Merkblatt über den Datenschutz

in der Evangelischen Kirche Berlin-Brandenburg-schlesische Oberlausitz

Für den Datenschutz in der Evangelischen Kirche Berlin-Brandenburg-schlesische Oberlausitz gilt neben den allgemeingültigen Bestimmungen zum Persönlichkeitsschutz das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) vom 12. November 1993 (KABl. 1994 S. 46, ABl. EKD S. 505), zuletzt geändert durch Kirchengesetz vom 7. November 2012 (ABl. EKD S. 452). Künftige Rechts- und Verwaltungsvorschriften für die Evangelische Kirche Berlin-Brandenburg-schlesische Oberlausitz sind in gleicher Weise zu beachten.

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

Mitarbeiterinnen und Mitarbeiter sind alle, denen zur ehrenamtlichen oder beruflichen Wahrnehmung Dienste in der Kirche übertragen worden sind, vgl. Artikel 4 Abs. 1 der Grundordnung der Evangelischen Kirche Berlin-Brandenburg-schlesische Oberlausitz vom 21./ 24. November 2003 (KABl.-EKiBB S. 159, ABl.-EKsOL S. 7), zuletzt geändert durch Kirchengesetz vom 26. Oktober 2013 (KABl. S. 235).

Jede Gemeinde und Dienststelle, jedes kirchliche Werk und jede kirchliche Einrichtung ist für den Schutz personenbezogener Daten im eigenen Bereich verantwortlich. Insbesondere sind dabei folgende Grundsätze zu beachten:

1. Dienst- oder arbeitsrechtliche Sanktionen; strafrechtliche Ahndung

Unberührt von den Bestimmungen des Datenschutzes bestehen und sind zu beachten die Vorschriften über

- Amts- bzw. Dienstverschwiegenheit (§ 31 Pfarrdienstgesetz der EKD, § 24 Kirchenbeamtengesetz der EKD, Artikel 6 Grundordnung der EKBO),
- Schweigepflicht (§ 3 Abs. 2 Tarifvertrag der EKBO),
- Steuergeheimnis (§ 30 Abgabenordnung),
- sonstige Geheimhaltungs- und Unterlassungspflichten im Strafgesetzbuch
  [z.B. § 202a (Ausspähen von Daten),
  § 202b (Abfangen von Daten)
  § 202c (Vorbereiten des Ausspähens und Abfangens von Daten)
  § 203 (Verletzung von Privatgeheimnissen),
  § 263a (Computerbetrug),
  § 303a (Datenveränderung),
  § 303b (Computersabotage)].

Auf dienst- oder arbeitsrechtliche Sanktionen sowie die strafrechtliche Ahndung nach den allgemeingültigen gesetzlichen Vorschriften bei Verstößen wird besonders hingewiesen.

2. Verpflichtung

Darüber hinaus haben alle, zu deren Tätigkeitsbereich oder Auftrag der Umgang mit personenbezogenen Daten gehört, eine weitere besondere Verpflichtung entsprechend dem nachstehenden Muster einzugehen. Diese zusätzliche Verpflichtung zur Einhaltung des Datengeheimnisses wirkt umfassender als die übliche generelle Verpflichtung zur Verschwiegenheit aufgrund der zuvor genannten oder anderer Rechtsvorschriften.

Das Datengeheimnis schränkt auch Mitteilungen im dienstlichen Verkehr ein, weil das Kirchengesetz über den Datenschutz (DSG-EKD) nicht nur die Verarbeitung personenbezogener Daten einschränkt, sondern auch verbietet, personenbezogene Daten unbefugt zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck bekannt zu geben, zugänglich zu machen oder sonst zu nutzen.

3. Beendigung des Dienst- oder Arbeitsverhältnisses

Alle Kenntnisse über Personen und ihre Daten, die eine Mitarbeiterin oder ein Mitarbeiter oder sonst Verpflichteter aufgrund seiner Tätigkeit an und mit Dateien, Karteien, Listen und anderen Datenträgern erhält, sind von ihm vertraulich zu behandeln. Diese Pflicht besteht auch nach Beendigung des Dienst- oder Arbeitsverhältnisses oder der Tätigkeit.

4. Belehrung; bereichsspezifische Probleme

Die auf den Datenschutz Verpflichteten sind auf bereichsspezifische Probleme und neue Bestimmungen durch den jeweiligen Dienstvorgesetzten oder den Leiter der Dienststelle in geeigneter Form hinzuweisen.

5. Personenbezogene Daten

Personenbezogene Daten sind nach § 2 Abs.1 DSG-EKD Einzelangaben

- einer bestimmten oder bestimmbaren (z.B. durch Namen, Personalnummer, Sozialversicherungsnummer) natürlichen Person (z.B. Gemeindeglied, kirchliche Mitarbeiterin oder kirchlicher Mitarbeiter)
- über persönliche oder sachliche Verhältnisse (z.B. durch Beschreibung eines auf sie bezogenen Sachverhalts wie Adresse, Geburtsdatum, Familienstand, Geschlecht, Staatsangehörigkeit, Religionszugehörigkeit, Berufsbezeichnung, Zeugnisnoten, Einkommen, Besitz, Rechtsbeziehungen zu Dritten).

Besondere Arten personenbezogener Daten nach § 2 Abs. 11 Satz 1 DSG-EKD sind Angaben über rassische und ethnische Herkunft, politische Meinungen, religiöse und weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Diese Daten unterliegen einem besonderen Schutz.

6. Zulässigkeit; Aufgabenerfüllung

Personenbezogene Daten dürfen nur zur Erfüllung der durch kirchliches oder allgemeingültiges Recht der jeweiligen Stelle zugewiesenen Aufgaben verarbeitet oder genutzt werden. Diese Aufgaben bestehen vornehmlich in der Verkündigung, Seelsorge, Vornahme von Amtshandlungen, Förderung des Gemeindelebens, Unterweisung, Diakonie sowie der jeweils obliegenden Verwaltung und dem Personalwesen.

7. Datenträger

Datenträger sind alle Medien, auf denen Daten verzeichnet sind, also insbesondere Belege, Formulare, Erfassungsbögen, Adressenaufkleber, Listen, Karteikarten, Mikrofilme, Disketten, Magnetplatten, Magnetbänder, Magnetkarten, Compact Discs (CDs), Memory Sticks.

8. Dateien

Dateien sind Sammlungen von Daten auf Massendatenträgern (z.B. Disketten, Magnetplatten, CDs, Memory Sticks). Eine Sammlung von gleichartig aufgebauten Einzeldatenträgern (z.B. Formularen, Adressenaufklebern, Karteikarten) ist ebenfalls eine Datei. Dabei ist die Zahl der in der Datei enthaltenen Betroffenen unerheblich. Auch kommt es nicht auf die Form der Aufbewahrung (z.B. Ordnern) an.

9. Verfahren; Programme

Gleichem Schutz wie personenbezogene Daten unterliegen auch Verfahren (z.B. Programme), die solche Daten beinhalten und verarbeiten.

10. Datenträgerverschluss

Personenbezogene Daten dürfen nicht an Unbefugte gelangen. Daher sind die Datenträger stets sicher und sorgfältig unter Verschluss zu verwahren und vor jeder Einsicht, Wegnahme, Zerstörung, Verände-

rung, Vervielfältigung oder sonstigen Nutzung durch Unbefugte zu schützen. Hierzu reicht gewöhnlich ein Abschließen des Raumes nicht aus; vielmehr sind die Datenträger selbst so zu verwahren bzw. zu verschließen, dass sie auch vor Personen geschützt sind, die zwar den Raum befugt betreten, jedoch nicht die Daten einsehen dürfen.

11. Datenträgertransport; Einsichtnahme

Personenbezogene Daten oder Datenträger dürfen nur Mitarbeitern zugänglich gemacht oder zum Transport übergeben werden, die aufgrund ihrer Aufgaben zum Empfang schriftlich ermächtigt und zur Wahrung des Datengeheimnisses entsprechend dem nachstehenden Muster verpflichtet worden sind. Es ist darüber hinaus untersagt, durch Anforderung von gespeicherten Daten oder durch sonstige Einsichtnahme sich oder anderen in unzulässiger Weise Kenntnisse über Personen oder Daten zu verschaffen oder anderen zu gestatten oder sie dabei zu fördern, derartige Kenntnisse zu erlangen.

12. Auskünfte

Auskünfte aus personenbezogenen Datensammlungen sowie Abschriften oder Kopien von Listen oder Dateien dürfen nur im Rahmen der Aufgabenerfüllung der über die Daten verfügenden kirchlichen Stelle unter Beachtung der bestehenden Datenschutzbestimmungen und anderen Rechtsvorschriften an Berechtigte erteilt oder für sie angefertigt werden. Derartige Mitteilungen zur geschäftlichen oder gewerblichen Verwendung dürfen nicht gegeben werden.

13. Veröffentlichung von Amtshandlungen, Jubiläen und Geburtstagen

Die Veröffentlichung von Amtshandlungen, Jubiläen und Geburtstagen geschieht in Erfüllung des kirchlichen Auftrages, nämlich zur Förderung des Gemeindelebens und der Kommunikation der Gemeindeglieder untereinander. Auf eine genaue Adressenangabe ist zu verzichten.

14. Übermittlung

Auch im zulässigen Falle ist die Übermittlung personenbezogener Daten auf das erforderliche Maß zu begrenzen und es sind keine über die Anforderungen hinausgehenden Informationen zu erteilen. Darauf ist insbesondere auch bei Übermittlung durch Einsichtnahme zu achten. Eine telefonische Übermittlung personenbezogener Daten ist wegen der unsicheren Identifikationsmöglichkeit grundsätzlich unzulässig. Unvermeidbare Ausnahmen sind nur möglich, wenn der Anrufer durch geeignete Maßnahmen zweifelsfrei identifiziert werden kann.

15. Personalwesen

Im Personalwesen bleibt das Recht auf Einsichtnahme, Prüfung und Auswertung der Unterlagen und Daten durch die nach staatlichem und kirchlichem Recht zuständigen Stellen (z.B. Steueraußenprüfer, Prüfer der Finanzverwaltung bei Zuschussgewährung, Prüfer der Sozialversicherungsträger, Prüfer des Kirchlichen Rechnungshofes) unberührt.

16. Datenträgervernichtung

Personenbezogene Datenbestände (z.B. Gemeindegliederlisten, Personallisten, Änderungslisten, Karteien, Mikrofilme, Dateien auf Disketten), die durch neue ersetzt und auch nicht aus besonderen zulässigen Gründen weiterhin benötigt werden, müssen in einer Weise vernichtet werden, die jeden Missbrauch der Daten ausschließt. Bestehende Rückgaberegelungen bleiben davon unberührt.

17. Sozialdaten

Sozialdaten, nämlich personenbezogene Daten, die von Sozialleistungsträgern übermittelt oder im Rahmen der Aufgabenüberlassung erhoben werden, insbesondere Geheimnisse des Betroffenen, die zu seinem persönlichen Lebensbereich gehören, unterliegen neben den Bestimmungen des kirchlichen Datenschutzgesetzes dem besonderen Schutz der Regelungen des Sozialgesetzbuches und einer besonderen beruflichen Schweigepflicht. Zum persönlichen Lebensbereich gehört ein Geheimnis, wenn es die Intim- oder Privatsphäre, das heißt den Gesundheitszustand, die Gefühlswelt, den Bereich des Fa-

milien- und sonstigen privaten Lebens betrifft. Das Sozialgeheimnis ist ein besonderes Amtsgeheimnis. Es gilt auch nach dem Tod des Betroffenen.

18. Sozialdaten - Offenbarung; Auftragsverarbeitung

Bei Verarbeitung und Nutzung der Sozialdaten ist besonders sorgsam darauf zu achten, dass eine Beteiligung anderer als der eigentlich zuständigen Stellen (Diakoniestationen, Hauspflegestellen, Krankenhäuser, Heime u.a.) nur im Rahmen der zulässigen Offenbarung, der Auftragsdatenverarbeitung oder mit Zustimmung der Betroffenen geschieht.

19. Personalcomputer

Beim Betrieb von isolierten Datenverarbeitungsanlagen oder Arbeitsplatzcomputern (Personalcomputern) sind geeignete organisatorische und technische Maßnahmen so zu treffen, dass personenbezogene Daten nicht schlechter geschützt sind als bei der Verarbeitung in einem arbeitsteilig organisierten Rechenzentrum.

Die Verpflichtung der Mitarbeiterinnen und Mitarbeiter zum Datenschutz schließt auch die Pflicht zur Einhaltung der zur Arbeit an diesen Geräten und Systemen erlassenen Dienstanweisungen ein.

20. Personalcomputer - Technische und organisatorische Maßnahmen -

Es ist unter anderem für die vorgenannten Anlagen sicherzustellen, dass

- bei Darstellung personenbezogener Daten auf Bildschirmen oder Druckern Unbefugten die Einsicht verwehrt wird,
- ein unbefugter Zugriff auf personenbezogene Daten oder Betriebsprogramme oder ein unbefugtes Benutzen der Geräte ausgeschlossen ist und
- ein unbefugtes oder unberechtigtes Abrufen oder Übertragen von Daten nicht stattfinden kann.

21. Passwörter

Den Mitarbeiterinnen und Mitarbeitern ist untersagt, ihre zum Zugriff auf bestimmte Arbeitsprogramme und Daten berechtigenden Passwörter unbefugt zu offenbaren oder Passwörter anderer Mitarbeiter auszuspähen oder sich unbefugt zu beschaffen.

22. Mängel beim Datenschutz

Mängel beim Datenschutz, der sicheren Verwahrung und der ordnungsgemäßen Verarbeitung personenbezogener Daten sind dem jeweiligen Vorgesetzten unverzüglich anzuzeigen.