

Kirchliches Amtsblatt

der Evang.-Luth. Landeskirche Mecklenburgs

19010 Schwerin
Postfach 11 10 63

Nr. 20–24
14. Dezember 2009

A 11042/DP AG Postvertriebsstück
Entgelt bezahlt

Inhalt	Seite
Datenschutz „Verordnung über die Anwendung des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) in der Evangelisch-Lutherischen Landeskirche Mecklenburgs vom 4. Dezember 2009 [Datenschutzanwendungsverordnung]	122
IT-Sicherheit „Verordnung zur Sicherstellung der Anforderungen an den Datenschutz in der Informationstechnik (IT) (IT-Sicherheitsverordnung) vom 4. Dezember 2009	154
Mitteilung: Umfang des KABl 2009.....	155

Herausgeber und Verlag: Oberkirchenrat
der Evang.-Luth. Landeskirche Mecklenburgs
Verantwortlich für den Inhalt im Sinne des Pressegesetzes:
Oberkirchenrat Rainer Rausch
Verlag und Redaktion: Postfach 11 10 63, 19010 Schwerin
Erscheint nach Bedarf, Bezugspreis jährlich: 18 EUR
Satz und Druck: cw Obotritendruck GmbH Schwerin

Anschrift

Die Kirchenleitung hat auf ihrer Sitzung am 4. Dezember 2009 folgende Verordnung beschlossen:

116.06/118

Verordnung
über die Anwendung des Kirchengesetzes über den
Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD)
in der Evangelisch-Lutherischen Landeskirche Mecklenburgs
vom 4. Dezember 2009
[Datenschutzanwendungsverordnung]

Die Kirchenleitung hat auf Grund von § 27 Absatz 2 des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland vom 12. November 1993 (ABl. EKD 1994 S. 35), geändert durch das Kirchengesetz vom 7. November 2002 (Bekanntmachung in der ab 1. Januar 2003 geltenden Fassung vom 20. Februar 2003 und vom 7. April 2003, ABl. EKD S. 74 und 117) die folgende Verordnung erlassen:

Inhaltsverzeichnis

Erster Abschnitt:**Ergänzende Durchführungsvorschriften zum Datenschutzgesetz der EKD**

§ 1	Geltungsbereich (Einrichtungen und Mitarbeiter) (zu § 1 Absatz 2 Satz 1 DSG-EKD)	123
§ 2	Führung der Übersichten über die kirchlichen Werke und Einrichtungen mit eigener Rechtspersönlichkeit (zu § 1 Absatz 2 Satz 2 und 3 DSG-EKD)	123
§ 3	Seelsorgedaten (zu § 1 Absatz 4 DSG-EKD)	123
§ 4	Verpflichtung auf das Datengeheimnis (zu § 6 DSG-EKD)	123
§ 5	Videoüberwachung (zu § 7a DSG-EKD)	124
§ 6	Anforderungen an Datenverarbeitungsanlagen (zu § 9 DSG-EKD)	124
§ 7	Einsatz von Programmen auf Datenverarbeitungsanlagen (zu § 9 DSG-EKD)	124
§ 8	Private Datenverarbeitungsanlagen (zu § 9 DSG-EKD)	124
§ 9	Genehmigung der Einrichtung automatisierter Abrufverfahren mit nichtkirchlichen Stellen (zu § 10 Absatz 3 Satz 2 DSG-EKD)	124
§ 10	Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten im Auftrag (zu § 11 DSG-EKD)	124
§ 11	Einhaltung und Durchführung des Datenschutzes (zu § 14 Absatz 1 DSG-EKD)	124
§ 12	Übersicht über automatisierte Verarbeitungen und Meldepflicht (zu §§ 14 Absatz 2 und 21 Absatz 1 und 2 DSG-EKD)	125
§ 13	Löschung (zu § 16 Absatz 2 DSG-EKD)	125
§ 14	Aufgaben der Datenschutzbeauftragten (zu §§ 18 und 19 DSG-EKD)	125
§ 15	Beanstandungen der Datenschutzbeauftragten (zu § 20 DSG-EKD)	126
§ 16	Betriebsbeauftragte und örtlich Beauftragte für den Datenschutz (zu § 22 DSG-EKD)	126

Zweiter Abschnitt: Gemeindeglieder- und Amtshandlungsdaten

§ 17	Gemeindegliederdaten	126
§ 18	Veröffentlichung von Gemeindeglieder- und Amtshandlungsdaten	126

Dritter Abschnitt: Verkündigungsdienste

§ 19	Theologiestudierende und Theologen	126
§ 20	Ehrenamtlich Tätige	127

Vierter Abschnitt: Bildungswesen

§ 21	Schüler sowie deren Sorgeberechtigte	127
§ 22	Lehrkräfte	127
§ 23	Bildungs-, Ausbildungs- und religionspädagogische Einrichtungen	127
§ 24	Tagungen und sonstige kirchliche Veranstaltungen	127

Fünfter Abschnitt: Kirchliche Abgaben, Finanzwesen, Grundstückswesen

§ 25	Steuergeheimnis, Steuerdaten	128
§ 26	Kirchgeld	128
§ 27	Übermittlung von Steuerdaten zwischen steuererhebenden Körperschaften und dem Oberkirchenrat	128
§ 28	Freiwillige Beiträge	128
§ 29	Nutzung von Grundstücken und Gebäuden	128
§ 30	Kirchliche Friedhöfe	128

Sechster Abschnitt: Daten von Beschäftigten, Verzeichnisse über Personen und Dienste

§ 31	Verzeichnisse, dienstliche Veröffentlichungen	128
§ 32	Personenangaben im Dienstbetrieb, Bearbeitung von Beihilfeangelegenheiten	129
§ 33	Mitglieder von Gremien und Ausschüssen	129
§ 34	Dienstwohnungen	129
§ 35	Darlehen, Gehaltsvorschüsse, Unterstützungen	129
§ 36	Versorgung	129

Siebter Abschnitt: Archiv

§ 37	Benutzer des Archivs	130
------	----------------------	-----

Achter Abschnitt: Diakonische Arbeitsbereiche

§ 38	Einrichtungen der Kinder- und Jugendhilfe	130
§ 39	Krankenhäuser, Vorsorge- und Rehabilitationseinrichtungen	130
§ 40	Forschung, Krebsregister	131
§ 41	Beratungsstellen	131
§ 42	Sonstige diakonische Einrichtungen	132
§ 43	Geltung weiterer Vorschriften, Sozialgeheimnis	132

Neunter Abschnitt: Fundraising

§ 44	Erhebung, Verarbeitung und Nutzung personenbezogener Fundraisingdaten	132
§ 45	Datenerhebung, -verarbeitung und -nutzung im Auftrag	132
§ 46	Übermittlung von Fundraisingdaten an kirchliche Stellen	133

§ 47	Ausschluss der Nutzung von Fundraisingdaten	133
§ 48	Löschung von Fundraisingdaten	133

Zehnter Abschnitt: Aufgaben der obersten kirchlichen Verwaltungsbehörde

§ 49	Genehmigungsbefugnisse des Oberkirchenrates	133
------	---	-----

Elfter Abschnitt: Schlussbestimmungen

§ 50	Anlagen	133
§ 51	Sprachliche Gleichstellung	133
§ 52	Ausführungsvorschriften	133
§ 53	Inkrafttreten, Außerkrafttreten	133
Anlagen 1 bis 10		134

**Erster Abschnitt:
Ergänzende Durchführungsvorschriften zum
Datenschutzgesetz der EKD**

**§ 1
Geltungsbereich (Einrichtungen und Mitarbeiter)
(zu § 1 Absatz 2 Satz 1 DSGVO-EKD)**

(1) Diese Rechtsverordnung gilt für die Evangelisch-Lutherische Landeskirche Mecklenburgs, ihre Kirchenkreise, Propsteien, Kirchgemeinden, Kirchgemeindeverbände und – ohne Rücksicht auf deren Rechtsform – für deren rechtlich selbständige Dienste, Werke und Einrichtungen, das Diakonische Werk der Evangelisch-Lutherischen Landeskirche Mecklenburgs und für die diesem angeschlossenen Einrichtungen („kirchliche Stellen“) sowie deren jeweiligen Mitarbeiter.

(2) Mitarbeiter im Sinne dieser Rechtsverordnung sind Pastoren, Mitarbeiter, ehrenamtlich Tätige, Auszubildende und den kirchlichen Stellen zur Ausbildung zugewiesene Personen (z. B. Vikare, Rechtsreferendare) sowie Praktikanten.

**§ 2
Führung der Übersichten über die kirchlichen Werke
und Einrichtungen mit eigener Rechtspersönlichkeit
(zu § 1 Absatz 2 Satz 2 und 3 DSGVO-EKD)**

(1) Der Oberkirchenrat soll eine Übersicht über die kirchlichen Dienste, Werke und Einrichtungen mit eigener Rechtspersönlichkeit führen. Die nach § 11 dieser Verordnung Aufsicht führenden kirchlichen Stellen sind verpflichtet, den Oberkirchenrat unverzüglich über die in ihrem Bereich gebildeten kirchlichen Dienste, Werke und Einrichtungen nach Satz 1 in Kenntnis zu setzen. Aufnahmen in die Übersicht und Löschungen werden den Beauftragten für den Datenschutz angezeigt.

(2) Absatz 1 gilt entsprechend für das Diakonische Werk der Evangelisch-Lutherischen Landeskirche Mecklenburgs.

**§ 3
Seelsorgedaten
(zu § 1 Absatz 4 DSGVO-EKD)**

(1) Seelsorgedaten sind personenbezogene Daten, die in Wahrnehmung des Seelsorgeauftrages bekannt werden. Sie beschreiben persönliche, insbesondere familiäre, wirtschaftliche oder berufliche Angelegenheiten des Kirchenmitgliedes oder anderer betroffener Personen.

(2) Aufzeichnungen, die in Wahrnehmung des Seelsorgeauftrages gemacht werden, dürfen nur für diese Zwecke verwendet werden und Dritten nicht zugänglich sein. Eine Weitergabe dieser Unterlagen ist unzulässig. Sie sind nach Gebrauch zu vernichten, wenn ihre Kenntnis für die Wahrnehmung des Seelsorgeauftrages nicht mehr erforderlich ist.

**§ 4
Verpflichtung auf das Datengeheimnis
(zu § 6 DSGVO-EKD)**

(1) Alle personenbezogenen Daten, von denen Mitarbeitende auf Grund ihrer Tätigkeit insbesondere mit Akten, Dateien, Listen und Karteien Kenntnis erhalten, sind von ihnen vertraulich zu behandeln.

(2) Die mit dem Umgang mit personenbezogenen Daten betrauten Mitarbeitenden sind bei der Aufnahme ihrer Tätigkeit schriftlich zur Einhaltung des Datenschutzes und auf das Datengeheimnis zu verpflichten.

(3) Die Verpflichtung nimmt der jeweilige Dienstvorgesetzte vor. Die Verpflichtung auf das Datengeheimnis nach § 6 DSGVO-EKD ist nach dem Muster der Anlage 1 unter Aushändigung des Merkblattes der Anlage 2 vorzunehmen. Das Original der Verpflichtungserklärung ist zur Personalakte der verpflichteten Person oder, sofern eine solche nicht geführt wird, zur Akte Datenschutz zu nehmen.

§ 5
Videoüberwachung
(zu § 7a DSGVO-EKD)

(1) Der Umstand der Beobachtung mit optisch-elektronischen Einrichtungen und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen.

(2) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über eine Verarbeitung oder Nutzung entsprechend § 15a DSGVO-EKD zu benachrichtigen.

§ 6
Anforderungen an Datenverarbeitungsanlagen
(zu § 9 DSGVO-EKD)

(1) Die Anforderungen an die Sicherheitseinstellungen sind in der Verordnung zur Sicherstellung der Anforderungen an den Datenschutz im IT-Bereich geregelt.

(2) Die kirchlichen Stellen nach § 1 dieser Verordnung, die über Datenverarbeitungsanlagen verfügen, haben die nach dem jeweiligen Schutzbedarf vorgeschriebenen Sicherheitseinstellungen zu übernehmen und der obersten kirchlichen Verwaltungsbehörde hierüber einen Nachweis zu erbringen.

§ 7
Einsatz von Programmen auf Datenverarbeitungsanlagen
(zu § 9 DSGVO-EKD)

(1) Der Einsatz nicht vereinbarter oder nicht genehmigter Programme auf Datenverarbeitungsanlagen ist unzulässig.

(2) Über die Freigabe von Programmen und über aktualisierte Versionen von freigegebenen Programmen entscheidet die oberste kirchliche Verwaltungsbehörde, soweit diese nicht die Befugnis nach Maßgabe einer Ausführungsvorschrift einer anderen Behörde übertragen hat. Programme, die bereits in einem kirchlichen Rechenzentrum geprüft sind und von einem von der EKD eingesetztem Gremium freigegeben sind, gelten als freigegeben.

(3) Eine Einsichtnahme der kirchlichen Stelle nach § 1 dieser Verordnung auf die dienstlichen Daten ist zu jeder Zeit zu gewährleisten.

§ 8
Private Datenverarbeitungsanlagen
(zu § 9 DSGVO-EKD)

(1) Die Benutzung privater Datenverarbeitungsanlagen zur Verarbeitung personenbezogener dienstlicher Daten ist nur ausnahmsweise nach Genehmigung durch die oberste kirchliche Verwaltungsbehörde erlaubt gemäß Anlage 3. Die Genehmigung kann befristet werden. Vor der Genehmigung ist eine Überprüfung der privaten Datenverarbeitungsanlage durch eine von der obersten kirchlichen Verwaltungsbehörde benannte autorisierte Person zu ermöglichen.

(2) Die Erhebung, Verarbeitung und Nutzung personenbezogener dienstlicher Daten auf privaten Datenverarbeitungsanlagen einer kirchlichen Stelle nach § 1 dieser Verordnung ist nur nach

Maßgabe der Sicherheitseinstellungen gemäß der Verordnung zur Sicherstellung der Anforderungen an den Datenschutz im IT-Bereich zulässig. Die oberste kirchliche Verwaltungsbehörde ist jederzeit berechtigt, die Einhaltung der Sicherheitseinstellungen zu überprüfen.

(3) Die Erhebung, Verarbeitung und Nutzung personenbezogener dienstlicher Daten, die einer besonderen Geheimhaltungspflicht (Beicht- und Seelsorgegeheimnis) unterliegen, ist auf einer privaten Datenverarbeitungsanlage nicht gestattet.

(4) Endet die nach Absatz 1 genehmigte dienstliche Benutzung einer privaten Datenverarbeitungsanlage, so hat die kirchliche Stelle nach § 1 dieser Verordnung die Löschung der dienstlichen Daten auf der privaten Datenverarbeitungsanlage sicherzustellen. Bei berechtigten Zweifeln an der ordnungsgemäßen Löschung ist die oberste kirchliche Verwaltungsbehörde berechtigt, die Löschung durch eine autorisierte Person durchführen zu lassen. Gegenüber der obersten kirchlichen Verwaltungsbehörde ist schriftlich zu bestätigen, dass die dienstlichen Daten gelöscht sind und keine weiteren privaten Datenträger die genutzten dienstlichen Daten enthalten.

§ 9
Genehmigung der Einrichtung automatisierter
Abrufverfahren mit nichtkirchlichen Stellen
(zu § 10 Absatz 3 Satz 2 DSGVO-EKD)

Die Einrichtung eines automatisierten Abrufverfahrens mit nichtkirchlichen Stellen bedarf der Genehmigung durch die oberste kirchliche Verwaltungsbehörde.

§ 10
Erhebung, Verarbeitung oder Nutzung von
personenbezogenen Daten im Auftrag
(zu § 11 DSGVO-EKD)

(1) Sollen personenbezogene Daten einer kirchlichen Stelle im Auftrag durch andere Stellen oder Personen erhoben, verarbeitet oder genutzt werden, so ist hierüber eine Vereinbarung nach dem Muster der Anlage 4 zu schließen.

(2) Für die nach § 11 Absatz 2 Satz 3 DSGVO-EKD erforderliche Genehmigung über die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten im Auftrag durch andere Stellen oder Personen ist die nach § 11 dieser Verordnung Aufsicht führende Stelle zuständig.

(3) Soweit es sich bei den beauftragenden Stellen um kirchliche Dienste, Werke oder Einrichtungen mit eigener Rechtspersönlichkeit handelt, die Mitglieder der Diakonischen Werke sind, ist für die Genehmigung der Vorstand des jeweiligen Diakonischen Werkes oder eine von ihm beauftragte Person zuständig.

(4) Die Erteilung einer allgemeinen Genehmigung in den Fällen des Absatzes 2 ist zulässig.

§ 11
Einhaltung und Durchführung des Datenschutzes
(zu § 14 Absatz 1 DSGVO-EKD)

(1) Im Bereich der Evangelisch-Lutherischen Landeskirche Mecklenburgs obliegt dem Oberkirchenrat die Aufsicht über die

Einhaltung des Datenschutzes und die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, bezogen auf die kirchlichen Stellen.

(2) Für die Einhaltung eines ausreichenden Datenschutzes in den Werken und Einrichtungen mit eigener Rechtspersönlichkeit, für die das kirchliche Datenschutzrecht gilt, sind die durch Kirchengesetz, Satzung, Vereinbarung oder Stiftungsurkunde bestimmten Aufsichtsorgane, Leitungs- oder Vertretungsorgane zuständig.

(3) Das Diakonische Werk der Landeskirche nimmt gegenüber den ihm angeschlossenen Werken und Einrichtungen, für die das kirchliche Datenschutzrecht gilt, die Aufsicht über die Einhaltung der Vorschriften über den Datenschutz wahr. Das Diakonische Werk hat den Oberkirchenrat über wichtige Vorgänge zu informieren. Der Oberkirchenrat ist befugt, beim Diakonischen Werk Auskünfte einzuholen, soweit diese die Aufsicht über die Einhaltung des Datenschutzes betreffen.

§ 12

Übersicht über automatisierte Verarbeitungen und Meldepflicht

(zu §§ 14 Absatz 2 und 21 Absatz 1 und 2 DSGVO)

(1) Die Übersicht nach § 14 Absatz 2 DSGVO wird von den kirchlichen Stellen jeweils für ihren Zuständigkeitsbereich nach dem Muster der Anlage 5 geführt; sie ist laufend auf dem neuesten Stand zu halten. Das Merkblatt der Anlage 6 ist zu beachten.

(2) Die Übersicht ist dem Datenschutzbeauftragten der Evangelisch-Lutherischen Landeskirche Mecklenburgs auf Anforderung zu übermitteln. Für den diakonischen Bereich ist die Übersicht an den Datenschutzbereich für den Diakonischen Bereich zu übermitteln.

§ 13

Löschung

(zu § 16 Absatz 2 DSGVO)

Bereichsspezifische Regelungen über die Aufbewahrung, Aussonderung und Löschung personenbezogener Daten sowie insbesondere die entsprechenden Vorschriften des Archivrechts bleiben unberührt.

§ 14

Aufgaben der Datenschutzbeauftragten

(zu §§ 18 und 19 DSGVO)

(1) In der Evangelisch-Lutherischen Landeskirche Mecklenburgs werden je ein Beauftragter für den Datenschutz und je ein ständiger Vertreter sowohl für den Bereich des Diakonischen Werkes der Evangelisch-Lutherischen Landeskirche Mecklenburgs (Datenschutzbeauftragter der Diakonie) als auch für den sonstigen Bereich (Landeskirchlicher Datenschutzbeauftragter) berufen, die den im Kirchengesetz über den Datenschutz beschriebenen Auftrag jeweils für ihr Aufgabengebiet wahrnehmen.

(2) Der Landeskirchliche Datenschutzbeauftragte und der Datenschutzbeauftragte der Diakonie sowie die jeweiligen ständigen

Vertreter werden von der Kirchenleitung gemäß den Vorschriften des Leitungsgesetzes berufen und abberufen. Der Oberkirchenrat hat dabei das Vorschlagsrecht des Diakonischen Rates für die Beauftragten der Diakonie zu beachten.

(3) Die Amtszeit der Datenschutzbeauftragten und ihrer ständigen Vertreter beträgt vier Jahre. Sie beginnt mit der Berufung. Eine Wiederberufung für weitere Amtszeiten ist zulässig.

(4) Ein Datenschutzbeauftragter ist abzuberufen, wenn Gründe vorliegen, aus denen ein Mitglied des Verfassungs- und Verwaltungsgerichts der Vereinigten Evangelisch-Lutherischen Kirche Deutschlands sein Amt verliert oder nicht mehr ausüben kann. Weiter können sie abberufen werden, wenn ein gedeihliches Zusammenwirken der Datenschutzbeauftragten nicht mehr gewährleistet ist. Scheidet ein Datenschutzbeauftragter oder ein ständiger Vertreter während seiner Amtsdauer aus, wird sein Nachfolger für den Rest der Amtsdauer des Vorgängers berufen.

(5) Die Berufung, der Dienstsitz sowie eine Abberufung sind im Kirchlichen Amtsblatt bekannt zu geben.

(6) Der Zuständigkeitsbereich der Datenschutzbeauftragten beurteilt sich nach dem Rechtsträger, bei dem die personenbezogenen Daten erhoben, verarbeitet oder verwaltet werden, unbeschadet dessen Rechtsform.

(7) Der Landeskirchliche Datenschutzbeauftragte und dessen ständiger Vertreter unterstehen der Dienstaufsicht des Vorsitzenden der Kirchenleitung. Der Datenschutzbeauftragte der Diakonie und dessen ständiger Vertreter unterstehen der Dienstaufsicht des Landespastors für Diakonie. Hiervon unberührt bleibt, dass die Datenschutzbeauftragten in Ausübung ihres Amtes an Weisungen nicht gebunden und nur dem kirchlichen Recht unterworfen sind.

(8) Soweit für die Datenschutzbeauftragten weitere Hilfskräfte tätig werden, ist bei einer Aufgabenerfüllung nach diesem Gesetz der zuständige Datenschutzbeauftragte Dienstvorgesetzter mit Weisungsbefugnis für diese Hilfskräfte.

(9) Die Datenschutzbeauftragten sind bei ihrer Aufgabenerfüllung gleichberechtigt. Sie sollen vertrauensvoll zusammenarbeiten.

(10) Eine Zusammenarbeit der Datenschutzbeauftragten mit staatlichen, kommunalen oder sonstigen Beauftragten für den Datenschutz hat im Benehmen mit dem jeweils anderen Datenschutzbeauftragten zu erfolgen. Bei Fragen, die den Gesamtbereich des kirchlichen Datenschutzes betreffen, stimmen sich die Datenschutzbeauftragten vor einer Stellungnahme gegenüber staatlichen und kirchlichen Stellen ab.

(11) Die Kirchenleitung kann mit anderen Gliedkirchen der Evangelischen Kirche in Deutschland Vereinbarungen über die Bestellung von gemeinsamen Datenschutzbeauftragten treffen.

(12) Die Berichte des Datenschutzbeauftragten sind der Landessynode zugänglich zu machen. Es kann eine Aussprache stattfinden.

(13) Die oberste kirchliche Verwaltungsbehörde und das Diakonische Werk haben die Datenschutzbeauftragten auf Verlangen bei Ihrer Aufgabenerfüllung zu unterstützen.

(14) Bei der Prüfung von Unterlagen durch die Datenschutzbeauftragten gehen die Vorschriften des Disziplinarrechts den Vorschriften des Datenschutzgesetzes der EKD vor, wenn gegen die betroffene Person ein Verfahren bei der Disziplinarkammer anhängig ist.

§ 15

Beanstandungen der Datenschutzbeauftragten (zu § 20 DSGVO-EKD)

Beanstandungen der Datenschutzbeauftragten gemäß § 20 DSGVO-EKD erfolgen gegenüber dem Leitungsorgan der betroffenen Dienststelle oder Einrichtung unter Benachrichtigung der für diese Dienststelle oder Einrichtung Aufsicht führenden Stelle.

§ 16

Betriebsbeauftragte und örtlich Beauftragte für den Datenschutz (zu § 22 DSGVO-EKD)

(1) Die Bestellung von Betriebsbeauftragten und örtlich Beauftragten für den Datenschutz erfolgt durch die gesetzlich oder satzungsgemäß berufenen Organe der Dienste, Werke oder Einrichtungen.

(2) Vor der Bestellung gemeinsamer Betriebsbeauftragter und örtlich Beauftragter für den Datenschutz hat jede beteiligte kirchliche Stelle ihre Zustimmung zur Bestellung zu erklären. Dabei können Vereinbarungen zum Arbeitsumfang und zur Finanzierung getroffen werden.

(3) Die Bestellung von Beauftragten nach Absatz 1 kann befristet oder unbefristet erfolgen. Sie erfolgt schriftlich nach dem Muster der Anlage 7, das Merkblatt der Anlage 8 ist zu beachten. Die Bestellung kann nach Anhörung der betroffenen Beauftragten schriftlich widerrufen werden, wenn ein Interessenkonflikt mit anderen Aufgaben oder sonst ein wichtiger Grund eintritt. Die Bestellung ist den Mitarbeitern in geeigneter Weise bekannt zu geben.

(4) Die Bestellung und der Widerruf von Beauftragten nach Absatz 1 ist dem Datenschutzbeauftragten und der für die Aufsicht über die Einhaltung des Datenschutzes gemäß § 11 zuständigen Stelle unverzüglich schriftlich anzuzeigen.

(5) Die kirchlichen Stellen sind verpflichtet, Verfahren automatisierter Verarbeitung vor Inbetriebnahme den Beauftragten nach Absatz 1 zu melden.

Zweiter Abschnitt: Gemeindeglieder- und Amtshandlungsdaten

§ 17

Gemeindegliederdaten

(1) Unbeschadet der Vorschriften des DSGVO-EKD über die Kirchenmitgliedschaft und der zu seiner Ergänzung und Durchführung ergangenen Vorschriften dürfen die von den kommunalen Stellen übermittelten Meldedaten und die von kirchlichen Stellen erhobenen personenbezogenen Daten für die Führung der Gemeindegliederverzeichnisse sowie für kirchengesetzlich bestimmte kirchliche Aufgaben verarbeitet und genutzt werden.

(2) Daten aus dem Kirchenbuchwesen, der Kirchgelderhebung und der Erhebung freiwilliger Beiträge dürfen mit Meldewesensdaten wechselseitig verknüpft werden.

(3) Die aus den kommunalen Melderegistern übermittelten Auskunfts- und Übermittlungssperren sind in die Gemeindegliederverzeichnisse aufzunehmen und zu beachten. Personenbezogene Daten von Personen, für die Auskunfts- oder Übermittlungssperren bestehen, dürfen für Veröffentlichungen nur genutzt werden, wenn vorher das schriftliche Einverständnis der betroffenen Personen eingeholt wurde.

(4) Auskünfte aus dem Gemeindegliederverzeichnis erteilen die zu dessen Führung verpflichteten kirchlichen Stellen nur nach Maßgabe des § 15 DSGVO-EKD.

(5) Die Weitergabe von personenbezogenen Daten von Gemeindegliedern zur gewerblichen, politischen oder vergleichbaren privaten Nutzung ist nicht zulässig.

§ 18

Veröffentlichung von Gemeindeglieder- und Amtshandlungsdaten

(1) Die Kirchengemeinden dürfen personenbezogene Daten im Zusammenhang mit Amtshandlungen und mit Geburtstagen oder Jubiläen von Gemeindegliedern in Gemeindebriefen und anderen örtlichen kirchlichen Publikationen mit Namen sowie Tag und Ort des Ereignisses veröffentlichen, soweit die Betroffenen im Einzelfall nicht widersprochen haben. Auf das Widerspruchsrecht sind die Betroffenen rechtzeitig vor der Veröffentlichung schriftlich hinzuweisen. Bei regelmäßigen Veröffentlichungen ist es ausreichend, wenn ein Hinweis auf das Widerspruchsrecht an derselben Stelle wie die Veröffentlichung erfolgt. Das in Anlage 9 enthaltene Merkblatt ist zu beachten.

(2) Die Veröffentlichung personenbezogener Daten im Internet ist nur zulässig, wenn die Einwilligung der betroffenen Person vorher schriftlich eingeholt wurde, dafür ist das Muster der Anlage 10 zu verwenden.

Dritter Abschnitt: Verkündigungsdienste

§ 19

Theologiestudierende und Theologen

(1) Die zuständige kirchliche Stelle darf personenbezogene Daten der in die Liste der Theologiestudierenden Eingetragenen erheben, verarbeiten und nutzen, soweit dies zur Förderung des Studiums, zur Begleitung und Beratung bei der Ausbildung, zu Prüfungszwecken sowie zur Durchführung der in § 24 Absatz 1 DSGVO-EKD genannten Maßnahmen erforderlich ist.

(2) Zur Förderung, Begleitung und Beratung der Theologiestudierenden dürfen Name, Vorname, Adresse einschließlich Telefonnummer, Fax-Nummer und E-Mail-Adresse sowie der Studienort an Konvente und Vorstand der Theologiestudierendenschaft und an den Konvent der Vikarinnen und Vikare übermittelt werden.

(3) Die zuständige kirchliche Stelle darf für die in § 24 Absatz 1 DSGVO-EKD genannten Zwecke bei Pastoren, Vikaren und Bewerbern für den Vorbereitungsdienst sowie bei den Theologiestudie-

renden personenbezogene Daten von Angehörigen erheben, verarbeiten und nutzen, soweit dies zur Aufgabenerfüllung erforderlich ist.

§ 20 Ehrenamtlich Tätige

Personenbezogene Daten der in der kirchlichen oder in der diakonischen Arbeit ehrenamtlich Tätigen dürfen von der zuständigen kirchlichen Stelle zur Wahrnehmung ihrer Aufgaben erhoben, verarbeitet und genutzt werden.

Vierter Abschnitt: Bildungswesen

§ 21 Schüler sowie deren Sorgeberechtigte

(1) Schulen in kirchlicher und in diakonischer Trägerschaft dürfen personenbezogene Daten ihrer Schüler sowie deren Sorgeberechtigten erheben, verarbeiten und nutzen, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist. Die zuständige kirchliche Stelle hat neben der Schule die Befugnisse nach Satz 1.

(2) Daten nach Absatz 1 Satz 1 dürfen im Zusammenhang mit dem Übergang von Schülern in eine andere Schule dieser Schule oder dem Schulträger übermittelt werden.

(3) Verhaltensdaten von Schülern, Daten über gesundheitliche Auffälligkeiten und etwaige Behinderungen und Daten aus psychologischen und ärztlichen Untersuchungen dürfen nicht automatisiert verarbeitet werden. Daten über besondere pädagogische, soziale und therapeutische Maßnahmen und deren Ergebnisse dürfen nur erhoben und verarbeitet werden, soweit für die Schüler eine besondere schulische Betreuung in Betracht kommt. Dies gilt auch für entsprechende außerschulische personenbezogene Daten, die der Schule amtlich bekannt geworden sind. Es ist durch technische und organisatorische Maßnahmen sicherzustellen, dass der Schutz der verarbeiteten personenbezogenen Daten gewährleistet ist und die Löschungsbestimmungen eingehalten werden.

(4) Daten nach Absatz 3 Satz 1 und 2 dürfen im Zusammenhang mit dem Übergang von Schülern in eine andere Schule dieser Schule oder dem Schulträger nicht übermittelt werden.

(5) Die in Absatz 1 Satz 1 genannten Daten dürfen einer kirchlichen Stelle sowie sonstigen Stellen außerhalb des kirchlichen Bereichs, insbesondere einer Schule, der Schulaufsichtsbehörde, dem Gesundheitsamt, dem Jugendamt, dem jeweiligen Jugendamt auf Länderebene, den Ämtern für Ausbildungsförderung und dem jeweiligen Amt für Ausbildungsförderung auf Länderebene nur übermittelt werden, soweit sie von diesen Stellen zur Erfüllung der ihnen durch Rechtsvorschrift übertragenen Aufgaben benötigt werden. Dem schulpädagogischen Dienst dürfen personenbezogene Daten nur mit schriftlicher Einwilligung der Betroffenen übermittelt werden.

(6) Die Verarbeitung personenbezogener Daten von Schülern in privaten Datenverarbeitungsanlagen von Lehrern für dienstliche Zwecke ist abweichend von § 8 dieser Verordnung zulässig, bedarf aber der schriftlichen Genehmigung durch die Schulleitung. Die Genehmigung darf nur erteilt werden, wenn die Verarbeitung der personenbezogenen Daten nach Art und Umfang für die Erfüllung der schulischen Aufgaben erforderlich ist und ein

angemessener technischer Zugangsschutz entsprechend der Verordnung zur Sicherstellung der Anforderungen an den Datenschutz in der Informationstechnik nachgewiesen wird. Die Lehrer sind verpflichtet, der Schulleitung sowie dem jeweiligen Beauftragten für den Datenschutz alle Auskünfte zu erteilen, die für die datenschutzrechtliche Verantwortung erforderlich sind.

§ 22 Lehrkräfte

(1) Schulen dürfen von ihren Lehrkräften personenbezogene Daten erheben, verarbeiten und nutzen, soweit dies zur Aufgabenerfüllung, insbesondere bei der Unterrichtsorganisation sowie in dienstrechtlichen, arbeitsrechtlichen oder sozialen Angelegenheiten erforderlich ist.

(2) Die in Absatz 1 genannten Daten dürfen kirchlichen Stellen, staatlichen Schulaufsichtsbehörden sowie weiteren Stellen außerhalb des kirchlichen Bereichs nur übermittelt werden, soweit sie von diesen zur Erfüllung der ihnen durch Rechtsvorschrift übertragenen Aufgaben benötigt werden.

§ 23 Bildungs-, Ausbildungs- und religionspädagogische Einrichtungen

(1) Bildungs-, Ausbildungs- und religionspädagogische Einrichtungen dürfen im Rahmen der von ihnen durchgeführten Maßnahmen personenbezogene Daten der Lehrenden und Teilnehmenden erheben, verarbeiten und nutzen, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist.

(2) Die in Absatz 1 genannten personenbezogenen Daten dürfen für Zwecke der Aus-, Fort- und Weiterbildung an staatliche Schulaufsichtsbehörden, Schulen und andere kirchliche Stellen übermittelt werden, soweit dies zur Aufgabenerfüllung dieser Stellen erforderlich ist. Eine Veröffentlichung der personenbezogenen Daten bedarf der vorherigen schriftlichen Einwilligung der Betroffenen.

(3) Kirchliche Stellen gemäß § 1 dieser Verordnung dürfen den Ausbildungsstätten bei Anmeldung zu Studium und Prüfung sowie bei Zuweisung zum fachtheoretischen Unterricht personenbezogene Daten der Kircheninspektorenanwärter übermitteln, soweit dies zur Aufgabenerfüllung der Ausbildungsstätten erforderlich ist; das gleiche gilt hinsichtlich der für die praktische Ausbildung zuständigen Verwaltungsstellen und die Prüfungsämter für Verwaltungslaufbahnen. Für kirchliche Angestellte gilt Satz 1 entsprechend.

§ 24 Tagungen und sonstige kirchliche Veranstaltungen

(1) Die zuständigen kirchlichen Stellen dürfen bei ihren Veranstaltungen personenbezogene Daten der Teilnehmenden und sonstigen Mitwirkenden erheben, verarbeiten und nutzen, soweit dies für die Durchführung der Veranstaltung notwendig ist.

(2) Die Teilnehmerlisten von Veranstaltungen dürfen allen Teilnehmern übermittelt werden, soweit nicht ein Betroffener vorher der Übermittlung seiner Daten widersprochen hat. Eine Übermittlung an weitere Dritte sowie die Veröffentlichung bedürfen der vorherigen schriftlichen Einwilligung der Betroffenen.

(3) Die personenbezogenen Daten von Teilnehmern dieser Veranstaltungen dürfen mit vorheriger Einwilligung der Betroffenen gespeichert und genutzt werden, soweit die kirchlichen Stellen diesen Personen weitere Schulungshinweise, Arbeits- und Informationsmaterial sowie weitere Auskünfte über Veranstaltungen und Entwicklungen einzelner Fortbildungssachgebiete vermitteln oder zielgruppengerichtete Einladungen zu weiteren kirchlichen Veranstaltungen ermöglichen wollen.

Fünfter Abschnitt: Kirchliche Abgaben, Finanzwesen, Grundstückswesen

§ 25

Steuergeheimnis, Steuerdaten

(1) Die Wahrung des Steuergeheimnisses geht den Regelungen des Datenschutzes vor.

(2) Diejenigen Personen, die mit der Bearbeitung von Steuer-sachen befasst sind oder von Steuersachen Kenntnis erlangen, sind zusätzlich schriftlich zur Wahrung des Steuergeheimnisses zu verpflichten.

(3) Personenbezogene Daten, die in Ausübung der Berufs- und Amtspflicht von einer zur Wahrung des Steuergeheimnisses verpflichteten Person übermittelt worden sind, dürfen nicht zu anderen Zwecken als zur Verwaltung der Kirchensteuer sowie zur Führung des Gemeindegliederverzeichnisses und zum Abgleich der Meldedaten gespeichert, verarbeitet oder genutzt werden.

§ 26

Kirchgeld

Die für die Festsetzung und Erhebung des Kirchgeldes benötigten personenbezogenen Daten dürfen aus dem Gemeindegliederverzeichnis erhoben und zweckentsprechend verarbeitet und genutzt werden. § 25 dieser Verordnung gilt entsprechend.

§ 27

Übermittlung von Steuerdaten zwischen steuererhebenden Körperschaften und dem Oberkirchenrat

Die Übermittlung der Steuerdaten zwischen den steuererhebenden Körperschaften und dem Oberkirchenrat ist zulässig, soweit dies zur ordnungsgemäßen Besteuerung und Verwaltung der Kirchensteuern erforderlich ist.

§ 28

Freiwillige Beiträge

Soweit die Kirchengemeinden von den Gemeindegliedern sonstige freiwillige Beiträge erheben, gilt § 25 dieser Verordnung entsprechend. Die für die Beitragserhebung benötigten personenbezogenen Daten dürfen aus dem Gemeindegliederverzeichnis, im übrigen nur bei den betroffenen Gemeindegliedern erhoben und zweckentsprechend verarbeitet und genutzt werden.

§ 29

Nutzung von Grundstücken und Gebäuden

Die zuständigen kirchlichen Stellen dürfen, sofern sie Dritten Grundstücke, Gebäude, Gebäudeteile oder Wohnraum zur Miete oder sonst zur Nutzung überlassen oder daran Rechte einräumen, die zur verwaltungsmäßigen Abwicklung und Überprüfung erforderlichen personenbezogenen Daten der Nutzungsberechtigten erheben, verarbeiten und nutzen.

§ 30

Kirchliche Friedhöfe

(1) Zur Bewirtschaftung und Verwaltung der Friedhöfe, insbesondere zur Festsetzung und Einziehung von Gebühren und Entgelten sowie zur Klärung der Übertragung von Nutzungsrechten dürfen vom Friedhofsträger, von der Kirchenkreisverwaltung oder von einer Friedhofsverwaltungsgemeinschaft die erforderlichen personenbezogenen Daten der Verstorbenen, der Nutzungsberechtigten und der Auftraggeber erhoben, verarbeitet und genutzt werden.

(2) Im Rahmen der Zulassung und Überwachung der auf den Friedhöfen tätigen Gewerbetreibenden dürfen vom Friedhofsträger oder in seinem Auftrag die erforderlichen personenbezogenen Daten erhoben, verarbeitet und genutzt werden.

(3) Der Friedhofsträger darf zum Zwecke der Bestattung die notwendigen personenbezogenen Daten der verstorbenen und der nutzungsberechtigten Person sowie von Angehörigen an die Stelle oder an den Pastor übermitteln, der die Bestattung vornimmt.

(4) Bei der Ausgrabung und Umbettung von Leichen dürfen den zuständigen Gesundheitsbehörden die notwendigen personenbezogenen Daten der Verstorbenen übermittelt werden.

(5) Lässt sich ein Friedhofsträger bei der Genehmigung von Grabmalen bezüglich deren Gestaltung von Sachverständigen beraten, so dürfen den Sachverständigen zur Prüfung der vorgelegten Anträge die dafür notwendigen personenbezogenen Daten übermittelt werden.

(6) Zum Zwecke der Vollstreckung von Friedhofsgebühren dürfen den zuständigen Behörden die notwendigen personenbezogenen Daten übermittelt werden.

(7) Die Lage von Grabstätten darf Dritten auf entsprechende Nachfrage bekannt gegeben werden, wenn diese ein berechtigtes Interesse glaubhaft machen und anzunehmen ist, dass schutzwürdige Belange der verstorbenen und der nutzungsberechtigten Person nicht beeinträchtigt werden.

Sechster Abschnitt: Daten von Beschäftigten, Verzeichnisse über Personen und Dienste

§ 31

Verzeichnisse, dienstliche Veröffentlichungen

(1) Verzeichnisse, die Namen, Vornamen, Dienst- oder Amtsbezeichnung, dienstliche Anschriften, E-Mail-Adressen und Telefonnummern von Pastoren, Kirchenbeamten, Mitarbeitern sowie sonstiger Inhaber kirchlicher Ämter oder Ehrenämter enthalten (Verzeichnisse), dürfen für die kirchliche und diakonische Arbeit unter Verwendung der vorliegenden personenbezogenen Daten

hergestellt, verarbeitet und genutzt werden; entsprechendes gilt für Pastoren im Ruhestand.

(2) Verzeichnisse dürfen für die Zusammenarbeit der kirchlichen Stellen, zur Information der ehrenamtlichen Mitglieder kirchlicher Gremien, der Mitarbeiter sowie der öffentlichen und sonstigen Stellen und Personen im Sinne der §§ 12 und 13 DSGVO übermitteln werden, soweit dies aus organisatorischen Gründen und zur Aufgabenerfüllung erforderlich ist.

(3) In die Verzeichnisse dürfen weitere personenbezogene Daten (z. B. Geburtsdatum, Einsegnung, Ordination, Dienstantritt, Ernennung, private Anschriften) sowie Daten, die für die notwendige innerkirchliche dienstliche Zusammenarbeit erforderlich sind, aufgenommen werden, wenn die vorherige schriftliche Einwilligung der Betroffenen vorliegt. Für ein Verzeichnis, das ausschließlich im Bereich der Personalverwaltung und der Visitation des Bischofs oder des Landessuperintendenten zur Verfügung steht, dürfen diese Daten auch ohne Einwilligung der Betroffenen erhoben und genutzt werden soweit dies für die Erreichbarkeit erforderlich ist; dies gilt nicht für die Daten von Inhabern kirchlicher Ehrenämter.

(4) Die Übermittlung von personenbezogenen Daten für Verzeichnisse nach Absatz 1 und Absatz 3 Satz 1 an Verlage oder an Herausgeber von Verzeichnissen ist nur zulässig, soweit ein in Auftrag gegebenes Verzeichnis für den kircheninternen Dienstgebrauch erforderlich ist und sofern bei dem nach Absatz 3 Satz 1 vorgesehenen Umfang des Verzeichnisses die Betroffenen vorher eingewilligt haben.

(5) Im Kirchlichen Amtsblatt dürfen die erforderlichen personenbezogenen Daten nach Absatz 1 von den bei kirchlichen Stellen beschäftigten Mitarbeitenden sowie von ehrenamtlich Tätigen veröffentlicht werden, wenn dies im kirchlichen Interesse liegt.

(6) Die Vorschriften des Vierten Abschnitts dieser Verordnung bleiben unberührt.

§ 32

Personenangaben im Dienstbetrieb, Bearbeitung von Beihilfeangelegenheiten

(1) Soweit in Ausübung von Dienst- und Arbeitsverhältnissen personenbezogene Daten erhoben, verarbeitet oder genutzt werden, ist § 24 DSGVO anzuwenden; dienst- und mitarbeiterrechtliche Regelungen, insbesondere die Bestimmungen des Mitarbeitervertretungsrechts, bleiben unberührt.

(2) Die in Anträgen auf die Gewährung von Beihilfen in Krankheits-, Pflege- und Geburtsfällen enthaltenen personenbezogenen Daten von Antragstellenden sowie ihrer Familienangehörigen dürfen nur von der für die Gewährung der Beihilfe zuständigen Stelle erhoben, verarbeitet und genutzt werden.

(3) Bei Wechsel des Anstellungsträgers des Beihilfeberechtigten oder der für die Festsetzung der Beihilfe zuständigen Stelle dürfen die für die Bearbeitung von Beihilfeanträgen notwendigen personenbezogenen Daten übermittelt werden.

(4) Soweit die zuständige Stelle sich zur Durchführung ihrer Aufgaben nach Absatz 2 eines Dritten bedient, dürfen die zur Festsetzung der Beihilfe erforderlichen Daten an diese Stelle weitergegeben werden, soweit diese Stelle ihrerseits auf die Geheimhaltung der Daten verpflichtet worden ist und dem Sicherheits-

standard der Verordnung zur Sicherstellung der Anforderungen an den Datenschutz in der Informationstechnik entspricht.

(5) Eine Datenübermittlung personenbezogener Daten an Rückdeckungsversicherungen zu Zwecken des Abschlusses von Rückdeckungsversicherungen für Pastoren zur Anstellung ist zulässig.

§ 33

Mitglieder von Gremien und Ausschüssen

Personenbezogene Daten von Mitgliedern der Gremien kirchlicher Stellen sowie von diesen gebildeter Ausschüsse und Arbeitsgruppen können erhoben, verarbeitet und genutzt werden, soweit dies für die Arbeit der Gremien erforderlich ist.

§ 34

Dienstwohnungen

(1) Die zuständigen kirchlichen Stellen dürfen, sofern sie Dienstwohnungen an Beschäftigte überlassen, die personenbezogenen Daten der Wohnungsinhaber erheben, verarbeiten und nutzen, die zur Durchführung der Nutzungsverhältnisse einschließlich der Abrechnung der Dienstwohnungsvergütung erforderlich sind. Diese Daten dürfen, soweit es zur ordnungsgemäßen Abwicklung der laufenden Vorgänge und zur Überprüfung erforderlich ist, zwischen den beteiligten Stellen ausgetauscht werden.

(2) Die steuerrechtlich geregelten Mitteilungspflichten bleiben unberührt.

§ 35

Darlehen, Gehaltsvorschüsse, Unterstützungen

Die zuständigen kirchlichen Stellen dürfen die für die Gewährung von Darlehen, Gehaltsvorschüssen und Unterstützungen erforderlichen personenbezogenen Daten der Empfänger sowie gegebenenfalls mithaftender Familienangehöriger oder Bürgen erheben, verarbeiten und nutzen; dies gilt auch zur Sicherung und Tilgung der Forderungen und zur Vorlage von Verwendungsnachweisen.

§ 36

Versorgung

(1) Die zuständigen kirchlichen Stellen dürfen zur Bearbeitung und Zahlung von Versorgungsbezügen einschließlich der Zahlung von Nachversicherungsbeiträgen und sämtlichen Arten des Versorgungslastenausgleichs sowie von Beihilfen in Krankheits-, Pflege- und Geburtsfällen diejenigen personenbezogenen Daten der betroffenen Personen erheben, verarbeiten und nutzen, die für die Erhebung der Versorgungsbeiträge und für die Berechnung und Zahlung der Versorgungsbezüge sowie für die Gewährung von Beihilfen und Leistungen nach dem Pflegeversicherungsgesetz erforderlich sind.

(2) Die Zusatzversorgungskassen dürfen zur Bearbeitung und Zahlung von Altersrenten, Erwerbsunfähigkeits- und Berufsunfähigkeitsrenten, Hinterbliebenenrenten sowie weiterer Versicherungsleistungen diejenigen personenbezogenen Daten der Mitarbeiter sowie der Empfänger von Renten erheben, verarbeiten und nutzen, die für die Zahlung der Umlagen und für die Berechnung und Zahlung der Renten und weiterer Versicherungsleistungen erforderlich sind.

Siebter Abschnitt: Archiv**§ 37****Benutzer des Archivs**

(1) Personenbezogene Daten von Benutzern der kirchlichen Archive dürfen erhoben, verarbeitet und genutzt werden, soweit dies für die Erfüllung der Aufgaben erforderlich ist.

(2) Personenbezogene Daten der Benutzer, die an wissenschaftlichen Themen oder Dissertationen arbeiten, dürfen mit den Angaben zum Thema der Arbeit an den zentralen Nachweis wissenschaftlicher Themen und Bearbeiter in kirchlichen Archiven übermittelt werden, soweit die Betroffenen im Einzelfall nicht widersprochen haben.

Achter Abschnitt: Diakonische Arbeitsbereiche**§ 38****Einrichtungen der Kinder- und Jugendhilfe**

(1) Betreibt eine kirchliche Stelle eine Einrichtung der Jugendhilfe, insbesondere eine Tageseinrichtung für Kinder, und ist für den Betrieb durch den Leistungserbringer oder Träger die Erhebung, Verarbeitung, insbesondere Übermittlung, sowie Nutzung personenbezogener Daten erforderlich, sind die Vorschriften über den Schutz personenbezogener Daten des Achten Buches Sozialgesetzbuch [SGB VIII] entsprechend anzuwenden.

(2) Tageseinrichtungen für Kinder dürfen personenbezogene Daten der Kinder und deren Sorgeberechtigter und der von diesen Beauftragten erheben, verarbeiten und nutzen, soweit dies zur Erfüllung des Auftrags der Tageseinrichtungen und ihrer Fürsorgeaufgaben erforderlich ist.

(3) Personenbezogene Daten, die für die Festsetzung der Elternbeiträge erforderlich sind, dürfen die Träger ausschließlich zu diesem Zweck erheben, verarbeiten und nutzen. Die Daten nach Satz 1 sind bei den Betroffenen selbst zu erheben; sie dürfen nicht an andere Stellen übermittelt werden, es sei denn, eine kommunale Körperschaft benötigt sie zur Festsetzung oder Erhebung der Beiträge. Unterlagen dürfen nur in dem Umfang übermittelt werden, wie sie zur Festsetzung der Elternbeiträge erforderlich sind. Auf die Pflicht zur Auskunft für die Berechnung, Übernahme und die Ermittlung oder den Erlass von Teilnahme- oder Kostenbeiträgen nach dem Achten Buch Sozialgesetzbuch [SGB VIII] soll hingewiesen werden.

(4) Personenbezogene Daten der in den Einrichtungen nach Absatz 1 aufgenommenen Kinder dürfen mit vorherigem Einverständnis der Sorgeberechtigten erhoben und durch den Träger oder die von ihm beauftragten Stellen verarbeitet und genutzt werden, sofern dies für Zwecke der Gemeindearbeit erforderlich ist. Das gleiche gilt für Zwecke des öffentlichen Schulwesens nach Maßgabe der hierfür geltenden Bestimmungen.

§ 39**Krankenhäuser, Vorsorge- und Rehabilitationseinrichtungen**

(1) Daten von Patienten (Patientendaten) dürfen in kirchlichen Krankenhäusern, Vorsorge- oder Rehabilitationseinrichtungen erhoben, verarbeitet und genutzt werden, soweit

1. dies im Rahmen des Behandlungsverhältnisses einschließlich der verwaltungsmäßigen Abwicklung und Leistungsberechnung, zur Erfüllung der mit der Behandlung im Zusammenhang stehenden Dokumentationspflichten oder eines damit zusammenhängenden Rechtsstreites erforderlich ist oder
2. eine staatliche oder kirchliche Rechtsvorschrift dies vorsieht oder
3. der Betroffene schriftlich eingewilligt hat.

Zu den Patientendaten zählen auch personenbezogene Daten Dritter, die dem Krankenhaus, der Vorsorge- oder Rehabilitationseinrichtung im Zusammenhang mit der Behandlung und Pflege bekannt werden.

(2) Für die Qualitätssicherung einschließlich Leistungsauswertung und -entwicklung im Krankenhaus und die Aus-, Fort- oder Weiterbildung ist der Zugriff auf Patientendaten nur in anonymisierter Form zulässig. Andernfalls ist eine vorherige schriftliche Einwilligung der Patienten erforderlich.

(3) Die Verarbeitung und Nutzung von Patientendaten durch den Sozialdienst und die Krankenhauseelsorge ist zulässig, soweit dies für die soziale Betreuung und zur Erfüllung seelsorgerlicher Aufgaben erforderlich ist.

(4) An die Seelsorger der für die Patienten zuständigen Gemeinde dürfen zur Erfüllung seelsorgerlicher Aufgaben Name, Vorname, Geburtsdatum, Bekenntnisstand, Wohnsitz und Aufnahme datum übermittelt werden, sofern der Patient der Übermittlung zugestimmt hat oder keine Anhaltspunkte dafür bestehen, dass eine Übermittlung nicht angebracht ist. Zu der Ermittlung der zuständigen Gemeinde können die Daten nach Satz 1 an die für das kirchliche Meldewesen zuständige Stelle übermittelt und von dort an die Seelsorger der für die Patienten zuständigen Gemeinde weitergeleitet werden. Der Patient ist bei der Aufnahme darauf hinzuweisen, dass der Übermittlung zuzustimmen ist.

(5) Die Übermittlung von Patientendaten an Stellen und Personen außerhalb des Krankenhauses und deren Nutzung ist neben der Erfüllung von Pflichten auf Grund bestehender Rechtsvorschriften nur zulässig, soweit dies erforderlich ist zur

1. Behandlung einschließlich der Mit-, Weiter- und Nachbehandlung, wenn der Patient nach Hinweis auf die beabsichtigte Übermittlung nicht etwas anderes bestimmt hat;
2. Abwehr einer gegenwärtigen Gefahr für das Leben, die Gesundheit oder die persönliche Freiheit des Patienten oder Dritter, sofern diese Rechtsgüter das Geheimhaltungsinteresse des Patienten erheblich überwiegen und die Abwendung der Gefahr ohne die Übermittlung nicht möglich ist;
3. Abrechnung und Durchsetzung von Ansprüchen auf Grund der Behandlung, zur Überprüfung der Leistungserbringung sowie zur Rechnungsprüfung;
4. Unterrichtung von Angehörigen, soweit es zur Wahrung ihrer berechtigten Interessen erforderlich ist, schutzwürdige Belange des Patienten nicht beeinträchtigt werden und die Einholung der Einwilligung für den Patienten gesundheitlich nachteilig wäre oder nicht möglich ist.

Im Übrigen ist eine Übermittlung nur mit Einwilligung des Patienten zulässig.

Als Übermittlung gilt auch die Weitergabe der Patientendaten zwischen Behandlungseinrichtungen verschiedener Fachrichtungen in einem Krankenhaus (Fachabteilungen), sofern diese Fachabteilungen nicht unmittelbar mit Untersuchung oder Behandlung und Pflege befasst sind.

Die übermittelnde Stelle hat die Empfänger, die Art der übermittelten Daten und die betroffenen Patienten aufzuzeichnen. Die datenempfangenden Stellen und Personen dürfen die übermittelten Patientendaten nur zu dem Zweck verwenden, zu dem sie ihnen übermittelt wurden, und haben sie in demselben Umfang geheim zu halten wie das Krankenhaus selbst.

(6) Patientendaten sind unverzüglich zu löschen, wenn sie zur Erfüllung der Aufgaben, für die sie erhoben wurden, nicht mehr erforderlich sind, die vorgeschriebenen Aufbewahrungsfristen abgelaufen sind und kein Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Belange Betroffener beeinträchtigt werden.

Bei Daten, die im automatisierten Verfahren mit der Möglichkeit des Direktabrufs gespeichert sind, ist die Möglichkeit des Direktabrufs zu sperren, sobald die Behandlung des Patienten im Krankenhaus oder der Vorsorge- oder Rehabilitationseinrichtung abgeschlossen, der Behandlungsbericht erstellt ist und die damit zusammenhängenden Zahlungsvergänge abgewickelt sind, spätestens jedoch ein Jahr nach Abschluss der Behandlung des Patienten.

(7) Das Krankenhaus darf sich zur Verarbeitung der Patientendaten, zur Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen anderer Personen und Stellen nur dann bedienen, wenn die Einhaltung der geltenden Datenschutzbestimmungen, der Geheimhaltungspflichten nach § 203 des Strafgesetzbuches und der Verordnung zur Sicherstellung der Anforderungen an den Datenschutz in der Informationstechnik gewährleistet ist.

(8) Das Krankenhaus soll die Auskunft nach § 15 DSGVO über die den Patienten betreffenden ärztlichen Daten und die Einsicht in die Behandlungsdokumentation nur durch einen Arzt vermitteln lassen. Ein Anspruch auf Auskunft oder Einsichtnahme steht dem Patienten nicht zu, soweit berechtigte Geheimhaltungsinteressen Dritter, deren Daten zusammen mit denen des Patienten aufgezeichnet sind, überwiegen.

§ 40

Forschung, Krebsregister

(1) Die Verarbeitung der Patientendaten aus kirchlichen Krankenhäusern und anderen diakonischen Einrichtungen ist zu Zwecken der wissenschaftlichen Forschung nur zulässig, soweit der Patient vorher schriftlich eingewilligt hat.

(2) Ohne Einwilligung dürfen diese Daten für eigene wissenschaftliche Forschungsvorhaben nur von den bei den kirchlichen Stellen beschäftigten Personen, die der ärztlichen Schweigepflicht unterliegen, verarbeitet oder genutzt werden.

(3) Ohne Einwilligung dürfen diese Daten zum Zwecke einer bestimmten wissenschaftlichen Forschung an Dritte übermittelt, durch diese verarbeitet oder genutzt werden, wenn der Zweck dieses Forschungsvorhabens nicht auf andere Weise erreicht werden kann und

1. das berechtigte Interesse der Allgemeinheit an der Durchführung des Forschungsvorhabens das Geheimhaltungsinteresse des Patienten erheblich überwiegt oder
2. es entweder nicht möglich oder für den Patienten auf Grund des derzeitigen Gesundheitszustandes nicht zumutbar ist, eine Einwilligung einzuholen. Die übermittelnde Stelle hat die Empfänger, den Zweck des Forschungsvorhabens, die betroffenen Patienten und die Art der übermittelten Daten aufzuzeichnen.

(4) Sobald es der Forschungszweck gestattet, sind die personenbezogenen Daten zu anonymisieren oder zu pseudonymisieren. Merkmale, mit deren Hilfe ein Personenbezug wieder hergestellt werden kann, sind gesondert zu speichern; sie sind zu löschen, sobald der Forschungszweck es erlaubt.

(5) Veröffentlichungen von Forschungsergebnissen dürfen keinen Rückschluss auf die Personen zulassen, deren Daten verarbeitet wurden, es sei denn, der Patient hat in die Veröffentlichung ausdrücklich schriftlich eingewilligt.

(6) Soweit die Bestimmungen dieser Verordnung auf die empfangenden Stellen oder Personen keine Anwendung finden, dürfen Patientendaten nur übermittelt werden, wenn diese sich verpflichten

1. die Daten nur für das von ihnen genannte Forschungsvorhaben zu verwenden,
2. die Bestimmungen der Absätze 4 und 5 einzuhalten und
3. dem Beauftragten für den Datenschutz auf Verlangen Einsicht und Auskunft zu gewähren. Die Empfänger müssen nachweisen, dass die technischen und organisatorischen Voraussetzungen zur Erfüllung der Verpflichtung nach Nummer 2 und der Verordnung zur Sicherstellung der Anforderungen an den Datenschutz in der Informationstechnik vorliegen.

(7) Für die Erhebung und Übermittlung von Daten für das Krebsregister gelten die jeweiligen bundes- bzw. landesrechtlichen Regelungen entsprechend.

§ 41

Beratungsstellen

(1) Kirchliche Beratungsstellen dürfen diejenigen personenbezogenen Daten erheben, verarbeiten und nutzen, die für die jeweils beantragte Beratung erforderlich sind.

(2) Die personenbezogenen Daten Betroffener, insbesondere alle Einzelangaben über persönliche und sachliche Verhältnisse, über Familienangehörige und ihre Lebensverhältnisse werden bei dem Betroffenen erhoben. Informationen von dem Betroffenen über Dritte, die nicht zur Familie gehören, dürfen nicht mit Hilfe von Datenverarbeitungsprogrammen verarbeitet werden.

(3) Die Daten nach Absatz 2 dürfen für Fallbesprechungen nur offenbart werden, wenn der Betroffene eingewilligt hat. Bei Verweigerung der Einwilligung dürfen die Daten nur in anonymisierter Form offenbart werden.

(4) Die Beratungsdokumentation mit den Daten nach Absatz 2, die persönlichen Aufzeichnungen, der Tätigkeitsnachweis des Beraters und die statistischen Unterlagen sind sicher aufzubewahren. Die regelmäßigen Aufbewahrungs-, Lösungs- und Vernichtungsfristen sind zu beachten.

(5) Nach Ablauf der Aufbewahrungsfristen und wenn keine Haftungsansprüche aus der Beratungstätigkeit gegen den Berater anhängig sind, wird die Beratungsdokumentation – ohne ärztliche und sonstige Schweigepflichtentbindungen – dem zuständigen kirchlichen Archiv angeboten. Nicht übernommene Unterlagen werden vernichtet.

(6) Die Verarbeitung und Nutzung der Daten nach Absatz 2 in nicht anonymisierter Form für Zwecke der wissenschaftlichen Forschung bedarf der Zustimmung des Betroffenen.

§ 42**Sonstige diakonische Einrichtungen**

(1) Sonstige diakonische Einrichtungen dürfen personenbezogene Daten der von ihnen betreuten oder behandelten Personen, ihrer Angehörigen, Bevollmächtigten sowie ihrer rechtlichen Betreuer erheben, verarbeiten und nutzen, soweit dies im Rahmen eines Behandlungs-, Betreuungs- oder sonstigen Vertragsverhältnisses einschließlich der verwaltungsmäßigen Abwicklung und Leistungsberechnung, zur Erfüllung der mit der Behandlung im Zusammenhang stehenden Dokumentationspflichten oder eines damit zusammenhängenden Rechtsstreites erforderlich ist.

(2) Personenbezogene Daten nach Absatz 1 dürfen an kirchliche Stellen gemäß § 1 dieser Verordnung übermittelt werden, soweit dies für die verwaltungsmäßige Abwicklung und Leistungsberechnung erforderlich ist.

(3) Für seelsorgerliche Aufgaben ist die Übermittlung von Name, Vorname, Anschrift, Geburtsdatum und Bekenntnisstand an den Seelsorger der für die betreute oder behandelte Person zuständigen Gemeinde zulässig, sofern die betroffene Person der Übermittlung nicht widersprochen hat. Der Betroffene ist bei Aufnahme des Behandlungs-, Betreuungs- oder sonstigen Vertragsverhältnisses darauf hinzuweisen, dass der Übermittlung zugestimmt werden muss.

(4) Die Übermittlung personenbezogener Daten betreuter oder behandelter Personen an Stellen und Personen außerhalb der diakonischen Einrichtung und deren Nutzung richtet sich nach § 39 Absatz 5 dieser Verordnung.

(5) Für die Datenverarbeitung im Auftrag sowie für die Fernwartung gilt § 39 Absatz 7 dieser Verordnung entsprechend. Die Verordnung zur Sicherstellung der Anforderungen an den Datenschutz in der Informationstechnik ist zu beachten.

§ 43**Geltung weiterer Vorschriften, Sozialgeheimnis**

(1) Neben den kirchlichen Datenschutzbestimmungen ist insbesondere § 203 des Strafgesetzbuches zu beachten. Auf die Erhebung, Verarbeitung, insbesondere Übermittlung, und Nutzung personenbezogener Daten in diakonischen Einrichtungen sind die jeweiligen Teile des Sozialgesetzbuches entsprechend anzuwenden, soweit in dieser Rechtsverordnung nichts anderes geregelt ist.

(2) Die Mitarbeiter der kirchlichen Stellen, die mit Sozialdaten im Sinne des Sozialgesetzbuches umgehen, sind zusätzlich auf die Einhaltung des Sozialgeheimnisses nach den Vorschriften des Sozialgesetzbuches zu verpflichten.

Neunter Abschnitt: Fundraising**§ 44****Erhebung, Verarbeitung und Nutzung personenbezogener Fundraisingdaten**

(1) Die kirchliche Aufgabe des Fundraising verbindet die Beziehungspflege mit dem Werben um persönlichen und finanziellen Einsatz für kirchliche und diakonische Zwecke. Die kirchlichen Stellen gemäß § 1 Absatz 2 DSGVO und § 1 dieser Ver-

ordnung dürfen für das Fundraising die im Gemeindegliederverzeichnis und in den Kirchenbüchern erhaltenen Daten von Kirchenmitgliedern und Angehörigen erheben, verarbeiten und nutzen, soweit ein melderechtlicher Sperrvermerk oder Widerspruch (Teilnutzungssperre) dem nicht entgegen steht.

(2) Weitere personenbezogene Daten von Gemeindegliedern und deren Angehörigen und den mit der kirchlichen und diakonischen Arbeit in Beziehung getretenen Personen dürfen kirchliche Stellen für das Fundraising erheben, verarbeiten und nutzen, soweit dies für die Durchführung des Fundraisings erforderlich ist, insbesondere

1. Name und Anschrift von Spendern, zugehörige Kirchengemeinde,
2. Art, Betrag, Zweck und Zeitpunkt der geleisteten Spenden,
3. Erteilung von Zuwendungsbestätigungen,
4. Daten des Kontaktes,
5. Daten der erforderlichen Buchhaltung,
6. Daten zur statistischen analytischen Auswertung.

(3) Die kirchlichen Stellen dürfen für das Fundraising Daten aus allgemein zugänglichen Quellen für diesen Zweck erheben, verarbeiten und nutzen.

(4) Es ist durch geeignete Maßnahmen sicherzustellen, dass Seelsorgedaten gemäß § 3 dieser Verordnung im Rahmen des Fundraisings Dritten nicht zugänglich sind. Seelsorgedaten dürfen nur mit schriftlicher Einwilligung der betroffenen Person für das Fundraising erhoben, verarbeitet und genutzt werden.

(5) Programme zur automatischen Verarbeitung von Spenderdaten (Spendenverwaltungsprogramme, Fundraisingprogramme) dürfen nur verwendet werden, wenn sie vom Oberkirchenrat freigegeben worden sind. Personenbezogene Daten dürfen nicht für eine automatisierte Verarbeitung erhoben, verarbeitet oder genutzt werden, soweit die betroffene Person widerspricht (Teilnutzungssperre). Die Verordnung zur Sicherstellung der Anforderungen an den Datenschutz in der Informationstechnik ist einzuhalten.

§ 45**Datenerhebung, -verarbeitung und -nutzung im Auftrag**

(1) Bei der Datenerhebung, -verarbeitung und -nutzung im Auftrag ist § 5 DSGVO i. V. m. § 9 dieser Verordnung zu beachten. Die Speicherung der personenbezogenen Daten hat mandantenbezogen zu erfolgen. Mandant ist, in dessen Auftrag oder zu dessen Gunsten das Fundraising durchgeführt wird.

(2) Personenbezogene Daten von Personen, für die Auskunftssperren wegen Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen bestehen, dürfen im Rahmen des Fundraisings an andere Stellen oder Personen nicht übermittelt werden.

(3) Eine Weitergabe der personenbezogenen Daten durch die beauftragte Stelle an Dritte ist auszuschließen.

(4) Der Betriebsbeauftragte für den Datenschutz oder der örtliche Beauftragte für den Datenschutz der beauftragten kirchlichen Stelle ist frühzeitig über die Auftragsdatenerhebung, -verarbeitung und -nutzung zu informieren.

(5) Werden personenbezogene Daten für das Fundraising im Auftrag durch andere Stellen oder Personen erhoben, verarbeitet oder genutzt, ist vor einer Beauftragung die Genehmigung nach § 9 dieser Verordnung einzuholen.

(6) Die Verordnung zur Sicherstellung der Anforderungen an den Datenschutz in der Informationstechnik ist zu beachten.

§ 46 Übermittlung von Fundraisingdaten an kirchliche Stellen

(1) Für das eigene Fundraising kirchlicher Stellen dürfen mit Zustimmung des Oberkirchenrates nur folgende Daten von Kirchenmitgliedern und ihren Familienangehörigen aus dem kirchlichen Meldewesen übermittelt werden:

1. Name und gegenwärtige Anschrift,
2. Geburtsdatum, Geschlecht, Staatsangehörigkeit(en), Familienstand, Stellung in der Familie,
3. Zahl und Alter der minderjährigen Kinder,
4. Religionszugehörigkeit und Zugehörigkeit zu einer Kirchengemeinde.

Soweit es für die Durchführung der Fundraisingmaßnahme erforderlich ist, können im Einzelfall weitere Daten aus den Kirchenbüchern und dem Gemeindegliederverzeichnis übermittelt werden.

(2) Zusätzlich zu den Daten nach Absatz 1 dürfen kirchliche Stellen gemäß § 1 Absatz 2 DSGVO und § 1 dieser Verordnung von ihnen erhobene und gespeicherte Daten im erforderlichen Umfang an andere kirchliche Stellen übermitteln

(3) Personenbezogene Daten können an kirchliche Stellen übermittelt werden, wenn

1. die empfangende kirchliche Stelle sie ausschließlich für das eigene Fundraising nutzt,
2. die empfangende kirchliche Stelle sicherstellt, dass der Umfang und der Zeitpunkt des Fundraising mit der übermittelnden kirchlichen Stelle abgestimmt wird,
3. die empfangende kirchliche Stelle sicherstellt, dass die melderechtlichen Sperrvermerke und Teilnutzungssperren beachtet und der übermittelnden kirchlichen Stelle mitgeteilt werden,
4. ausreichende technische und organisatorische Datenschutzmaßnahmen unter Beachtung des Schutzbedarfs der Anforderungen der Anlage zu § 9 Satz 1 DSGVO vorliegen, von denen sich im Zweifelsfall die übermittelnde kirchliche Stelle zu überzeugen hat und
5. die Betriebsbeauftragten für den Datenschutz oder die örtlichen Beauftragten für den Datenschutz der beteiligten kirchlichen Stellen über Umfang und Zweck der Datenübermittlung informiert werden.

§ 47 Ausschluss der Nutzung von Fundraisingdaten

Es ist sicherzustellen, dass Personen, die den Erhalt von Spendenaufrufen ausdrücklich nicht wünschen, von der Durchführung des Fundraisings ausgenommen werden.

§ 48 Löschung von Fundraisingdaten

Werden die für das Fundraising erhobenen und genutzten Daten nicht mehr benötigt oder wird deren weiterer Nutzung widersprochen, sind diese Daten zu löschen, soweit nicht ihrer Löschung Rechtsvorschriften oder Aufbewahrungsfristen entgegenstehen.

Zehnter Abschnitt: Aufgaben der obersten kirchlichen Verwaltungsbehörde

§ 49 Genehmigungsbefugnisse des Oberkirchenrates

Die Genehmigung des Oberkirchenrates ist erforderlich für

1. die Einrichtung eines automatisierten Abrufverfahrens mit nichtkirchlichen Stellen (zu § 11 Absatz 3 Satz 2 DSGVO),
2. die Benutzung privater Datenverarbeitungsanlagen zur Verarbeitung personenbezogener dienstlicher Daten gemäß § 9 Absatz 2 dieser Verordnung.

Elfter Abschnitt: Schlussbestimmungen

§ 50 Anlagen

Der Oberkirchenrat wird ermächtigt, die Anlagen 1 bis 10, die Bestandteil dieser Verordnung sind, zu ändern.

§ 51 Sprachliche Gleichstellung

Soweit in diesem Gesetz Bezeichnungen, die für Frauen und Männer gelten, in der männlichen Sprachform verwendet werden, gelten diese Bezeichnungen für Frauen in der weiblichen Sprachform.

§ 52 Ausführungsvorschriften

Der Oberkirchenrat ist berechtigt, Ausführungsvorschriften zu erlassen.

§ 53 Inkrafttreten, Außerkrafttreten

(1) Diese Rechtsverordnung tritt am 1. Januar 2010 in Kraft.

(2) Gleichzeitig tritt die Verordnung zum Kirchengesetz über die Anwendung des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) in der Evangelisch-Lutherischen Landeskirche Mecklenburgs vom 22. März 1997 (KABl. S. 107) außer Kraft.

Schwerin, 4. Dezember 2009

Der Vorsitzende der Kirchenleitung

Dr. von Maltzahn
Landesbischof

Anlage 1 zu § 4 Datenschutzanwendungsverordnung:

- Muster „Verpflichtung auf das Datengeheimnis“

**Verpflichtung auf das Datengeheimnis
für Ehrenamtliche**
(nach § 6 DSGVO-EKD i.V.m. § 6 MAG DSGVO-EKD)

Ich, _____

Geb. am _____

wohnhaft _____

bin bei/ in _____

ehrenamtlich tätig.

Ich verpflichte mich,

alle datenschutzrechtlichen Bestimmungen einzuhalten und aller personenbezogenen Angaben, die ich auf Grund meines Ehrenamtes erhalten habe oder die mir im Zusammenhang mit meinem Ehrenamt zur Kenntnis gelangt sind, während der Tätigkeit und nach ihrer Beendigung vertraulich zu behandeln. Ich bin darüber informiert, dass Verstöße gegen das Datengeheimnis zum Entzug des Ehrenamtes führen können. Auf mögliche Schadensersatzansprüche einer unzulässigen Weitergabe personenbezogener Daten wurde ich hingewiesen.

Ort, Datum

Unterschrift der Verpflichteten / des Verpflichteten

Verpflichtung auf das Datengeheimnis (nach § 6 DSG-EKD i. V. m. § 6 MAG DSG-EKD)

Frau/Herr _____
(Nichtzutreffendes streichen)

wohnhaft _____

ist als _____

bei _____
beschäftigt und bestätigt:

1. Ich wurde zur Wahrung des Datengeheimnisses nach § 6 des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland vom 12. November 1993 (KABl 1995, 4) und nach § 6M des Kirchengesetzes über die Anwendung des Kirchengesetzes über den Datenschutz der EKD in der Evangelisch-Lutherischen Landeskirche Mecklenburgs (KABl 1997, 67) darauf verpflichtet, personenbezogene Daten nicht unbefugt zu verarbeiten oder zu nutzen. Ich wurde darauf hingewiesen, dass diese Pflicht auch nach Beendigung meiner Tätigkeit fortbesteht.

2. Mir ist bekannt, dass Verstöße gegen das Datengeheimnis dienst-, arbeits-, urheber-, straf-, disziplinar- und haftungsrechtlich geahndet werden können.

3. Das Merkblatt „Datenschutz in der Evangelisch-Lutherischen Kirche Mecklenburgs“ habe ich erhalten und von seinem Inhalt, den ich sorgfältig beachten werde, Kenntnis genommen.

Ich nehme zur Kenntnis, dass das Original dieser Verpflichtungserklärung zu meiner Personalakte / zur Akte Datenschutz genommen wird.

Eine Ausfertigung ist für die Verpflichtete / den Verpflichteten bestimmt.

Ort, Datum

Unterschrift der Verpflichteten / des Verpflichteten

Unterschrift der Verpflichtenden / des Verpflichtenden

Anlage 2 zu § 4 Datenschutzanwendungsverordnung:

Merkblatt „Datenschutz in der Evangelisch-Lutherischen Landeskirche Mecklenburgs“

Merkblatt

Datenschutz in der Evangelisch-Lutherischen Landeskirche Mecklenburgs

Datenschutzbestimmungen

Für den Datenschutz in der Evangelisch-Lutherischen Landeskirche Mecklenburgs (ELLM) sind zu beachten:

1. Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) vom 12. November 1993 (KABI 1995 S. 4)
2. Kirchengesetz über die Anwendung des Kirchengesetzes über den Datenschutz der EKD in der Evangelisch-Lutherischen Landeskirche Mecklenburgs (KABI 1997 S. 67)
3. Kirchengesetz über die Kirchenmitgliedschaft, das kirchliche Meldewesen und den Schutz der Daten der Kirchenmitglieder in der Evangelisch-Lutherischen Landeskirche Mecklenburgs vom 4. November 1990 in Änderung vom 19.11.2000 (KABI 2000 S. 72)
4. Besondere Bestimmungen über den Schutz des Beicht- und Seelsorgegeheimnisses, die Amtsverschwiegenheit sowie sonstige gesetzliche Geheimhaltungs- und Verschwiegenheitspflichten oder von Berufs- bzw. besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen.
5. Besondere Regelungen in kirchlichen Rechtsvorschriften, die auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind.

In gleicher Weise sind künftige Rechts- und Verwaltungsvorschriften sowie Veröffentlichungen der Evangelischen Kirche in Deutschland und der Evangelisch-Lutherischen Landeskirche Mecklenburgs zum Datenschutz zu beachten.

Grundsätze des Datenschutzes

Dieses Merkblatt versucht nicht, jede erdenkliche Situation zu beschreiben, sondern definiert allgemeine Prinzipien für den Umgang mit Daten und Informationen. Es wird erwartet, dass sich jeder Benutzer, wenn er mit unvorhersehbaren Situationen konfrontiert wird, an diese Prinzipien hält.

Für den Umgang mit personenbezogenen Daten in der Evangelisch-Lutherischen Landeskirche Mecklenburgs gelten insbesondere folgende Grundsätze:

1. Aufgabe der Datenverarbeitung im kirchlichen Bereich ist es, kirchliches Handeln zu fördern. Dabei muss gewährleistet sein, dass der Einzelne beim Umgang mit personenbezogenen Daten nicht in seinem Persönlichkeitsrecht beeinträchtigt wird.

Personenbezogene Daten dürfen nur für die rechtmäßige Erfüllung kirchlicher Aufgaben erhoben, verarbeitet und genutzt werden. Maßgebend sind die durch das kirchliche

Recht bestimmten oder herkömmlichen Aufgaben auf dem Gebiet der Verkündigung, Seelsorge, Diakonie und Unterweisung sowie der kirchlichen Verwaltung.

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.

Personenbezogene Daten sind Einzelangaben über persönliche Verhältnisse (z. B. Name, Geburtsdatum, Anschrift, Konfession, Beruf, Familienstand) oder sachliche Verhältnisse (z. B. Grundbesitz, finanzielle Belastungen, Rechtsbeziehungen zu Dritten) einer bestimmten oder bestimmbaren natürlichen Person.

Besonders sensibel sollte mit besonderen Arten personenbezogener Daten im Sinne von § 2 Absatz 11 DSG-EKD umgegangen werden.

Die Datenschutzregelungen gelten für

- automatisierte Verarbeitungen, darunter versteht man die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen,
- Datensammlungen, die gleichartig aufgebaut sind und nach bestimmten Merkmalen zugänglich sind und ausgewertet werden können (nicht automatisierte Dateien),
- Akten und Aktensammlungen mit einigen Einschränkungen.

Einzelheiten, die auch den Umfang des kirchlichen Datenschutzes betreffen, sind dem DSG-EKD zu entnehmen (siehe insbesondere §§ 1-5, 11-13, 23-26).

2. Die Übermittlung von personenbezogenen Daten, von Kopien aus Akten und Auskünfte aus Datensammlungen sind an kirchliche Stellen, andere öffentlich-rechtliche Religionsgesellschaften sowie an Behörden und sonstige öffentliche Stellen des Bundes, der Länder, der Gemeinden etc. zulässig, soweit sie insbesondere zur Erfüllung kirchlicher Aufgaben erforderlich sind (beachte aber auch die weiteren Vorgaben der §§ 5 und 12 DSG-EKD). Die Datenübermittlung an sonstige Stellen oder Personen ist nur in Ausnahmefällen statthaft (siehe § 13 DSG-EKD). Widersprüche von betroffenen Personen, die sich gegen eine Erhebung, Verarbeitung oder Nutzung ihrer personenbezogenen Daten richten, sind zu beachten – Ausnahmen regeln die kirchlichen Vorschriften sowie § 16 Abs. 4a DSG-EKD. Auskünfte zur geschäftlichen oder gewerblichen Verwendung der Daten dürfen ohne Einwilligung der betroffenen Person in keinem Fall gegeben werden. Daten oder Datenträger dürfen nur kirchlichen Mitarbeiterinnen und Mitarbeitern zugänglich gemacht werden, die auf Grund ihrer dienstlichen Aufgaben zum Empfang der Daten ermächtigt worden sind.
3. Über die Verschwiegenheitsverpflichtung des § 8 des Arbeitsvertrages hinaus, sind alle Informationen, die eine Mitarbeite-

rin oder ein Mitarbeiter auf Grund ihrer / seiner Arbeit an und mit Akten, Dateien, Listen und Karteien erhält, von ihr / ihm vertraulich zu behandeln. Diese Pflicht besteht auch nach Beendigung der Tätigkeit fort.

4. Jede Mitarbeiterin und jeder Mitarbeiter trägt für die vorschriftsgemäße Ausübung der jeweiligen Tätigkeit die volle datenschutzrechtliche Verantwortung. Der Umgang mit Daten und Informationen erfordert ein hohes Maß an Verantwortungsbewusstsein. Die sorgsame und vertrauliche Behandlung von Daten ist ein wichtiges Gebot im Rahmen der Informationsverarbeitung. Die Sammlung, Aufbereitung und Verwendung personenbezogener Daten unterliegen einer erhöhten Schutzbedürftigkeit.

Soweit mit einem Personalcomputer (PC) personenbezogene Daten eingegeben, verarbeitet oder genutzt werden, sind die technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit zu beachten, insbesondere die in der Anlage zu § 9 DSGVO aufgeführten Kontrollmaßnahmen.

Die Regelungen und Hinweise zum Datenschutz und zur Datensicherheit aus bestehenden Dienst- und Organisationsanweisungen sind zu beachten. Unabhängig davon sind eigenmächtige Änderungen bzw. Erweiterungen der bestehenden Hardware durch Zusatzgeräte ebenso wie die Verwendung privater Hardware und privater Datenträger nicht gestattet. Des Weiteren sind eigenmächtige Änderungen der bestehenden Software, die Verwendung privater Software und die Weitergabe und Veränderung von Programmen untersagt. Soweit aus Gründen der Aufgabenerfüllung Daten von dritter Seite mittels eines Datenträgers auf den PC übernommen werden müssen, ist durch geeignete Maßnahmen sicherzustellen, dass die auf dem Datenträger enthaltenen Daten nicht mit Viren befallen sind.

Datenträger mit personenbezogenen Daten sind stets sicher zu verwahren und vor jeder Einsicht oder sonstigen Nutzung durch Unbefugte zu schützen.

5. Datenbestände, insbesondere Dateien, Listen und Karteien, die durch neue ersetzt und auch nicht aus besonderen Gründen weiterhin benötigt werden (z. B. für Prüf- und Archivzwecke), müssen in einer Weise vernichtet oder gelöscht werden, die jeden Missbrauch der Daten ausschließt. Gleiches gilt für die Verschrottung von PC-Technik mit Speichermedien (Festplatten o.ä.).
6. Mängel, die bei der Datenerhebung, -verarbeitung und -nutzung auffallen, sind unverzüglich den Vorgesetzten zu melden. Dies gilt auch für den Fall, dass in den Bereichen Datenschutz und Datensicherheit unzureichende organisatorische und technische Maßnahmen ergriffen wurden.

Soweit vorhanden, können auch die oder der Betriebsbeauftragte für den Datenschutz, die oder der örtlich Beauftragte

für den Datenschutz und sonstige mit dem Datenschutz befasste Stellen zur Beratung herangezogen werden.

7. Verstöße gegen das Datengeheimnis können dienst- bzw. arbeitsrechtlich, urheberrechtlich, disziplinarisch und haftungsrechtlich geahndet werden. Bestimmte Handlungen, die einen Verstoß gegen das Datengeheimnis beinhalten, stellen Straftatbestände dar. Danach kann beispielsweise mit Freiheitsstrafe oder mit Geldstrafe bestraft werden,
- wer sich oder einem Dritten unbefugt besonders gesicherte Daten aus fremden Datenbanksystemen verschafft (§ 202a StGB „Ausspähen von Daten“),
 - wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis offenbart, dies betrifft insbesondere Ärztinnen und Ärzte, Angehörige eines anderen Heilberufs, z. B. aus dem Krankenpflegebereich, einschließlich ihrer berufsmäßig tätigen Gehilfen und Personen, die bei ihnen zur Vorbereitung auf den Beruf tätig sind (z. B. Auszubildende), Psychologinnen und Psychologen, Ehe-, Familien-, Erziehungs- oder Jugendberaterinnen und -berater sowie Beraterinnen und Berater für Suchtfragen in einer Beratungsstelle, Mitglieder einer anerkannten Beratungsstelle nach dem Schwangerschaftskonfliktgesetz, Sozialarbeiterinnen und Sozialarbeiter, Sozialpädagoginnen und Sozialpädagogen, Personen, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnehmen (§ 203 StGB „Verletzung von Privatgeheimnissen“),
 - wer fremdes Vermögen durch unbefugtes Einwirken auf einen Datenverarbeitungsvorgang schädigt (§ 263a StGB „Computerbetrug“),
 - wer rechtswidrig Daten verändert oder beseitigt (§ 303a StGB „Datenveränderung“),
 - wer den Ablauf der Datenverarbeitung einer Behörde oder eines Wirtschaftsunternehmens stört (§ 303b StGB „Computersabotage“) und
 - wer unbefugt Verhältnisse in Steuersachen einschl. fremder Betriebs- oder Geschäftsgeheimnisse offenbart oder verwertet (§ 355 StGB „Verletzung des Steuergeheimnisses“).

Auch weitere Verschwiegenheitsvorschriften und Geheimhaltungspflichten (z. B. dienst- und arbeitsrechtliche Regelungen, Sozialgeheimnis, Brief-, Post- und Fernmeldegeheimnis) sind zu beachten.

Die oben erwähnten Datenschutzgesetze finden Sie unter folgenden links:

Datenschutzgesetz EKD: <http://www.kirche-mv.de/fileadmin/ELLM-Gesetze/Verwaltung/DatenschutzgesetzEKD.pdf>

Anwendungsgesetz ELLM: <http://www.kirche-mv.de/fileadmin/ELLM-Gesetze/Verwaltung/DatenschutzAnwendung.pdf>

Anlage 3 zu § 6 Datenschutzanwendungsverordnung:

- Muster „Vertrag über die Nutzung einer privaten Datenverarbeitungsanlage zur Verarbeitung personenbezogener dienstlicher Daten“

**Vertrag
über die Nutzung einer privaten Datenverarbeitungsanlage
zur Verarbeitung personenbezogener dienstlicher Daten**

Zwischen

(Bezeichnung der kirchlichen Stelle - vertreten durch),

nachfolgend Dienststelle genannt, und

Frau / Herrn (Nichtzutreffendes streichen)

nachfolgend Eigentümerin / Eigentümer genannt,
wird der folgende Vertrag über die befristete Nutzung der privaten Datenverarbeitungsanlage der Eigentümerin / des Eigentümers zur Verarbeitung personenbezogener dienstlicher Daten geschlossen:

**§ 1
Soft- und Hardware**

(1) Die durch diesen Vertrag betroffene eingebrachte Soft- und Hardware ist nachfolgend vollständig aufgeführt:

Eingesetzte Software bzw. Anwendungssoftware
Sicherheitssoftware (Virenschutz, Firewall) / Version
Textverarbeitung / Version
Tabellenkalkulation / Version
Datenbank / Version
Grafik, Bildbearbeitung / Version
Sonstige Standardsoftware
Selbsterstellte Programme / Anwendungen
Eingesetzte Hardware bzw. Betriebssoftware
Rechnertyp / Hersteller / Modell mit Gerätenummer
Betriebssystem(e) / Version
Festplatte(n) (Anzahl / Größe)
Diskettenlaufwerk (nein / ja)
andere Laufwerke (nein / ja, dann Typ / Modell)
Drucker (Hersteller / Druckertyp mit Gerätenummer)
CD-ROM- bzw. DVD-Laufwerk (nein / ja, dann Typ / Modell)
Monitor (Typ / Modell mit Gerätenummer)
Grafikkarte (Typ)
Internetzugang (nein / ja)
Netzwerkadapter (nein / ja, dann Typ / Modell)

Wireless LAN, Drahtlosnetzwerk (nein / ja)
Modem / ISDN-Karte (nein / ja, dann Typ / Modell)
USB-Anschluss (nein / ja)
Sonstiges

(2) Die oben genannte Hard- und Software steht im Amtszimmer / den Diensträumen / (anderer Standort) der Eigentümerin / des Eigentümers.

(3) Veränderungen an Hard- und Software während der Laufzeit dieses Vertrages bedürfen der Vertragsergänzung.

§ 2 Laufzeit des Vertrages

(1) Die Gültigkeit dieses Vertrages beginnt am _____
und endet am _____.

(2) Die Eigentümerin / Der Eigentümer erkennt an und stellt sicher, dass die dienstlichen Daten jederzeit der Verfügung der Dienststelle unterliegen. Der Dienststelle muss es jederzeit ermöglicht werden, dienstliche Daten zu verarbeiten und zu nutzen.

(3) Die Vertragspartner sind berechtigt, den Vertrag ohne Angabe von Gründen jederzeit vorzeitig zu kündigen. Die Kündigung ist schriftlich gegenüber dem anderen Vertragspartner auszusprechen.

(4) Bevor die private Datenverarbeitungsanlage, die zur Verarbeitung personenbezogener dienstlicher Daten benutzt worden ist, wieder in eine private Nutzung übernommen wird, sind alle gespeicherten personenbezogenen Daten zu löschen. Dies gilt auch für Datenträger.

§ 3 Einhaltung des Datenschutzes

Die Eigentümerin / Der Eigentümer verpflichtet sich, im Rahmen der dienstlichen und privaten Nutzung die Vorschriften des kirchlichen Datenschutzes zu beachten. Die Nutzung der Datenverarbeitungsanlage unterliegt insofern während der Laufzeit dieses Vertrages der uneingeschränkten Kontrolle durch die Dienststelle und die Datenschutzbeauftragte oder den Datenschutzbeauftragten der Evangelisch-Lutherischen Landeskirche Mecklenburgs.

§ 4 Nutzung

(1) Die private Datenverarbeitungsanlage darf nur für die folgenden dienstlichen Zwecke genutzt werden:

- _____
- _____
- _____

(2) Eine Erweiterung der Einsatzzwecke bedarf der vorherigen Einwilligung durch die Dienststelle.

(3) Bei jeder dienstlichen Nutzung der Datenverarbeitungsanlage sind alle Arbeitsergebnisse, Zwischenergebnisse und Arbeitswege so zu dokumentieren, dass sichergestellt ist, dass Vertretungen oder Vorgesetzte jederzeit in der Lage sind, alle Arbeiten auch ohne Nutzung der privaten Datenverarbeitungsanlage nachzuvollziehen. In begründeten Einzelfällen hat die Eigentümerin oder der Eigentümer der Vertretung die Nutzung der privaten Datenverarbeitungsanlage zur Wahrnehmung der Vertretung zu gestatten. Die Gestattung ist aktenkundig zu machen.

§ 5

Datensicherheit

(1) Der Zugriff von Unbefugten auf dienstliche Daten, die auf Speichermedien der privaten Datenverarbeitungsanlage gespeichert werden, ist durch folgende Vorkehrungen zu verhindern:

- verschlossenes Arbeitszimmer
- Passwortschutz
- bei Internetzugang: Installation einer Firewall
- ggf. weitere Maßnahmen (z. B. Verschlüsselung)
- _____

(2) Es ist eine Antiviren-Software zu installieren.

(3) Zur Beseitigung von Sicherheitslücken sind Betriebssysteme, Antiviren-Software und Firewall regelmäßig durch Updates zu aktualisieren.

§ 6

Datensicherung

(1) Die Eigentümerin / Der Eigentümer ist verpflichtet, nach der Installation der privaten Datenverarbeitungsanlage und danach in regelmäßigen Abständen – mindestens jedoch _____ – eine komplette Datensicherung durchzuführen. Es sind alle Betriebssysteme, Programme und Nutzerdaten zu sichern.

(2) Die Sicherungskopien sind unter Verschluss aufzubewahren, bei Benutzung der privaten Datenverarbeitungsanlage außerhalb der Diensträume sind die Sicherungskopien jederzeit zugänglich für die Dienststelle aufzubewahren. Für die Sicherungskopien gelten die gleichen Datensicherheitsanforderungen wie für die Originaldateien.

§ 7

Vernetzung

Eine Vernetzung der privaten Datenverarbeitungsanlage mit anderen Datenverarbeitungsanlagen ist nur nach vorheriger Genehmigung durch die Dienststelle gestattet.

§ 8 Verbrauchsmaterialien

Die Kosten für Verbrauchsmaterialien werden durch die Dienststelle nach dem Umfang der dienstlichen Benutzung übernommen.

§ 9 Haftung

Die Dienststelle haftet bei Beschädigung, Zerstörung oder Verlust der privaten, bereits installierten und hinsichtlich ihrer Einsetzbarkeit abgenommenen Datenverarbeitungsanlage nur, wenn der Schaden bei der dienstlichen Benutzung der Anlage durch die Eigentümerin / den Eigentümer oder durch Dritte eingetreten ist. Dies gilt nicht, wenn die Eigentümerin / der Eigentümer oder Dritte den Schaden zu vertreten haben oder Dritte der Eigentümerin / dem Eigentümer gegenüber zum Schadensersatz verpflichtet sind. Ist die private Datenverarbeitungsanlage beim Transport zur Dienststelle und von der Dienststelle, vor der Installation in den Diensträumen, bei der Benutzung zu privaten Zwecken durch die Eigentümerin / den Eigentümer oder durch Dritte beschädigt oder zerstört worden oder abhanden gekommen, so wird der Eigentümerin / dem Eigentümer kein Ersatz geleistet. Die Dienststelle leistet auch keinen Ersatz bei Abnutzungsschäden durch Gebrauch zu dienstlichen Zwecken. Die Eigentümerin / Der Eigentümer bestätigt durch Unterschrift, auf die vorstehenden Haftungseinschränkungen hingewiesen worden zu sein. Die schriftliche Bestätigung ist Voraussetzung für die Wirksamkeit dieses Vertrages.

(Ort, Datum)

(Eigentümer / Eigentümerin)

Für die Dienststelle

(Unterschrift)

(Unterschrift)

(Stempel)

Anlage 4 zu § 8 Datenschutzanwendungsverordnung:

- Muster „Vereinbarung über eine Datenverarbeitung im Auftrag“

Vereinbarung über eine Datenverarbeitung im Auftrag

1. Der Auftraggeber

(Bezeichnung der kirchlichen Stelle - vertreten durch)
beauftragt hiermit den Auftragnehmer

(Bezeichnung)

mit der ordnungsgemäßen und datenschutzgerechten Erledigung folgender Arbeiten:

2. Folgende technische und organisatorische Maßnahmen zur Datensicherung im Sinne der Anlage zu § 9 DSGVO sind beim Auftragnehmer getroffen:

3. Der Auftragnehmer verarbeitet die ihm übergebenen personenbezogenen Daten ausschließlich im Rahmen der vertraglich festgelegten Weisungen des Auftraggebers.

4. Der Auftragnehmer verpflichtet sich, die Bestimmungen des kirchlichen Datenschutzrechts und die ergänzenden landeskirchlichen Regelungen einzuhalten. Er unterstellt sich der Kontrolle durch den kirchlichen Datenschutzbeauftragten. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen das Datenschutzgesetz der EKD oder andere Vorschriften über den Datenschutz verstoßen, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

5. Der Auftragnehmer ist verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit seine Daten und Unterlagen betroffen sind. Nicht mehr erforderliche Daten sind beim Auftragnehmer unverzüglich zu löschen.

6. Verarbeitet der Auftragnehmer auf der Datenverarbeitungsanlage auch andere Daten als solche des Auftraggebers, so sind diese Daten durch technische und organisatorische Maßnahmen von denen des Auftraggebers zu trennen.

7. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei besonderen Vorkommnissen – wie z. B. technischen oder organisatorischen Störungen im Rahmen der vertragsgemäßen Verarbeitung/Löschung der Daten – unverzüglich zu benachrichtigen und die weitere Behandlung der Daten mit diesem abzustimmen. Entstehen dem Auftraggeber oder einem Dritten durch Fehler in der Auftragsdatenverarbeitung oder durch den Einsatz fehlerhafter Hard- oder Software hierbei Schäden, so hat der Auftragnehmer dem Auftraggeber seine Schäden zu ersetzen und ihn von Schadensersatzansprüchen Dritter freizustellen. Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

8. Der Auftragnehmer verpflichtet sich, die ihm übergebenen personenbezogenen Daten grundsätzlich nur in seinen eigenen Geschäftsräumen in _____ und ohne Einschaltung von Subunternehmern / Unterauftragnehmern zu verarbeiten. Sollte dennoch einmal die Einschaltung eines Subunternehmers / Unterauftragnehmers

erforderlich sein (z. B. bei technischen Störungen), ist vorher die Einwilligung des Auftraggebers einzuholen.

9. Diese Vereinbarung kann bei Verstoß gegen ihre Bestimmungen fristlos gekündigt werden.

10. Bei Beendigung des Auftragsverhältnisses hat der Auftragnehmer dem Auftraggeber seine Daten in der Form, in der sie vorliegen (maschinenlesbar oder schriftlich) herauszugeben und die bei ihm vorhandenen Daten zu löschen bzw. die Datenträger zu vernichten. Der Auftraggeber kann dies auch schon vor Ablauf der Kündigungsfrist jederzeit verlangen. Zuvor hat der Auftragnehmer das Recht, sie zum Zwecke der Leistungsabrechnung auszuwerten, wenn dies zur Wahrung seiner Interessen erforderlich ist und unverzüglich geschieht. Ein Zurückbehaltungsrecht gegenüber dem Auftraggeber steht ihm nicht zu.

11. Diese Vereinbarung und Änderungen hierzu treten erst in Kraft, wenn die erforderliche Genehmigung durch die nach §§ 8 und 9 DSGVO-KD AG zuständige Stelle erteilt ist.

(Ort, Datum) (Auftragnehmer)

(Ort, Datum) (Auftraggeber)

(Stempel)

Anlage 5 zu § 10 Datenschutzanwendungsverordnung:

- Muster „Übersicht über automatisierte Verarbeitungen“

Übersicht über automatisierte Verarbeitungen

(Angaben nach § 14 Abs. 2 DSGVO)

Nr. 1: Name der verantwortlichen Stelle:

Nr. 2.1: Bezeichnung der Verarbeitungsprogramme

Nr. 2.2: Art der Verarbeitungsprogramme

Nr. 3: Zweckbestimmung

Nr. 4: Art der gespeicherten Daten

Nr. 5: Betroffener Personenkreis

Nr. 6.1: Art der regelmäßig zu übermittelnden Daten

Nr. 6.2: Datenempfangende Stellen

Nr. 7: Regelfristen der Löschung der Daten

Nr. 8: Zugriffsberechtigter Personenkreis

Nr. 9: Rechtsgrundlage für die Datenverarbeitung

Erstellt von: _____

(Name, Vorname, Funktion)

(Datum) (Unterschrift)

Anlage 6 zu § 10 Datenschutzanwendungsverordnung:

- Merkblatt „Erläuterungen zur Übersicht über automatisierte Verarbeitungen“

Erläuterungen zur Übersicht über automatisierte Verarbeitungen

1. Sinn und Zweck der Übersicht

Eine Übersicht über die eingesetzten Datenverarbeitungsprogramme schafft Transparenz und ermöglicht die Überwachung der Datenverarbeitung. Die Mitarbeitenden der kirchlichen Stelle können sich anhand des Verzeichnisses einen Überblick über die für sie zutreffenden Arbeitsabläufe und Verfahren verschaffen. Die Übersicht hilft auch bei der Erfüllung der Auskunftspflicht nach § 15 des Kirchengesetzes über den Datenschutz in der Evangelischen Kirche in Deutschland (DSG-EKD) gegenüber betroffenen Personen, besonders dann, wenn die Angaben im Auskunftersuchen nicht sofort zum Auffinden der gewünschten Daten führen. Die Übersicht ist ein wichtiges Instrumentarium

- bei der Datenschutzselbstkontrolle durch die oder den Betriebsbeauftragte/n bzw. örtliche/n Beauftragte/n für den Datenschutz,
- für die Leitung sowie die für die Datenverarbeitung zuständigen Personen,
- für eine mögliche Fremdkontrolle durch die oder den Datenschutzbeauftragte/n bzw. die zuständigen Aufsichtsgremien.

2. Meldepflicht – Anzeige und Verfahren automatisierter Verarbeitung

Grundsatz

Kirchliche Stellen sind nach § 21 DSG-EKD grundsätzlich verpflichtet, alle Verfahren, die zur automatisierten Verarbeitung personenbezogener Daten dienen, vor der Inbetriebnahme der oder dem zuständigen Datenschutzbeauftragten zu melden. Demnach unterliegen Datenverarbeitungsprogramme, mit denen personenbezogene Daten erhoben, gespeichert oder übermittelt werden, vor der Einführung bei der kirchlichen Stelle der Meldepflicht. Wann muss gemeldet werden?

Die Meldung hat bereits vor der Inbetriebnahme des neuen Datenverarbeitungsprogramms zu erfolgen.

Bei wem muss gemeldet werden?

Die Meldung muss an die oder den Datenschutzbeauftragte/n erfolgen. Die Adresse lautet:

Datenschutzbeauftragte der Evangelisch-Lutherischen Landeskirche:

Kirchenkreisverwaltung Parchim
Lindenstr. 1
19370 Parchim
E-Mail: c.buller@pch.ellm.de

Ausnahmen von der Meldepflicht

Die Meldepflicht entfällt nach § 21 Absatz 3 DSG-EKD, wenn die verantwortliche kirchliche Stelle eine Beauftragte oder einen Beauftragten für den Datenschutz nach § 22 DSG-EKD bestellt hat. Das gleiche gilt, wenn bei der verantwortlichen kirchlichen Stelle höchstens sechs Personen mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten betraut sind.

3. Zuständigkeit für die Führung der Übersicht

Es bietet sich an, dass die oder der Betriebsbeauftragte bzw. örtlich Beauftragte für den Datenschutz die Übersicht über die Datenverarbeitungsprogramme führt. Die Übersichten sind in enger Zusammenarbeit mit den in der Datenverarbeitung sowie in den Sachgebieten tätigen Personen zu erstellen. Soweit keine Betriebsbeauftragte oder örtlich Beauftragte für den Datenschutz bestellt sind, müsste diese Aufgabe entweder von der Leitung der kirchlichen Stelle selber oder durch von ihr beauftragte Personen (z. B. Leitung der Datenverarbeitung) wahrgenommen werden.

4. Einsichtnahme von betroffenen Personen

§ 21 Absatz 2 Satz 2 DSG-EKD gestattet es allen Personen, die Übersichten einzusehen, sofern sie ein berechtigtes Interesse an der Einsichtnahme nachweisen können.

Schon allein aus diesem Grunde sollten die Übersichten laufend aktualisiert werden, soweit Veränderungen in den Datenverarbeitungsverfahren eintreten.

5. Erläuterungen zur Erstellung der Übersicht

Mit der Übersicht wird nicht nur der Name des eingesetzten Datenverarbeitungsprogramms aufgelistet, sondern sie besteht aus einer ausführlichen Beschreibung für alle in der kirchlichen Stelle genutzten automatisierten Verfahren. Der Inhalt der Verfahrensbeschreibungen ist in § 14 Absatz 2 DSG-EKD geregelt. Für automatisierte Verarbeitungen, die in gleicher oder ähnlicher Weise mehrfach geführt werden, können die Festlegungen zusammengefasst werden.

Ausgenommen von der Erfassung in den Übersichten sind:

- Dateien, die nur vorübergehend vorgehalten und innerhalb von drei Monaten nach ihrer Erstellung gelöscht werden und
- automatisierte Verarbeitungen, die allgemeinen Verwaltungszwecken dienen, einschließlich deren Datensicherung.

Zu Nummer 1: Name der verantwortlichen Stelle

Es ist der Name der kirchlichen Stelle oder der Einrichtung zu benennen, die ein Datenverarbeitungsprogramm einsetzt, mit dem personenbezogene Daten erhoben, verarbeitet oder genutzt werden. Kirchliche Stellen und deren Einrichtungen können sowohl juristische Personen des Privatrechts als auch Körperschaften des öffentlichen Rechts sein.

Zu Nummer 2.1: Bezeichnung der Verarbeitungsprogramme

Es ist der offizielle Name des Datenverarbeitungsprogramms mit Nummer der Version einzutragen (z. B. Microsoft Excel 2003), um die Gefahr einer Verwechslung mit anderen Programmen auszuschließen.

Zu Nummer 2.2: Art der Verarbeitungsprogramme

Da die Programmnamen oftmals nicht aussagekräftig genug sind, wäre an dieser Stelle die Art der Verarbeitungsprogramme anzugeben (z. B. E-Mail-Programm, Kalkulationsprogramm, Meldewesenprogramm, Personalabrechnungsverfahren).

Zu Nummer 3: Zweckbestimmung

Darunter ist die Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung zu verstehen (z. B. Patientenbetreuung, Spendenwerbung, Abonnentenbetreuung, Adressdatenbank der Gremiumsmitglieder, Telefon-, Gehalts-, Beihilfeabrechnung).

Zu Nummer 4: Art der gespeicherten Daten

Es ist die informatorische Beschreibung der Daten mit möglichst griffigen Namen einzutragen.

Es ist nicht notwendig, in die Beschreibung alle personenbezogenen Daten selbst aufzunehmen. Die Inhaltsbezeichnungen müssen allgemein verständlich sein, weil die Übersicht von jedermann bei berechtigtem Interesse eingesehen werden kann. Auch noch nicht besetzte Datenfelder sind in die Beschreibung aufzunehmen sowie die Inhalte, die eventuell in vorhandene Freitextfelder eingetragen werden dürfen (z. B. Adressdaten, Bankverbindungsdaten, Alter, Einkommen, Familienstand, Konfirmationsdaten, Traudaten, Freitextfeld für die Erreichbarkeit).

Zu Nummer 5: Betroffener Personenkreis

Es ist festzulegen, welche Personenkreise erfasst werden dürfen. Dies geschieht durch die Bezeichnung der allen Betroffenen gemeinsamen Merkmale, die sich aus dem Inhalt der Aufgabe und der Zweckbestimmung des Programms ergeben. Die Beschreibung des Personenkreises sollte so präzise erfolgen, dass für jede beliebige Person entschieden werden kann, ob sie zum Kreis gehört oder nicht (z. B. alle Mitarbeitenden bei einem Personalabrechnungsverfahren, alle Spenderinnen und Spender bei Spenden-Mailing-Aktionen, alle Gremiumsmitglieder bei einer Personendatenbank).

Zu Nummer 6.1: Art der regelmäßig zu übermittelnden Daten

Sofern die personenbezogenen Daten regelmäßig an Dritte übermittelt werden, ist anzugeben, um welche Datenarten es sich handelt (z. B. Patientendatenübermittlung mit Diagnoseschlüsseln

und Abrechnungsmerkmalen, Namen und Adresdaten von Spenderinnen und Spendern für Mailing-Aktionen).

Zu Nummer 6.2: Datenempfangende Stellen

Es sind die Namen der kirchlichen, öffentlichen oder sonstigen Stellen oder von Personen einzutragen, die regelmäßig die unter Nr. 6.1 eingetragenen Daten erhalten (z. B. AOK, Jugendamt der Stadt, Rechenzentrum, Druckerei).

Zu Nummer 7: Regelfristen der Löschung der Daten

Die Löschung der Daten hat nach Ablauf der gesetzlichen, satzungsmäßigen oder vertraglichen Aufbewahrungsfristen zu erfolgen. Soweit für Daten solche Aufbewahrungsfristen nicht bestehen, sind sie zu löschen, wenn die Zweckbestimmung (siehe Nummer 3) entfallen ist. Bei unterschiedlichen Lösungsfristen ist herauszustellen, auf welche Daten sich die jeweiligen Fristen beziehen.

Zu Nummer 8: Zugriffsberechtigter Personenkreis

Diese Eintragung dient dem internen Datenschutz. Es ist die Person oder der Personenkreis zu benennen, die oder der mit den Daten arbeitet (z. B. Personalleitung, Personalsachbearbeitung, Rechnungsprüfung, Sozialarbeiterinnen und -arbeiter).

Zu Nummer 9: Rechtsgrundlage für die Datenverarbeitung

Es sind die einschlägigen Vorschriften so genau wie möglich anzugeben, nach denen die Datenerhebung, -verarbeitung oder -nutzung zulässig ist. Dies können bereichsspezifische Vorschriften (z. B. Kirchengesetz der EKD über die Kirchenmitgliedschaft, Verordnung der EKD über die in das Gemeindegliederverzeichnis aufzunehmenden Daten der Kirchenmitglieder mit ihren Familienangehörigen, Kirchengesetz über die Kirchenmitgliedschaft der ELLM) oder die entsprechenden Bestimmungen des DSGVO-EKD oder der DSGVO-EKD AG sein.

Anlage 7 zu § 14 Datenschutzanwendungsverordnung:

- Muster „Bestellung von Betriebs- und örtlich Beauftragten für den Datenschutz“

**Bestellung
einer / eines Betriebsbeauftragten
einer / eines örtlich Beauftragten für den Datenschutz**

Frau / Herr _____
(Nichtzutreffendes streichen)

wird für _____
(Name und Adresse der kirchlichen Stelle, bei gemeinsamen Betriebs- oder örtlich Beauftragten
alle beteiligten kirchlichen Stellen auführen)

ab dem _____

zur / zum Betriebsbeauftragten für den Datenschutz
(Kirchliche Werke und Einrichtungen mit eigener Rechtspersönlichkeit,
z. B. diakonische Einrichtungen als e.V. oder GmbH, kirchliche Stiftungen)

als Vertretung der oder des Betriebsbeauftragten für den Datenschutz

zur / zum örtlich Beauftragten für den Datenschutz
(Kirchengemeinde, Kirchenkreis, kirchlicher Verband)

als Vertretung der oder des örtlich Beauftragten für den Datenschutz
bestellt.

Die Bestellung erfolgt

auf unbestimmte Zeit

zeitlich befristet bis zum _____

Im Rahmen der Datenschutzaufgaben sind Sie weisungsfrei und dürfen wegen dieser Tätigkeit nicht benachteiligt werden. Ihre Aufgaben ergeben sich aus dem kirchlichen Datenschutzrecht und werden in dem ausgehändigten Merkblatt „Datenschutz in der kirchlichen Stelle unter Einbindung von Betriebs- und örtlich Beauftragten für den Datenschutz“ unter Nummer 6 näher beschrieben.

Im Rahmen dieser Tätigkeit sind Sie unmittelbar

(Bezeichnung des gesetzlich oder verfassungsmäßig berufenen Organs / bei gemeinsamen Beauftragten
für alle beteiligten kirchlichen Stellen die Organe auführen)

unterstellt.

Ort, Datum, Unterschrift (Leitung)

Empfangsbestätigung

Das Berufungsschreiben sowie ein Exemplar des Merkblatts „Datenschutz in der kirchlichen Stelle unter Einbindung von örtlich Beauftragten für den Datenschutz und Betriebsbeauftragten für den Datenschutz“ habe ich erhalten.

(Ort, Datum, Unterschrift der bestellten Person)

- Exemplar an Mitarbeiterin/Mitarbeiter
- Exemplar zur Personalakte
- Exemplar an die / den Datenschutzbeauftragte/n der ELLM
- Exemplar an das kirchliche Werk / die kirchliche Einrichtung
- bei der Bestellung zur / zum Betriebsbeauftragten für den Datenschutz
- Exemplar an die aufsichtführende Stelle
- bei der Bestellung zur / zum örtlich Beauftragten für den Datenschutz

Anlage 8 zu § 16 Datenschutzanwendungsverordnung:

- Merkblatt „Datenschutz in der kirchlichen Stelle unter Einbindung von Betriebs- und örtlich Beauftragten für den Datenschutz“

Datenschutz in der kirchlichen Stelle unter Einbindung von Betriebs- und örtlich Beauftragten für den Datenschutz

1. Datenschutz in der kirchlichen Stelle: Verantwortung, Kontrolle und Unterstützung

Die Verantwortung für den Datenschutz in der kirchlichen Stelle trägt die Leitung. Sie hat die Einhaltung der allgemeinen und bereichsspezifischen Datenschutzbestimmungen und die Rechtmäßigkeit der bei ihr durchzuführenden Verwaltungsverfahren sicherzustellen. Das bedeutet, dass sie auch Vorsorge für die Einhaltung datenschutzrechtlicher Bestimmungen treffen muss. Die oder der Betriebs- bzw. örtlich Beauftragte für den Datenschutz unterstützt die Leitung in dieser Aufgabe und kontrolliert die Umsetzung des Datenschutzes in der Verwaltungspraxis.

Nicht selten wird diese Aufgabenverteilung zwischen Leitung und Beauftragten für den Datenschutz missverstanden. Weder ist der Datenschutz bei einer kirchlichen Stelle mit der Benennung einer oder eines Beauftragten für den Datenschutz automatisch sichergestellt, noch können die Beauftragten für den Datenschutz in ihren kirchlichen Stellen die Einhaltung datenschutzrechtlicher Vorschriften gewährleisten.

Die Betriebs- und örtlich Beauftragten für den Datenschutz können Verstöße gegen datenschutzrechtliche Bestimmungen feststellen und auf Abhilfe dringen, sie können auch datenschutzfreundliche Verfahren anregen, aber sie haben in letzter Konsequenz keine Möglichkeit, ihre Forderungen gegenüber den einzelnen Mitarbeiterinnen und Mitarbeitern durchzusetzen. Diese Aufgabe obliegt der Leitung. Sie haben die Mitarbeiterinnen und Mitarbeiter ihrer Verwaltungen und Einrichtungen zu einer datenschutzfreundlichen Arbeitsweise anzuleiten. Eine Leitung, die aktiv Datenschutz betreibt, erfüllt so einen berechtigten Anspruch, den Gemeindeglieder, Eltern von in Kindertagesstätten betreuten Kindern, Patientinnen und Patienten von diakonischen Einrichtungen usw. an die jeweilige kirchliche Stelle richten.

2. Welche kirchliche Stelle muss Beauftragte für den Datenschutz bestellen?

Nach § 22 Absatz 1 des Kirchengesetzes über den Datenschutz in der Evangelischen Kirche in Deutschland (DSG-EKD) sollen bei kirchlichen Werken und Einrichtungen mit eigener Rechtspersönlichkeit Betriebsbeauftragte, bei den übrigen kirchlichen Stellen (Kirchgemeinden, Kirchenkreise, kirchliche Verbände) örtlich Beauftragte für den Datenschutz bestellt werden. Die Bestellung kann sich auf mehrere Werke, Einrichtungen und kirchliche Körperschaften erstrecken und sollte erfolgen, wenn mehr als sechs Personen mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten befasst sind. Bei kleineren kirchlichen Stellen dürfte es sich anbieten, dass ein/e von diesen Stellen berufene/r „gemeinsame/r Beauftragte/r für den Datenschutz“ sich der Aufgabe annimmt. Für diesen Fall sollten über eine Vereinbarung der Aufgabenbereich und insbesondere die Kostenregelung festgeschrieben werden. Nähere Ausführungen zur Bestellung von Personen als „gemeinsame Beauftragte für den Datenschutz“ finden sich unter der Nummer 4 dieses Merkblatts.

Im Zusammenhang mit der Bestellung von Beauftragten für den Datenschutz ist die Vertretung zu regeln.

3. Welche Personen können zu Betriebs- oder örtlich Beauftragten für den Datenschutz bestellt werden?

Die gesetzliche Vorgabe von § 22 Absatz 2 DSG-EKD lautet: „Zu Beauftragten ... dürfen nur Personen bestellt werden, die die zur Erfüllung ihrer Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzen.“

Die oder der Betriebs- bzw. örtlich Beauftragte für den Datenschutz muss danach in fachlicher und persönlicher Hinsicht für die Aufgabe geeignet sein.

Zu den fachlichen Kenntnissen, die die oder der Beauftragte haben, bzw. erwerben sollte, gehört die Kenntnis der datenschutzrechtlichen Grundlagen. Dies sind insbesondere die allgemeinen Datenschutzbestimmungen nach dem DSG-EKD, dem DSG-EKD AG sowie eventuell bestehende bereichsspezifische Datenschutzbestimmungen und Hinweise des Oberkirchenrates. Außerdem sollen die Beauftragten gute Kenntnisse über die Organisation der kirchlichen Stelle und Verständnis für Fragen der Informationstechnik besitzen. Nur wenn den Beauftragten die Aufgaben, die Arbeitsweise und die Abläufe einschließlich der Datenströme in den Arbeitsbereichen vertraut sind, können sie ihre Beratungs- und Kontrollaufgaben effizient wahrnehmen. Des Weiteren sollten die Beauftragten für den Datenschutz über gute Kenntnisse der Datenverarbeitung und technisches Verständnis verfügen. Sie müssen den Aufbau, die Funktionsweise und die Anforderungen der eingesetzten Datenverarbeitungssysteme in ihren Grundzügen begreifen, um die eingesetzten Verfahren bewerten und sinnvolle Datensicherungs- und Datenschutzmaßnahmen vorschlagen zu können. In der Praxis werden nur wenige Personen von vornherein alle diese Voraussetzungen erfüllen. Hier wird die oder der Beauftragte für den Datenschutz ihre oder seine Kenntnisse und Fähigkeiten weiterentwickeln müssen. Dazu sollte die Gelegenheit zur Teilnahme an geeigneten Fortbildungsveranstaltungen genutzt werden.

Im Hinblick auf die persönliche Zuverlässigkeit der oder des Beauftragten ist neben anderen grundlegenden Charakterstärken vor allem wichtig, dass sie oder er über eine innere Unabhängigkeit verfügt und die Verpflichtung zur Verschwiegenheit ernst nimmt. Beauftragte haben Zugang zu allen sensiblen, personenbezogenen Daten.

Sie werden nur dann datenschutzgerecht und vertrauensvoll mit der Leitung sowie den Mitarbeiterinnen und Mitarbeitern zusammenarbeiten können, wenn sie über diese Kenntnisse Verschwiegenheit bewahren.

Für die oder den Betriebs- bzw. örtlich Beauftragten für den Datenschutz selbst wird es eine besondere Schwierigkeit darstellen, sich eine innere Unabhängigkeit in der Bewertung der datenschutzrechtlich relevanten Sachverhalte zu erhalten. Wer die Aufgabe ernst nimmt, erfährt schnell, dass Datenschutz vielfach als lästig empfunden wird. Man wird die Beauftragten möglicherweise drängen, von Datenschutzforderungen Abstand zu nehmen. Da die oder der Beauftragte üblicherweise selbst Mitarbeiterin beziehungsweise Mitarbeiter der kirchlichen Stelle ist, die sie oder ihn beauftragt hat, ist sie oder er teilweise selbst betroffen von neuen Datenschutzmaßnahmen. Es ist deswegen im Interesse der Unabhängigkeit der Beauftragten darauf zu achten, dass eine Interes-

senkollision zwischen der Aufgabe als Betriebs- bzw. örtlich Beauftragte/r für den Datenschutz und den sonstigen Aufgaben als Mitarbeiterin oder Mitarbeiter nicht entsteht.

4. Wie kann eine Interessenkollision vermieden werden?

Die Betriebs- bzw. örtlich Beauftragten für den Datenschutz dürfen während ihrer Tätigkeit nicht mit Aufgaben betraut sein, deren Wahrnehmung zu Interessenkollisionen führen könnte. Es gilt das Prinzip, dass die oder der zu Kontrollierende nicht zum Kontrolleur werden kann. So sollen die Beauftragten beispielsweise nicht gleichzeitig leitende Aufgaben in den Bereichen der Informationstechnik wahrnehmen und es darf ihnen auch nicht die Aufsicht über die Einhaltung des Datenschutzes obliegen.

Gerade in kleinen Stellen fehlen aber häufig sachkundige Mitarbeiterinnen und Mitarbeiter, die nicht auch zugleich in datensensiblen Arbeitsbereichen tätig sind. In diesen Fällen bietet § 22 Absatz 1 Satz 2 DSGVO eine Lösung an. Es können mehrere Stellen gemeinsam eine oder einen Beauftragten bzw. eine Vertretung bestellen. In der Praxis sind hier verschiedene Varianten denkbar:

- Mehrere gleichartige kirchliche Stellen benennen gemeinsam eine/n Beauftragte/n und eine/n Vertreter/in. Ein solches Modell bietet sich besonders für Kirchengemeinden, kleinere kirchliche Verbände, kleinere diakonische Einrichtungen und für kirchliche Stiftungen an. In dieser Weise könnte die Zusammenarbeit der kirchlichen Stellen untereinander gefördert werden.
- Dieses Modell mag sich zum Beispiel für besonders große diakonische Werke schon nicht mehr eignen, weil das Aufkommen an personenbezogenen Daten aus den unterschiedlichsten Bereichen beträchtlich sein kann. Hier könnte zwar ebenfalls wegen der Gleichartigkeit der Struktur dieser diakonischen Stellen ein/e gemeinsame/r Betriebsbeauftragte/r für den Datenschutz für mehrere diakonische Werke bestellt werden. Aber statt einer/eines gemeinsamen Vertreterin/Vertreters würde es sich anbieten, in den einzelnen diakonischen Werken Vertreter/innen zu benennen, die der/dem Betriebsbeauftragten für den Datenschutz zuarbeiten.

Insgesamt bietet das Gesetz hinreichende Lösungsansätze, um den Gegebenheiten vor Ort Rechnung zu tragen und zugleich Interessenkollisionen zu vermeiden. Zudem können Synergieeffekte durch das Zusammenwirken mehrerer Personen (beauftragte und vertretende Personen) genutzt werden, wenn zum Beispiel die/der mehr rechtlich vorgebildete Beauftragte mit der/dem technisch vorgebildeten vertretenden Beauftragten eng zusammenarbeitet.

5. Die Beauftragten für den Datenschutz in der kirchlichen Stelle: Bestellung, Bekanntmachung, Stellung und Abberufung

Ein Handschlag reicht zur Bestellung einer/eines Beauftragten nicht aus. Die Übertragung von Verantwortung in diesem Umfang erfordert eine schriftliche Bestellung der/des Beauftragten und der Vertreter/innen. Damit die Beauftragten ihre Aufgabe erfüllen können, müssen sie darüber hinaus auch den Beschäftigten in geeigneter Weise bekannt gemacht werden. Die/der Beauftragte sollte darüber hinaus im Geschäftsverteilungs- und Organisationsplan der kirchlichen Stelle ausgewiesen sein.

Eine unabhängige und organisatorisch herausgehobene Stellung ist für eine wirkungsvolle Tätigkeit der Beauftragten von entscheidender Bedeutung. Deshalb können sich die Beauftragten

jederzeit unmittelbar an die Leitung der kirchlichen Stelle wenden und sind nur ihr gegenüber rechenschaftspflichtig. Organisatorisch bietet sich dort, wo die Größe der kirchlichen Stelle es erlaubt, die Zuordnung der/des Beauftragten im engeren Wirkungskreis der Leitung bzw. Geschäftsführung an. Dies ermöglicht der Leitung, dass sie frühzeitig über Datensicherheitsbeeinträchtigungen, Gesetzesverstöße oder Verbesserungsvorschläge unterrichtet wird und entsprechend schnell reagieren kann. Es verhindert außerdem, dass die/der Beauftragte einer Interessenkollision ausgesetzt ist.

Die Beauftragten sind in der Wahrnehmung ihrer Aufgabe nach § 22 Absatz 3 Satz 2 DSGVO weisungsfrei. Sie können danach selbst über den Zeitpunkt und die Art und Weise des Tätigwerdens entscheiden. Dies umfasst die Entscheidung, ob sie eine datenschutzrechtliche Prüfung durchführen oder ob sie diese unterlassen ebenso wie die Freiheit, sich für die ihrer begründeten Überzeugung nach zutreffende Rechtsauffassung im Einzelfall zu entscheiden.

Eine Benachteiligung der/des Beauftragten wegen dieser Tätigkeit ist nach § 22 Absatz 3 Satz 3 DSGVO verboten. Dieses Benachteiligungsverbot ist weit gefasst.

Es richtet sich nicht nur an die Leitung oder Geschäftsführung, sondern auch an die Mitarbeitenden und die Mitarbeitervertretung. Auch darf die Tätigkeit als Beauftragte/r keine negativen Auswirkungen auf die berufliche Entwicklung derjenigen haben, die diese Funktion ausüben. In engem Zusammenhang mit der Stellung von Beauftragten steht die Frage, ob eine Abberufung aus dieser Funktion möglich ist. Hier regelt § 14 Absatz 2 DSGVO, dass die Bestellung widerrufen werden kann, wenn ein Interessenkonflikt mit anderen Aufgaben oder sonst ein wichtiger Grund eintritt. Eine Abberufung darf deswegen nicht aus Gründen erfolgen, die offensichtlich eine Benachteiligung der/des Beauftragten für den Datenschutz wegen ihrer/ seiner Aufgabenerfüllung bedeuten würden. Es sind in der Praxis Fälle denkbar, in denen eine Abberufung notwendig wird. Eine Abberufung kommt beispielsweise in Betracht, wenn die/der Beauftragte für den Datenschutz mit neuen fachlichen Aufgaben betraut werden soll, die die Fortsetzung der Tätigkeit als Beauftragte/r nicht mehr zulassen. Vor der Entscheidung über den Widerruf ist die/der Betriebsbeauftragte bzw. die/der örtlich Beauftragte für den Datenschutz zu hören. Diese Regelung soll mit zur Stärkung der Stellung der Betriebsbeauftragten oder örtlichen Beauftragten beitragen.

Mit dem Ausscheiden der/des Beauftragten aus dem Dienst- oder Arbeitsverhältnis einer kirchlichen Stelle endet im Normalfall die Bestellung. Nur ausnahmsweise, wenn keine andere Person zur Verfügung steht, sollte für einen begrenzten Zeitraum überlegt werden, ob das Amt der/des Beauftragten als sogenannte „externe Datenschutzbeauftragung“ fortgeführt werden kann.

6. Aufgaben der Betriebs- und örtlich Beauftragten für den Datenschutz

a. Datenschutz braucht Verbündete vor Ort

Gesetze, Verordnungen, Erlasse und Dienstanweisungen zum Datenschutz sind notwendig, sie sind den Mitarbeiterinnen und Mitarbeitern aber bei der täglichen Arbeit selten in allen Nuancen und Details präsent. Deshalb ist es wichtig, dass die Beauftragten für den Datenschutz werben, über ihn informieren, neue Datenverarbeitungsverfahren möglichst schon vor ihrer Einführung beurteilen und die Einhaltung des Datenschutzes kontrollieren.

Die Beauftragten für den Datenschutz beraten und unterstützen die Leitung der kirchlichen Stelle und die Arbeitsbereiche, die

personenbezogene Daten verarbeiten, in allen Fragen des Datenschutzes sowie der datenschutzgerechten Organisation.

Hierzu gehören die Beratung und Mitwirkung bei der Erstellung eines Sicherheitskonzepts für die in der kirchlichen Stelle eingesetzte Informationstechnik, beim Verfassen von Richtlinien, Rundschreiben und Dienstvereinbarungen, bei der Ausgestaltung von Verträgen mit Auswirkungen für den Datenschutz (z. B. bei Datenverarbeitung im Auftrag). Hilfreich ist es in diesem Zusammenhang auch, wenn die Beauftragten an allen datenschutzrelevanten Vorgängen beteiligt werden und ihnen Planungen, die den Umgang mit personenbezogenen Daten betreffen, rechtzeitig bekannt gegeben werden.

Eine enge Zusammenarbeit mit der Leitung der kirchlichen Stelle kann dadurch gefördert werden, indem man regelmäßig Gespräche führt, wie der Datenschutz tatsächlich praktiziert wird, welche Schwachpunkte bestehen und wie diese auszuräumen sind. Hilfreich sind auch schriftliche Protokolle und Berichte, die gegebenenfalls ganz oder auszugsweise auch an alle Mitarbeitenden bekannt gegeben werden können, damit diese für die Belange des Datenschutzes weiter sensibilisiert werden.

Die Beauftragten für den Datenschutz haben unmittelbaren Kontakt zu den Mitarbeiterinnen und Mitarbeitern und schulen sie in Fragen des Datenschutzes.

b. Verfahrensverzeichnisse geben Überblick

Das DSGVO-EKD legt in § 14 Absatz 2 fest, dass die kirchlichen Stellen für ihre Zuständigkeitsbereiche Übersichten über die eingesetzten Datenverarbeitungsprogramme zu führen haben. Die Dezentralisierung und die Beschränkung auf Datenverarbeitungsverfahren soll eine einfache Führung der Übersichten, die ohne großen Aufwand aktuell gehalten werden können, begünstigen. Ihr Nutzen als Kontrollinstrument vor Ort ist für die Beauftragten größer als bei einem zentral geführten Register.

Das Verfahrensverzeichnis, das unmittelbar in den öffentlichen Stellen geführt wird, dient dazu, den Überblick darüber zu behalten, wo sich in der Behörde personenbezogene Daten befinden und wie sie behandelt werden. So können mögliche „Datenlecks“ schneller gefunden und geschlossen werden.

Dieses Verfahrensverzeichnis kann von jeder Person unentgeltlich eingesehen werden, wenn diese ein berechtigtes Interesse nachweisen kann (§ 21 Absatz 2 Satz 2 DSGVO-EKD).

c. Weitere Aufgaben der Beauftragten

Die/der Beauftragte für den Datenschutz ist über die Einrichtung von automatisierten Abrufverfahren möglichst frühzeitig zu infor-

mieren. Mit Abrufverfahren kann z. B. einer anderen kirchlichen Stelle die Möglichkeit und Berechtigung geschaffen werden, auf einen zentralen Datenbestand zu Auskunftszwecken oder auch zur weiter gehenden Nutzung zuzugreifen.

Bei der Verarbeitung personenbezogener Daten im Auftrag bietet es sich an, die Beauftragten für den Datenschutz vor der schriftlichen Auftragserteilung einzubinden und ihnen auch das Recht einzuräumen, sich von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen beim Auftragnehmer jederzeit überzeugen zu können.

Da für die Abwicklung der Verwaltungsabläufe häufig Vordrucke verwendet werden, bietet es sich an, bei der Erstellung oder Veränderung von Vordrucken und Merkblättern die Beauftragten für den Datenschutz zu beteiligen. Der Beratungsschwerpunkt dürfte sich dabei auf die Zulässigkeit der Datenerhebung konzentrieren.

Soweit Betroffene Auskunft über die von ihnen gespeicherten personenbezogenen Daten verlangen oder Anfragen zum Datenschutz in der kirchlichen Stelle haben, sollte die/der Beauftragte für den Datenschutz beteiligt werden oder federführend mit der Abwicklung beauftragt werden.

Die Schulung der Mitarbeitenden über die Bestimmungen über den Datenschutz unter Berücksichtigung der besonderen Verhältnisse ihres Aufgabenbereiches obliegt der/dem Beauftragten für den Datenschutz. Dies kann beispielsweise wie folgt bestehen:

- Einweisung neuer Mitarbeitender,
- Schulung im Rahmen der allgemeinen Aus- und Fortbildung,
- Vorträge oder Referate bei Dienstbesprechungen,
- Ausgabe von Merkblättern,
- Mitteilungen am Schwarzen Brett,
- Berichte bei Mitarbeiterversammlungen,
- Beiträge in Hauszeitschriften oder Mitteilungsblättern.

d. Weiterbildung und Zusammenarbeit

Zur sachgemäßen Durchführung der Aufgaben sollte den Beauftragten für den Datenschutz die Möglichkeit zur Weiterbildung und zum Erfahrungsaustausch mit Kolleginnen und Kollegen aus anderen kirchlichen Stellen eröffnet werden. Der Oberkirchenrat, die Diakonischen Werke und die Beauftragten für den Datenschutz der Evangelisch-Lutherischen Kirche bieten regelmäßig Fort- und Weiterbildungsveranstaltungen an. Auch über das Internet sind insbesondere über die staatlichen Beauftragten für den Datenschutz umfangreiche Informationen zu nahezu allen datenschutzrechtlich relevanten Fragestellungen abrufbar. Die Kosten der Fort- und Weiterbildung sowie für die Anschaffung von Literatur hat die kirchliche Stelle zu tragen.

Anlage 9 zu § 16 Datenschutzausführungsgesetz der EKD:

- Merkblatt „Veröffentlichung von Gemeindeglieder- und Amtshandlungsdaten“

**Veröffentlichung
von Gemeindeglieder- und Amtshandlungsdaten**

Die Abkündigung von Amtshandlungen im Gottesdienst ist agendarisch geregelt (Evangelisches Gottesdienstbuch 1999 S. 548 ff.). § 16 Absatz 1 DSGVO-EKD Ausführungsgesetz erlaubt den Kirchgemeinden zusätzlich, Alters- und Ehejubiläen von Gemeindegliedern und kirchliche Amtshandlungsdaten im Gemeindebrief und anderen örtlichen kirchlichen Publikationen mit Namen und Anschriften sowie Tag und Ort des Ereignisses zu veröffentlichen, soweit die Betroffenen im Einzelfall nicht widersprochen haben. Das Widerspruchsrecht der Betroffenen bezieht sich vorrangig darauf, dass eine Veröffentlichung der Anschriften unterbleibt.

Die Kirchgemeinde kann entweder die Betroffenen vor Veröffentlichung der Jubiläumsdaten einzeln schriftlich auf die Möglichkeit hinweisen, der Veröffentlichung widersprechen zu können, oder im Gemeindebrief einen Hinweis auf das Widerspruchsrecht aufnehmen. Im letzteren Fall ist es ausreichend, wenn der Hinweis regelmäßig, mindestens einmal im Jahr, an derselben Stelle wie die Veröffentlichung der Jubiläumsdaten erfolgt.

Nur in Ausnahmefällen, wenn die Betroffenen ein überwiegendes schutzwürdiges Interesse am Ausschluss der Veröffentlichung geltend machen, hat eine Veröffentlichung der kirchlichen Amtshandlungen in Gemeindebriefen und anderen örtlichen kirchlichen Publikationen zu unterbleiben.

Die Medien- und Presseverbände sind angehalten, in ihren kirchlichen Publikationen, in denen solche Veröffentlichungen regelmäßig erfolgen, auf das in § 16 DSGVO-EKD Ausführungsgesetz enthaltene Widerspruchsrecht hinzuweisen.

Eine Weitergabe von Gemeindeglieder- und Amtshandlungsdaten an Tageszeitungen und sonstige nichtkirchliche Publikationen ist nicht zulässig.

Die Widersprüche von Gemeindegliedern gegen eine Veröffentlichung ihrer Jubiläums- und Amtshandlungsdaten sind in Gemeindeglieder-Datenverwaltungsprogramme aufzunehmen.

Die Veröffentlichung von Namen und Anschriften von Gemeindegliedern, ihrer Alters- und Ehejubiläen sowie von kirchlichen Amtshandlungsdaten im Internet sind nur zulässig, wenn die betroffenen Personen vorher schriftlich einer Veröffentlichung zugestimmt haben (siehe das Muster in Anlage 10 zu § 16 DSGVO-EKD Ausführungsgesetz). Vor der Unterzeichnung der Einwilligungserklärung sollte auf die Gefahren, die durch anderweitige, weltweite, nicht mehr kontrollierbare Nutzung der Daten durch Dritte möglich ist, hingewiesen werden.

Soweit von den kommunalen Meldebehörden Auskunfts- und Übermittlungssperren übermittelt worden sind, dürfen nach § 15 Absatz 3 DSGVO-EKD AG Veröffentlichungen nur erfolgen, wenn vorher das Einverständnis der betroffenen Person eingeholt wurde.

Anlage 10 zu § 18 Datenschutzanwendungsverordnung:

- Muster „Einwilligungserklärung zur Veröffentlichung von Gemeindeglieder- und Amtshandlungsdaten im Internet“

Einwilligungserklärung zur Veröffentlichung von Gemeindeglieder- und Amtshandlungsdaten im Internet

Frau/Herr _____ erklärt:
(Name, Vorname, Geburtsdatum)

Ich bin mit der Veröffentlichung

aller Alters- und Ehejubiläen mit Namen und Anschriften sowie Tag und Ort des Ereignisses

aller kirchlichen Amtshandlungen mit Namen, Anschriften sowie Tag und Ort der vorgenommenen Amtshandlung im Internet auf der Homepage der (bitte Namen der kirchlichen Stelle angeben) einverstanden.

Meine dort veröffentlichten personenbezogenen Daten sind weltweit abrufbar und von dritter Seite für andere Zwecke einschließlich Werbung nutzbar.

(Datum, Unterschrift)

Die Kirchenleitung hat auf ihrer Sitzung am 4. Dezember 2009 folgende Verordnung beschlossen:

116.06/119

Verordnung zur Sicherstellung der Anforderungen an den Datenschutz in der Informationstechnik (IT) (IT-Sicherheitsverordnung) vom 4. Dezember 2009

Die Kirchenleitung hat auf Grund von § 27 Absatz 2 des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland vom 12. November 1993 (ABl. EKD 1994 S. 35), geändert durch das Kirchengesetz vom 7. November 2002 (Bekanntmachung in der ab 1. Januar 2003 geltenden Fassung vom 20. Februar 2003 und vom 7. April 2003, ABl. EKD S. 74 und 117) die folgende Verordnung erlassen:

Inhaltsverzeichnis

<p>§ 1 Geltungsbereich</p> <p>§ 2 IT-Sicherheitsstandard</p> <p>§ 3 IT-Sicherheitsziele</p> <p>§ 4 Zuständigkeit für die Umsetzung der IT-Sicherheitsverordnung</p> <p>§ 5 IT-Sicherheitsbeauftragter</p> <p>§ 6 Kontrolle über die Einhaltung der IT-Sicherheitsverordnung</p>	<p>§ 7 Änderung und Aktualisierung der IT-Sicherheitsverordnung</p> <p>§ 8 Sprachliche Gleichstellung</p> <p>§ 9 Durchführungsvorschriften</p> <p>§ 10 Inkrafttreten</p>
---	--

§ 1 Geltungsbereich

Die IT-Sicherheitsverordnung ist verbindlich für sämtliche Mitarbeitende im Sinne des § 1 Datenschutzverordnung sowie für Dritte, mit denen die Benutzung von Computern und Netzen von kirchlichen und diakonischen Einrichtungen vereinbart worden ist.

§ 2 IT-Sicherheitsstandard

Der Oberkirchenrat und der Vorstand des Diakonischen Werkes werden beauftragt, den gestaffelten IT-Sicherheitsstandard auf Basis des IT-Grundschutzes des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in der Evangelisch-Lutherischen Landeskirche Mecklenburgs und der Diakonie einheitlich festzulegen.

§ 3 IT-Sicherheitsziele

(1) Die IT-Sicherheitsverordnung definiert grundlegende Ziele einer IT-Sicherheit und legt Verantwortlichkeiten sowie Rahmenbedingungen für die Umsetzung des IT-Sicherheitsstandards fest.

(2) Die mit der Informationstechnik erhobenen, verarbeiteten, übertragenen und gespeicherten Daten sind zu schützen, insbesondere im Hinblick auf

1. deren Zugänglichkeit/Verfügbarkeit
Daten und Anwendungen müssen dem jeweiligen Nutzungsprofil entsprechend jederzeit bei Bedarf verfügbar sein. Vor-

aussetzung für die Aufrechterhaltung der Datenverfügbarkeit ist die Sicherung aller IT-Komponenten und der technischen und räumlichen Infrastruktur gegen organisationsbedingte, technische und umweltbedingte Ausfälle. Zentrale, aber auch dezentrale IT-Systeme müssen funktionieren, um die Verfügbarkeit der Daten zu garantieren.

2. deren Integrität
Daten und Anwendungen dürfen nicht gelöscht, zerstört oder manipuliert werden.
3. den Schutz der Daten vor Verlust
Der Verlust der Daten ist durch geeignete Maßnahmen zu verhindern.
4. Vertraulichkeit
Daten und Anwendungen dürfen grundsätzlich nur von Personen gelesen und benutzt werden, die dazu eine Zugriffsberechtigung besitzen. Die Festlegung der Zugriffsberechtigung und des erforderlichen Kontrollumfangs obliegt dem jeweiligen Verfügungsberechtigten.
5. die Einführung, Auswahl, Gestaltung und Änderung von Verfahren
In die Gestaltung und Auswahl von Verfahren zur Verarbeitung personenbezogener Daten ist der zuständige kirchliche Datenschutzbeauftragte rechtzeitig einzubinden. Gleiches gilt für die Neueinführung und Änderung der Verfahren.

§ 4 Zuständigkeit für die Umsetzung der IT-Sicherheitsverordnung

Zuständig für die Umsetzung der IT-Sicherheitsverordnung ist im Bereich der Evangelisch-Lutherischen Landeskirche Meck-

lenburgs der Oberkirchenrat, im Bereich des Diakonischen Werkes der Träger der jeweiligen Einrichtung, soweit nicht im IT-Grundsatz etwas anderes festgelegt wird. Diese Aufgabe kann im Rahmen des Direktionsrechts an den IT-Sicherheitsbeauftragten delegiert werden.

§ 5

IT-Sicherheitsbeauftragter

Der IT-Sicherheitsbeauftragte sowie ein Stellvertreter werden für den Bereich der Evangelisch-Lutherischen Landeskirche Mecklenburgs vom Oberkirchenrat, für den Bereich des Diakonischen Werkes vom Vorstand bestellt. Die Evangelisch-Lutherische Landeskirche Mecklenburgs und das Diakonische Werk können gemeinsam einen IT-Sicherheitsbeauftragten bestellen.

§ 6

Kontrolle über die Einhaltung der IT-Sicherheitsverordnung

Bei Verstößen gegen die IT-Sicherheitsverordnung sind neben den arbeitsrechtlichen und datenschutzrechtlichen folgende Sanktionen möglich:

1. die Beanstandung bei geringfügigen individuellen Verstößen,
2. die Aufforderung an die Leitung der Einrichtung, den Missstand unter Wahrung einer Frist zu beseitigen,
3. bei Zuwiderhandlung oder Nichteinhaltung der Frist nach Nummer 2 die Mitteilung an die Aufsichtsbehörde, im Wege der Aufsicht die Beseitigung des Missstandes anzuordnen,
4. die vorübergehende Sperrung der Zugangsberechtigung zur Datenverarbeitungsanlage bis der Nachweis über die Beseitigung des Missstandes erbracht ist.

§ 7

Änderung und Aktualisierung der IT-Sicherheitsverordnung

Die Kirchenleitung hat die IT-Sicherheitsverordnung in regelmäßigen Abständen zu aktualisieren.

§ 8

Sprachliche Gleichstellung

Soweit in dieser Verordnung Bezeichnungen, die für Frauen und Männer gelten, in der männlichen Sprachform verwendet werden, gelten diese Bezeichnungen für Frauen in der weiblichen Sprachform.

§ 9

Durchführungsvorschriften

Der Oberkirchenrat ist berechtigt, Durchführungsvorschriften zu erlassen.

§ 10

Inkrafttreten

Diese Rechtsverordnung tritt am 1. Januar 2010 in Kraft.

Schwerin, 4. Dezember 2009

Der Vorsitzende der Kirchenleitung

Dr. von Maltzahn
Landesbischof

Mitteilung

Das Kirchliche Amtsblatt des Jahrganges 2009 umfasst 156 Seiten.

