

Datenschutz in der Evangelisch-Lutherischen Landeskirche Mecklenburgs

Datenschutzbestimmungen

Für den Datenschutz in der Evangelisch-Lutherischen Landeskirche Mecklenburgs (ELLM) sind zu beachten:

1. Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) vom 12. November 1993 (KABl. 1995 S. 4)
2. Kirchengesetz über die Anwendung des Kirchengesetzes über den Datenschutz der EKD in der Evangelisch-Lutherischen Landeskirche Mecklenburgs (KABL 1997. S. 67)
3. Kirchengesetz über die Kirchenmitgliedschaft, das kirchliche Meldewesen und den Schutz der Daten der Kirchenmitglieder in der Evangelisch-Lutherischen Landeskirche Mecklenburgs vom 4. November 1990 in Änderung vom 19.11.2000 (KABl. 2000 S. 72)
3. 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.
4. Besondere Regelungen in kirchlichen Rechtsvorschriften, die auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind.

In gleicher Weise sind künftige Rechts- und Verwaltungsvorschriften sowie Veröffentlichungen der Evangelischen Kirche in Deutschland und der Evangelisch-Lutherischen Landeskirche Mecklenburgs zum Datenschutz zu beachten.

Grundsätze des Datenschutzes

Dieses Merkblatt versucht nicht, jede erdenkliche Situation zu beschreiben, sondern definiert allgemeine Prinzipien für den Umgang mit Daten und Informationen. Es wird erwartet, dass sich jeder Benutzer, wenn er mit unvorhersehbaren Situationen konfrontiert wird, an diese Prinzipien hält.

Für den Umgang mit personenbezogenen Daten in der Evangelisch-Lutherischen Landeskirche Mecklenburgs gelten insbesondere folgende Grundsätze:

1. Aufgabe der Datenverarbeitung im kirchlichen Bereich ist es, kirchliches Handeln zu fördern. Dabei muss gewährleistet sein, dass der Einzelne beim Umgang mit personenbezogenen Daten nicht 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.

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, wenn das DSG-EKD oder eine andere 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.

Besonders sensibel sollte mit besonderen Arten personenbezogener Daten im Sinne von § 2 Abs. 11 DSG-EKD umgegangen werden.

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.

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

2. Die Übermittlung von personenbezogenen Daten, von Kopien aus Akten und Auskünfte aus Datensammlungen 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 (beachte aber auch die weiteren Vorgaben der §§ 5 und 12 DSG-EKD). Die Datenübermittlung an sonstige Stellen oder Personen ist nur in Ausnahmefällen statthaft (siehe § 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 aufgrund ihrer dienstlichen Aufgaben zum Empfang der Daten ermächtigt worden sind.

3. Über die Verschwiegenheitsverpflichtung des § 8 des Arbeitsvertrages hinaus, sind alle Informationen, die eine Mitarbeiterin oder ein Mitarbeiter aufgrund ihrer / seiner Arbeit an und mit Akten, Dateien, Listen und Karteien erhält, von ihr / ihm vertraulich zu behandeln. Diese Pflicht besteht auch nach Beendigung der Tätigkeit fort.

4. Jede Mitarbeiterin und jeder Mitarbeiter trägt für die 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, insbesondere die in der Anlage zu § 9 DSGVO aufgeführten Kontrollmaßnahmen.

Die Regelungen und Hinweise zum Datenschutz und zur Datensicherheit aus bestehenden Dienst- und Organisationsanweisungen sind zu beachten. Unabhängig davon sind eigenmächtige Änderungen bzw. Erweiterungen der bestehenden Hardware durch Zusatzgeräte ebenso wie die Verwendung privater Hardware und privater Datenträger nicht gestattet. Des Weiteren sind eigenmächtige Änderungen der bestehenden Software, die Verwendung privater Software und die Weitergabe und Veränderung von Programmen untersagt. 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.

Datenträger mit personenbezogenen Daten sind stets sicher zu verwahren und vor jeder Einsicht oder sonstigen Nutzung durch Unbefugte zu schützen.

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. Gleiches gilt für die Verschrottung von PC-Technik mit Speichermedien (Festplatten o.ä.).

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 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 sich oder einem Dritten unbefugt besonders gesicherte Daten aus fremden Datenbanksystemen verschafft (§ 202a StGB „Ausspähen von Daten“),

- 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 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 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.

Die oben erwähnten Datenschutzgesetze finden Sie unter folgenden links:

Datenschutzgesetz EKD: <http://www.kirche-mv.de/fileadmin/ELLM-Gesetze/Verwaltung/DatenschutzgesetzEKD.pdf>

Anwendungsgesetz ELLM: <http://www.kirche-mv.de/fileadmin/ELLM-Gesetze/Verwaltung/DatenschutzAnwendung.pdf>