

Merkblatt zur Verpflichtungserklärung

Für den Datenschutz im Bereich des Diakonischen Werks in Niedersachsen e. V. sind folgende Rechtsvorschriften zu beachten:

-Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG EKD) vom 12. November 1993 (Kirchl. Amtsbl. 1994 S. 30), geändert durch Kirchengesetz vom 07. November 2002 (Abl.EKD S. 381) und durch Kirchengesetz vom 7. November 2012 (Abl.EKD 2012 S. 452)

-Kirchengesetz der Konföderation evangelischer Kirchen in Niedersachsen zur Ergänzung und Durchführung des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (Gemeinsames Datenschutz-Anwendungsgesetz - DSAG) vom 23. November 1995 (Kirchl. Amtsbl. S. 166), geändert durch Kirchengesetz vom 9. März 2013 (Kirchl. Amtsbl. S. 46)

-Verordnung des Rates der Konföderation evangelischer Kirchen in Niedersachsen zur Ergänzung und Durchführung datenschutzrechtlicher Vorschriften (Datenschutz-durchführungsverordnung - DATVO) vom 12. Dezember 1995 (Kirchl. Amtsbl. S. 190), geändert durch Verordnung vom 19. Juni 2001 (Kirchl. Amtsbl. S. 114), durch Verordnung vom 14. September 2010 (Kirchl. Amtsbl. S. 102) und durch Verordnung vom 10. Dezember 2013 (Kirchl. Amtsbl. S. 182)

-Rechts- und Verwaltungsvorschriften für die Durchführung des kirchlichen Datenschutzes der beteiligten Landeskirchen

In gleicher Weise sind künftige Rechts- und Verwaltungsvorschriften der Evangelischen Kirche in Deutschland, der Konföderation evangelischer Kirchen in Niedersachsen und der beteiligten Landeskirchen zum Datenschutz zu beachten.

Für den Schutz personenbezogener Daten gelten insbesondere folgende Grundsätze:

1. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlicher Person (betroffene Person). Soweit personenbezogene Daten von Sozialleistungsträgern übermittelt werden, gelten zum Schutz dieser Daten ergänzend die staatlichen Bestimmungen entsprechend.

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, wenn das DSG EKD oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit die betroffene Person eingewilligt hat (s. § 3 DSG-EKD). Einzelheiten sind u. a. den §§ 1 bis 5 und den §§ 11 bis 13 DSG-EKD zu entnehmen.

2. Personenbezogene Daten und Datenkategorien (z. B. Belege, Karteikarten, EDV-Listen, Magnetbänder, Magnetplatten, Disketten, Datenverarbeitungsanlagen) sind stets sicher und verschlossen zu verwahren und vor dem Zutritt Unbefugter zu schützen.

3. Personenbezogene Daten und Datenkategorien dürfen nur solchen Personen zugänglich gemacht werden, die auf Grund ihrer dienstlichen Aufgaben oder ehrenamt-

lichen Tätigkeit zum Zugriff auf die Daten ermächtigt und ausdrücklich auf die Wahrung des Datengeheimnisses verpflichtet worden sind.

4. Eine Übermittlung (Einsichtnahme, Abruf, Weitergabe) ist nur zulässig, wenn eine kirchliche oder staatliche Rechtsvorschrift dies vorsieht, zwingend voraussetzt oder die Wahrnehmung des kirchlichen Auftrages dies erfordert. Auskünfte zur geschäftlichen oder gewerblichen Verwendung der Daten dürfen in keinem Fall gegeben werden.

5. Datenbestände, insbesondere Dateien, Listen und Karteien, die durch neue ersetzt und auch nicht aus besonderen Gründen weiterhin benötigt werden, müssen in einer Weise vernichtet oder gelöscht werden, die jeden Missbrauch der Daten ausschließt.

6. Alle Informationen, die Mitarbeiter oder Mitarbeiterinnen oder ehrenamtlich Tätige aufgrund der Arbeit mit personenbezogenen Daten und Datenkategorien erhalten, sind von ihnen vertraulich zu behandeln. Diese Pflicht besteht auch nach Beendigung des Dienstverhältnisses oder der ehrenamtlichen Tätigkeit.

7. Verstöße gegen das Datengeheimnis sind Verletzungen der Dienstpflicht im Sinne des Disziplinarrechts und der dienstrechtlichen Vorschriften und können Schadenersatzansprüche des Dienstherrn oder Dritter begründen.

8. Die Vorschriften über die Amtsverschwiegenheit der kirchlichen Mitarbeiter und über sonstige Geheimhaltungspflichten (z. B. Steuergeheimnis) bleiben unberührt.

9. Bestimmte Handlungen, die einen Verstoß gegen das Datengeheimnis beinhalten, werden durch das Strafgesetzbuch mit Strafe bedroht. Auf die Straftatbestände § 303 a ("Datenveränderung"), § 303 b ("Computersabotage"), § 202 a ("Ausspähen von Daten") und § 263 a ("Computerbetrug") wird besonders hingewiesen. Danach kann bestraft werden, wer rechtswidrig Daten verändert oder beseitigt, wer den Ablauf der Datenverarbeitung einer Behörde oder eines Wirtschaftsunternehmens stört, wer sich oder einem Dritten unbefugt besonders gesicherte Daten aus fremden Datensystemen verschafft und wer fremdes Vermögen durch unbefugtes Einwirken auf einen Datenverarbeitungsvorgang schädigt.

10. Nach urheberrechtlichen Bestimmungen (§ 106 Urheberrechtsgesetz - UrhG -i. V. m. § 69 a UrhG) sind u. a. die Weitergabe oder Vervielfältigung lizenzierter Computerprogramme strafbar. Die zeitlich parallele Mehrfachnutzung eines Originaldatenträgers oder davon angefertigter Sicherungskopien sowie die Mehrfachnutzung über ein Netzwerk ist unzulässig, sofern vertraglich nichts anderes vereinbart worden ist.

11. Der Einsatz privater Computerprogramme oder die Verarbeitung privater Daten auf einem dienstlichen Personalcomputer ist nicht zulässig.

12. Der Einsatz dienstlicher Computerprogramme oder die Verarbeitung dienstlicher personenbezogener Daten auf einem privaten Personalcomputer ist nicht zulässig.

13. Mängel beim Datenschutz, der Datensicherung und der ordnungsgemäßen Erhebung, Verarbeitung oder Nutzung personenbezogener Daten sind den jeweiligen Vorgesetzten unverzüglich anzuzeigen.