Merkblatt über den Datenschutz
der Evangelischen Kirche der Pfalz

Für den Datenschutz innerhalb
der Evangelischen Kirche der Pfalz
sind zu beachten:

Bereichsspezifische Datenschutzbestimmungen

1. Besondere Bestimmungen über den Schutz des Beicht- und Seelsorgegeheimnisses, die Amtsverschwiegenheit sowie sonstige gesetzliche Geheimhaltungs- und Verschwiegenheitspflichten oder von Berufs- bzw. besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen.
2. Besondere Regelungen in kirchlichen Rechtsvorschriften, die auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind.

Allgemeine Datenschutzbestimmungen

1. Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD)
2. Verordnung zur Durchführung des Kirchengesetzes über den Datenschutz der EKD
3. Verordnung über den Einsatz von elektronischer Datenverarbeitung in der kirchlichen Verwaltung in der Fassung der Bekanntmachung
4. Dienst- und Organisationsanweisungen für den Einsatz und Betrieb in der Informations- und Kommunikationstechnik (IuK-Technik) sowie für die Durchführung des Datenschutzes und der Datensicherheit, soweit sie von den kirchlichen Körperschaften und Dienststellen erlassen wurden.

Grundsätze des Datenschutzes

Soweit die bereichsspezifischen Datenschutzbestimmungen keine anders lautenden Regelungen enthalten, gelten für den Schutz personenbezogener Daten folgende Grundsätze:

1. 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.

   Personenbezogene Daten dürfen nur für die rechtmäßige Erfüllung kirchlicher Aufgaben erhoben, verarbeitet und genutzt werden. Maßgebend sind die durch das kirchliche Recht bestimmten oder herkömmlichen Aufgaben auf dem Gebiet der Verkündigung, Seelsorge, Diakonie und Unterweisung sowie der kirchlichen Verwaltung (einschließlich Gemeinde- und Pfarrbüro).

   Eine Verarbeitung personenbezogener Daten und deren Nutzung sind grundsätzlich nur zulässig, wenn das DSG-EKD oder eine Rechtsvorschrift sie erlaubt oder anordnet oder soweit die betroffene Person eingewilligt hat.

   Personenbezogene Daten sind Einzelangaben über persönliche Verhältnisse (z. B. Name, Geburtsdatum, Anschrift, Konfession, Beruf, Familienstand) oder sachliche Verhältnisse (z. B. Grundbesitz, finanzielle Belastungen, Rechtsbeziehungen zu Dritten) einer bestimmten oder bestimmbaren natürlichen Person (z. B. Gemeindeglieder, kirchliche Mitarbeitende).

Die Datenschutzregelungen gelten für

- automatisierte Verarbeitungen, darunter versteht man die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen,
- Datensammlungen, die gleichartig aufgebaut sind und nach bestimmten Merkmalen zugänglich sind und ausgewertet werden können (nicht automatisierte Dateien),
- Akten und Aktensammlungen mit einigen Einschränkungen (z.B. §§ 16 Abs. 1 Satz 2, Abs. 5 DSG-EKD).

Einzelheiten, die auch den Umfang des kirchlichen Datenschutzes betreffen, sind dem DSG-EKD zu entnehmen (siehe insbesondere §§ 1-5, 11-13, 23-26).

2. Auskünfte aus Datensammlungen sowie die Übermittlung von personenbezogenen Daten (Abschriften oder Ablichtungen von Listen und Karteien, Kopien aus Akten sowie Duplizierungen von Disketten, Magnetbändern usw.) sind an kirchliche Stellen, andere öffentlich-rechtliche Religionsgesellschaften sowie an Behörden und sonstige öffentliche Stellen des Bundes, der Länder, der Gemeinden etc. zulässig, soweit sie insbesondere zur Erfüllung kirchlicher Aufgaben erforderlich sind (siehe auch § 12 DSG-EKD). Die Datenübermittlung an sonstige Stellen oder Personen ist nur in Ausnahmefällen statthaft (siehe auch § 13 DSG-EKD). Widersprüche von betroffenen Personen, die sich gegen eine Erhebung, Verarbeitung oder Nutzung ihrer personenbezogenen Daten richten, sind zu beachten – Ausnahmen regeln die kirchlichen Vorschriften sowie § 16 Abs. 4a DSG-EKD. Auskünfte zur geschäftlichen oder gewerblichen Verwendung der Daten dürfen ohne Einwilligung der betroffenen Person in keinem Fall gegeben werden. Daten oder Datenträger dürfen nur kirchlichen Mitarbeiterinnen und Mitarbeitern zugänglich gemacht werden, die auf Grund ihrer dienstlichen Aufgaben zum Empfang der Daten ermächtigt worden sind.

3. Alle Informationen, die eine Mitarbeiterin oder ein Mitarbeiter auf Grund ihrer/seiner Arbeit an und mit Akten, Dateien, Listen und Karteien erhält, sind von ihr/ihm vertraulich zu behandeln. Diese Pflicht besteht auch nach Beendigung der Tätigkeit fort.

4. Jede Mitarbeiterin und jeder Mitarbeiter trägt für vorschriftsgemäße Ausübung der jeweiligen Tätigkeit die volle datenschutzrechtliche Verantwortung. Der Umgang mit Daten und Informationen erfordert ein hohes Maß an Verantwortungsbewusstsein. Die sorgsame und vertrauliche Behandlung von Daten ist ein wichtiges Gebot im Rahmen der Informationsverarbeitung. Die Sammlung, Aufbereitung und Verwendung personenbezogener Daten unterliegen einer erhöhten Schutzbedürftigkeit.

   Soweit mit einem Personalcomputer (PC) personenbezogene Daten eingegeben, verarbeitet oder genutzt werden, sind die technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit zu beachten.

   Eigenmächtige Änderungen der Hardware-Konfiguration, insbesondere der Einbau von Karten, Anschluss von Druckern oder anderer Zusatzgeräte sind ebenso wie die

Verwendung privater Hardware und privater Datenträger nicht gestattet. Soweit aus Gründen der Aufgabenerfüllung Daten von dritter Seite mittels eines Datenträgers auf den PC übernommen werden müssen, ist durch geeignete Maßnahmen sicherzustellen, dass die auf dem Datenträger enthaltenen Daten nicht mit Viren befallen sind.

Des Weiteren ist es untersagt

- Änderungen in der bestehenden Konfiguration, insbesondere das Aufspielen zusätzlicher Dateien und Programme, vorzunehmen,
- private Software zu verwenden,
- Programme weiterzugeben oder zu verändern.

Daten, Datenträger, Systemliteratur und Zubehör (z. B. Belege, Karteikarten, EDV-Listen, Magnetbänder, Magnetplatten, Disketten, Schlüssel) sind stets sicher und verschlossen zu verwahren und vor jeder Einsicht oder sonstigen Nutzung durch Unbefugte zu schützen.

Die Regelungen und Hinweise zum Datenschutz und zur Datensicherheit aus bestehenden Dienst- und Organisationsanweisungen sind zu beachten.

5. Datenbestände, insbesondere Dateien, Listen und Karteien, die durch neue ersetzt und auch nicht aus besonderen Gründen weiterhin benötigt werden (z. B. für Prüf- und Archivzwecke), müssen in einer Weise vernichtet oder gelöscht werden, die jeden Missbrauch der Daten ausschließt.
6. Mängel, die bei der Datenerhebung, -verarbeitung und -nutzung auffallen, sind unverzüglich den Vorgesetzten zu melden. Dies gilt auch für den Fall, dass in den Bereichen Datenschutz und Datensicherheit unzureichende organisatorische und technische Maßnahmen ergriffen wurden.
   Soweit vorhanden, können auch die oder der Betriebsbeauftragte für den Datenschutz, die oder der örtlich Beauftragte für den Datenschutz, die DV-Benutzerbetreuung und sonstige mit dem Datenschutz befasste Stellen zur Beratung herangezogen werden.

7. Verstöße gegen das Datengeheimnis können dienst- bzw. arbeitsrechtlich, urheberrechtlich, disziplinarisch und haftungsrechtlich geahndet werden.

Bestimmte Handlungen, die einen Verstoß gegen das Datengeheimnis beinhalten, stellen Straftatbestände dar. Danach kann beispielsweise mit Freiheitsstrafe oder mit Geldstrafe bestraft werden,

- wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis offenbart, dies betrifft insbesondere Ärztinnen und Ärzte, Angehörige eines anderen Heilberufs, z.B. aus dem Krankenpflegebereich, einschließlich ihre und ihrer berufsmäßig tätigen Gehilfen und Personen, die bei ihnen zur Vorbereitung auf den Beruf tätig sind (z.B. Auszubildende), Psychologinnen und Psychologen, Ehe-, Familien-, Erziehungs- oder Jugendberaterinnen und -berater sowie Beraterinnen und Berater für Suchtfragen in einer Beratungsstelle, Mitglieder einer anerkannten Beratungsstelle nach dem Schwangerschaftskonfliktgesetz, Sozialarbeiterinnen und

Sozialarbeiter, Sozialpädagoginnen und Sozialpädagogen, Personen, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnehmen (§ 203 StGB „Verletzung von Privatgeheimnissen“),

- wer sich oder einem Dritten unbefugt besonders gesicherte Daten aus fremden Datenbanksystemen verschafft (§ 202a StGB „Ausspähen von Daten“),
- wer fremdes Vermögen durch unbefugtes Einwirken auf einen Datenverarbeitungsvorgang schädigt (§ 263a StGB „Computerbetrug“),
- wer rechtswidrig Daten verändert oder beseitigt (§ 303a StGB „Datenveränderung“),
- wer den Ablauf der Datenverarbeitung einer Behörde oder eines Wirtschaftsunternehmens stört (§ 303b StGB „Computersabotage“) und
- wer unbefugt Verhältnisse in Steuersachen einschl. fremder Betriebs- oder Geschäftsgeheimnisse offenbart oder verwertet (§ 355 StGB „Verletzung des Steuergeheimnisses“).

Auch weitere Verschwiegenheitsvorschriften und Geheimhaltungspflichten (z. B. dienst- und arbeitsrechtliche Regelungen, Sozialgeheimnis, Brief-, Post- und Fernmeldegeheimnis) sind zu beachten.

8. Das Merkblatt informiert über einige wichtige Regelungen aus dem Datenschutzbereich. Die Erläuterungen und Hinweise müssen im jeweiligen Zusammenhang, der sich aus Anwendungsfragen aus der täglichen Arbeit sowie den jeweils geltenden Rechtsvorschriften ergibt, gesehen werden. Des Weiteren haben Sie sich auch über zukünftige Rechts- und Verwaltungsvorschriften, Dienst- und Organisationsanweisungen zu den Bereichen IuK-Technik, Datenschutz und Datensicherheit zu informieren.