Anlage 1.2
Merkblatt für den Datenschutz
in der Evangelischen Kirche im Rheinland
für Mitarbeitende

In diesem Merkblatt erhalten Sie einige Informationen über den wesentlichen Inhalt des Datengeheimnisses und den Sinn der Verpflichtungserklärung. Die Erläuterungen und Hinweise müssen im jeweiligen Zusammenhang, der sich aus Anwendungsfragen aus der täglichen Arbeit sowie den jeweils geltenden Rechtsvorschriften ergibt, gesehen werden.

Welche rechtlichen Grundlagen gelten für den Datenschutz?

1. Zunächst gelten die allgemeinen Datenschutzbestimmungen. Die sind jeweils in ihrer geltenden Fassung
   a) das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD),
   b) die Verordnung zur Durchführung des Kirchengesetzes über den Datenschutz der EKD (DSVO),
   c) das IT-Sicherheitskonzept der Evangelischen Kirche im Rheinland in der jeweils aktuellen Fassung,
   d) 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.
2. Außerdem gelten, den allgemeinen Regelungen zum Datenschutz vorgehende, bereichsspezifische Datenschutzbestimmungen, dies sind

a) 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

b) und besondere Regelungen in kirchlichen Rechtsvorschriften, die auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind (z.B. § 20 Friedhofswesenverordung).

Sie finden diese Vorschriften in der Rechtssammlung aus www.kirchenrecht-ekir.de unter den Ordnungsziffern 430 und 432. In gleicher Weise sind künftige Rechts- und Verwaltungsvorschriften sowie Veröffentlichungen der Evangelischen Kirche in Deutschland und der Evangelischen Kirche im Rheinland zu den Bereichen IuK-Technik, Datenschutz und Datensicherheit zu beachten.

Weshalb ist Datenschutz notwendig?

Jeder Mensch hat das Recht, über die Erhebung und weitere Verarbeitung seiner personenbezogenen Daten selbst zu bestimmen. Der Datenschutz verfolgt daher das Ziel, jede einzelne Person davor zu schützen, dass sie durch Umgang mit ihren personenbezogenen Daten in ihren Persönlichkeitsrechten beeinträchtigt wird.

Was sind personenbezogene Daten?

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 oder kirchliche Mitarbeitende).

Welche grundsätzlichen Regelungen gelten für den Datenschutz?

Zunächst gelten die Datenschutzregelungen für

- Datensammlungen, die gleichartig aufgebaut 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) und
- automatisierte Verarbeitungen (§ 1 Abs. 2 DSG-EKD). Darunter versteht man die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen (IT, PC, Laptop ...).

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

1. Eine Verarbeitung personenbezogener Daten und deren Nutzung ist nur zulässig, wenn das DSG-EKD oder eine Rechtsvorschrift dies erlaubt oder anordnet oder soweit die betroffene Person eingewilligt hat.
2. Personenbezogene Daten dürfen nur für die rechtmäßige Erfüllung kirchlicher Aufgaben erhoben, verarbeitet und genutzt werden. Maßgebend sind die herkömmlichen oder durch das kirchliche Recht bestimmten Aufgaben auf dem Gebiet der Verkündigung, Seelsorge, Diakonie und Unterweisung sowie der kirchlichen Verwaltung (einschließlich Gemeinde- und Pfarrbüro).
3. Daten dürfen nur zu dem Zweck verwendet werden, für den sie erhoben oder gespeichert sind (Grundsatz der Zweckbindung). Andere Verwendungen bedürfen einer rechtlichen Grundlage oder der Zustimmung der betroffenen Personen.
4. 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 zulässig an kirchliche Stellen, anderen öffentlich-rechtlichen Religionsgesellschaften sowie an Behörden

und sonstigen öffentlichen Stellen des Bundes, der Länder, der Gemeinden etc., soweit eine Rechtsgrundlage für die Datenübermittlung vorhanden ist und sie zur Erfüllung kirchlicher Aufgaben erforderlich sind (siehe auch § 12 DSG-EKD). Die Datenübermittlung an sonstige Stellen oder Personen ist nur in Ausnahmefallen 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.

5. Alle Informationen, die Mitarbeitende auf Grund ihrer Arbeit an und mit Akten, Dateien, Listen und Karteien erhalten, sind vertraulich zu behandeln. Diese Pflicht besteht auch nach Beendigung der Tätigkeit fort.
6. 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.

Welche Maßnahmen sind aus Gründen des Datenschutzes und zur Datensicherung zu treffen?

1. Wenn mit einer IT-Anlage (z.B. PC) personenbezogene Daten eingegeben, verarbeitet oder genutzt werden, sind die technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit zu beachten (z.B. zum Passwortschutz).
2. Eigenmächtige Änderungen der Hardware-Konfiguration - insbesondere der Einbau von Karten und der Anschluss von Druckern oder anderen Zusatzgeräten - 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.
3. Es ist untersagt, Änderungen in der bestehenden Konfiguration vorzunehmen (insbesondere durch das Aufspielen zusätzlicher Dateien und Programme), private Software zu verwenden, Programme weiterzugeben oder zu verändern und Benutzerkennungen und Passwörter weiterzugeben.

4. 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.
5. Die Regelungen und Hinweise zum Datenschutz und zur Datensicherheit aus bestehenden Dienst- und Organisationsanweisungen sind zu beachten.
6. 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.
7. Mängel, die bei der Datenerhebung, -verarbeitung und -nutzung auffallen, sind unverzüglich dem Vorgesetzten zu melden. Dies gilt auch für den Fall, dass in den Bereichen Datenschutz und Datensicherheit unzureichende organisatorische und technische Maßnahmen ergriffen wurden. Auch der Beauftragte für den Datenschutz der EKD, dem die Aufgabe der Datenschutzaufsicht obliegt, kann kontaktiert werden.

Welche Konsequenzen können im Einzelfall drohen?

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

a) unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihr oder ihm anvertraut wurde in Ausübung der Berufe Ärztin oder Arzt (oder Angehörige oder Angehöriger eines anderen Heilberufs), Psychologin oder Psychologe, Ehe-, Familien-, Erziehungs- oder Jugendberaterin sowie -berater sowie Beraterinnen und Berater für Suchtfragen in einer Beratungsstelle, Mitglieder einer anerkannten Beratungsstelle nach dem Schwangerschaftskonfliktgesetz, Sozialarbeiterinnen und Sozialarbeiter (§ 203 StGB „Verletzung von Privatgeheimnissen“),
b) Schriftstücke oder andere bewegliche Sachen, die sich in dienstlicher Verwahrung befinden oder ihm oder einem anderen dienstlich in Verwahrung gegeben worden sind, zerstört, beschädigt, unbrauchbar macht oder der dienstlichen Verfügung entzieht (§ 133 StGB),
c) unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft (§ 202a StGB „Ausspähen von Daten“),
d) Passwörter Dritten verkauft oder überlässt oder entsprechende Computerprogramme installiert (§ 202c Vorbereiten des Ausspähens und Abfangens von Daten),
e) fremdes Vermögen durch unbefugtes Einwirken auf einen Datenverarbeitungsvorgang schädigt (§ 263a StGB „Computerbetrug“),

f) rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert (§ 303a StGB „Datenveränderung“),

g) den Ablauf der Datenverarbeitung eines anderen oder eines Wirtschaftsunternehmens erheblich stört (§ 303b StGB „Computersabotage“),

h) unbefugt Verhältnisse eines anderen sowie Brief- oder Geschäftsgeheimnisse, die ihm als Amtsträger in Steuersachen bekannt geworden sind, offenbart oder verwertet (§ 355 StGB „Verletzung des Steuergeheimnisses“),

i) Schriftstücke oder andere bewegliche Sachen zerstört, beschädigt, unbrauchbar macht oder der dienstlichen Verfügung entzieht, die sich in amtlicher Verwahrung einer Kirche oder anderen Religionsgesellschaft des öffentlichen Rechts befinden (§ 133 II StGB „Verwahrungsbruch“).

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

Neben strafrechtlichen Folgen drohen bei Verstößen auch dienstrechtliche und arbeitsrechtliche Konsequenzen.

Wo erhält man weitere Auskünfte?

Wenn Sie weitere Fragen zum Datenschutz haben oder in einem Einzelfall eine Rechtsauskunft benötigen, wenden Sie sich an die Dienstvorgesetzten oder an die örtlich Beauftragte oder den örtlich Beauftragten für den Datenschutz bzw. im Bereich der rechtlich selbständigen Diakonie an die Betriebsbeauftragte oder den Betriebsbeauftragten für den Datenschutz. Den Namen und die Kontaktdaten erhalten Sie über die kirchliche Stelle, die Sie für Ihre Aufgabe beauftragt.

Die Aufgaben der Datenschutzaufsicht obliegt der oder dem Beauftragten für den Datenschutz der EKD. Weitere Informationen und die Kontaktdaten erhalten Sie über das Internet unter www.ekd.de/datenschutz.