

Merkblatt über den Datenschutz in der Evangelischen Kirche von Westfalen

(Auszug aus dem Kirchlichen Amtsblatt der EkvW Nr. 4 vom 16. Juli 1997, Seite 86)

Für den Datenschutz in der Evangelischen Kirche von Westfalen 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 einschl. deren Veröffentlichung anzuwenden sind (z.B. Verordnung zum Schutz von Patientendaten in kirchlichen Krankenhäusern, Vorsorge- und Rehabilitationseinrichtungen)

Allgemeine Datenschutzbestimmungen

1. Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) vom 12.11.1993 (KABl. 1994 S. 34)
2. Verordnung zur Durchführung des Kirchengesetzes über den Datenschutz der EKD (DSVO) vom 11.06.1997 (KABl. 1997 S. 77).
3. Verordnung über den Einsatz von elektronischer Datenverarbeitung in der kirchlichen Verwaltung in der Fassung der Bekanntmachung vom 13.10.1994 (KABl. 1994 S. 187)
4. Dienst- und Organisationsanweisung 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.

Soweit die bereichsspezifischen Datenschutzbestimmungen keine anderslautenden 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 bestimmbarer natürlichen Person (z.B. Gemeindeglieder, kirchliche Mitarbeiter).

Die Datenschutzregelungen gelten für Datensammlungen, die

- Mit Hilfe der automatisierten Datenverarbeitung vorgehalten und ausgewertet werden können (automatisierte Daten),
- gleichartig aufgebaut sind und nach bestimmten Merkmalen geordnet, umgeordnet und ausgewertet werden können (nicht-automatisierte Daten),
- in Akten und Aktensammlungen enthalten sind.

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 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. Die Datenübermittlung an sonstige Stellen oder Personen ist nur in Ausnahmefällen statthaft und bedarf der vorherigen Zustimmung des Landeskirchenamtes. Auskünfte zur geschäftlichen oder gewerblichen Verwendung der Daten dürfen ohne Einwilligung der betroffenen Personen in keinem Fall gegeben werden. Daten oder Datenträger dürfen nur kirchlichen Mitarbeiterinnen und Mitarbeitern zugänglich gemacht werden, die aufgrund ihrer dienstlichen Aufgaben zum Empfang der Daten ermächtigt worden sind.
3. Alle Informationen, die eine Mitarbeiterin oder Mitarbeiter aufgrund seiner Arbeit an und mit Akten, Dateien, Listen und Karteien erhält, sind von ihm vertraulich zu behandeln. Diese Pflicht besteht auch nach Beendigung der Tätigkeit fort.
4. Jede Mitarbeiterin und jeder Mitarbeiter trägt für vorschriftsmäßige 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 Informationsvereinbarung. Die Sammlung, Aufbereitung und Verwendung per-

sonenbezogener Daten unterliegen einer erhöhten Schutzbedürftigkeit.

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

Eigenmächtige Änderung der Hardware-Konfiguration, insbesondere der Einbau von Karten, Anschluss von Druckern oder anderer Zusatzgeräte sind ebenso wie die Verwendung privater Hardware oder privater Datenträger nicht gestattet. Soweit aus Gründen der Aufgabenerfüllung von dritter Seite mittels eines Datenträgers auf den APC 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 Daten, 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 dem Dienstvorgesetzten 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 Ansprechpartnerin oder der Ansprechpartner für Datenschutzfragen, die ADV-Benutzer-Betreuung und sonstige mit dem Datenschutz befasste Stellen zur Beratung herangezogen werden.

7. Verstöße gegen das Datengeheimnis können 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 sich oder einem Dritten unbefugt besonders gesicherte Daten aus fremden Datenbanksystemen beschafft (§202a StGB „Ausspähen von Daten“),
- wer unbefugt ein fremdes Geheimnis im Rahmen der beruflichen Tätigkeit offenbart (§203 StGB „Verletzung von Privatgeheimnissen“),
- 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- und Geschäftsgeheimnisse offenbart oder verwertet (§ 355 StGB „Verletzung des Steuergeheimnisses“).

Auch weitere Verschwiegenheitsvorschriften und Geheimhaltungspflichten (z.B. dienst- und arbeitsrechtliche Regelungen, Sozialgeheimnis) 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.