Merkblatt
über die Datenschutzbestimmungen der
Evangelischen Kirche der Pfalz (Protestantische Landeskirche)

Zusätzlich zu den schon bestehenden Verpflichtungen, dienstlich erlangte Kenntnisse vertraulich zu behandeln (zum Beispiel § 9 BAT, § 70 des Landesbeamtengesetzes, § 18 des Pfarrerdienstgesetzes), sind für den Datenschutz folgende Rechtsvorschriften zu beachten:

- Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) vom 12. November 1993 (ABl. 1994 S. 14), zuletzt geändert durch das Erste Kirchengesetz zur Änderung des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland vom 7. November 2002 (ABl. 2003 S. 22);
- Datenschutzverordnung der Evangelischen Kirche der Pfalz (Protestantische Landeskirche) - DSVO-Pfalz - vom 30. März 2004 (ABl. S. 89);
- Verordnung zum Schutz von Patientendaten in kirchlichen Krankenhäusern (DSVO KH-Pfalz) vom 15. Januar 1991 (ABl. S. 36), zuletzt geändert durch Verordnung vom 17. Januar 1995 (ABl. S. 41);
- Verordnung zum Schutz vor dem Verlust von in Datenverarbeitungsanlagen gespeicherten Informationen der kirchlichen Dienststellen sowie Werke und Einrichtungen der Evangelischen Kirche der Pfalz (Protestantische Landeskirche) – Datensicherungsverordnung - vom 19. Februar 2002 (ABl. S. 114);
- Verordnung zum Schutz vor missbräuchlicher Einflussnahme durch Computerviren auf Programme und Daten auf Datenverarbeitungsanlagen der kirchlichen Dienststellen sowie Werke und Einrichtungen der Evangelischen Kirche der Pfalz (Protestantische Landeskirche) - Computervirenschutzverordnung - vom 19. Februar 2002 (ABl. S. 115);
- Verordnung zur Verschlüsselung von Daten auf Datenverarbeitungsanlagen der kirchlichen Dienststellen sowie Werke und Einrichtungen der Evangelischen Kirche der Pfalz (Protestantische Landeskirche) – Datenverschlüsselungsverordnung - vom 19. Februar 2002 (ABl. S. 117);
- Ordnung für die Führung der Kirchenbücher (Kirchenbuchordnung) vom 22. Mai 2002 (ABl. S. 174);
- Verordnung über die Nutzung von rechnergestützten Kommunikationseinrichtungen in Pfarrämtern und anderen Dienststellen im Bereich der Evangelischen Kirche der Pfalz (Protestantische Landeskirche) vom 28. September 2004 (ABl. S. 264).

In gleicher Weise sind künftige Rechts- und Verwaltungsvorschriften der Evangelischen Kirche in Deutschland und der Evangelischen Kirche der Pfalz (Protestantische Landeskirche) zu beachten.

Zweck des kirchlichen Datenschutzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Das Merkblatt informiert über einige wichtige Regelungen aus dem Datenschutzbereich. Die Erläuterungen und Hinweise müssen im jeweiligen Zusammenhang, der sich aus der täglichen Arbeit und den jeweils geltenden Rechtsvorschriften ergebenden Anwendungsfragen gesehen werden. Jede Mitarbeiterin und jeder Mitarbeiter trägt für die rechtmäßige Ausübung der jeweiligen Tätigkeit die datenschutzrechtliche Verantwortung.

Für den Schutz personenbezogener Daten gelten insbesondere folgende Grundsätze:

1. Personenbezogene Daten dürfen nur für die rechtmäßige Erfüllung kirchlicher Aufgaben erhoben, verarbeitet und genutzt werden. Maßgebend sind die durch Rechtsnormen oder Herkommen be-

stimmten Aufgabenbereiche; dazu gehören etwa die Verkündigung, Seelsorge, Unterweisung, Diakonie, Mission sowie der Bereich der kirchlichen Verwaltung. Grundregel für den Umgang mit personenbezogenen Daten ist, dass er durch eine Rechtsvorschrift oder die Einwilligung der Betroffenen oder einen anderen besonderen Tatbestand nach den §§ 4 Abs. 2 oder 5 Abs. 2 DSG-EKD gedeckt sein muss. Einzelheiten sind u. a. den §§ 1 bis 5 und den §§ 11 bis 13 DSG-EKD zu entnehmen. Personenbezogene Daten sind Einzelangaben über persönliche Verhältnisse (z. B. Name, Geburtsdatum, Anschrift, Konfession, Beruf, Familienstand) oder sachliche Verhältnisse (z.B. Grundbesitz, Rechtsbeziehungen zu Dritten) einer bestimmten oder bestimmbaren natürlichen Person (zum Beispiel Gemeindeglieder, kirchliche Mitarbeiter/Mitarbeiterinnen).

2. Alle Informationen, die ein haupt-, neben- oder ehrenamtlicher kirchlicher Mitarbeiter/eine haupt-, neben- oder ehrenamtliche kirchliche Mitarbeiterin aufgrund seiner/ihrer Arbeit an und mit Dateien (zum Beispiel Listen und Karteien) erhält, sind von ihm/ihr vertraulich zu behandeln. Diese Pflicht besteht auch nach Beendigung seines/ihres Dienstverhältnisses oder Ehrenamtes fort.
3. Soweit in einem Personalcomputer (PC) personenbezogene Daten eingegeben oder mit ihm verarbeitet oder genutzt werden, sind die technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit zu beachten. Personenbezogene Daten oder Datenkategorien (zum Beispiel Belege, Karteikarten, Magnetkarten, Magnetbänder, Magnetplatten, Disketten, CDs, Datenverarbeitungsanlagen) sind stets sicher und verschlossen zu verwahren und vor jeder Einsicht oder sonstigen Nutzung durch Unbefugte zu schützen.
4. Personenbezogene Daten oder Datenkategorien dürfen nur kirchlichen Mitarbeiterinnen/Mitarbeitern zugänglich gemacht werden, die aufgrund ihrer dienstlichen Aufgaben zum Empfang der Daten ermächtigt und unter Aushändigung dieses Merkblattes ausdrücklich zur Einhaltung des Datenschutzes verpflichtet worden sind.
5. Auskünfte aus Datensammlungen (Dateien), Duplizierungen von Disketten und Magnetbändern sowie Abschriften oder Ablichtungen von Listen und Karteien u.a. dürfen nur erteilt und angefertigt werden, wenn es zur Erfüllung kirchlicher Aufgaben erforderlich ist und die Voraussetzungen des Datenschutzes beim Empfänger/bei der Empfängerin vorliegen (siehe auch Nr. 1). Auf keinen Fall dürfen personenbezogene Daten an Dritte weitergegeben oder zur Einsichtnahme bereitgehalten werden, wenn eine geschäftliche oder gewerbliche Verwertung der Daten zu befürchten ist. Widersprüche von betroffenen Personen, die sich gegen eine Erhebung, Verarbeitung oder Nutzung ihrer personenbezogenen Daten richten, sind nach Maßgabe des § 16 Abs. 4 DSG-EKD zu beachten.
6. Datenbestände (zum Beispiel Dateien, Listen und Karteien), die durch neue ersetzt und auch nicht aus besonderen Gründen weiterhin benötigt werden, müssen in einer Weise vernichtet oder gelöscht werden, die jeden Missbrauch der Daten ausschließt; vor allem dürfen die Daten Unbefugten nicht zugänglich werden können.
7. Mängel beim Datenschutz, der Datensicherung und der ordnungsgemäßen Datenerhebung, -verarbeitung und -nutzung sind dem/der jeweiligen Vorgesetzten unverzüglich anzuzeigen. Es können auch die oder der Betriebsbeauftragte für den Datenschutz, die oder der örtlich Beauftragte für den Datenschutz und sonstige mit dem Datenschutz befasste Stellen zur Beratung herangezogen werden, sofern diese bestellt sind.
8. Den bei der Datenverarbeitung beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten oder zu nutzen (Datengeheimnis). Verstöße gegen das Datengeheimnis sind Verletzungen der Dienstpflicht i.S. des Disziplinarrechts und der arbeitsrechtlichen Vorschriften und können Schadenersatzansprüche des Dienstherrn oder Dritter begründen.
9. Eine Einsicht in Kirchenbücher, die seit dem 1. Januar 1876 geführt werden, darf Dritten nicht gewährt werden. Bei Auskünften aus Kirchenbüchern ist zu beachten, dass diese aus Kirchenbüchern, die seit dem 1. Januar 1876 geführt werden, nur an Berechtigte und auf Antrag erfolgen dürfen. Daten, die in staatlichen Personenstandsregistern geführt werden, sind bei den dafür zuständigen staatli-

chen Stellen zu erfragen. Auskünfte zu Zwecken der Familienforschung über noch lebende Personen dürfen nicht erteilt werden.

10. Bestimmte Handlungen, die einen Verstoß gegen das Datengeheimnis beinhalten, werden durch das Strafgesetzbuch mit Strafe bedroht. Auf die Straftatbestände § 303a („Datenveränderung“), § 303 b („Computersabotage“), § 202 a („Ausspähen von Daten“) und § 263 a („Computerbetrug“) wird besonders hingewiesen. Danach kann bestraft werden, wer rechtswidrig Daten verändert oder beseitigt, wer den Ablauf der Datenverarbeitung einer Behörde oder eines Wirtschaftsunternehmens stört, wer sich oder einem/einer Dritten unbefugt besonders gesicherte Daten aus fremden Datenbanksystemen verschafft sowie wer fremdes Vermögen durch unbefugtes Einwirken auf einen Datenverarbeitungsvorgang schädigt.

11. Nach urheberrechtlichen Bestimmungen (§ 106 UrhG in Verbindung mit § 69 a UrhG) ist die Vervielfältigung lizensierter Softwareprodukte und deren Weitergabe an Dritte sowie die Eigennutzung von Raubkopien strafbar. Die zeitlich parallele Mehrfachnutzung eines Originaldatenträgers und/oder davon angefertigter Sicherungskopien sowie die Mehrfachnutzung über ein Netzwerk ist unzulässig, sofern vertraglich nichts Anderes vereinbart worden ist. Insbesondere ist der Einsatz privater Programme auf einem dienstlichen Personalcomputer (PC) nicht zulässig.