Merkblatt
Datenschutz und Datensicherheit

Für den Umgang mit personenbezogenen Daten sowie für den Schutz und die Sicherheit dieser Daten gelten u.a. nachfolgende, rechtsverbindliche Regelungen.

1. Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG EKD)
2. Grundgesetz Artikel 1 und 2
3. Telekommunikationsvorschriften (TKG, TMG)
4. Sozialdatenschutzregelungen des Sozialgesetzbuches
5. Regelungen des Strafgesetzbuches (insbesondere §§ 201 bis 206, 263a, 303a und b, 355 StGB)

Diese Regelungen sowie auf ihrer Grundlage erlassene Richtlinien sind von allen Mitarbeitern zu beachten und einzuhalten.

Dazu dienen folgende Hinweise:

1. **Personenbezogene Daten** sind alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen (z.B. Name, Geburtstag, Anschrift, Beruf, Familienstand, Gesundheitsdaten, Grundbesitz, Rechtsbeziehungen zu Dritten, Steuermerkmale, Schulden, Vorstrafen u.a.)

2. **Besondere Kategorien personenbezogener Daten** (nach KDG) sind Angaben über rassische und ethnische Herkunft, politische Meinungen, religiöse und weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, **Gesundheit** oder Sexualleben, genetische und biometrische Daten. **Bei der Verarbeitung dieser Daten ist besondere Sorgfalt zu üben**. Alle **Patientendaten** sind hierunter einzuordnen. **Dies betrifft auch die Tatsache, wenn nur der Name des Patienten zur Verarbeitung gelangt!! Auch eine bloße Kenntnisnahme, dass Patient oder Bewohner XY sich in der Einrichtung AB befindet, fällt unter diese Rubrik.**

3. Beim Umgang mit personenbezogenen Daten muss gewährleistet werden, dass der Einzelne in seinem „Persönlichkeitsrecht auf informationelle Selbstbestimmung“ nicht verletzt wird.

4. Personenbezogene Daten dürfen nur verarbeitet werden, wenn die Datenschutzgesetze bzw. spezielle Rechtsvorschriften dies zulassen oder der Betroffene eingewilligt hat **und die Daten zur Erfüllung der Aufgabe erforderlich sind.**

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. **Dies gilt u.a. auch für Mitarbeiter, welche ggf. sensible Patienten- und Bewohnerdaten im Rahmen ihrer Tätigkeit zur Kenntnis nehmen können (z.B. Reinigung von Räumen in denen schriftliche Unterlagen nicht verschlossen wurden)**

6. Personenbezogene Daten dürfen auf mobilen Geräten (Notebooks, Tablets, Smartphones u.ä.) i.d.R. **nicht gespeichert werden.** Wenn dies im **Ausnahmefall** doch erforderlich ist, müssen diese Daten mittels **Passwort gesichert und verschlüsselt** werden. Dies **gilt auch für andere mobile Datenträger** wie CD-ROM, USB-Sticks, externe Festplatten.

7. Eine Übermittlung sensibler personenbezogener Daten mittels **unverschlüsselter Email ist unzulässig.**

8. 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.

9. Datenschutz beinhaltet auch den Schutz vor vorsätzlichem Verändern und/oder Löschen personenbezogener Daten, z.B. durch Bedienfehler oder technische Veränderungen sowie Missbrauch. Mitarbeitern 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**. Die Entsorgung bzw. Vernichtung der Datenträger muss in einer Weise geschehen, die jeden Missbrauch der Daten ausschließt.

11. Auch bei **Papierunterlagen** ist auf eine datenschutzgerechte Vernichtung zu achten. **Dies darf keinesfalls im Papierkorb oder sonstigem Hausmüll** geschehen, sondern hierfür sind **Schredder zu verwenden, welche der DIN 66399 entsprechen oder verschlossene Datentonnen**.

12. **Verletzungen des Schutzes personenbezogener Daten** (so genannte **Datenpannen)**, welche voraussichtlich zu einem nicht unerheblichen Risiko für die betroffenen Personen führen, sind **unverzüglich (Orientierung: innerhalb 72 Stunden) der Aufsichtsbehörde zu melden.** Ggf. sind auch die betroffenen Personen zu benachrichtigen**. Jeder Mitarbeiter** ist verpflichtet, solche Vorkommnisse **sofort dem Vorgesetzten bzw. der Geschäftsführung zu melden.**

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

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

15. **J**eder Mitarbeiter darf sich an den Datenschutzbeauftragten wenden. Er darf deswegen nicht benachteiligt werden.

    Die Kontaktdaten des Datenschutzbeauftragten sind:

    Herr Christoph Sydow
    Tel.: 0361 – 7897242

    Email: christoph.sydow@t-online.de