Merkblatt

- **Grundsätze des Datenschutzes und der Datensicherheit -**

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

a. Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland, Neufassung vom 15.11.2017 (DSG-EKD) sowie die IT-Sicherheitsverordnung (ITSVO);
b. Landesspezifische kirchliche Durchführungsbestimmungen zum DSG-EKD;
c. EU-Datenschutzgrundverordnung vom 27.4.2016 (EU-DSGVO);
d. Grundgesetz Art. 2 Abs. 1 „Recht auf informationelle Selbstbestimmung“;
e. Telekommunikationsvorschriften (Telekommunikations- und Telemediengesetz);
f. Sozialdatenschutzregelungen der Sozialgesetzbücher (in entsprechender Anwendung etwa § 35 SGB I und §§ 67, 69 bis 71 Abs. 1 sowie §§ 75 bis 78 SGB X)
g. Regelungen des Strafgesetzbuches (insbesondere §§ 201 bis 206, 263a, 303a und 303b, 355 StGB).

Diese Regelungen sowie auf ihrer Grundlage erlassene Richtlinien und alle im Bereich der Diakonie Hessen geltenden Rechtsvorschriften zum Datenschutz und zur Datensicherheit sind von allen haupt-, neben- und ehrenamtlichen Mitarbeitenden zu beachten und einzuhalten.

2. Schutzgegenstand aller Datenschutz- und Datensicherheitsregelungen sind sämtliche personenbezogenen Daten (§ 4 Ziffern 1 und 2 DSG-EKD) der betroffenen Person (etwa Klient*in, Patient*in, Mitarbeitende aller Art, Bewohner*in, Betreute, Nutzer*in von Beratungsangeboten, Spender*in u.a.), die Eingang in den Kenntnisbereich der für die Datenverarbeitung verantwortlichen Stelle (§ 4 Ziffer 9 DSG-EKD: Diakonische Dienste, Einrichtungen, Werke) finden. Daneben gilt es die berufliche Schweigepflicht, das Dienst- und Seelsorgegeheimnis sowie das Ansehen von Kirche und Diakonie zu wahren.

3. Zur Erfüllung des zu Gunsten der betroffenen Person abgeschlossenen Leistungsvertrages (einschließlich der notwendigen Grundlageninformationen, der Hilfe- und Maßnahmenplanung und -durchführung sowie der Dokumentation) bzw. sonstigen Rechtsverhältnisses oder aufgrund gesetzlicher Verpflichtungen müssen regelmäßig personenbezogene Daten von den diakonischen Einrichtungen, Diensten und Werken verarbeitet werden.

Bei der Verarbeitung (§ 4 Ziffer 3 DSG-EKD) der personenbezogenen Daten im diakonischen und kirchlichen Bereich muss gewährleistet sein, dass die betroffene Person in seinem „Persönlichkeitsrecht auf informationelle Selbstbestimmung“ nicht beeinträchtigt bzw. verletzt wird.

Personenbezogene Daten dürfen nur unter den Voraussetzungen des § 6 DSG-EKD verarbeitet werden. Insbesondere, wenn eine spezielle Rechtsvorschrift dies zulässt oder die Verarbeitung für die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist, erforderlich ist oder die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung der verantwortlichen Stelle erforderlich ist, schließlich wenn die betroffene Person in die Datenverarbeitung eingewilligt hat. Zu anderen als den in § 6 DSG-EKD genannten Zwecken dürfen die Daten nicht verwendet werden.

Handelt es sich bei den Daten um sog. „besondere Kategorien personenbezogener Daten“, kommen außerdem die Bestimmungen des § 13 DSG-EKD zur Anwendung, insbesondere Ziffer 2 („Beschäftigten- und Sozialversicherungsdaten“), Ziffer 3 („Schutz lebenswichtiger Interessen“) und Ziffer 8 („Zwecke der Gesundheitsvorsorge, Versorgung oder Behandlung

im Gesundheits- oder Sozialbereich etc.“) sowie § 13 Abs. 3 DSG-EKD finden besondere Beachtung.

Die Einrichtung muss dafür Sorge tragen, dass ein Verlust bzw. ein Verändern der personenbezogenen Daten organisatorisch und technisch ausgeschlossen ist (Datensicherheit).

Alle Informationen, die Mitarbeitende aufgrund der Tätigkeit mit Daten, Datenträgern, Unterlagen und Akten oder im persönlichen Gespräch erhalten, sind gem. Dienstpflicht vertraulich zu behandeln. Dies gilt auch nach Beendigung der Tätigkeit.

Sofern externe Dienstleister mit Datenverarbeitungsvorgängen beauftragt werden, ist die Einhaltung des Datenschutzes und der Datensicherheit gemäß § 30 DSG-EKD zu gewährleisten.

4. Eine Übermittlung (Weitergabe und Einsichtsgewährung) der Daten bedarf immer der Einwilligung der betroffenen Person, sofern nicht eine Rechtsvorschrift die Übermittlung zulässt oder vorschreibt (etwa Meldepflichten) oder sofern die Daten für die Übermittlung anonymisiert (statistische Zwecke) wurden.

Zu Prüfzwecken und zur Qualitätssicherung dürfen Berechtigte (z. B. Medizinischen Dienst der Krankenversicherung, Prüfdienst der Privaten Krankenversicherung oder von den Landesverbänden der Pflegekassen bestellte Sachverständige (§§ 276, 284 SGB V, §§ 93, 97, 97a, 114 SGB XI), Heimaufsicht, Landesrechnungshof, Datenschutzaufsicht) unter strenger Einhaltung der geltenden Datenschutzbestimmungen in die Daten Einsicht nehmen, ggf. Daten übermittelt erhalten.

Werden Daten an die Kranken- und Pflegekassen (§§ 284, 302 SGB V bzw. §§ 93, 94, 104, 105 SGB XI), bei Sozialhilfeempfängern an den Sozialhilfeträger (§§ 93 ff. SGB XI und §§ 67 ff. SGB X), an behandelnde Ärzte und Therapeuten übermittelt, geschieht dies ebenfalls nur im Rahmen der jeweils geltenden Datenschutz- und Schweigepflichtvorschriften.

Nach einer Anonymisierung (§ 4 Ziffer 7 DSG-EKD) können die Daten für statistische und wissenschaftliche Zwecke ausgewertet werden.

Auf ausdrückliches Verlangen der betroffenen Person können gemäß § 24 DSG-EKD automatisiert verarbeitete personenbezogene Daten in einem gängigen Format zur Verfügung gestellt oder auf Wunsch an einen Dritten weitergegeben werden (z. Bsp. bei einem Wechsel der betrauten Einrichtung).

5. Werden personenbezogene Daten bei der betroffenen Person erhoben, so informiert die verantwortliche Stelle die betroffene Person gemäß § 17 DSG-EKD auf Verlangen in geeigneter und angemessener Weise über die wesentlichen Aspekte der Datenerhebung. Bei mittelbarer Datenerhebung gelten die Spezialbestimmungen des § 18 DSG-EKD, die die Datenherkunft bzw. die empfangende Stelle einbeziehen.

Es besteht nach § 19 DSG-EKD die grundsätzliche Möglichkeit, Auskunft über die gespeicherten personenbezogenen Daten (insbesondere die Verarbeitungszwecke, Kategorien, ggf. Empfänger und die geplante Dauer der Speicherung, ggf. die Herkunft der Daten) zu erhalten. Dabei ist auch auf die nachfolgend unter 6. bis 10. dargestellten Rechte hinzuweisen.

Im Übrigen ermöglichen ggf. (landesrechtliche) Spezialvorschriften das Recht auf Information und Auskunft hinsichtlich der verarbeiteten Daten.

6. Unrichtige personenbezogene Daten werden gem. § 20 DSG-EKD jederzeit berichtigt oder vervollständigt.

7. Wenn keine rechtliche Verpflichtung zur Aufbewahrung mehr besteht oder eine Speicherung der Daten nicht mehr erforderlich ist, kann unter den Voraussetzungen des § 21 DSG-EKD deren Löschung verlangt werden. Die Löschung muss in einer Weise geschehen, die jeden Missbrauch der Daten ausschließt.

Personenbezogene Daten werden 5 Jahre nach Ablauf des Kalenderjahres, in dem die Beratung beendet wurde, gelöscht.

Soweit Leistungen der Behandlungspflege erbracht werden, ist eine Aufbewahrungspflicht von 10 Jahren zu beachten (§ 630 f. Absatz 3 BGB). Aus handelsrechtlichen Vorschriften kann sich eine Aufbewahrungspflicht von Belegen von 6 oder 10 Jahren ergeben (§ 257 HGB). Darüber hinaus kann im Einzelfall nach den Vorschriften des Zivilrechts eine Aufbewahrung von mind. 30 Jahren erforderlich sein (§ 197 BGB).

8. Gemäß § 22 DSG-EKD kann unter bestimmten Voraussetzungen die weitere Verarbeitung von personenbezogenen Daten beschränkt bzw. auf bestimmte Zwecke eingegrenzt werden. Die Daten werden gut geschützt und vor Zugriff gesichert aufbewahrt.

9. Unter den Voraussetzungen von § 25 DSG-EKD ist die Datenverarbeitung durch die Einrichtung im Falle eines Widerspruches der betroffenen Person zu unterlassen. Die betroffene Person kann ihr Widerspruchsrecht jederzeit ausüben.

10. Datenverarbeitungen der verantwortlichen Stelle können mittels Beschwerde bei einer unabhängigen kirchlichen Aufsichtsbehörde (§§ 39 ff. DSG-EKD) beanstandet werden. Die zuständige Aussichtsbehörde ist:

Der Beauftragte für den Datenschutz der EKD (BfD EKD)

Michael Jacob

Böttcherstraße 7

30419 Hannover

Telefon: + 49 (0)511 768128-0

Telefax: + 49 (0)511 768128-20

Daneben sind ggf. Betriebsbeauftragte für den Datenschutz (§§ 36 ff. DSG-EKD) zu bestellen, die regelmäßig unter der Postadresse der verantwortlichen Stelle (Einrichtung, Dienst, Werk) mit dem Zusatz „z. H. des/der betrieblichen Datenschutzbeauftragte(n)“ erreicht werden können.[1]

[1] Hier bitte ggf. Kontaktdaten des Betriebsbeauftragten für den Datenschutz einfügen.