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 (EKD-Datenschutzgesetz - DSG-EKD) in der Bekanntmachung der Neufassung vom 1. Januar 2013, Berichtigung vom 1. Februar 2013
2. Landeskirchlich spezifische Durchführungsbestimmungen zum DSG-EKD
3. EU-Datenschutzgrundverordnung (EU-DSGVO) vom 25.05.2016, in Kraft zum 25.05.2018
4. Grundgesetz Art. 2 Abs. 1 „Recht auf informationelle Selbstbestimmung“
5. Telekommunikationsvorschriften (TKG, TMG)
6. Sozialdatenschutzregelungen des Sozialgesetzbuches
7. Regelungen des Strafgesetzbuches (insbesondere §§ 201 bis 206, 263a, 303a 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 Mitarbeitenden zu beachten und einzuhalten.

Schutzgegenstand aller Datenschutzregelungen sind vordergründig personenbezogene Daten, aber auch Dienstgeheimnisse, sowie das Seelsorgegeheimnis und das Ansehen von Kirche und Diakonie.

1. Personenbezogene Daten sind Einzelangaben über persönliche (z.B. Name, Geburtstag, Anschrift, Beruf, Familienstand) oder sachliche Verhältnisse (Grundbesitz, Rechtsbeziehungen zu Dritten, Steuermerkmale, Schulden, Vorstrafen) einer bestimmten oder bestimmbaren natürlichen Person (betroffene Person), z.B. Klient, Patient, Mitarbeitende, Heimbewohner, Betreuer, Berater, Nutzungsberechtigter.
2. Besondere Arten personenbezogener (nach § 2 Abs. 11 DSG-EKD) Daten sind Angaben über rassische und ethnische Herkunft, politische Meinungen, religiöse und weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Bei der Erhebung, Verarbeitung und Nutzung dieser Daten ist besondere Sorgfalt zu üben. Automatisierte Verfahren, die diese Daten verarbeiten, unterliegen der Vorabkontrolle des Datenschutzbeauftragten.
3. Beim Umgang mit personenbezogenen Daten im diakonischen und kirchlichen Bereich muss gewährleistet werden, dass der Einzelne in seinem „Persönlichkeitsrecht auf informationelle Selbstbestimmung“ nicht verletzt wird.
4. Personenbezogene Daten dürfen nur erhoben, verarbeitet oder genutzt werden, wenn eine spezielle Rechtsvorschrift oder das Datenschutzgesetz der EKD dies zulässt oder der Betroffene eingewilligt hat und die Daten zur Erfüllung der Aufgabe erforderlich sind.
5. Alle Informationen, die ein Mitarbeitender auf Grund seiner Tätigkeit mit Daten, Datenträgern, Unterlagen und Akten oder im persönlichen Gespräch erhält, sind von ihm vertraulich zu behandeln.
6. Personenbezogene Daten und Datenträger (dazu gehören auch CD-ROM, Flash-Speicher, Speicher-Sticks, Belege, Karteikarten, Listen, Mikrofiches, Festplatten, Magnetbänder, 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 nicht autorisierte elektronische Übertragung per Email oder Internet.

7. Der Mitarbeiter hat dafür Sorge zu tragen, dass sein PC und die darauf verfügbaren Anwendungen mit personenbezogenen Daten Unbefugten nicht zugänglich sind. Dazu gehört auch der verantwortliche Umgang mit Passwörtern und anderen 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 Übermittlungsbefugnisse des Datenschutzes dies zulassen oder der Betroffene eingewilligt hat.

9. Datenschutz beinhaltet auch den Schutz vor vorsätzlichem Verändern und/oder Löschen personenbezogener Daten, z.B. durch Bedienfehler oder technische Veränderungen sowie Missbrauch. Mitarbeitenden ist es daher untersagt, private Software und Datenträger in die Dienststelle unkontrolliert einzubringen.

10. 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.

11. Jeder Mitarbeitende darf sich an den Datenschutzbeauftragten wenden. Er darf deswegen nicht benachteiligt werden.

12. Verstöße gegen den Datenschutz, also die Vertraulichkeit der Daten, sind Verletzungen der Dienstpflicht im Sinne der arbeitsrechtlichen und disziplinarischen Bestimmungen. Sie können daher bei vorsätzlichem Verschulden Schadenersatzansprüche des Dienstherrn oder Dritter begründen und disziplinarische Maßnahmen (bis zur fristlosen Kündigung) zur Folge haben.

13. Die Verpflichtung zur Wahrung des Datengeheimnisses besteht nach Beendigung der Tätigkeit fort.