vornahme religiöser Handlungen in Krankenanstalten zuzulassen, wobei jeder Zwang fernzuhalten ist. Daher können alle Krankenhäuser, unabhängig von ihrer Trägerschaft, das Merkmal der Konfessionszugehörigkeit erfragen, ggf. aufzeichnen und an den Krankenhausseelsorger bzw. die zur Krankenhausseelsorge beauftragten Personen weitergeben. Dabei ist jedoch zu berücksichtigen:

- Das die Angaben des Patienten zur Religionszugehörigkeit freiwillig erfolgen. Der Patient ist hierauf hinzuweisen.
- Eine Weiterleitung der Daten an die Krankenhausseelsorge nur mit Einwilligung des Patienten erfolgen darf.

Sofern der Patient aufgrund eines besonderen Umstandes nicht nach seiner Konfessionszugehörigkeit befragt werden kann, seine Zugehörigkeit aber der Krankenhausverwaltung bekannt ist, bestehen keine Bedenken, wenn auf den mutmaßlichen Willen des Betroffenen abgestellt wird. Hinweise hierauf können sich aus der Befragung von Angehörigen oder aus einem mitgeführten kirchlichen Notfallpass oder ähnlichem ergeben.

In vielen Fällen werden die Daten nicht bei der Aufnahme des Kranken von der Klinik erhoben und weitergeleitet. Stattdessen wird dem Seelsorger Gelegenheit gegeben, die Stationen zu besuchen und die Krankenzimmer zu betreten, so dass er seine Hilfe unmittelbar anbieten kann. Die seelsorgliche Betreuung Kranker gehört zu den zentralen Aufgaben der Kirche. Daher sind auch gemäß Artikel 11 des Konkordates zwischen dem Heiligen Stuhl und dem Land Niedersachsen vom 01. 07. 1965 in der Fassung vom 21. 05. 1973 (Nds. Gesetz- und Verordnungsblatt 1965, S. 191 ff., 1973, S. 376 ff.) in Krankenhäusern die zuständigen katholischen Geistlichen im Rahmen der allgemeinen Hausordnung zur Vornahme seelsorglicher Besuche und kirchlicher Handlungen zugelassen. Diese Aufgabe wird in den Kirchengemeinden oft von Laienhelfern in der Seelsorge und Seelsorgern übernommen. Anliegen

des Datenschutzes kann es insofern nicht sein, menschliche Zuwendung und geistlichen Zuspruch zu erschweren oder gar zu unterbinden. Der betroffene Patient wird in seinen schutzwürdigen Belangen nicht beeinträchtigt, wenn er den Besuch des Krankenhausbesuchsdienstes erhält. Wünscht er die Gespräche nicht, kann er dies dem Geistlichen oder ehrenamtlichen Helfer mitteilen.

III. Regelung der Zugriffsrechte und Schutz der gespeicherten Daten

1. Zugriffssperren durch die Software

Die Programme zur Bearbeitung und Nutzung der Gemeindemitgliederdatei werden vom (Erz-)Bistum vorgegeben. Zwei entscheidende Gründe sind hierfür verantwortlich, nämlich

1. dass nur eine gemeinsame Software sicherstellen kann, dass auf den Systemen aller verarbeitenden Stellen einheitliche Schnittstellen und Standards vorhanden sind, die die Darstellung der Daten ohne Probleme ermöglichen;
2. die Gestaltung der Datenbank in einer Form, die ein effektives Arbeiten ermöglicht zugleich aber auf datenschutzrechtlich zulässige Inhalte beschränkt ist und eine notwendige Sicherung der Datenbestände vorsieht.

Sie verschlüsseln die Daten auf der Festplatte des Arbeitsplatzcomputers und erlauben so nur autorisierten Personen, mit entsprechendem Passwort, die Datensätze zu lesen, zu bearbeiten, auszuwerten und zu nutzen. Das Gleiche gilt auch für einen elektronischen Fernabruf von Daten oder Auswertungen vom Rechenzentrum an die Gemeinde. Dabei wird die Übertragung verschlüsselt und nur an berechtigte Empfänger, die sich mit einem entsprechenden Account angemeldet haben, vorgenommen.

Auf die Gemeindemitgliederdatei können also nur wenige Personen Zugriff nehmen. Die Entscheidung, welche Mitarbeiter zugriffsberechtigt sein sollen und somit ein Passwort zum Start der Software oder des Fernabrufs erhalten, obliegt nach § 5 Abs. 6 Satz 4 KMAO dem Pfarrer bzw. dem verantwortlichen Leiter der Gemeinde. Auf Grund der Sensibilität der Daten und zur Vermeidung unautorisierter Veränderungen und Löschungen eines Teils des Datenbestandes, sollte nur ein kleiner Kreis von Personen Zugriff hierauf erhalten. In der Regel reicht es aus, wenn der Pfarrer selbst und die für ihn arbeitende Pfarrsekretärin zugriffsberechtigt sind.

Außer ihnen sind noch weitere Personen hauptamtlich in der Seelsorge der Gemeinde tätig, insbesondere Diakone, Pastoral- und Gemeindereferenten. Für sie reicht es im Allgemeinen aus, wenn ihnen lediglich ein Teil der Informationen durch entsprechende Auswertungen zur Verfügung gestellt werden, die sie zur Erfüllung ihrer Aufgaben benötigen. Ein Gesamtzugriff auf die Datenbank ist hier normalerweise nicht erforderlich. Das gilt erst recht für ehrenamtliche Helfer.

Alle Mitarbeiter der Gemeinde, die erlaubterweise zur Nutzung der Mitgliederdatei berechtigt sind, müssen die **Verpflichtungserklärung** zur Wahrung des Datengeheimnisses nach § 4 KDO unterschreiben! Dabei ist das Muster aus Ziffer II und III der Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz zu verwenden.

2. Eigene Sicherungsmaßnahmen / Hardwaresicherung

Neben der Gemeindemitgliederdatei werden eine Fülle weiterer Daten gespeichert, verarbeitet und genutzt. Beispielsweise werden Schreiben an Gemeindemitglieder verfasst und separate Adressenlisten über KV- und PGR-Mitglieder geführt. Auch Daten über Gemeindehelfer, Kantoren, Lektoren, Kinder- und Jugendgruppenleiter, Angehörige von Gruppen und Verbänden und viele andere mehr werden in verschiedenen Programmen, außerhalb der Gemeindemitgliederdatei verwaltet. Auch hier handelt es sich oftmals um sensible Informationen, die im Interesse der Betroffenen zu schützen sind. Ihr Schutz umfasst eine Reihe notwendiger Maßnahmen:

1. Schutz vor unautorisierter Nutzung
2. Schutz vor unautorisierter Veränderung des Inhalts der Daten
3. Erhalt der Daten durch Datensicherungsmaßnahmen
4. Schutz vor Viren, Trojanern und anderen schadensstiftenden Programmen
5. "Komplettlöschung" des Datenbestandes bei Entsorgung des PCs

Wie erreicht man diese Ziele? Und vor allem die bange Frage: "Welche Kosten werden hierdurch verursacht?" Das Bundesamt für Sicherheit in der Informationstechnik hat vor kurzem eine informative Broschüre zu diesen Fragen herausgegeben. Im Dezember 2015 erschien unter dem Titel "Sichere Nutzung von PCs unter Microsoft Windows 7 – Empfehlungen für kleine Unternehmen und Selbstständige" eine auch für Computer-Laien sehr gut verständliche Anleitung, die Empfehlungen vom Erwerb eines Systems über die erste Inbetriebnahme, die regelmäßige Nutzung bis hin zur Entsorgung eines alten Gerätes umfasst. Die Broschüre kann im Internet kostenlos geladen werden, unter der Anschrift:

https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_003.html

Auch auf der Internetseite des Diözesandatenschutzbeauftragten wird unter der Rubrik >Themen - Computer (PC)< auf diese Schrift hingewiesen und ein entsprechender Link zur Verfügung gestellt. Hier kann nur noch einmal der Hinweis wiederholt werden, dass für kleinere Einrichtungen, die nicht über einen Systemadministrator verfügen und daher in Eigenleistung ihre Systeme sichern müssen, die Broschüre eine **Pflichtlektüre** darstellen sollte.

Viele Hilfsmittel sind bereits in Windows 7 integriert danach kostenlos oder gegen geringe Gebühr zu erhalten. Hierzu zählt das BSI zum Beispiel:

- „Personal Firewall“ als Teil von Windows 7 integriert
- "Backup and Restore" als Teil von Windows 7 zur Datensicherung
- Vorhandene Auto-Update-Funktion
- "Threatfire" zur verhaltensbasierten Erkennung von Schadprogrammen
- "BitLocker Drive Encryption" zur Verschlüsselung der Festplatte bei den Versionen ‚Ultimate‘ und ‚Enterprise‘
- „VeraCrypt“ als kostenlose freie Verschlüsselungssoftware

Sicherheit scheitert heute keineswegs mehr an dem Argument, sie sei zu teuer und 'das können wir uns nicht leisten'.

Wer lieber Computer mit Apples Betriebssystem OS X einsetzt, kann seit Mitte Oktober 2012 vom Bundesamt für Sicherheit in der Informationstechnik die Schrift "Sichere Nutzung von Macs unter Apple OS X Mountain Lion" kostenlos herunterladen. Sie hat die gleiche inhaltliche Ausrichtung wie die Empfehlung für Windows PCs, allerdings abgestimmt auf das Betriebssystem von Apple. Erreichbar ist diese Schrift unter der Adresse

https://www.bsi-fuer-buerger.de/SharedDocs/Downloads/DE/BSIFB/Publikationen/BSIe010-Mac_OS_X_Mountain_Lion.pdf

Auch die Wahl eines geeigneten Internet- und E-Mail-Providers sollte bestimmte Voraussetzungen erfüllen.

- Schutz vor Internet Kriminalität durch Botnetze
  (Ein Test des eigenen Rechners kann unter https://botfrei.de/teilnhmer.html durchgeführt werden.)
- Bereitstellung von E-Mail Virenfiltern
- Schutz vor Spam-Mails
- Unterstützung sicherer Verbindungen unter "https", "pop3s", "imaps" und "smtps"

Alle eingesetzten Rechner, auf denen personenbezogene Daten gespeichert und bearbeitet werden, müssen mit den genannten Sicherheitsvorkehrungen ausgestattet sein. Das gilt auch dann, wenn private Hardware genutzt werden soll. **Ein privater Rechner darf nicht zur Schwachstelle des gesamten Systems werden!** Auf Grund der rechtlichen Situation, die einen Zugriff des Dienstgebers auf einen im privaten Eigentum stehenden PC verhindert und ein Betreten der Privaträume, ohne Zustimmung des Mitarbeiters ausschließt, kann eine dienstliche Nutzung von Privatgeräten nur auf Grund einer eingehenden schriftlichen Vereinbarung gestattet werden. Diese sollte vor allem zu folgenden Fragen Regelungen enthalten:

- Welche Daten dürfen auf dem PC gespeichert und verarbeitet werden?
- Dürfen auch seelsorgliche Daten auf der privaten Hardware verarbeitet werden?
- Dürfen auch dienstliche Mails auf dem Privatrechner empfangen und bearbeitet werden?
- Welche Programme werden zum Schutz dieser Daten eingesetzt?
- Wer ist für deren regelmäßige Aktualisierung verantwortlich?
- Erfolgt eine Speicherung zugleich oder in regelmäßigen Abständen auch auf dem Dienstrechner?
- Falls nicht, welche Möglichkeit besteht für den Dienstgeber, sich Kenntnis von den Daten zu verschaffen?
- Wie wird sichergestellt, dass die Daten nicht durch unautorisierte Personen gesehen werden? (Das gilt auch für die eigene Familie)

- Was geschieht, wenn die Daten nicht mehr benötigt werden? Übertragung auf den Dienstrechner und vollständige Löschung auf dem Privat-PC?
- Kann der Datenschutzbeauftragte auch diese Datenverarbeitung prüfen?
- Was geschieht bei einem Verlust des Rechners?

Bei der Lektüre wird schnell deutlich, dass sich diese Fragen nicht von allein beantworten. Sie setzen ein Gespräch mit dem Mitarbeiter, in dem dieser seine Vorstellungen über den Umgang und den Schutz der Daten mitteilt und eine für beide Seiten tragbare Einigung voraus. Diese sollte schriftlich erfolgen, damit jederzeit nachweisbar ist, was vereinbart wurde.

IV. Veröffentlichung von Mitgliederdaten

1. Veröffentlichung von Altersjubiläen und Sakramentsspendung

Die Veröffentlichung von Altersjubiläen und Sakramentsspendungen im gedruckten Pfarrbrief der Gemeinde, war in letzter Zeit wieder mehrfach Gegenstand von Beschwerden der Betroffenen. So beschwerte sich eine Dame darüber, dass ihre Freunde und Bekannten durch die Veröffentlichung nun ihr wahres Alter erfahren haben. Andererseits beschweren sich auch Menschen, die in der Geburtstagsliste vergessen wurden. Eine für alle befriedigende Lösung wird es wohl kaum geben. Daher sei an dieser Stelle noch einmal darauf hingewiesen, was aus datenschutzrechtlicher Sicht zulässig ist. Die seelsorgerische Verantwortung bleibt davon unberührt.

a) Veröffentlichung von Geburtstagen

Bei der Veröffentlichung von Geburtstagen ist es in der Regel nicht möglich, die Betroffenen einzeln anzusprechen und deren Einwilligung einzuholen. Es ist auch noch immer so, dass der weit überwiegende Teil der Senioren Wert darauf legt, zu erfahren, dass die Gemeinde an ihrem Ehrentag an sie denkt und sie in ihre Gemeinschaft mit einbezieht. Dies umso mehr, als viele Senioren aus gesundheitlichen Gründen nicht mehr zur Kirche kommen können und der Pfarrbrief oft den einzigen Kontakt mit der Gemeinde darstellt. Für diese Fälle hat sich daher die „Widerspruchslösung“ bewährt: Im Pfarrbrief ist einmal jährlich darauf hinzuweisen, dass die Veröffentlichung von Geburtstagen bestimmter Altersjahrgänge geplant sei. Diejenigen, die dieses nicht wünschen, werden gebeten, dem Pfarrbüro hierüber Mitteilung zu geben. Personen, die einer Veröffentlichung widersprochen haben, sind aus der Veröffentlichungsliste zu streichen. Der nachfolgende Text hat sich bewährt:

> *„Wir beabsichtigen, im Laufe des Jahres die Geburtstage der über 70-Jährigen im Pfarrbrief zu veröffentlichen. Betroffene, die dies nicht wünschen, sollten dem Pfarrbüro rechtzeitig vor dem Termin schriftlich oder telefonisch Bescheid geben.“*

Die Veröffentlichung soll, wegen der damit verbundenen Gefahr der Begehung von Straftaten (z.B. Einbruchdiebstahl), und der Möglichkeit unerwünschter Werbung ohne Angabe der vollständigen Wohnanschrift erfolgen, also etwa in der folgenden Weise:

80 Jahre *Margarethe Müller, Pastor-Schmitz-Weg*

Der Wegfall der Hausnummer führt hier in der Regel schon zum gewünschten Erfolg.

Keinesfalls dürfen Personen veröffentlicht werden, für die ein Sperrvermerk im Datensatz eingetragen ist! Sollten sie dennoch ausnahmsweise mit einbezogen werden, ist dies zuvor mit ihnen persönlich zu klären!

b) Veröffentlichung von Sakramentsspendungen

Im Vorfeld von Sakramentsspendungen besteht ein intensiver Kontakt zwischen der Gemeinde und den Sakramentenempfängern bzw. ihren Sorgeberechtigten. So gehen der Spendung der Kommunion und der Firmung in der Regel länger dauernde Vorbereitungskurse voraus. Auch bei Taufen, Eheschließungen und Begräbnissen gibt es zuvor Gespräche mit den Betroffenen (Taufgespräch, Eheseminar, etc.). Bei dieser Gelegenheit können daher auch die Modalitäten einer Veröffentlichung / Bekanntgabe im Pfarrbrief mit den Beteiligten unmittelbar besprochen werden. Eine „Widerspruchslösung“ wie bei der Veröffentlichung von Geburtstagen ist daher hier nicht ausreichend. Bei einer, der oben geschilderten Gelegenheiten sollte deshalb darauf hingewiesen werden, dass es in der Gemeinde üblich und auch aus theologischer Sicht wünschenswert bzw. notwendig sei, die Gemeinde über die geplante / erfolgte Sakramentsspendung zu informieren. Dabei ist auch darauf hinzuweisen, in welcher Form dies geschieht. Von den Beteiligten hat dann jeder die Möglichkeit, sich hierzu zu äußern. Will sich jemand tatsächlich ausschließen, muss dies allerdings respektiert werden.

Die gleichen Grundsätze gelten auch für Ehejubilare (Silberne, Goldene Hochzeit). Hier wird eine Veröffentlichung ohnehin nur in Betracht kommen, wenn das Fest auch innerhalb der Kirche gefeiert wird.

2. Veröffentlichung / Bekanntgabe von Kirchenaustritten

Eine öffentliche Bekanntgabe von Kirchenaustritten durch Veröffentlichung im Pfarrbrief, Verlesung oder Aushang ist **strikt unzulässig!** Sie verletzt das verfassungsmäßig garantierte Recht der negativen Bekenntnisfreiheit und das kirchenrechtlich geschützte Recht auf Wahrung der Intimsphäre (can. 220 CIC). Es kann weder nach staatlichem Recht noch theologisch Aufgabe der Kirchengemeinde sein, Menschen als konfessionslos zu outen oder gar kirchliche Straftaten (Abfall vom Glauben) bekannt zu geben. Das seelsorgerische Gespräch im Einzelfall wird hierdurch nicht betroffen. Es liegt im Verantwortungsbereich des Seelsorgers und seinem pflichtgemäßen Ermessen, ob er hierüber das Gespräch mit dem Betroffenen sucht.

Eine Bekanntgabe gegenüber Angehörigen ist nur dann zulässig, wenn sie zur Erfüllung des kirchlichen Auftrages erforderlich ist (§ 12 Abs. 1 KDO). Dies bedeutet im Ergebnis, dass es auch hier dem pflichtgemäßen Ermessen des Pfarrers überlassen bleiben muss, ob er eine derartige Mitteilung aus pastoralen Gründen für zwingend erforderlich hält. Dabei sollte berücksichtigt werden, dass es auch unter seelsorgerischen Gesichtspunkten angebracht ist, zunächst das Gespräch oder den brieflichen Kontakt mit dem aus der Gemeinschaft Ausgetretenen zu suchen. Familiärer Zwang löst keine Glaubensprobleme!

Es wird dringend empfohlen, auch bei der Bekanntgabe des Kirchenaustritts gegenüber Angehörigen restriktiv zu verfahren!

3. Hauswerbung Kirchenzeitung

Die Kirchenzeitung (Kirchenbote) erscheint im Auftrage des Bischofs. Sie hat Anteil am seelsorgerischen Auftrag der Kirche. Zur Erfüllung ihres Auftrages muss sie Leser gewinnen und gezielt Werbung durchführen. Die hierbei genutzten Daten sind für seelsorgerische Zwecke erhoben und gespeichert worden, so dass keine Durchbrechung der Zweckbindung vorliegt. Der Kirchenzeitung (Kirchenbote) dürfen daher gemäß § 11 Abs. 1 Ziff. 1 KDO Namen, Vornamen und Anschriften von Kirchengemeindemitgliedern überlassen werden. Bei einer Werbeaktion ist jedoch darauf zu achten, dass nur diejenigen Personen angesprochen werden, die nicht bereits Bezieher der Kirchenzeitung sind.

Soll an den Haustüren der Gemeindemitglieder für den Bezug, der im Auftrag des Bischofs erscheinenden Kirchenzeitung geworben werden, so sind zunächst die allgemeinen datenschutzrechtlichen Regeln einzuhalten, an die hier noch einmal erinnert werden soll.

1. Folgende Daten der katholischen Haushaltsvorstände können auf Anforderung der KiZ aus dem Gemeindemitgliederverzeichnis übermittelt werden: Vor- und Zuname, Anschrift, Geburtsdatum, Geschlecht und Familienstand. Die Daten dürfen nur für die Hauswerbung verwendet werden und sind spätestens sechs Monate nach Abschluss der Werbeaktion dauerhaft physikalisch zu löschen.
2. Die übermittelten Daten können mit den Bestandsdaten der Abonnentendatei abgeglichen werden.
3. Die Werber erhalten, jeweils für ihren Bezirk, Listen mit den Namen und Anschriften der Personen, die sie aufsuchen wollen. Die Listen sind nach Bearbeitung vollständig an die Kirchenzeitung zurückzugeben. Den Werbern ist untersagt, sich hiervon Kopien zu fertigen oder die Daten für andere Zwecke, als zur Durchführung der Werbemaßnahme zu verwenden. Über das Datengeheimnis (§ 4 KDO) sind sie zu belehren. Vor Aushändigung der Listen ist von ihnen die Verpflichtungserklärung nach § 4 KDO zu unterschreiben.
4. Bei der Einschaltung von Fremdunternehmen ist darauf zu achten, dass diese sich schriftlich zur Einhaltung der Vorschriften der Anordnung über den kirchlichen Datenschutz – KDO verpflichten. Die Vorschriften über die Auftragsdatenverarbeitung (§ 8 KDO) sind zu beachten.
5. Vor Durchführung der Werbeaktion ist den Pfarrämtern rechtzeitig eine schriftliche Anzeige über die geplante Maßnahme, unter Angabe des Zeitraums in dem sie durchgeführt werden soll, zu übersenden.

Probleme bestehen dann, wenn bei einem Gemeindemitglied ein Sperrvermerk wegen Gefahr für Leib und Leben eingetragen ist. Diese Daten können auch innerhalb des kirchlichen Bereichs nicht ohne Rücksprache und Zustimmung der Betroffenen weitergegeben werden. Zu berücksichtigen ist dabei, dass trotz des Vertrauens in die Integrität der eingesetzten Werber ein Missbrauch dieser Daten niemals vollständig ausgeschlossen werden kann.

In den anderen Fällen, steht die Datenübermittlung nicht im Widerspruch zum Schutzzweck des jeweiligen Sperrvermerks. Übermittelt werden können also die oben angegebenen Daten der katholischen Haushaltsvorstände, soweit nicht ein Sperrvermerk nach § 21 Abs. 5 MRRG eingetragen ist.

Diese Regelung gilt nur für die Kirchenzeitung, nicht jedoch für überregionale Zeitungen, die der Kirche nahestehen, da eine klar erkennbare Zuordnung zu einer kirchlichen Stelle nicht besteht. Im Übrigen nehmen diese Zeitschriften – im Gegensatz zur Kirchenzeitung – am allgemeinen Wettbewerb mit ähnlichen Presseerzeugnissen teil. Im Übrigen sollten auch schriftliche Empfehlungen für die Werbung von anderen Zeitungen und Zeitschriften von den Pfarrämtern nicht ausgestellt werden.

4. Weitergabe von Daten in anderen Fällen

Nach § 5 Abs. 5 KMAO hat jedes Pfarramt zu gewährleisten, dass die melderechtlichen Sperrvermerke entsprechend ihrem Zweck beachtet werden. Das bedeutet, dass

1. selbstverständlich das Adoptionsgeheimnis aus §§ 61 Abs. 2 Personenstandsgesetz (PStG), 1758 Bürgerliches Gesetzbuch (BGB) zu schützen ist. In Fällen, in denen inzwischen erwachsene Kinder die Person ihrer leiblichen Eltern ausfindig machen wollen, sind diese an die zuständigen Standesämter zu verweisen. Solche Ermittlungen gehören nicht zum Aufgabenbereich der Kirche.
2. der § 61 Abs. 3 PStG in Verbindung mit dem Gesetz über die Änderung der Vornamen und die Feststellung der Geschlechtszugehörigkeit (Transsexuellengesetz) zu beachten ist. Dort geregelte gesetzliche Auskunftspflichten an Behörden müssen jedoch befolgt werden.
3. bei Gefahren für Leib oder Gesundheit des Betroffenen mit diesem möglichst in einem persönlichen Gespräch geklärt werden sollte, wie in bestimmten Fällen verfahren werden soll. Ist eine gesprächsweise Klärung nicht möglich, käme auch ein Anschreiben in Frage. Es ist hier allerdings kaum möglich, eine allgemein gültige Empfehlung zu geben. Die Gründe für die Eintragung einer solchen Sperre reichen vom Schutz vor „Stalking“ bis hin zu politischen oder polizeilichen Geheimnisträgern.
4. bei Personen mit Auskunftssperre nach § 22 Abs. 2 MRRG (Ehe- und Altersjubiläen) eine Veröffentlichung im Pfarrbrief oder der Kirchenzeitung zu unterbleiben hat. Darüber hinaus ist wie bisher einmal im Jahr auf eine geplante Veröffentlichung hinzuweisen, damit auch Gemeindemitglieder ohne entsprechende Sperre die Möglichkeit haben, einer Bekanntgabe ihres Jubiläums zu widersprechen.

In jedem Fall ist ein hohes Maß an Fingerspitzengefühl erforderlich und bei der Vorgehensweise sicherzustellen, dass der Schutzzweck der jeweiligen Auskunftssperre erreicht wird.

V. Der Internetauftritt der Gemeinde

Viele Pfarrgemeinden besitzen heute auch eine eigene Webpräsenz. Ein solcher Internetauftritt wirft eine Reihe von Fragen aus den Bereichen des Datenschutz- und Urheberrechts auf. Zur Unterstützung der Dienststellen hat das Sekretariat der Deutschen Bischofskonferenz eine ausführliche Arbeitshilfe veröffentlicht.

→ **Internetpräsenz - Arbeitshilfe Nr. 234 vom 22. Juni 2009**

Diese Schrift sollte in jedem Fall ausführlich zur Kenntnis genommen werden. Sie kann auf der Webseite der Deutschen Bischofskonferenz als Printversion bestellt oder heruntergeladen werden.

http://www.dbk-shop.de/de/Deutsche-Bischofskonferenz/Arbeitshilfen/Internetpraesenz-.html

Sie ist auch auf der Internetseite des Diözesandatenschutzbeauftragten zu erhalten, allerdings nur in elektronischer Form, als PDF-Datei.

http://www.datenschutz-kirche.de/sites/default/files/file/download/ah_234.pdf

In dieser Arbeitshilfe soll daher nur auf einige datenschutzrechtlich wesentliche Punkte eingegangen werden.

1. Zu beachtende Vorschriften

Das kirchliche Selbstverwaltungsrecht ist gebunden an die Schranken, der für alle geltenden Gesetze. Hierzu gehören auch das Telemediengesetz (TMG) und das Kunsturhebergesetz (KunstUrhG).

Von den Vorschriften des Telemediengesetzes sind folgende Vorschriften zu beachten:

- § 5 TMG (Pflicht zur Erstellung eines Impressums)
- § 6 TMG (für den Fall einer kommerziellen Kommunikation)
- § 7 TMG (Verantwortlichkeit für eigene und fremde Inhalte)
- § 11 TMG (Anbieter-Nutzer-Verhältnis)
- § 13 TMG (Pflichten des Dienstanbieters) hier insbesondere die Pflicht zur Erstellung einer Datenschutzerklärung, Abs. 1 die Pflicht zur Kennzeichnung von Links auf andere Webseiten, Abs. 5
- § 15 TMG (Erhebung und Verwendung der Nutzungsdaten)
- § 16 TMG (Bußgeldvorschriften)

Die Beachtung dieser Vorschriften ist in einer besonderen Arbeitshilfe zum Thema "Das neue Telemediengesetz (TMG) - Pflichten für kirchliche Internetanbieter bei der Gestaltung von Webseiten" dargestellt, so dass hierauf Bezug genommen werden kann. Die Broschüre kann auf der Webseite des Diözesandatenschutzbeauftragten als PDF-Datei heruntergeladen werden.

http://www.datenschutz-kirche.de/sites/default/files/file/download/tmg-280607.pdf

2. Veröffentlichung personenbezogener Daten auf der Webseite

Die Übermittlung personenbezogener Daten an nicht kirchliche Stellen ist nach § 12 KDO an bestimmte Voraussetzungen gebunden. Im vorliegenden Falle kommt noch erschwerend hinzu, dass eine Veröffentlichung im Internet an einen nicht feststehenden und daher nicht bestimmbaren Empfängerkreis erfolgt. Eine solche Bekanntgabe ist daher in der Regel

- zur Erfüllung der Aufgaben der Pfarrgemeinde nicht erforderlich und
- erfolgt nicht für die Zwecke, für die die Daten erhoben worden sind.

Sie können daher nur mit Einwilligung der Betroffenen eingestellt werden (§ 3 Abs. 1 Nr. 2 KDO). Eine allgemein gehaltene Formulierung ist hierfür nicht ausreichend. § 3 Abs. 2 KDO verpflichtet die veröffentlichende Stelle, den Betroffenen auf den Zweck der Nutzung hinzuweisen und sich auf der Grundlage der Freiwilligkeit, **schriftlich** bestätigen zu lassen, dass die Betroffenen hiermit einverstanden sind. Eine Einwilligungserklärung könnte also wie folgt lauten:

"Über meine Person sollen folgende Daten ..... im Internet auf der Webseite der Katholischen Pfarrgemeinde St. Peter unter der Adresse "www.st-peter-pfarrei.de" in allgemeiner Form und somit für jeden Nutzer sichtbar, veröffentlicht werden. Über die Gefahren und die Missbrauchsmöglichkeiten einer Bekanntgabe im Internet bin ich unterrichtet.

Ich willige hierin ein. Meine Einwilligung kann ich jederzeit frei widerrufen. In diesem Fall wird die Pfarrgemeinde, die über mich veröffentlichten Daten sofort von der Internetseite entfernen.

D-dorf, den ..... Unterschrift"

3. Veröffentlichungen von Bildern im Internet

a) Berichte von Gemeindefesten, etc. mit Fotos im Internet

Vor einer Online-Veröffentlichung von Bildern von Gemeindemitgliedern, Besuchern und Mitarbeitern ist grundsätzlich die Einwilligung der Betroffenen einzuholen. Dies gilt für die Einstellung von Fotos von Einzelpersonen und Gruppen ebenso, wie für Fotos von Feiern und anderen Veranstaltungen.

Rechtsgrundlage sind die §§ 22, 23 Kunsturhebergesetz (KunstUrhG). Hierin heißt es:

> ***§ 22 Recht am eigenen Bilde***
>
> *Bildnisse dürfen nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Die Einwilligung gilt im Zweifel als erteilt, wenn der Abgebildete dafür, dass er sich abbilden ließ, eine Entlohnung erhielt. Nach dem Tode des Abgebildeten bedarf es bis zum Ablaufe von 10 Jahren der Einwilligung der Angehörigen des Abgebildeten. Angehörige im Sinne dieses Gesetzes sind der überlebende Ehegatte oder Lebenspartner und die Kinder des Abgebildeten und, wenn weder ein Ehegatte oder Lebenspartner noch Kinder vorhanden sind, die Eltern des Abgebildeten.*
>
> ***§ 23 Ausnahmen zu § 22***
>
> *(1) Ohne die nach § 22 erforderliche Einwilligung dürfen verbreitet und zur Schau gestellt werden:*
> 1. Bildnisse aus dem Bereiche der Zeitgeschichte;
> 2. Bilder, auf denen die Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen;
> 3. Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben;
> *4.* Bildnisse, die nicht auf Bestellung angefertigt sind, sofern die Verbreitung oder Schaustellung einem höheren Interesse der Kunst dient.
>
> *(2) Die Befugnis erstreckt sich jedoch nicht auf eine Verbreitung und Schaustellung, durch die ein berechtigtes Interesse des Abgebildeten oder, falls dieser verstorben ist, seiner Angehörigen verletzt wird.*

Von den Ausnahmetatbeständen kommen im kirchlichen Bereich nur die Ziffern 2 und 3 in Betracht. Aber selbst dann, wenn diese Voraussetzungen vorliegen, ist die Frage zu stellen, ob hierdurch ein berechtigtes Interesse des Abgebildeten verletzt wird. Dabei ist zu berücksichtigen, dass das Internet ein weltweites Kommunikationsmedium ist, das der Veröffentlichung eine wesentlich größere Verbreitung ermöglicht, als eine gedruckte Publikation. Zudem können Fotos, die in einfacher Form auf die Website gestellt werden, jederzeit heruntergeladen und mit Bildbearbeitungsprogrammen bearbeitet und verändert werden. Die Betroffenen können also nicht mehr abschätzen, wer, wann, wie und bei welcher Gelegenheit von ihren Fotos Gebrauch macht oder sie gar zu völlig anderen Zwecken missbraucht. Daher ist für Bildveröffentlichungen im Internet **in allen Fällen** die Zustimmung der abgebildeten Personen erforderlich.

b) Sonderfall Kindergärten und Schulen

Auch Kindertagesstätten präsentieren sich zunehmend mit Fotos im Internet. Zu den oben beschriebenen Gefahren kommt hier hinzu, dass das Internet zunehmend auch zur Verbrei-

tung von Kinderpornographie genutzt wird. Unabhängig vom Vorliegen eines der Ausnahmetatbestände des § 23 KunstUrhG ist in diesen Fällen die Zustimmung der Sorgeberechtigten zwingend erforderlich. Die Erklärung ist schriftlich zu erteilen und muss sich jeweils auf den konkreten Einzelfall beziehen. Eine generelle Einwilligung im Aufnahmevertrag ist unzulässig und rechtlich unwirksam.

Hierzu hat die Konferenz der Datenschutzbeauftragten im Bereich der Katholischen Kirche Deutschlands gemeinsam mit der Konferenz der Datenschutzbeauftragten der evangelischen Landeskirchen im Februar/März 2008 eine gemeinsame Erklärung herausgegeben.

http://www.datenschutz-kirche.de/sites/default/files/file/download/Gemeinsame_Erklaerung.pdf

Wichtig zu wissen:

Die Verbreitung von Bildern entgegen den Vorschriften des Kunsturhebergesetzes kann gem. § 33 Abs. 1 KunstUrhG mit einer Freiheitsstrafe von bis zu einem Jahr oder mit einer Geldstrafe geahndet werden.

VI. Kommunikationstechniken

1. Regelungen zum Telefongebrauch

In Deutschland gilt seit jeher das Fernmeldegeheimnis. Es ist durch Art. 10 des Grundgesetzes besonders geschützt, wobei sich dieses Grundrecht gegen den Staat richtet. Telefongesellschaften sind durch § 88 Telekommunikationsgesetz (TKG) hieran gebunden. § 206 Abs. 5 Satz 2 StGB bestimmt hierzu: *„Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.“*

a) Einzelverbindungsnachweis - § 99 Telekommunikationsgesetz (TKG)

Eine Möglichkeit, festzustellen, ob jemand an einem Telekommunikationsvorgang beteiligt war, ist der Einzelverbindungsnachweis (EVN) nach § 99 TKG. In Pfarrämtern kann dieser von dem Pfarrer schriftlich bei der Telefongesellschaft angefordert werden. Hierbei ist allerdings Mitarbeitervertretungsrecht zu beachten. Nach § 99 Abs. 1 Satz 4 TKG legt fest, dass *„Bei Anschlüssen in Betrieben und Behörden ist die Mitteilung nur zulässig, wenn der Teilnehmer in Textform erklärt hat, dass die Mitarbeiter informiert worden sind und künftige Mitarbeiter unverzüglich informiert werden und dass der Betriebsrat oder die Personalvertretung entsprechend den gesetzlichen Vorschriften beteiligt worden ist oder eine solche Beteiligung nicht erforderlich ist.“*

Zunächst sollte dabei entschieden werden, ob im heutigen Zeitalter der „Flatrates“ überhaupt ein EVN erforderlich ist. Die Kosten der Telekommunikation hängen danach nicht mehr von der Häufigkeit und der Länge der Gespräche ab. Wird ein EVN nicht angefordert, besteht datenschutzrechtlich kein Problem.

Wird er erstellt, sind drei Gesprächsmöglichkeiten zu unterscheiden:

1. das normale Dienstgespräch
2. die Beratungsgespräche von Personen, die der Schweigepflicht nach § 203 StGB unterliegen, und
3. die als Privatgespräche einzustufenden Verbindungen.

Für die Erfassung von normalen Dienstgesprächen unter Zi. 1, bestehen datenschutzrechtlich keine Einschränkungen. Die Verschwiegenheitspflicht von Personen, die nach Zi. 2 Beratungsgespräche führen, umfasst auch den Umstand, dass jemand Kontakt zu Ihnen aufgenommen hat. Daher könnte ein EVN zu einer unbefugten Offenbarung führen. Es sollten daher für diesen Zweck eigenständige Rufnummern eingerichtet werden. Ein EVN für diese Nummern erfolgt entweder nicht, oder zumindest nach § 99 Abs. 1 Satz 2 TKG nur unter der Verkürzung der Teilnehmernummer des Anrufers um die letzten drei Ziffern. Soweit das Führen von Privatgesprächen nach Zi. 3 über den Gemeindeanschluss zumindest in gerin-

gem Umfang erlaubt wird, ist den Mitarbeitern vor Auswertung des EVN Gelegenheit zu geben, die privat angerufenen Teilnehmernummern zu schwärzen. Nur so bleibt ihr informationelles Selbstbestimmungsrecht hierbei gewahrt.

b) Nichtanzeige von Beratungsgesprächen in fremden Einzelverbindungsnachweisen - § 99 Abs. 2 TKG

Der Einzelverbindungsnachweis darf nach § 99 Abs. 2 TKG nicht Verbindungen zu Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen erkennen lassen, die grundsätzlich anonym bleibenden Anrufern ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit besonderen Verschwiegenheitsverpflichtungen unterliegen. Die Pfarrei kann daher bei der Bundesnetzagentur einen Antrag stellen, in die entsprechende Liste aufgenommen zu werden, die von den Telefongesellschaften regelmäßig abzufragen und bei Erstellung des EVN zu berücksichtigen ist. Vorzulegen ist hierfür die Bescheinigung des Bistums, dass sie eine entsprechende Beauftragung erhalten haben. Die Betroffenen werden insoweit geschützt, als das Gespräch nicht in einem EVN fremder Anschlüsse zum Beispiel dem des Arbeitgebers der betreffenden Person sichtbar ist.

Hat man für Beratungsgespräche eine eigene Rufnummer eingerichtet, kann dies auch durch Unterdrückung der eigenen Rufnummernmitteilung geschehen.

2. Verwendung des Faxanschlusses

Der Versand von Schriftstücken über Telefax stellt eine offene Übermittlung dar. Bei Übertragung von Schreiben mit personenbezogenem Inhalt ist daher besonders vorsichtig und sorgfältig zu verfahren. In der Regel und das gilt insbesondere für Daten, die der Verschwiegenheitspflicht unterliegen, ist die Übermittlung per Fax nur statthaft

- in unbedingt notwendigen Eilfällen, wo der Postweg zu lange dauert,
- in Absprache mit dem Empfänger, der die sofortige Übernahme der Sendung sicherstellt, damit das übertragene Schreiben nicht von Dritten gelesen werden kann.

Die Empfehlungen zum "Datenschutz bei der Übermittlung personenbezogener Daten über Telefaxgeräte" sind unbedingt zu beachten!

3. Einrichtung von Mail-Konten, Wahrung des Fernmeldegeheimnisses

E-Mails sind elektronische Briefe, die über ein Netzwerk, meist das Internet übertragen werden und entweder als reine Textdatei oder in HTML-Form verfasst sind. Beim Diözesandatenschutzbeauftragten machen Mails inzwischen den weit überwiegenden Teil der Schriftkommunikation aus. Sie haben sich auch in anderen Bereichen allgemein zum Standard entwickelt und die normale Post weitgehend verdrängt. Die Vorteile liegen auf der Hand. Zum einen, ermöglichen Mails einen wesentlich schnelleren Austausch untereinander, ande-

rerseits sind sie wesentlich kostengünstiger. Wer einmal einen Internetanschluss besitzt, kann sie ohne zusätzliche Berechnung übertragen, wobei auch die hierfür benötigten Programme „Open Source“ sind und somit kostenlos installiert werden können. Andrerseits weist die EMail-Nutzung eine Reihe von rechtlichen Problemen auf.

a) Abgrenzung „Dienstliche E-Mails“ - „Private E-Mails“

Dienststellen, die Ihren Mitarbeitern auch die private Nutzung des E-Mail-Services erlauben, werden hierdurch zu Diensteanbietern im Sinne von § 11 Telemediengesetz (TMG). Die Vorschrift nimmt von der Geltung der Datenschutzvorschriften nur Mails aus, soweit diese „im Dienst- und Arbeitsverhältnis zu ausschließlich beruflichen oder dienstlichen Zwecken“ verwendet werden. Einem privaten E-Mail-Absender ist der Dienstgeber zur Wahrung des Fernmeldegeheimnisses verpflichtet. Vom Inhalt solcher Mails darf er keine Kenntnis erhalten. Das ist praktisch nur sicherzustellen entweder durch die Einrichtung separater E-Mail-Adressen für die private Nutzung oder durch die Erlaubnis einen eigenen Webmail-Service nutzen zu dürfen.

Bei dienstlichen E-Mails darf der Dienstgeber im gleichen Maße vom Inhalt Kenntnis nehmen, wie vom normalen dienstlichen Schriftverkehr. Ausnahmen bestehen insoweit

- für Mails der Mitarbeitervertretung, der Schwerbehindertenvertretung sowie der Frauen- bzw. Gleichstellungsbeauftragten,
- bei Beschäftigten, denen in ihrer Tätigkeit persönliche Geheimnisse anvertraut werden und die deshalb in einem besonderen Vertrauensverhältnis zu den betroffenen Personen stehen, muss eine Kenntnisnahme des Arbeitgebers vom Inhalt der Nachrichten und den Verkehrsdaten, die einen Rückschluss auf die betroffenen Personen zulassen, ausgeschlossen werden.

Hierzu hat der Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im September 2007 eine „Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz“ veröffentlicht, die im Anhang abgedruckt ist.

b) Übermittlung personenbezogener Daten bei Standard-Versand

Die Mail-Übertragung erfolgt meist als offene, unverschlüsselte Text- oder HTML-Datei. Hierfür sind bestimmte Netzwerkprotokolle erforderlich. Dabei sind für den Empfang „POP3“ und „IMAP“ vorgesehen, für den Versand „SMTP“. Die elektronische Post durchläuft dabei eine nicht vorhersehbare Strecke durch das Netz. Anders ausgedrückt, ein Mail das in Hannover abgeschickt wird und einen anderen Empfänger in der gleichen Stadt erreichen soll, kann durchaus über Afrika nach China, die USA und wieder nach Europa transportiert werden, bevor es hier den Empfänger erreicht. Mit geeigneten Softwaretools kann ein böswilliger Internetteilnehmer diese Mails abfangen, lesen, bearbeiten und anschließend in ver-

fälschter Form weiterschicken. Dabei lässt sich der Mail-Transport - im Gegensatz zur Briefpost - auf technisch einfache Art nach bestimmten Stichworten durchsuchen und auswerten.

Zudem werden Mails meist bei einem Dienstleister gespeichert und sind dort als offene Post les- und bearbeitbar. Die Sicherheit eines derartigen Mails ist daher nicht größer, sondern eher noch geringer als bei einer Postkarte! Das führt dazu, dass eine Übermittlung personenbezogener Daten, vertraulicher Inhalte und Informationen, die der Verschwiegenheitspflicht unterliegen, in dieser Form **strikt unzulässig** ist.

Dennoch wird häufig die Weiterleitung personenbezogener Daten per Mail-Versand wegen der Unkompliziertheit des Verfahrens, seiner Schnelligkeit und der direkten Zustellung beim Empfänger angestrebt. Wie kann dieses Vorhaben in datenschutzgerechter Weise verwirklicht werden?

c) Übermittlung bei geschützter Übertragung

Die Verbindungen beim Empfang oder Versand von E-Mails lassen sich verschlüsseln. Äußerlich erkennbar ist dies daran, dass die URL im Browserfenster mit „https://“ beginnt. Der Zusatz „s“ kennzeichnet dabei eine vom Seitenbetreiber eingesetzte SSL/TLS-Verschlüsselung (Secure Socket Layer oder Transport Layer Security), die ein sicheres Übertragen der Nachrichten ermöglicht. Das geschieht direkt beim Verbindungsaufbau, also noch bevor irgendwelche Daten verschickt werden. Die hierbei benutzten Protokolle werden ebenfalls um ein „s“ erweitert und somit als „POP3S“, „IMAPS“ und „SMTPS“ bezeichnet. Wichtig dabei ist, dass der eigene Rechner diese Protokolle verarbeiten kann. **Hierzu muss in den Einstellungen des Mail-Programms die Verschlüsselung „SSL“, „TLS“ oder „Start-TLS“ aktiviert sein!** Hierbei sind die Vorgaben des Mail-Providers zu beachten.

Hierdurch wird Folgendes erreicht:

- Schutz der Vertraulichkeit - Lesbarkeit nur für den Empfänger
- Schutz der Authentizität - Das Mail stammt wirklich vom Absender
- Schutz der Integrität - Keine Veränderung des Mails nach dem Absenden

Die geschützte Übertragung ist jedoch vom Anbieter abhängig. Viele Anbieter sehen sie inzwischen vor. Bei Banken, Warenkorbsystemen und anderen empfindlichen Bereichen ist dies heute Standard. Leider hilft das aber nicht beim freien E-Mail-Verkehr, wo keine Sicherung des Anbieters vorhanden ist. Hier hilft es nur weiter, wenn man selbst eine Verschlüsselung einsetzen kann.

d) Verschlüsselte E-Mail-Kommunikation mit S/MIME oder GPG

S/MIME (Secure/Multipurpose Internet Mail Extensions) ist eine Standard-Anwendung für die Verschlüsselung von E-Mails. Sie ist in allen gängigen Browsern (Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, usw.) integriert. Allerdings lässt sie sich nur mit einem vom Anbieter erstellten Zertifikat nutzen. Dabei werden 3 Zertifikatsklassen unter-

schieden. Klasse 1 bezieht sich nur darauf, dass die E-Mail-Adresse wirklich besteht, Klasse 2 sichert darüber hinaus zu, dass das Mail von einer bestimmten Person oder Einrichtung versandt wurde, in Klasse 3 muss sich der Absender sogar persönlich ausweisen. Schwierigkeiten hierbei können sich daraus ergeben, dass kostenlos erteilte Zertifikate (z.B. von CAcert) von vielen Browsern nicht als vertrauenswürdig eingestuft werden und eine entsprechende Fehlermeldung hervorrufen.

Eine kostenfreie Lösung ist die Benutzung von Gpg4Win, die zunächst als Erweiterung in den Mail-Browser installiert werden muss. Mit ihr lassen sich vom Anwender zwei Schlüssel erstellen, der „Public Key“ der dazu dient, dass der Absender seine Nachricht hiermit verschlüsselt und der „Private Key“ mit dem der Empfänger die Nachricht entschlüsseln kann. Der Public Key kann allgemein bekannt gegeben werden, beispielsweise durch Veröffentlichung auf der eigenen Webseite. Der Private Key muss vom Anwender geheim gehalten werden. Das Prinzip ist einleuchtend: Ich verschlüssele die Nachricht mit dem Public Key des Empfängers und der kann sie nur mit Hilfe seines Private Keys entschlüsseln und somit lesbar machen. Die Public Keys anderer Teilnehmer kann ich in Gpg4Win speichern, so dass schon mit Betätigung des „Senden“-Buttons das Mail-Programm automatisch eine Verschlüsselung durchführt, so dass ich in der täglichen Arbeit durch dieses Verfahren nicht behindert werde. Auch die Geschwindigkeit mit das Mail versandt wird, ändert sich hierbei nur unwesentlich. Eine Anleitung zur Benutzung ist auf der Webseite des Bundesamtes für Sicherheit in der Informationstechnik zu erhalten.

https://www.bsi.bund.de/DE/Themen/ProdukteTools/Gpg4win/gpg4win_node.html

e) Personenbezogene Daten im verschlüsselten E-Mail-Anhang

Bei einem ständigen Korrespondenzpartner, wie zum Beispiel einem Mitglied des Kirchenvorstandes, dem Vorstand des Gemeindekindergartens und ähnlichen Fällen, gibt es eine einfache und praktisch wirksame Möglichkeit zur vertrauensvollen Übertragung sensibler Daten, wie zum Beispiel nicht-öffentlicher Protokolle.

Die vertrauenswürdigen Daten werden normal mit einer Textverarbeitung erstellt. Die dabei entstandene Datei wird in ein, meist kostenlos erhältliches ZIP-Programm kopiert, das nicht nur den Anhang komprimiert sondern bei entsprechender Einstellung auch verschlüsselt. Das Passwort zur Entschlüsselung darf dabei dem Empfänger nicht durch das E-Mail bekannt gegeben werden. Es kann aber bei einem gemeinsamen Treffen oder telefonisch vereinbart werden. Wird so verfahren, sollte den Programmen der Vorzug gegeben werden, die mit einer vollständigen, mindestens mit 128 Bit AES-Verschlüsselung arbeiten.

- **Beispiele** für entsprechende freie Software: AxCrypt, FileCrypter, PDF-Creator und andere
- **nicht jedoch:** FreePDF von Adobe (nur rudimentäres Verschlüsselungsverfahren)

Dieses Verfahren funktioniert auch plattformunabhängig. Dabei ist es egal, ob der Empfänger einen Windows-, Apple- oder Linux-Rechner einsetzt.

Risiken des allgemeinen E-Mail-Austauschs

- Unsicherer Übertragungsweg
- Möglichkeit des Abfangens und Veränderns
- Daher kein „grenzenloses“ Vertrauen in die Richtigkeit des Inhalts
- Offene Postfachlagerung beim Provider
- Zuverlässigkeit des Mail-Dienstes wird durch Anfertigung von Kopien der Mails durch den Anbieter hergestellt.
- Möglichkeit nach schneller Auswertung auf Grund einer Stichwortsuche
- Keine Unterschrift auf E-Mails! Rechtlich daher: **Fehlende Beweiskraft!**

Sicherungen

- **Verschlüsselte Übertragung!**
- Sichere Webseiten (https://...)
- S/MIME durch SignCard, SignTrust, etc. (in der Regel kostenpflichtig)
- PGP/GPG-Verschlüsselung (kostenlos, Open Source Software)
- Einsatz von kostenlosen ZIP-Programmen zur Verschlüsselung des Anhangs

Weitere Informationen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) betreibt auch eine Internetseite „BSI für Bürger“. Hier findet sich eine Fülle von Hinweisen für Ihre Sicherheit:

- Gefahren des Online-Banking
- Einkaufen im Internet (worauf beim Online-Shopping zu achten ist)
- Rechtsprobleme rund um Internet, Handy & Co
- Kinderschutz (wichtig für die Kinderpastoral!)
- Suchmaschinen
- Soziale Netzwerke

Die Website www.klicksafe.de ist Bestandteil des Safer Internet Programms der Europäischen Union. Hier gibt es zu vielen aktuellen Themen Broschüren und weitere Informationen.

VII. Vernichtung / Löschung

1. Vernichtung von Schriftgut

Schriftstücke, sonstige EDV-Ausdrucke, Abfallpapiere und Altpapiere, die ausgesondert werden können, sind so zu vernichten, dass personenbezogene Daten vor Missbrauch geschützt sind. Es ist dafür zu sorgen, dass bei der Vernichtung des auszusondernden Aktengutes, Altpapiers etc. die Daten nicht mehr lesbar sind. Für den Alltag des Pfarrbüros reicht hierfür meist ein eigener Shredder, wie er im Bürofachhandel vertrieben wird, aus.

DIN 32757-1 unterscheidet 5 Sicherheitsstufen. Dabei sollte die Stufe 2 nicht unterschritten werden. Eine Reproduktion von max. 6 mm breiten Streifen ist nur mit technischen Hilfsmitteln und unter großem Zeitaufwand möglich. Sie wird empfohlen für internes, nicht besonders vertrauliches Schriftgut.

Besser und inzwischen meist auch Standard bei gewerblichen Aktenvernichtern ist die Sicherheitsstufe 3, mit einer Streifenbreite maximal 2 mm oder einem "Cross Cut", bei dem zusätzlich ein zweiter, waagerechter Schnitt vorgenommen wird von max. 4 mm Breite. Sie wird empfohlen bei vertraulichem Schriftgut. Besonders schützenswerte Daten, die dem Seelsorge- oder Sozialgeheimnis unterliegen, sind **in jedem Fall** nach Stufe 3 zu vernichten.

Die höheren Sicherheitsstufen werden von der DIN 32757-1 empfohlen für geheim zuhaltendes Schriftgut (Stufe 4) oder maximale Sicherheitsanforderungen (Stufe 5) und dürften im pfarramtlichen Bereich kaum vorkommen.

Berücksichtigt werden sollte auch, dass die Sicherheit bei der Aktenvernichtung nicht nur von der Streifenbreite abhängig ist, sondern auch von der Menge des zu vernichtenden Materials. Bei dem Zerreißprozess werden die einzelnen Seiten durcheinandergewirbelt und miteinander vermischt. Wird nur ein einzelnes Blatt vernichtet ist eine anschließende Wiederzusammenfügung relativ einfach, da bekannt ist, dass alle Teile zusammengehören und nur in der richtigen Reihenfolge wieder sortiert werden müssen. Werden große Mengen Papier zur gleichen Zeit vernichtet, ist das erheblich schwieriger. Zur Steigerung der Sicherheit sollten also zu festgelegten Zeitpunkten größere Mengen zugleich vernichtet werden. Erreicht werden kann das vor allem in der Weise, dass auszuscheidendes Material zunächst in einen Sicherheitsbehälter gegeben wird und später dann gemeinsam zerschreddert wird.

2. Vernichtung von Einmalfarbbändern und Kohlepapier

Oft wird für Mehrfachdrucke Endlospapier mit Kohlepapiereinlagen benutzt. Das Kohlepapier wird nur einmal benutzt, so dass auf ihm die Texte in Spiegelschrift gelesen werden können. Daher ist Kohlepapier, das beim Ausdrucken personenbezogener Daten benutzt wurde, in gleicher Weise durch Aktenvernichter zu entsorgen wie sonstige Unterlagen mit personen-

bezogenen Daten. Bei Schreibmaschinen mit Einmalfarbbändern sind die geschriebenen Texte ebenfalls leicht rekonstruierbar. Volle Farbbandkassetten sind daher zu sammeln und zuverlässig zu vernichten.

3. Beauftragung von Fremdunternehmen

Die Vernichtung großer Mengen von Altmaterial durch Büromaschinen ist meist zu umständlich, da diese in der Regel nur 4 bis 8 Seiten in einem Arbeitsgang vernichten können. Zudem müssen die zu vernichtenden Dokumente zuvor von Fremdkörpern, wie Büroklammern befreit werden, um das Mahlwerk nicht zu beschädigen. Deshalb werden für größere Aktenvernichtungen meist gewerbliche Anbieter mit entsprechend großen Aktenvernichtungsanlagen eingeschaltet. Dabei ist folgendes zu beachten:

- Es handelt sich um eine Auftragsdatenverarbeitung im Sinne von § 8 KDO
- Es ist daher eine schriftliche Vereinbarung, die das angewandte Verfahren festlegt, zu schließen (Hierfür kann das Muster hierfür auf der Webseite "www.datenschutz-kirche.de/node/47" verwendet werden.)
- Dabei sind zumindest die Sicherheitsstufe, das Verfahren der Bereitstellung des Materials, die Übernahme, der gesicherte Transport bis zur endgültigen Vernichtung und die Verschwiegenheitspflicht der Mitarbeiter zu regeln.
- Der Auftragnehmer hat dabei auch die Regeln des kirchlichen Datenschutzes, insbesondere die §§ 4 und 6 KDO zu beachten.

Meist wird das Material gebündelt an den Auftragnehmer abgegeben. Dieser hat sich dabei schriftlich verpflichtet jeden Missbrauch auszuschließen. Wichtig ist besonders darauf zu achten, dass das zu vernichtende Papiergut beim Verladen, Transport oder Bündeln nicht verlorengeht.

Für eine Vernichtung von Dokumenten, deren Inhalt der strafrechtlichen Verschwiegenheitspflicht nach § 203 StGB unterliegen, wie die Familien-, Ehe-, Erziehungs- und Jugendberatungen, Suchtberatungen und Schwangerschaftsberatungen reicht das jedoch nicht aus! Die Wahrung dieser Geheimnisse setzt voraus, dass der Berater **ausschließt**, dass andere, nicht autorisierte Personen vom Inhalt dieser Dokumente Kenntnis erlangen können. Bei einer Übergabe an den Auftragnehmer ist diese Voraussetzung jedoch nicht gewährleistet. Daher kommt nur ein Verfahren in Frage, bei dem das zu vernichtende Material in einem verschlossenen Spezialcontainer gesammelt wird, um anschließend in einer fahrbaren Vernichtungsanlage **vor Ort und in Beisein des Auftraggebers** eingefüllt und vernichtet wird.

4. Löschen von Daten auf Magnetplatten, Bändern und Disketten

Löschen bedeutet das Unkenntlichmachen gespeicherter Daten. Die Betätigung der Löschtaste auf dem PC reicht hierfür nicht aus. Die betroffene Datei wird lediglich, unter Verkürzung des ersten Buchstabens ihres Namen in den Papierkorb des Rechners verschoben und

ist dort jederzeit wiederherstellbar. Auch ein Leeren des Papierkorbs hat lediglich zur Folge, dass die Datei nicht mehr vom Verwaltungssystem des Rechners auf der Festplatte oder einem anderen Datenträger gefunden wird. Es ist so, als würde man ein Buch im Regal einer Bibliothek stehen lassen und lediglich die Karteikarte zum Auffinden des Buches vernichten. Das Buch ist damit keineswegs gelöscht. Mit sogenannten Datenrettungsprogrammen sind auch solche Dateien im großen Umfange wieder aufzufinden und zu reaktivieren.

Im Falle der Beseitigung des Rechners insgesamt sollte daher überlegt werden, ob die Datenträger nicht ausgebaut und vollständig körperlich zerstört werden können.

Für den Fall, dass nur einzelne Dateien vernichtet werden sollen, der PC und die Datenträger aber weiterhin benutzt werden sollen, stehen eine Reihe, meist kostenloser Programme, die ein endgültiges und unwiderrufliches Löschen bei Anwendung mehrerer Verfahren unterstützen. Einen guten Überblick mit Downloadmöglichkeit gibt die Seite vom Heise Verlag:

http://www.heise.de/download/sicherheit/sicheres-loeschen-50000505307/

24. September 2007

Arbeitskreis Medien[1]

Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz

Viele Beschäftigte im öffentlichen Dienst haben heute die Möglichkeit, das Internet auch am Arbeitsplatz zu nutzen. Öffentliche Stellen des Bundes und der Länder haben beim Umgang mit den dabei anfallenden personenbezogenen Daten der Beschäftigten, ihrer Kommunikationspartner und anderer Betroffener (beispielsweise Dritter, deren Namen in einer E-Mail genannt werden) bestimmte datenschutzrechtliche Anforderungen zu beachten, die davon abhängen, ob den Bediensteten neben der dienstlichen die private Nutzung des Internet am Arbeitsplatz gestattet wird. E-Mail und andere Internetdienste sind geeignet, das Verhalten und die Leistung der Beschäftigten zu überwachen. Die Orientierungshilfe stellt die bei der Nutzung dieser Dienste geltenden datenschutzrechtlichen Anforderungen dar.

I. Allgemeines

a. Bei der Nutzung von E-Mail und anderen Internetdiensten durch die Beschäftigten sind die eingesetzten Verfahren technisch so zu gestalten, dass von vornherein so wenige personenbezogene Daten wie möglich verarbeitet werden (Grundsatz von Datenvermeidung und Datensparsamkeit). Hierzu bietet es sich an, datenschutzfreundliche Verfahren einzusetzen. Ebenso ist die Kontrolle der Nutzung dieser Dienste durch den Arbeitgeber[2] so zu gestalten, dass sie zunächst ohne, zumindest aber mit so wenigen personenbezogenen Daten wie möglich durchgeführt wird. Dabei sind präventive Maßnahmen gegen unbefugte Nutzung nachträglichen Kontrollen vorzuziehen.

b. Die Bediensteten sind mit den technischen Möglichkeiten vertraut zu machen, wie die eingesetzten Verfahren datenschutzgerecht angewendet werden können. Um Art und Umfang der Verarbeitung ihrer personenbezogenen Daten nachvollziehen zu können, sind die Bediensteten umfassend darüber zu informieren (Grundsatz der Transparenz).

c. Es sind geeignete Maßnahmen zu treffen, um die Vertraulichkeit und Integrität der Kommunikation zu gewährleisten. Insbesondere sollte jeder internetfähige PC mit leicht bedienbarer, auch bei den Kommunikationspartnern vorhandener Verschlüsselungssoftware ausgestattet sein, um zu verhindern, dass aus Be-

[1] Die Orientierungshilfe wurde unter Beteiligung des AK Personalwesen erstellt. Sie richtet sich in erster Linie an öffentliche Stellen des Bundes und der Länder. Die hier dargestellten Grundsätze können auch auf den nicht-öffentlichen Bereich übertragen werden.

[2] Zur Vereinfachung bezeichnet „Arbeitgeber“ sowohl den Arbeitgeber als auch den öffentlich-rechtlichen Dienstherren

quemlichkeit personenbezogene oder andere sensible Daten unverschlüsselt übertragen werden.

d. Automatisierte zentrale und wegen einer Verschlüsselung auch lokale Virenchecks sind notwendig. Um aktive Inhalte zu überprüfen, empfiehlt sich der Einsatz von lokaler Sandbox-Software.

e. Es gibt eine Vielzahl an Möglichkeiten zur Abwehr unerwünschter Nachrichten (Spam), die in verschiedensten Kombinationen und Ausprägungen eingesetzt werden können. Welche Maßnahmen dafür grundsätzlich in Betracht kommen, kann etwa der Anti-Spam-Studie des BSI[3] entnommen werden. Die auf dieser Grundlage denkbaren Lösungen unterscheiden sich sowohl hinsichtlich ihrer Eignung als auch hinsichtlich des Ausmaßes, in dem sie in die Persönlichkeitsrechte der Kommunikationspartner oder Dritter eingreifen. Daher sollte jede Stelle, bevor sie Maßnahmen zur Spam-Abwehr ergreift, eine schriftliche Konzeption hierfür erstellen, der zu entnehmen ist, dass unter den in Betracht kommenden Varianten die datenschutzfreundlichste gewählt wurde.

   Die Konzeption sollte dabei folgenden Grundsätzen Rechnung tragen:

   - Filter, die Header oder Inhalt elektronischer Post automatisch auf unerwünschte Nachrichten (Spam) prüfen, sollten erst an einem Punkt eingesetzt werden, der außerhalb der Reichweite des Fernmeldegeheimnisses liegt.
   - Die (zentrale) Markierung spamverdächtiger Nachrichten ist dabei der zentralen Löschung von E-Mails ohne Kenntnis des Empfängers vorzuziehen.
   - Um Verletzungen von Vertraulichkeit und Integrität zu vermeiden, sollten die Empfänger der Nachrichten in größtmöglicher Autonomie über den Umgang mit den an sie gerichteten E-Mails selbst entscheiden können.

II. Dienstliche Nutzung

a. Gestattet der Arbeitgeber die Nutzung von E-Mail und Internet ausschließlich zu dienstlichen Zwecken, ist er nicht Anbieter im Sinne des Telekommunikations- (TK-) bzw. Telemedienrechts (vgl. § 11 Abs. 1 Nr. 1 Telemediengesetz, TMG); die Erhebung und Verarbeitung von Daten über das Nutzungsverhalten der Beschäftigten richtet sich in diesen Fällen nach den jeweils einschlägigen, am Erforderlichkeitsmaßstab orientierten Vorschriften des Beamtenrechts sowie des BDSG bzw. der Landesdatenschutzgesetze.

b. Der Arbeitgeber hat grundsätzlich das Recht, stichprobenartig zu prüfen, ob das Surfen bzw. E-Mail-Versenden der Beschäftigten dienstlicher Natur ist. Eine automatisierte Vollkontrolle durch den Arbeitgeber ist als schwerwiegender Eingriff in das Persönlichkeitsrecht der Beschäftigten hingegen nur bei konkretem Missbrauchsverdacht im Einzelfall zulässig. Es wird empfohlen über die Nutzung von E-Mail und Internet eine Dienstvereinbarung mit dem Personalrat abzuschließen, in der die Fragen der Protokollierung, Auswertung

[3] www.bsi.de/literat/studien/antispam/antispam.pdf

und Durchführung von Kontrollen eindeutig geregelt werden. Auf mögliche Überwachungsmaßnahmen und in Betracht kommende Sanktionen sind die Beschäftigten hinzuweisen.

c. Bei Beschäftigten, denen in ihrer Tätigkeit persönliche Geheimnisse anvertraut werden und die deshalb in einem besonderen Vertrauensverhältnis zu den betroffenen Personen stehen, muss eine Kenntnisnahme des Arbeitgebers vom Inhalt der Nachrichten und den Verkehrsdaten, die einen Rückschluss auf die betroffenen Personen zulassen, ausgeschlossen werden.

d. Der Arbeitgeber darf die Nutzungs- und Verkehrsdaten der Personalvertretung, der Schwerbehindertenvertretung sowie der Frauen- bzw. Gleichstellungsbeauftragten u.ä. nur insoweit kontrollieren, als dies im Einzelfall aus Gründen der Kostenkontrolle erforderlich ist. Soweit allerdings nur unerhebliche Kosten bei der Nutzung von Internet und E-Mail anfallen – was überwiegend der Fall sein wird –, ist eine Auswertung dieser Daten unzulässig.

e. Eine Betriebs- oder Dienstvereinbarung kann nur dann als besondere Rechtsvorschrift angesehen werden, wenn die Datenerhebung, -verarbeitung und -nutzung ausreichend und präzise innerhalb des Erlaubnisumfangs gesetzlicher Bestimmungen geregelt wird und sie das gesetzliche Schutzniveau nicht unterschreitet.

f. Im Regelfall sollte darauf verzichtet werden, die Verarbeitung von Protokolldaten auf die Einwilligung der Beschäftigten zu stützen, da sie aufgrund des Abhängigkeitsverhältnisses zum Arbeitgeber nicht immer freiwillig entscheiden können. Nur ausnahmsweise ist auch die Einwilligung der Beschäftigten in eine Verarbeitung der Protokolldaten über die unter a. genannten Vorschriften hinaus möglich. Die Beschäftigten können z. B. die Verwertung ihrer Protokolldaten verlangen, um den Verdacht einer unbefugten Internetnutzung auszuräumen.

g. Soweit die Nutzung von E-Mail und Internet zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherung des ordnungsgemäßen Betriebs der Verfahren protokolliert wird, dürfen diese Daten nach dem BDSG, den Landesdatenschutzgesetzen und dem Beamtenrecht des Bundes und der Länder auch nur zu diesen Zwecken genutzt werden, nicht aber zur Verhaltens- und Leistungskontrolle der Beschäftigten.

h. Von ein- und ausgehenden dienstlichen E-Mails seiner Beschäftigten darf der Arbeitgeber im selben Maße Kenntnis nehmen wie von deren übrigem dienstlichen Schriftverkehr. Beispielsweise könnte der Vorgesetzte verfügen, dass ihm seine Mitarbeiter jede ein- oder ausgehende E-Mail einzeln zur Kenntnis zuleiten.

i. Aus Gründen der Datensicherheit dürfen Teilinhalte oder Anlagen von E-Mails unterdrückt werden, wenn sie ein Format aufweisen, das zu Sicherheitsrisiken auf Rechnern oder im Netzwerk führen kann.

III. Private Nutzung

1. Allgemeines

a. Wenn ein Arbeitgeber den Beschäftigten die private Nutzung von Internet oder E-Mail erlaubt, ist er ihnen gegenüber TK- bzw. Telemediendienste-Anbieter.

b. Vom Arbeitgeber beauftragte Zugangsanbieter (Access Provider) sind zwar diesem gegenüber TK- bzw. Telemediendienste-Anbieter, gegenüber den privat nutzenden Beschäftigten sind die Provider aber lediglich Auftragnehmer des dann als Anbieter zu qualifizierenden Arbeitgebers.

c. Der Arbeitgeber ist gegenüber den Beschäftigten und den Absendern zur Einhaltung des Fernmeldegeheimnisses verpflichtet. Daher gelten die gleichen Bedingungen wie beim privaten Telefonieren.

d. Es gelten die Regelungen der Telekommunikationsgesetzes, des Telemediengesetzes bzw. des Rundfunkstaatsvertrages.

e. Der Arbeitgeber ist nicht verpflichtet, den Beschäftigten die private Nutzung des Internet zu erlauben. Entschließt er sich jedoch dazu, muss es ihm grundsätzlich möglich sein, diese Erlaubnis an einschränkende Voraussetzungen zu knüpfen (z. B. eine angemessene Art der Kontrolle durchzuführen). Beschäftigte, die diese Beschränkungen nicht akzeptieren wollen, können ihre Einwilligung ohne jeden dienstlichen Nachteil verweigern.

f. Der Umfang der privaten Nutzung, ihre Bedingungen sowie Art und Umfang der Kontrolle, ob diese Bedingungen eingehalten werden, müssen – am sinnvollsten durch Dienstvereinbarung oder -anweisung – unter Beteiligung des Personalrats eindeutig geregelt werden.

g. Eine Protokollierung darf ohne Einwilligung erfolgen, wenn sie zu Zwecken der Datenschutzkontrolle, der Datensicherung, zur Sicherung des ordnungsgemäßen Betriebs der Verfahren oder zu Abrechnungszwecken erforderlich ist.

2. Besonderheiten bei E-Mail

a. Private E-Mails sind wie private schriftliche Post zu behandeln. So sind eingehende private, aber fälschlich als Dienstpost behandelte E-Mails den betreffenden Mitarbeitern unverzüglich nach Bekanntwerden ihres privaten Charakters zur alleinigen Kenntnis zu geben.

b. Der Arbeitgeber sollte vor dem Hintergrund des von ihm zu wahrenden Fernmeldegeheimnisses entweder für die Beschäftigten separate E-Mail-Adressen zur privaten Nutzung einrichten oder – falls privates Surfen erlaubt ist – sie auf die Nutzung eines Web-Mail-Dienstes verweisen.

c. Wie bei der dienstlichen Nutzung (s. II.i.) dürfen aus Gründen der Datensicherheit eingegangene private E-Mails oder deren Anhänge unterdrückt werden, wenn sie ein Format aufweisen, das zu Sicherheitsrisiken führen kann.

Die Verfahrensweise ist den Beschäftigten zuvor bekannt zu geben. Generell sind die Beschäftigten darüber zu unterrichten, wenn an sie gerichtete oder von ihnen abgesendete E-Mails ganz oder teilweise unterdrückt werden oder virenverseucht sind. Eine Untersuchung von virenverseuchten E-Mails mit Kenntnisnahme des Inhalts, etwa durch den Systemadministrator, ist nur unter Einbeziehung der betreffenden Beschäftigten zulässig.

d. Eine zentrale Spam-Filterung, bei der automatisch auf den Header oder Inhalte zugegriffen wird, darf nur mit Einwilligung des Empfängers erfolgen, da die Reichweite des Fernmeldegeheimnisses erst endet, wenn die E-Mail in seine vollständige Verfügungsgewalt gelangt ist. Auch dies ist als einschränkende Voraussetzung für die Erlaubnis zur privaten Nutzung (s. o., III.1.e) anzusehen und damit Bestandteil der Einwilligung. Die Einwilligung kann pauschal vorab erfolgen. Die Beschäftigten sind über die Art und Weise der Spam-Filterung, insbesondere über die dabei stattfindende Verarbeitung personenbezogener Daten, zu informieren.

e. Eine darüber hinaus gehende inhaltliche Kontrolle ist nicht zulässig.