Anlage 2
(zu § 3)

Merkblatt
Datenschutz und Datensicherheit

Für den Umgang mit personenbezogenen Daten sowie für den Schutz und die Sicherung dieser Daten gelten nachfolgende, rechtsverbindliche Regelungen:

1. Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland in der Neufassung vom 15. November 2017 (DSG-EKD),
2. Rechtsverordnung zur Durchführung des EKD-Datenschutzgesetzes,
3. Verordnung über den Einsatz von Informationstechnologie (IT) in der Evangelisch-Lutherischen Landeskirche Sachsens vom 9. August 2010,
4. Grundgesetz Art. 2 Abs. 1 „Recht auf freie Entfaltung der Persönlichkeit“,
5. Telekommunikationsvorschriften (TKG, TMG),
6. Regelungen des Strafgesetzbuches (insbesondere §§ 201 bis 206, 263 a, 270, 303 a und b, 355 StGB).

Diese Regelungen sowie auf ihrer Grundlage erlassene Richtlinien und alle im Bereich des Diakonischen Werkes geltenden Rechtsvorschriften zum Datenschutz und Datenumgang sind von allen haupt-, neben- und ehrenamtlichen Mitarbeitern zu beachten und einzuhalten.

Schutzgegenstand aller Datenschutzregelungen sind personenbezogene Daten. Neben den Datenschutzvorschriften sind Dienstgeheimnisse, besondere Berufsgeheimnisse, wie z. B. das Seelsorgegeheimnis, die berufliche Schweigepflicht nach § 203 StGB, das Steuergeheimnis und das Fernmeldegeheimnis zu beachten.

1. Personenbezogene Daten (nach § 4 Nummer 1 DSG-EKD) sind alle Informationen, die sich auf eine identifizierte (z. B. Name, Geburtstag, Anschrift, Beruf, Familienstand) oder identifizierbare natürliche Person beziehen; identifizierbar ist eine natürliche Person, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.
2. Besondere Kategorien personenbezogener Daten (nach § 4 Nummer 2 DSG-EKD) sind alle Informationen, aus denen religiöse oder weltanschauliche Überzeugungen einer natürlichen Person hervorgehen, ausgenommen Angaben über die Zugehörigkeit zu einer Kirche oder einer Religions- oder Weltanschauungsgemeinschaft, alle Informationen, aus denen die rassische und ethnische Herkunft, politische Meinungen oder die Gewerkschaftszugehörigkeit einer natürlichen Person hervorgehen, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Bei der Erhebung, Verarbeitung und Nutzung dieser Daten ist besondere Sorgfalt zu üben. Automatisierte Verfahren, die diese Daten verarbeiten, unterliegen der Datenschutz-Folgenabschätzung (nach § 34 DSG-EKD).
3. Beim Umgang mit personenbezogenen Daten im diakonischen und kirchlichen Bereich muss gewährleistet werden, dass der Einzelne in seinem Recht auf freie Entfaltung seiner Persönlichkeit nicht verletzt wird.
4. Personenbezogene Daten dürfen nur verarbeitet werden, wenn eine spezielle Rechtsvorschrift oder das Datenschutzgesetz der EKD dies zulässt, der Betroffene eingewilligt hat oder die Verarbeitung zur Erfüllung der Aufgabe der verantwortlichen Stelle erforderlich ist.

5. Alle Informationen, die ein Mitarbeiter auf Grund seiner Tätigkeit mit Daten, Datenträgern, Unterlagen und Akten oder im persönlichen Gespräch erhält, sind von ihm vertraulich zu behandeln und nach folgenden Grundsätzen zu verarbeiten: Rechtmäßigkeit, Verhältnismäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz.

6. Personenbezogene Daten und Datenträger (dazu gehören auch CD-ROM, Flash-Speicher, insbesondere Speicher-Sticks, SD-Karten, Belege, Karteikarten, Listen, Mikrofiches, Festplatten, Disketten) dürfen nicht an Unbefugte gelangen. Diese Daten sind stets physisch unter Verschluss oder im Falle des Technikeinsatzes durch Nutzung entsprechender Sicherheitsmechanismen (sicheres Passwort, Verschlüsselung o. ä.) zu verwahren. Gleiches gilt auch für die elektronische Übertragung per Email oder Internet bzw. durch Bereitstellung in Cloud-Speichern.

7. Der Mitarbeiter hat dafür Sorge zu tragen, dass sein elektronischer Arbeitsplatz und die dort verfügbaren Anwendungen mit personenbezogenen Daten Unbefugten nicht zugänglich sind. Dazu gehört insbesondere der verantwortliche Umgang mit Nutzer-Kennungen.

8. Auskünfte aus Datensammlungen (Akten, Unterlagen, Dateien, etc.) dürfen an Dritte (öffentliche oder nicht-öffentliche Stellen oder Personen) nur gegeben werden – sofern eine Rechtsvorschrift dies ausdrücklich zulässt oder vorschreibt (Meldepflicht) – wenn die Offenlegungsbefugnisse des DSG-EKD (nach § 8 bis 10) dies zulassen oder der Betroffene eingewilligt hat.

9. Datenträger (vgl. Nr. 6) mit personenbezogenen Daten, die zur Erfüllung der zugewiesenen Aufgabe und für gesetzlich vorgeschriebene Nachweise nicht mehr benötigt werden, sind datenschutzgerecht zu entsorgen, sofern es sich nicht um archivwürdige Inhalte handelt. Die Entsorgung bzw. Vernichtung der Datenträger muss in einer Weise geschehen, die jeden Missbrauch der Daten ausschließt.

10. Jeder Mitarbeiter darf sich an den Datenschutzbeauftragten wenden. Er darf deswegen nicht benachteiligt werden.

11. Verstöße gegen das Datengeheimnis können dienst- bzw. arbeitsrechtliche, urheberrechtliche, disziplinarische, haftungsrechtliche oder auch strafrechtliche Konsequenzen haben.