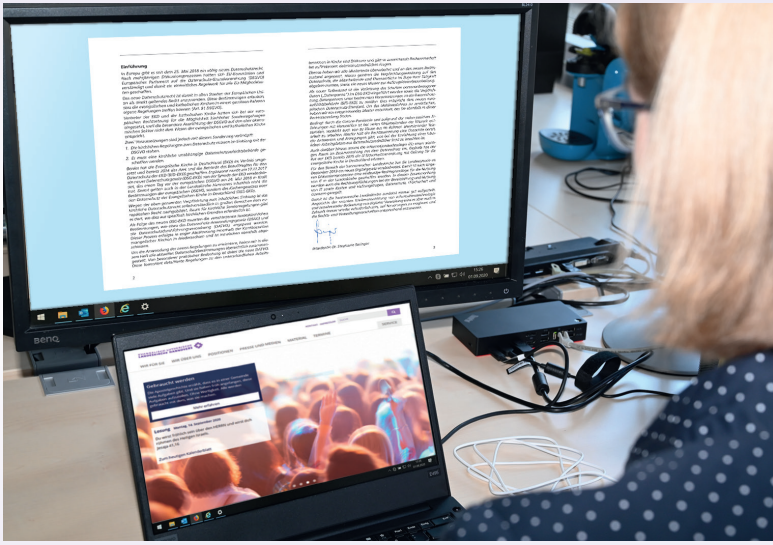
Datenschutzvorschriften in der Evangelisch-lutherischen Landeskirche Hannovers



Eine Zusammenstellung der Gesetze, Verordnungen, Muster und Checklisten für die kirchliche Arbeit

Evangelisch-lutherische Landeskirche Hannovers

**Datenschutzvorschriften in der
Evangelisch-lutherischen Landeskirche Hannovers**

Herausgeber:
Landeskirchenamt der
Evangelisch-lutherischen Landeskirche Hannovers

Verantwortlich:
Annegret v. Collande
Rote Reihe 6, 30169 Hannover
Fon: 0511 1241-751
E-Mail: anne.voncollande@evlka.de
Umschlagsgestaltung: werner.hentrich@t-online.de
Titelfoto: Bernd Grumblies
Satz und Layout: Werner.hentrich@t-online.de
Druck: www.rimi-grafik.de

Erscheinungsdatum: November 2020

Die abgedruckten Texte entsprechen dem Stand vom 01.11.2020. Nachfolgende Änderungen sind nicht berücksichtigt. Wir weisen darauf hin, dass die Gesetze, Verordnungen und Verwaltungsvorschriften laufenden Aktualisierungen unterliegen. Die vollständigen und verbindlichen Texte sind im Kirchlichen Amtsblatt bzw. auf der Internetseite der Evangelisch-lutherischen Landeskirche Hannovers (**www.evlka.de**) zu finden.

Inhaltsverzeichnis

Einführung

In Europa gibt es seit dem 25. Mai 2018 ein völlig neues Datenschutzrecht. Nach mehrjährigen Diskussionsprozessen hatten sich EU-Kommission und Europäisches Parlament auf die Datenschutz-Grundverordnung (DSGVO) verständigt und damit ein einheitliches Regelwerk für alle EU-Mitgliedstaaten geschaffen.

Das neue Datenschutzrecht ist damit in allen Staaten der Europäischen Union als direkt geltendes Recht anzuwenden. Diese Bestimmungen erlauben, dass die evangelischen und katholischen Kirchen in einem gewissen Rahmen eigene Regelungen treffen können (Art. 91 DSGVO).

Vertreter der EKD und der katholischen Kirche hatten sich bei der europäischen Rechtsetzung für die Möglichkeit kirchlicher Sonderregelungen eingesetzt, weil die besondere Ausrichtung der DSGVO auf den eher ökonomischen Sektor nicht dem Wesen der evangelischen und katholischen Kirche entspricht.

Zwei Voraussetzungen sind jedoch mit diesem Sonderweg verknüpft:

1. *Die kirchlichen Regelungen zum Datenschutz müssen im Einklang mit der DSGVO stehen.*
2. *Es muss eine kirchliche unabhängige Datenschutzaufsichtsbehörde geschaffen werden.*

Beides hat die Evangelische Kirche in Deutschland (EKD) im Vorfeld umgesetzt und bereits 2014 das Amt und die Behörde des Beauftragten für den Datenschutz der EKD (BfD-EKD) geschaffen. Ergänzend wurde am 17.11.2017 ein neues Datenschutzgesetz (DSG-EKD) von der Synode der EKD verabschiedet, das einen Tag vor der europäischen DSGVO am 24. Mai 2018 in Kraft trat. Damit gelten auch in der Landeskirche Hannovers inhaltlich nicht die Bestimmungen der europäischen DSGVO, sondern des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD).

Wegen der oben genannten Verpflichtung zum inhaltlichen Einklang ist das kirchliche Datenschutzrecht selbstverständlich in großen Bereichen dem europäischen Recht nachgebildet. Raum für kirchliche Sonderregelungen gibt es dort, wo dies aus spezifisch kirchlichen Gründen erforderlich ist.

Als Folge des neuen DSG-EKD mussten die verschiedenen landeskirchlichen Bestimmungen, wie etwa das Datenschutz-Anwendungsgesetz (DSAG) und die Datenschutzdurchführungsverordnung (DATVO), angepasst werden. Dieser Prozess erfolgte in enger Abstimmung innerhalb der Konföderation evangelischer Kirchen in Niedersachsen und ist inzwischen ebenfalls abgeschlossen.

Um die Anwendung der neuen Regelungen zu erleichtern, haben wir in diesem Heft alle aktuellen Datenschutzbestimmungen übersichtlich zusammengestellt. Von besonderer praktischer Bedeutung ist dabei die neue DATVO. Diese formuliert detaillierte Regelungen zu den unterschiedlichen Arbeits-

bereichen in Kirche und Diakonie und gibt so ausreichende Rechtssicherheit bei auftretenden datenschutzrechtlichen Fragen.

Ebenso haben wir alle Mustertexte überarbeitet und an den neuen Rechtszustand angepasst. Hierzu gehören die Verpflichtungserklärung auf den Datenschutz, die Mitarbeitende und Ehrenamtliche im Zuge Ihrer Tätigkeit abgeben müssen, sowie ein neues Muster zur Auftrags(daten)verarbeitung.

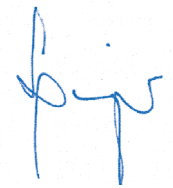
Als neuer Tatbestand ist die Verletzung des Schutzes personenbezogener Daten („Datenpanne") im DSG-EKD eingeführt worden sowie die Verpflichtung, Datenpannen unter bestimmten Voraussetzungen an die Datenschutzaufsichtsbehörde (BfD-EKD) zu melden. Dies entspricht dem neuen europäischen Datenschutz-Standard. Um das Meldeverfahren zu vereinfachen, haben wir ein entsprechendes Muster entwickelt, das Sie ebenfalls in dieser Rechtssammlung finden.

Bedingt durch die Corona-Pandemie und aufgrund der vielen positiven Erfahrungen mit Homeoffice ist bei vielen Mitarbeitenden der Wunsch entstanden, verstärkt auch von zu Hause aus im Rahmen alternierender Telearbeit zu arbeiten. Hierfür hält die Rechtssammlung eine Checkliste bereit, die Antworten und Anregungen gibt, was bei der Einrichtung eines häuslichen Arbeitsplatzes aus datenschutzrechtlicher Sicht zu beachten ist.

Auch darüber hinaus nimmt die Informationstechnologie (IT) einen wichtigen Raum im Zusammenhang mit dem Datenschutz ein. Deshalb hat der Rat der EKD bereits 2015 die IT-Sicherheitsverordnung mit Geltung für die evangelische Kirche in Deutschland erlassen.

Für den Bereich der hannoverschen Landeskirche hat die Landessynode im Dezember 2019 ein neues Digitalgesetz verabschiedet. Damit ist nach längeren Diskussionsprozessen eine eindeutige Rechtsgrundlage für die Nutzung von IT in der Landeskirche geschaffen worden. In diesem Zusammenhang wurden auch die Rechtsverpflichtungen bei der Bereitstellung und Nutzung von IT sowie Kosten und Haftungsfragen, Datenschutz, IT-Sicherheit und Lizenzen geregelt.

Damit ist die hannoversche Landeskirche zunächst einmal gut aufgestellt. Angesichts der rasanten Weiterentwicklung von Informationstechnologie und zunehmender Bedeutung von digitaler Verwaltung wird es aber auch in Zukunft immer wieder erforderlich sein, auf Neuerungen zu reagieren und die Rechts- und Verwaltungsvorschriften entsprechend anzupassen.



Präsidentin Dr. Stephanie Springer

Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz – DSG-EKD) vom 15. November 2017 (ABl. EKD S. 353), zuletzt berichtigt am 15. September 2018 (ABl. EKD S. 215)

Die Synode der Evangelischen Kirche in Deutschland hat mit Zustimmung der Kirchenkonferenz auf Grund des Artikels 10 Absatz 1, des Artikels 10 Absatz 2 Buchstabe a und des Artikels 10a Absatz 1 der Grundordnung der Evangelischen Kirche in Deutschland das folgende Kirchengesetz beschlossen:

Inhaltsübersicht

Präambel

Dieses Kirchengesetz wird erlassen in Ausübung des verfassungsrechtlich garantierten Rechts der evangelischen Kirche, ihre Angelegenheiten selbstständig innerhalb der Schranken des für alle geltenden Gesetzes zu ordnen und zu verwalten. Dieses Recht ist europarechtlich geachtet und festgeschrieben in Artikel 91 und Erwägungsgrund 165 Verordnung EU 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) sowie Artikel 17 Vertrag über die Arbeitsweise der Europäischen Union (AEUV). In Wahrnehmung dieses Rechts stellt dieses Kirchengesetz den Einklang mit der Datenschutz-Grundverordnung her und regelt die Datenverarbeitung im kirchlichen und diakonischen Bereich. Die Datenverarbeitung dient der Erfüllung des kirchlichen Auftrags.

Kapitel 1 – Allgemeine Bestimmungen

§ 1

Schutzzweck

Zweck dieses Kirchengesetzes ist es, die einzelne Person davor zu schützen, dass sie durch den Umgang mit ihren personenbezogenen Daten in ihrem Persönlichkeitsrecht beeinträchtigt wird.

§ 2

Anwendungsbereich

(1) Dieses Kirchengesetz gilt für die Verarbeitung personenbezogener Daten durch die Evangelische Kirche in Deutschland, die Gliedkirchen und die gliedkirchlichen Zusammenschlüsse, alle weiteren kirchlichen juristischen Personen des öffentlichen Rechts sowie die ihnen zugeordneten kirchlichen und diakonischen Dienste, Einrichtungen und Werke ohne Rücksicht auf deren Rechtsform (kirchliche Stelle). Die Evangelische Kirche in Deutschland, die Gliedkirchen und die gliedkirchlichen Zusammenschlüsse stellen sicher, dass auch in den ihnen zugeordneten Diensten, Einrichtungen und Werken dieses Kirchengesetz sowie die zu seiner Ausführung und Durchführung erlasse-

nen weiteren Bestimmungen Anwendung finden. Die Evangelische Kirche in Deutschland und die Gliedkirchen führen jeweils für ihren Bereich eine Übersicht über die kirchlichen Werke und Einrichtungen mit eigener Rechtspersönlichkeit, für die dieses Kirchengesetz gilt. In die Übersicht sind Name, Anschrift, Rechtsform und Tätigkeitsbereich der kirchlichen Werke und Einrichtungen aufzunehmen.

(2) Dieses Kirchengesetz gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

(3) Dieses Kirchengesetz findet Anwendung auf die Verarbeitung personenbezogener Daten im Rahmen der Tätigkeit einer kirchlichen Stelle oder in deren Auftrag, unabhängig vom Ort der Verarbeitung.

(4) Dieses Kirchengesetz findet keine Anwendung auf die Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten.

(5) Die Vorschriften dieses Kirchengesetzes gehen denen des Verwaltungsverfahrens- und Zustellungsgesetzes der Evangelischen Kirche in Deutschland vor, soweit bei der Ermittlung des Sachverhaltes personenbezogene Daten verarbeitet werden.

(6) Soweit andere Rechtsvorschriften, die kirchliche Stellen anzuwenden haben, die Verarbeitung personenbezogener Daten regeln, gehen sie diesem Kirchengesetz vor.

§ 3

Seelsorgegeheimnis und Amtsverschwiegenheit

Aufzeichnungen, die in Wahrnehmung eines kirchlichen Seelsorgeauftrages erstellt werden, dürfen Dritten nicht zugänglich sein. Die besonderen Bestimmungen über den Schutz des Beicht- und Seelsorgegeheimnisses bleiben unberührt. Gleiches gilt für die sonstigen Verpflichtungen zur Wahrung gesetzlicher Geheimhaltungs- und Verschwiegenheitspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen.

§ 4

Begriffsbestimmungen

Im Sinne dieses Kirchengesetzes bezeichnet der Ausdruck:

1. „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; identifizierbar ist eine natürliche Person, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;
2. „besondere Kategorien personenbezogener Daten“
   a. alle Informationen, aus denen religiöse oder weltanschauliche Überzeugungen einer natürlichen Person hervorgehen, ausgenommen Angaben über die Zugehörigkeit zu einer Kirche oder einer Religions- oder Weltanschauungsgemeinschaft,
   b. alle Informationen, aus denen die rassische und ethnische Herkunft, politische Meinungen oder die Gewerkschaftszugehörigkeit einer natürlichen Person hervorgehen,
   c. genetische Daten,
   d. biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,
   e. Gesundheitsdaten,
   f. Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.
3. „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;
4. „Einschränkung der Verarbeitung“ die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;

5. „Profiling“ jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;
6. „Pseudonymisierung“ die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;
7. „Anonymisierung“ die Verarbeitung personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig hohen Aufwand an Zeit, Kosten und Arbeitskraft einer betroffenen Person zugeordnet werden können;
8. „Dateisystem“ jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird;
9. „verantwortliche Stelle“ die natürliche oder juristische Person, kirchliche Stelle im Sinne von § 2 Absatz 1 Satz 1 oder sonstige Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;
10. „Auftragsverarbeiter“ eine natürliche oder juristische Person, kirchliche oder sonstige Stelle, die personenbezogene Daten im Auftrag der verantwortlichen Stelle verarbeitet;
11. „Empfänger“ eine natürliche oder juristische Person, kirchliche oder sonstige Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht;
12. „Dritter“ eine natürliche oder juristische Person, kirchliche oder sonstige Stelle, außer der betroffenen Person, der verantwortlichen Stelle, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung der kirchlichen Stelle oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;

13. „Einwilligung“ jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung der betroffenen Person in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;

14. „Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von oder zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;

15. „genetische Daten“ personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden;

16. „biometrische Daten“ mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten;

17. „Gesundheitsdaten“ personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen;

18. „Drittland“ einen Staat, in dem die Datenschutz-Grundverordnung keine Anwendung findet.

19. „Unternehmen“ eine natürliche oder juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personen-, Kapitalgesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen;

20. „Beschäftigte“

    a. die in einem Pfarrdienst- oder in einem kirchlichen Beamtenverhältnis oder in einem sonstigen kirchlichen öffentlich-rechtlichen Dienstverhältnis stehenden Personen,

b. Arbeitnehmerinnen und Arbeitnehmer, einschließlich der Leiharbeitnehmerinnen und Leiharbeitnehmer im Verhältnis zum Entleiher,

c. zu ihrer Berufsausbildung Beschäftigte,

d. Teilnehmende an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobungen (Rehabilitationen),

e. Beschäftigte in anerkannten Werkstätten für Menschen mit Behinderungen,

f. nach dem Bundesfreiwilligen- oder dem Jugendfreiwilligendienstgesetz oder in vergleichbaren Diensten Beschäftigte,

g. Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,

h. Bewerbende für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist;

21. „IT-Sicherheit" den Schutz der mit Informationstechnik verarbeiteten Daten insbesondere vor unberechtigtem Zugriff, vor unerlaubten Änderungen und vor der Gefahr des Verlustes, um deren Vertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten.

Kapitel 2 – Verarbeitung personenbezogener Daten

§ 5

Grundsätze

(1) Personenbezogene Daten sind nach folgenden Grundsätzen zu verarbeiten:

1. Rechtmäßigkeit, Verhältnismäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz;

2. Zweckbindung: Personenbezogene Daten werden für festgelegte, eindeutige und legitime Zwecke erhoben. Sie dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Eine Weiterverarbeitung für im kirchlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische

Forschungszwecke oder für statistische Zwecke gilt als vereinbar mit den ursprünglichen Zwecken;

3. Datenminimierung: Die Verarbeitung personenbezogener Daten wird auf das dem Zweck angemessene und notwendige Maß beschränkt; personenbezogene Daten sind zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert;
4. Richtigkeit: Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden;
5. Speicherbegrenzung: Personenbezogene Daten werden in einer Form gespeichert, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Personenbezogene Daten dürfen länger gespeichert werden, soweit sie für die Zwecke des Archivs, der wissenschaftlichen und historischen Forschung sowie der Statistik verarbeitet werden;
6. Integrität und Vertraulichkeit: Personenbezogene Daten werden in einer Weise verarbeitet, die eine angemessene Sicherheit gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Zerstörung oder unbeabsichtigter Schädigung.

(2) Die verantwortliche Stelle muss die Einhaltung der Grundsätze nachweisen können (Rechenschaftspflicht).

§ 6

Rechtmäßigkeit der Verarbeitung

Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

1. eine Rechtsvorschrift erlaubt die Verarbeitung der personenbezogenen Daten oder ordnet sie an;
2. die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
3. die Verarbeitung ist zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich, einschließlich der Ausübung kirchlicher Aufsicht,

4. die Verarbeitung ist für die Wahrnehmung einer sonstigen Aufgabe erforderlich, die im kirchlichen Interesse liegt,
5. die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgt;
6. die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der die kirchliche Stelle unterliegt;
7. die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
8. die Verarbeitung ist zur Wahrung der berechtigten Interessen eines Dritten erforderlich, sofern nicht die schutzwürdigen Interessen der betroffenen Person überwiegen, insbesondere dann, wenn diese minderjährig ist.

§ 7

Rechtmäßigkeit der Zweckänderung

(1) Die Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden (Zweckänderung), ist nur rechtmäßig, wenn

1. eine kirchliche Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,
2. eine staatliche Rechtsvorschrift dies vorsieht und kirchliche Interessen nicht entgegenstehen;
3. die betroffene Person eingewilligt hat;
4. offensichtlich ist, dass sie im Interesse der betroffenen Person liegt, und kein Grund zu der Annahme besteht, dass diese in Kenntnis des anderen Zweckes ihre Einwilligung verweigern würde;
5. Angaben der betroffenen Person überprüft werden müssen, weil Anhaltspunkte für deren Unrichtigkeit bestehen;
6. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen darf, es sei denn, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Zweckänderung offensichtlich überwiegt;

7. Grund zu der Annahme besteht, dass andernfalls die Wahrnehmung des kirchlichen Auftrages gefährdet würde;
8. es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist;
9. sie zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse der betroffenen Person an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann oder
10. sie für statistische Zwecke zur Erfüllung des kirchlichen Auftrages erforderlich ist.

(2) In anderen Fällen muss die kirchliche Stelle feststellen, ob die Zweckänderung mit dem Zweck, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist. Dabei berücksichtigt sie unter anderem

1. jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung;
2. den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und der kirchlichen Stelle;
3. die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß § 14 verarbeitet werden;
4. die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen;
5. das Vorhandensein geeigneter Garantien, zu denen die Verschlüsselung, die Pseudonymisierung oder die Anonymisierung gehören kann.

(3) Eine Verarbeitung für andere Zwecke liegt nicht vor, wenn sie der Wahrnehmung von Visitations-, Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung, der Revision oder der Durchführung von Organisationsuntersuchungen für die verantwortliche Stelle dient. Das gilt auch für die Verarbeitung zu Ausbildungs- und Prüfungszwecken durch die verantwortliche Stelle, soweit nicht überwiegende schutzwürdige Interessen der betroffenen Person entgegenstehen.

(4) Personenbezogene Daten, die ausschließlich für Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.

(5) Die Verarbeitung von besonderen Kategorien personenbezogener Daten für andere Zwecke ist nur rechtmäßig, wenn die Voraussetzungen vorliegen, die eine Verarbeitung nach § 13 Absatz 2 zulassen.

§ 8

Offenlegung an kirchliche oder öffentliche Stellen

(1) Die Offenlegung von personenbezogenen Daten an kirchliche Stellen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der offenlegenden oder der empfangenden kirchlichen Stelle liegenden Aufgaben erforderlich ist und
2. die Zulässigkeitsvoraussetzungen des § 6 vorliegen.

(2) Die Verantwortung für die Zulässigkeit der Offenlegung trägt die offenlegende verantwortliche Stelle. Erfolgt die Offenlegung auf Ersuchen der empfangenden kirchlichen Stelle, trägt diese die Verantwortung. In diesem Fall prüft die offenlegende verantwortliche Stelle nur, ob das Ersuchen im Rahmen der Aufgaben der datenempfangenden kirchlichen Stelle liegt, es sei denn, dass besonderer Anlass zur Prüfung der Rechtmäßigkeit der Offenlegung besteht.

(3) Die datenempfangende kirchliche Stelle darf die offengelegten Daten für den Zweck verarbeiten, zu dessen Erfüllung sie ihr offengelegt werden. Eine Verarbeitung für andere Zwecke ist nur unter den Voraussetzungen des § 7 zulässig.

(4) Sind mit personenbezogenen Daten, die nach Absatz 1 offengelegt werden dürfen, weitere personenbezogene Daten der betroffenen oder einer anderen Person so verbunden, dass eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, so ist die Offenlegung auch dieser Daten zulässig, soweit nicht berechtigte Interessen der betroffenen oder einer anderen Person an deren Geheimhaltung offensichtlich überwiegen; eine Nutzung dieser Daten ist unzulässig.

(5) Absatz 4 gilt entsprechend, wenn personenbezogene Daten innerhalb einer kirchlichen Stelle weitergegeben werden.

(6) Personenbezogene Daten dürfen an Stellen anderer öffentlich-rechtlicher Religionsgesellschaften offengelegt werden, wenn das zur Erfüllung der Aufgaben erforderlich ist, die der offenlegenden oder der empfangenden Stelle obliegen, und sofern sichergestellt ist, dass bei der empfangenden Stelle ausreichende Datenschutzmaßnahmen getroffen werden und nicht offensichtlich berechtigte Interessen der betroffenen Person entgegenstehen.

(7) Personenbezogene Daten dürfen an Behörden und sonstige öffentliche Stellen des Bundes, der Länder und der Gemeinden und der sonstigen der Aufsicht des Bundes oder eines Landes unterstehenden juristischen Personen des öffentlichen Rechts offengelegt werden, wenn dies eine Rechtsvorschrift zulässt oder dies zur Erfüllung der Aufgaben erforderlich ist, die der offenlegenden Stelle obliegen, und offensichtlich berechtigte Interessen der betroffenen Person nicht entgegenstehen.

(8) Die datenempfangenden Stellen nach Absatz 6 und 7 dürfen die offengelegten Daten nur für den Zweck verarbeiten, zu dessen Erfüllung sie ihnen offengelegt werden. Die offenlegende Stelle hat sie darauf hinzuweisen.

§ 9

Offenlegung an sonstige Stellen

(1) Die Offenlegung von personenbezogenen Daten an sonstige Stellen oder Personen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der offenlegenden kirchlichen Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Verarbeitung nach § 8 zulassen, oder
2. eine Rechtsvorschrift dies zulässt oder
3. die datenempfangenden Stellen oder Personen ein berechtigtes Interesse an der Kenntnis der offenzulegenden Daten glaubhaft darlegen und die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Offenlegung hat, es sei denn, dass Grund zu der Annahme besteht, dass durch die Offenlegung die Wahrnehmung des Auftrags der Kirche gefährdet würde.

(2) Das Offenlegen von besonderen Kategorien personenbezogener Daten ist abweichend von Absatz 1 Nummer 3 nur zulässig, soweit

dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist.

(3) Die Verantwortung für die Zulässigkeit der Offenlegung trägt die offenlegende kirchliche Stelle; durch Kirchengesetz oder durch kirchliche Rechtsverordnung kann die Offenlegung von der Genehmigung einer anderen kirchlichen Stelle abhängig gemacht werden.

(4) In den Fällen der Offenlegung nach Absatz 1 Nummer 3 unterrichtet die offenlegende kirchliche Stelle die betroffene Person von der Offenlegung ihrer Daten. Dies gilt nicht, wenn damit zu rechnen ist, dass sie davon auf andere Weise Kenntnis erlangt oder die Wahrnehmung des Auftrages der Kirche gefährdet würde.

(5) Die datenempfangenden Stellen und Personen dürfen die offengelegten Daten nur für den Zweck verarbeiten, zu dessen Erfüllung sie ihnen offengelegt werden. Die offenlegende Stelle hat sie darauf hinzuweisen.

§ 10

Datenübermittlung an und in Drittländer oder an internationale Organisationen

(1) Jede Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen, die bereits verarbeitet werden oder nach ihrer Übermittlung verarbeitet werden sollen, ist über die weiteren Voraussetzungen der Datenverarbeitung hinaus nur zulässig, wenn

1. die EU-Kommission ein angemessenes Datenschutzniveau entsprechend den Bestimmungen des Artikel 45 Absatz 2 Datenschutz-Grundverordnung festgestellt hat,

2. als geeignete Garantien Standarddatenschutzklauseln verwendet werden, die von der Kommission gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 Datenschutz-Grundverordnung erlassen oder genehmigt worden sind.

(2) Falls die Voraussetzungen des Absatz 1 nicht vorliegen, ist die Übermittlung zulässig, wenn

1. die betroffene Person in die vorgeschlagene Datenübermittlung ausdrücklich eingewilligt hat, nachdem sie über die für sie bestehenden möglichen Risiken aufgeklärt worden ist;

2. die Übermittlung für die Erfüllung eines Vertrages oder Rechtsverhältnisses zwischen der betroffenen Person und der verantwortlichen Stelle oder zur Durchführung von vertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich ist;
3. die Übermittlung zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person von der verantwortlichen Stelle mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrages erforderlich ist;
4. die Übermittlung aus wichtigen Gründen des kirchlichen Interesses notwendig ist;
5. die Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist oder
6. die Übermittlung zum Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen erforderlich ist, sofern die betroffene Person aus physischen oder rechtlichen Gründen außer Stande ist, ihre Einwilligung zu geben.

§ 11

Einwilligung

(1) Beruht die Verarbeitung auf einer Einwilligung, muss die verantwortliche Stelle nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.

(2) Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erfolgen, so dass es von anderen Sachverhalten klar zu unterscheiden ist. Soweit die Erklärung unter Umständen abgegeben worden ist, die gegen dieses Kirchengesetz verstoßen, ist sie unwirksam.

(3) Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffene Person wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.

(4) Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Maß Rechnung getragen werden,

ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind.

§ 12

Einwilligung Minderjähriger in Bezug auf elektronische Angebote

Minderjährige, denen elektronische Angebote von kirchlichen Stellen gemacht werden, können in die Verarbeitung ihrer Daten wirksam einwilligen, wenn sie religionsmündig sind. Sind die Minderjährigen noch nicht religionsmündig, ist die Verarbeitung nur rechtmäßig, wenn die Sorgeberechtigen die Einwilligung erteilt oder der Einwilligung zugestimmt haben. Die Einwilligung der Sorgeberechtigten ist nicht erforderlich, wenn kirchliche Präventions- oder Beratungsdienste einem Kind unmittelbar angeboten werden.

§ 13

Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Besondere Kategorien personenbezogener Daten dürfen nicht verarbeitet werden.

(2) Abweichend von Absatz 1 dürfen besondere Kategorien personenbezogener Daten verarbeitet werden, wenn

1. die betroffene Person in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt hat;

2. die Verarbeitung erforderlich ist, damit die verantwortliche Stelle oder die betroffene Person die ihr aus dem Arbeits- und Dienstrecht sowie dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach kirchlichem oder staatlichem Recht oder nach einer Dienstvereinbarung nach den kirchlichen Mitarbeitervertretungsgesetzen, die geeignete Garantien für die Rechte und die Interessen der betroffenen Person vorsehen, rechtmäßig ist;

3. die Verarbeitung zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person aus körperlichen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben;
4. die Verarbeitung durch eine verantwortliche Stelle im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung erfolgt, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der verantwortlichen Stelle oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden;
5. die Verarbeitung sich auf personenbezogene Daten bezieht, die die betroffene Person öffentlich gemacht hat;
6. die Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Kirchengerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich ist;
7. die Verarbeitung auf der Grundlage kirchlichen Rechts, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen kirchlichen Interesses erforderlich ist;
8. die Verarbeitung für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage kirchlichen oder staatlichen Rechts oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Absatz 3 genannten Bedingungen und Garantien erforderlich ist;
9. die Verarbeitung aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten, auf der Grundlage des kirchlichen oder staatlichen Rechts, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses vorsieht, erforderlich ist, oder

10. die Verarbeitung für im kirchlichen Interesse liegende Zwecke des Archivs, der wissenschaftlichen oder historischen Forschung oder der Statistik erfolgt und die Interessen der betroffenen Person durch angemessene Maßnahmen gewahrt sind.

(3) Besondere Kategorien personenbezogener Daten dürfen für die in Absatz 2 Nummer 8 genannten Zwecke verarbeitet werden, wenn diese Daten von Fachpersonal oder unter dessen Verantwortung verarbeitet werden und dieses Fachpersonal nach kirchlichem oder staatlichem Recht der Berufsgeheimnispflicht unterliegt, oder wenn die Verarbeitung durch eine andere Person erfolgt, die ebenfalls nach kirchlichem oder staatlichem Recht einer Geheimhaltungspflicht unterliegt.

§ 14

Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten

Die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln ist unter den Voraussetzungen des § 6 zulässig, wenn dies das kirchliche oder staatliche Recht, das geeignete Garantien für die Rechte der betroffenen Personen vorsieht, zulässt.

§ 15

Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist

(1) Ist für die Zwecke, für die eine verantwortliche Stelle personenbezogene Daten verarbeitet, die Identifizierung der betroffenen Person durch die verantwortliche Stelle nicht oder nicht mehr erforderlich, so ist diese nicht verpflichtet, zur bloßen Einhaltung dieses Kirchengesetzes zusätzliche Informationen aufzubewahren, einzuholen oder zu verarbeiten, um die betroffene Person zu identifizieren.

(2) Kann die verantwortliche Stelle in Fällen gemäß Absatz 1 nachweisen, dass sie nicht in der Lage ist, die betroffene Person zu identifizieren, so unterrichtet sie die betroffene Person hierüber, sofern dies möglich ist. In diesen Fällen finden die §§ 17 bis 24 keine Anwendung, es sei denn, die betroffene Person stellt zur Ausübung ihrer in diesen Vorschriften niedergelegten Rechte zusätzliche Informationen bereit, die ihre Identifizierung ermöglichen.

Kapitel 3 – Rechte der betroffenen Person

§ 16

Transparente Information, Kommunikation

(1) Die verantwortliche Stelle trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen, die nach diesem Kirchengesetz hinsichtlich der Verarbeitung zu geben sind, in präziser, transparenter, verständlicher und leicht zugänglicher Form zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Minderjährige richten.

(2) Die verantwortliche Stelle erleichtert der betroffenen Person die Ausübung ihrer Rechte gemäß den §§ 19 bis 25.

(3) Die verantwortliche Stelle stellt der betroffenen Person Informationen über die ergriffenen Maßnahmen gemäß den §§ 19 bis 25 innerhalb von drei Monaten nach Eingang des Antrags zur Verfügung. Diese Frist kann um zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl der Anträge erforderlich ist. Die verantwortliche Stelle unterrichtet die betroffene Person innerhalb von drei Monaten nach Eingang über eine Fristverlängerung zusammen mit den Gründen für die Verzögerung.

(4) Wird die verantwortliche Stelle auf den Antrag der betroffenen Person hin nicht tätig, so unterrichtet sie die betroffene Person ohne Verzögerung, spätestens aber innerhalb von drei Monaten nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, bei der Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen.

(5) Informationen werden unentgeltlich zur Verfügung gestellt. Bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person kann die verantwortliche Stelle sich weigern, aufgrund des Antrags tätig zu werden, oder ein angemessenes Entgelt verlangen.

§ 17

Informationspflicht bei unmittelbarer Datenerhebung

(1) Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt die verantwortliche Stelle der betroffenen Person auf Verlangen in geeigneter und angemessener Weise Folgendes mit:

1. den Namen und die Kontaktdaten der verantwortlichen Stelle;
2. gegebenenfalls die Kontaktdaten der oder des örtlich Beauftragten;
3. die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
4. gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten.

(2) Zusätzlich zu den Informationen gemäß Absatz 1 stellt die verantwortliche Stelle der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten auf Verlangen folgende weitere Informationen zur Verfügung:

1. falls möglich die Dauer, für die die personenbezogenen Daten gespeichert werden, oder falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
2. das Bestehen eines Rechts auf Auskunft, auf Berichtigung, auf Löschung, auf Einschränkung der Verarbeitung, auf Datenübertragbarkeit sowie eines Widerspruchsrechts gegen die Verarbeitung;
3. das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde;
4. ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, und welche möglichen Folgen die Nichtbereitstellung hätte.

(3) Beabsichtigt die verantwortliche Stelle, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so stellt sie der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß Absatz 2 zur Verfügung.

(4) Die Absätze 1, 2 und 3 finden keine Anwendung, wenn und soweit die betroffene Person bereits über die Informationen verfügt, oder die Informationspflicht einen unverhältnismäßigen Aufwand erfordern würde.

§ 18

Informationspflicht bei mittelbarer Datenerhebung

(1) Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, so teilt die verantwortliche Stelle der betroffenen Person

über die in § 17 Absatz 1 und 2 aufgeführten Informationen hinaus die zu ihr gespeicherten Daten mit, auch soweit sie sich auf Herkunft oder empfangende Stellen beziehen. § 17 Absatz 4 gilt entsprechend.

(2) Von dieser Verpflichtung ist die verantwortliche Stelle befreit, soweit die Daten oder die Tatsache ihrer Speicherung aufgrund einer speziellen Rechtsvorschrift oder wegen überwiegender berechtigter Interessen Dritter geheim gehalten werden müssen und das Interesse der betroffenen Person an der Auskunftserteilung zurücktreten muss oder wenn durch die Auskunft die Wahrnehmung des Auftrags der Kirche gefährdet wird.

§ 19

Auskunftsrecht der betroffenen Person

(1) Der betroffenen Person ist auf Antrag Auskunft zu erteilen über die zu ihr gespeicherten personenbezogenen Daten. Die Auskunft muss folgende Informationen enthalten:

1. die Verarbeitungszwecke;
2. die Kategorien personenbezogener Daten;
3. die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind;
4. falls möglich, die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
5. das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch die verantwortliche Stelle oder eines Widerspruchsrechts gegen diese Verarbeitung;
6. das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde;
7. wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten.

(2) Auskunft darf nicht erteilt werden, soweit die Daten oder die Tatsache ihrer Speicherung aufgrund einer speziellen Rechtsvorschrift oder wegen überwiegender berechtigter Interessen Dritter geheim gehalten werden müssen und das Interesse der betroffenen Person an der Auskunftserteilung zurücktreten muss, oder wenn durch die Auskunft die Wahrnehmung des Auftrags der Kirche gefährdet wird.

(3) Die Auskunft ist unentgeltlich.

(4) Absatz 1 findet keine Anwendung, soweit die Auskunft einen unverhältnismäßigen Aufwand erfordern würde.

§ 20

Recht auf Berichtigung

(1) Unrichtige personenbezogene Daten sind auf Antrag der betroffenen Person unverzüglich zu berichtigen. Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person das Recht, die Vervollständigung unvollständiger personenbezogener Daten – auch mittels einer ergänzenden Erklärung – zu verlangen.

(2) Das Recht auf Berichtigung besteht nicht, wenn die personenbezogenen Daten zu Archivzwecken im kirchlichen Interesse verarbeitet werden. Bestreitet die betroffene Person die Richtigkeit der personenbezogenen Daten, ist ihr die Möglichkeit einer Gegendarstellung einzuräumen. Das zuständige Archiv ist verpflichtet, die Gegendarstellung den Unterlagen hinzuzufügen.

§ 21

Recht auf Löschung

(1) Personenbezogene Daten sind zu löschen, wenn

1. ihre Speicherung unzulässig ist oder
2. ihre Kenntnis für die verantwortliche Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist;
3. die betroffene Person ihre Einwilligung bezüglich der Verarbeitung ihrer Daten widerruft und es an einer anderweitigen Rechtsgrundlage für die Verarbeitung fehlt;
4. die betroffene Person gemäß § 25 Widerspruch gegen die Verarbeitung einlegt und keine vorrangigen berechtigten Gründe für die Verarbeitung vorliegen;
5. die Löschung der personenbezogenen Daten zur Erfüllung rechtlicher Verpflichtungen der verantwortlichen Stelle notwendig ist;

6. die Löschung personenbezogener Daten verlangt wird, die bei elektronischen Angeboten, die Minderjährigen direkt gemacht worden sind, erhoben wurden.

(2) Hat die verantwortliche Stelle die personenbezogenen Daten öffentlich gemacht und ist sie gemäß Absatz 1 zu deren Löschung verpflichtet, so trifft sie unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, um die für die Datenverarbeitung verantwortlichen Stellen, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.

(3) Die Absätze 1 und 2 gelten nicht, soweit die Verarbeitung erforderlich ist

1. zur Ausübung des Rechts auf freie Meinungsäußerung und Information;
2. zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach kirchlichem oder staatlichem Recht, dem die verantwortliche Stelle unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im kirchlichen Interesse liegt oder in Ausübung hoheitlicher Gewalt erfolgt, die der verantwortlichen Stelle übertragen wurde;
3. aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß § 13 Absatz 2 Nummer 8 bis 9;
4. für im kirchlichem Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke, soweit das in Absatz 1 genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, oder
5. zur Geltendmachung von Rechtsansprüchen sowie zur Ausübung oder Verteidigung von Rechten.

(4) Ist eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich, tritt an die Stelle des Rechts auf Löschung das Recht auf Einschränkung der Verarbeitung gemäß § 22.

(5) Vorschriften über das Archiv- und Kirchenbuchwesen bleiben unberührt.

§ 22

Recht auf Einschränkung der Verarbeitung

(1) Die betroffene Person hat das Recht gegenüber der verantwortlichen Stelle auf Einschränkung der Verarbeitung, wenn eine der folgenden Voraussetzungen gegeben ist:

1. die Richtigkeit der personenbezogenen Daten wird von der betroffenen Person bestritten, und zwar für eine Dauer, die es der verantwortlichen Stelle ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen;
2. die Verarbeitung ist unrechtmäßig, die betroffene Person lehnt die Löschung der personenbezogenen Daten ab und verlangt stattdessen die Einschränkung der Nutzung der personenbezogenen Daten;
3. die verantwortliche Stelle benötigt die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger, die betroffene Person benötigt sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen, oder
4. die betroffene Person hat Widerspruch gegen die Verarbeitung gemäß § 25 eingelegt und es steht noch nicht fest, ob die berechtigten Gründe der verantwortlichen Stelle gegenüber denen der betroffenen Person überwiegen.

(2) Wurde die Verarbeitung gemäß Absatz 1 eingeschränkt, so dürfen diese personenbezogenen Daten – von ihrer Speicherung abgesehen – nur mit Einwilligung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen kirchlichen Interesses verarbeitet werden.

(3) Eine betroffene Person, die eine Einschränkung der Verarbeitung gemäß Absatz 1 erwirkt hat, wird von der verantwortlichen Stelle unterrichtet, bevor die Einschränkung aufgehoben wird.

(4) Bei automatisierten Dateisystemen ist technisch sicherzustellen, dass eine Einschränkung der Verarbeitung eindeutig erkennbar ist und eine Verarbeitung für andere Zwecke nicht ohne weitere Prüfung möglich ist.

(5) Vorschriften über das Archiv- und Kirchenbuchwesen bleiben unberührt.

§ 23

Informationspflicht bei Berichtigung, Löschung oder Einschränkung der Verarbeitung

Die verantwortliche Stelle teilt allen Empfängern, denen personenbezogene Daten offengelegt werden, jede Berichtigung oder Löschung der personenbezogenen Daten oder eine Einschränkung der Verarbeitung nach den §§ 20 bis 22 mit, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. Die verantwortliche Stelle unterrichtet die betroffene Person über diese Empfänger, wenn die betroffene Person dies verlangt.

§ 24

Recht auf Datenübertragbarkeit

(1) Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einer verantwortlichen Stelle bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einer anderen verantwortlichen Stelle ohne Behinderung durch die verantwortliche Stelle, der die personenbezogenen Daten bereitgestellt wurden, zu übermitteln, sofern

   1. die Verarbeitung auf einer Einwilligung oder auf einem Vertrag beruht und
   2. die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

   Die betroffene Person kann verlangen, dass die personenbezogenen Daten direkt von der verantwortlichen Stelle einem anderen Dritten übermittelt werden, soweit dies technisch machbar ist.

(2) Das Recht auf Datenübertragbarkeit gilt nicht für eine Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im kirchlichen Interesse liegt oder in Ausübung kirchlicher Aufsicht erfolgt, die der kirchlichen Stelle übertragen wurde.

(3) Das Recht gemäß Absatz 1 darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

§ 25

Widerspruchsrecht

(1) Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten gemäß § 6 Nummer 1, 3, 4 oder 8 Widerspruch einzulegen; dies gilt auch für die Verarbeitung personenbezogener Daten im Rahmen eines Profilings.

(2) Der Widerspruch verpflichtet die verantwortliche Stelle dazu, die Verarbeitung zu unterlassen, soweit nicht an der Verarbeitung ein zwingendes kirchliches Interesse besteht, das Interesse einer dritten Person überwiegt oder eine Rechtsvorschrift zur Verarbeitung verpflichtet.

Kapitel 4 – Pflichten der verantwortlichen Stellen und Auftragsverarbeiter

§ 26

Datengeheimnis

Den bei der Datenverarbeitung tätigen Personen ist untersagt, personenbezogene Daten unbefugt zu verarbeiten (Datengeheimnis). Diese Personen sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis schriftlich zu verpflichten, soweit sie nicht aufgrund anderer kirchlicher Bestimmungen zur Verschwiegenheit verpflichtet wurden. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

§ 27

Technische und organisatorische Maßnahmen, IT-Sicherheit

(1) Die verantwortliche Stelle und der kirchliche Auftragsverarbeiter haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten und einen Nachweis hierüber führen zu können. Diese Maßnahmen schließen unter anderem ein:

1. die Pseudonymisierung, die Anonymisierung und die Verschlüsselung personenbezogener Daten;
2. die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
3. die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall unverzüglich wiederherzustellen;
4. ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung, unbefugte Offenlegung von oder unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

(3) Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

(4) Die Einhaltung eines nach dem EU-Recht zertifizierten Verfahrens kann als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten der verantwortlichen Stelle gemäß Absatz 1 nachzuweisen.

(5) Die verantwortliche Stelle und der kirchliche Auftragsverarbeiter stellen sicher, dass natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf ihre Weisung verarbeiten.

(6) Verantwortliche Stellen und Auftragsverarbeiter sind verpflichtet, IT-Sicherheit zu gewährleisten. Das Nähere regelt der Rat der Evangelischen Kirche in Deutschland durch Rechtsverordnung mit Zustimmung der Kirchenkonferenz.

§ 28

Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der mit der Verarbeitung verbundenen Risi-

ken für die Rechte natürlicher Personen trifft die verantwortliche Stelle sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung technische und organisatorische Maßnahmen, die geeignet sind, die Datenschutzgrundsätze wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieses Kirchengesetzes zu genügen und die Rechte der betroffenen Personen zu schützen.

(2) Die verantwortliche Stelle trifft technische und organisatorische Maßnahmen, die geeignet sind, durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, zu verarbeiten. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere geeignet sein, dass personenbezogene Daten nicht ohne Eingreifen der verantwortlichen Stelle durch Voreinstellungen einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

(3) Die Einhaltung eines nach EU-Recht zertifizierten Verfahrens kann als Gesichtspunkt herangezogen werden, um die Erfüllung der in den Absätzen 1 und 2 genannten Maßnahmen nachzuweisen.

§ 29

Gemeinsam verantwortliche Stellen

(1) Legen zwei oder mehr verantwortliche Stellen gemeinsam die Zwecke und die Mittel zur Verarbeitung fest, so sind sie gemeinsam verantwortliche Stellen. Sie legen in einer Vereinbarung in transparenter Form fest, wer welche Verpflichtung gemäß diesem Kirchengesetz erfüllt, soweit die jeweiligen Aufgaben der verantwortlichen Stellen nicht durch Rechtsvorschriften festgelegt sind.

(2) In der Vereinbarung kann eine Anlaufstelle für die betroffenen Personen angegeben werden. Das Wesentliche der Vereinbarung wird der betroffenen Person auf Verlangen zur Verfügung gestellt.

(3) Ungeachtet der Einzelheiten der Vereinbarung kann die betroffene Person ihre Rechte im Rahmen dieses Kirchengesetzes bei und gegenüber jeder einzelnen verantwortlichen Stelle geltend machen.

§ 30

Verarbeitung von personenbezogenen Daten im Auftrag

(1) Werden personenbezogene Daten im Auftrag durch andere Stellen oder Personen verarbeitet, ist die auftraggebende kirchliche Stelle für die Einhaltung der Vorschriften dieses Kirchengesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Die in Kapitel 3 genannten Rechte sind ihr gegenüber geltend zu machen. Zuständig für die Aufsicht ist die Aufsichtsbehörde der beauftragenden kirchlichen Stelle.

(2) Für eine Auftragsverarbeitung in Drittländern gilt § 10.

(3) Der Auftragsverarbeiter ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind:

1. der Gegenstand und die Dauer des Auftrags;
2. der Umfang, die Art und der Zweck der vorgesehenen Verarbeitung, die Art der Daten und der Kreis der Betroffenen;
3. die nach § 27 zu treffenden technischen und organisatorischen Maßnahmen sowie ihre Kontrolle durch den Auftragsverarbeiter;
4. die Berichtigung, Löschung und Sperrung von Daten;
5. die Verpflichtung der Beschäftigten des Auftragsverarbeiters auf das Datengeheimnis;
6. gegebenenfalls die Berechtigung zur Begründung sowie die Bedingungen von Unterauftragsverhältnissen;
7. die Kontrollrechte der beauftragenden kirchlichen Stelle und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragsverarbeiters;
8. mitzuteilende Verstöße des Auftragsverarbeiters oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen;
9. der Umfang der Weisungsbefugnis, die sich die beauftragende kirchliche Stelle gegenüber dem Auftragsverarbeiter vorbehält;
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragsverarbeiter gespeicherter Daten nach Beendigung des Auftrags.

Die beauftragende kirchliche Stelle hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.

(4) Der Auftragsverarbeiter darf die Daten nur im Rahmen der Weisungen der kirchlichen Stelle verarbeiten. Ist er der Ansicht, dass eine Weisung der kirchlichen Stelle gegen dieses Kirchengesetz oder andere Vorschriften über den Datenschutz verstößt, hat er die kirchliche Stelle unverzüglich darauf hinzuweisen.

(5) Sofern die kirchlichen Datenschutzbestimmungen auf den Auftragsverarbeiter keine Anwendung finden, ist die kirchliche Stelle verpflichtet sicherzustellen, dass der Auftragsverarbeiter diese oder gleichwertige Bestimmungen beachtet. In diesem Fall dürfen sich abweichend von Absatz 3 die Vertragsinhalte an Artikel 28 EU-Datenschutz-Grundverordnung orientieren. Der Auftragsverarbeiter unterwirft sich der kirchlichen Datenschutzaufsicht.

(6) Die Absätze 1 bis 5 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

(7) Das Recht der Evangelischen Kirche in Deutschland, der Gliedkirchen und der gliedkirchlichen Zusammenschlüsse kann bestimmen, dass vor der Beauftragung die Genehmigung einer kirchlichen Stelle einzuholen ist oder Mustervereinbarungen zu verwenden sind. Bei der Beauftragung anderer kirchlicher Stellen kann in den Rechtsvorschriften von Absatz 3 Satz 2 Nummer 3, 5, 7 und 9 und Satz 4 abgesehen werden.

(8) Die Einhaltung von genehmigten Verhaltensregeln und die Verwendung zertifizierter und kirchlich geprüfter Informationstechnik können herangezogen werden, um die Erfüllung der datenschutzrechtlichen Anforderungen durch den Auftragsverarbeiter nachzuweisen.

§ 31

Verzeichnis von Verarbeitungstätigkeiten

(1) Jede verantwortliche Stelle führt ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält folgende Angaben:

1. den Namen und die Kontaktdaten der verantwortlichen Stelle und gegebenenfalls der gemeinsam mit ihr verantwortlichen Stelle sowie gegebenenfalls der oder des örtlich Beauftragten;
2. die Zwecke der Verarbeitung;
3. eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
4. gegebenenfalls die Verwendung von Profiling;
5. die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfängern in Drittländern oder internationalen Organisationen;
6. gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe der dort getroffenen geeigneten Garantien;
7. wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
8. wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 27.

(2) Jeder Auftragsverarbeiter führt ein Verzeichnis zu allen Kategorien von im Auftrag einer verantwortlichen Stelle durchgeführten Tätigkeiten der Verarbeitung, das Folgendes enthält:

1. den Namen und die Kontaktdaten der Auftragsverarbeiter und jeder verantwortlichen Stelle, in deren Auftrag der Auftragsverarbeiter tätig ist, sowie der örtlich Beauftragten;
2. die Kategorien von Verarbeitungen, die im Auftrag jeder verantwortlichen Stelle durchgeführt werden;
3. gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe der dort getroffenen geeigneten Garantien;
4. wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 27.

(3) Das in den Absätzen 1 und 2 genannte Verzeichnis ist schriftlich oder elektronisch zu führen.

(4) Verantwortliche Stellen und Auftragsverarbeiter stellen der Aufsichtsbehörde die Verzeichnisse auf Anfrage zur Verfügung.

(5) Die in den Absätzen 1 und 2 genannten Pflichten gelten nicht für verantwortliche Stellen, die weniger als 250 Beschäftigte haben. Kirchliche Stellen, die weniger als 250 Beschäftigte haben, erstellen Verzeichnisse nach Absatz 1 und 2 nur hinsichtlich der Verfahren, die die Verarbeitung besonderer Kategorien personenbezogener Daten einschließen.

(6) Das Recht der Evangelischen Kirche in Deutschland, der Gliedkirchen und der gliedkirchlichen Zusammenschlüsse kann vorsehen, dass für einheitliche Verfahren das Verzeichnis zentral geführt wird.

§ 32

Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

(1) Im Falle einer Verletzung des Schutzes personenbezogener Daten, die voraussichtlich zu einem nicht unerheblichen Risiko für die Rechte natürlicher Personen führt, meldet die verantwortliche Stelle dies unverzüglich der Aufsichtsbehörde.

(2) Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese der verantwortlichen Stelle unverzüglich.

(3) Die Meldung gemäß Absatz 1 enthält insbesondere folgende Informationen:

1. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
2. den Namen und die Kontaktdaten der oder des örtlich Beauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
3. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
4. eine Beschreibung der von der verantwortlichen Stelle ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(4) Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, kann die verantwortliche Stelle diese Informationen unverzüglich schrittweise zur Verfügung stellen.

(5) Die verantwortliche Stelle hat Verletzungen des Schutzes personenbezogener Daten zu dokumentieren. Die Dokumentation hat alle mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Abhilfemaßnahmen zu umfassen. Diese Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Paragraphen ermöglichen.

§ 33

Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

(1) Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte natürlicher Personen zur Folge, so benachrichtigt die verantwortliche Stelle die betroffene Person unverzüglich von der Verletzung.

(2) Die Benachrichtigung der betroffenen Person hat in klarer und einfacher Sprache zu erfolgen und enthält zumindest die Art der Verletzung des Schutzes personenbezogener Daten und die in § 32 Absatz 3 Nummer 2, 3 und 4 genannten Informationen und Maßnahmen.

(3) Von der Benachrichtigung der betroffenen Person kann abgesehen werden, wenn

1. die verantwortliche Stelle durch nachträgliche Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte der betroffenen Personen gemäß Absatz 1 aller Wahrscheinlichkeit nach nicht mehr besteht, oder

2. die Benachrichtigung mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall hat stattdessen eine im kirchlichen Bereich übliche öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

§ 34

Datenschutz-Folgenabschätzung

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte natürlicher Personen zur Folge, so führt die verantwortliche Stelle vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

(2) Die verantwortliche Stelle holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat der oder des örtlich Beauftragten ein, sofern ein solcher benannt wurde.

(3) Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:

1. systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;
2. umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß § 14 oder
3. systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

(4) Die Folgenabschätzung umfasst insbesondere:

1. eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von der verantwortlichen Stelle verfolgten berechtigten Interessen;
2. eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
3. eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen und

4. die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass die datenschutzrechtlichen Regelungen eingehalten werden.

(5) Die Aufsichtsbehörden sollen sowohl Listen zu Verarbeitungsvorgängen, für die gemäß Absatz 1 eine Datenschutz-Folgenabschätzung durchzuführen ist, als auch Listen zu Verarbeitungsvorgängen, für die keine Datenschutz-Folgenabschätzung erforderlich ist, erstellen und diese veröffentlichen.

(6) Die Aufsichtsbehörden sind gehalten, den Austausch mit staatlichen Aufsichtsbehörden und dem Europäischen Datenschutzausschuss zu suchen, um durch die Aufstellung aufeinander abgestimmter Listen die Zusammenarbeit zwischen kirchlichen und nichtkirchlichen Stellen zu erleichtern.

(7) Falls die Verarbeitung auf einer Rechtsgrundlage im kirchlichen, staatlichen oder europäischen Recht, dem die verantwortliche Stelle unterliegt, beruht und falls diese Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge regeln und bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte, gelten die Absätze 1 bis 5 nicht.

(8) Erforderlichenfalls führt die verantwortliche Stelle eine Überprüfung durch, um zu bewerten, ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird; dies gilt zumindest, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind.

(9) Die verantwortliche Stelle konsultiert vor der Verarbeitung die Aufsichtsbehörde, wenn aus der Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hat.

§ 35

Audit und Zertifizierung

Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch geeignete Stellen prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. Näheres kann der Rat der Evangelischen Kirche in Deutschland durch Rechtsverordnung regeln.

Kapitel 5 – Örtlich Beauftragte für den Datenschutz

§ 36

Bestellung der örtlich Beauftragten für den Datenschutz

(1) Bei verantwortlichen Stellen sind örtlich Beauftragte oder Betriebsbeauftragte für den Datenschutz (örtlich Beauftragte) zu bestellen, wenn

1. bei ihnen in der Regel mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten betraut sind, oder
2. die Kerntätigkeit der verantwortlichen Stelle in der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten besteht. Die Vertretung ist zu regeln.

(2) Die Bestellung kann sich auf mehrere verantwortliche Stellen erstrecken. Das Recht der Evangelischen Kirche in Deutschland, der Gliedkirchen und der gliedkirchlichen Zusammenschlüsse kann bestimmen, dass mehrere verantwortliche Stellen zur gemeinsamen Bestellung eines örtlich Beauftragten verpflichtet werden.

(3) Zu örtlich Beauftragten dürfen nur Personen bestellt werden, die die zur Erfüllung ihrer Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzen. Die Bestellung kann befristet für mindestens drei Jahre erfolgen.

(4) Zu örtlich Beauftragten sollen diejenigen nicht bestellt werden, die mit der Leitung der Datenverarbeitung beauftragt sind oder denen die Leitung der kirchlichen Stelle obliegt.

(5) Die Bestellung von örtlich Beauftragten erfolgt schriftlich und ist der Aufsichtsbehörde und der nach dem jeweiligen Recht für die allgemeine Aufsicht zuständigen Stelle anzuzeigen; die Kontaktdaten sind zu veröffentlichen. Ist der örtlich Beauftragte nicht Beschäftigter einer verantwortlichen Stelle, sind seine Leistungen vertraglich zu regeln.

(6) Soweit bei verantwortlichen Stellen keine Rechtsverpflichtung für die Bestellung von Personen als örtlich Beauftragte besteht, hat die Leitung die Erfüllung der Aufgabe in anderer Weise sicherzustellen.

§ 37

Stellung

(1) Die örtlich Beauftragten sind den gesetzlich oder verfassungsmäßig berufenen Organen der verantwortlichen Stellen unmittelbar zu unterstellen. Sie sind im Rahmen ihrer Aufgaben weisungsfrei. Sie dürfen wegen dieser Tätigkeit nicht benachteiligt werden. Sie können Auskünfte verlangen, Einsicht in Unterlagen nehmen und erhalten Zugang zu personenbezogenen Daten und den Verarbeitungsvorgängen. Die verantwortliche Stelle unterstützt die örtlich Beauftragten bei der Erfüllung ihrer Aufgaben und stellt die notwendigen Mittel zur Verfügung. § 42 Absatz 6 und 7 gilt entsprechend.

(2) Die Abberufung der örtlich Beauftragten ist nur in entsprechender Anwendung des § 626 des Bürgerlichen Gesetzbuches zulässig. Die Kündigung eines Arbeitsverhältnisses ist nur zulässig, wenn Tatsachen vorliegen, die zur Kündigung aus wichtigem Grund berechtigen. Gleiches gilt für den Zeitraum eines Jahres nach Beendigung der Bestellung.

(3) Zur Erlangung und zur Erhaltung der erforderlichen Fachkunde hat die verantwortliche Stelle den örtlich Beauftragten die Teilnahme an Fort- und Weiterbildungsveranstaltungen zu ermöglichen und die Kosten zu tragen. Die dazu notwendige Freistellung hat ohne Minderung der Bezüge oder des Erholungsurlaubes zu erfolgen. Im Konfliktfall kann die Aufsichtsbehörde angerufen werden.

(4) Betroffene Personen und Mitarbeitende können sich unmittelbar an die örtlich Beauftragten wenden.

(5) Staatliche Vorschriften über Zeugnisverweigerungsrechte für Datenschutzbeauftragte finden für örtlich Beauftragte entsprechende Anwendung.

(6) Die verantwortlichen Stellen stellen sicher, dass örtlich Beauftragte ordnungsgemäß und frühzeitig bei allen mit dem Schutz personenbezogener Daten zusammenhängenden Fragen beteiligt werden.

§ 38

Aufgaben

Die örtlich Beauftragten wirken auf die Einhaltung der Bestimmungen für den Datenschutz hin und unterstützen die verantwortlichen Stellen bei der Sicherstellung des Datenschutzes. Sie haben insbesondere

1. die verantwortliche Stelle und die Beschäftigten zu beraten;
2. die ordnungsmäßige Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen;
3. die bei der Verarbeitung personenbezogener Daten tätigen Personen zu informieren und zu schulen;
4. mit der Aufsichtsbehörde zusammenzuarbeiten;
5. die verantwortliche Stelle bei der Datenschutz-Folgenabschätzung zu beraten und deren Durchführung zu überwachen.

Kapitel 6 – Unabhängige Aufsichtsbehörden

§ 39

Errichtung der Aufsichtsbehörden und Bestellung der Beauftragten für den Datenschutz

(1) Über die Einhaltung dieses Kirchengesetzes in der Evangelischen Kirche in Deutschland, den Gliedkirchen und den gliedkirchlichen Zusammenschlüssen wachen unabhängige kirchliche Aufsichtsbehörden für den Datenschutz (Aufsichtsbehörden). Jede Aufsichtsbehörde wird von einem oder einer Beauftragten für den Datenschutz geleitet und nach außen vertreten.

(2) Der Rat der Evangelischen Kirche in Deutschland errichtet die Aufsichtsbehörde für den Bereich der Evangelischen Kirche in Deutschland und ihres Evangelischen Werkes für Diakonie und Entwicklung sowie für die gesamtkirchlichen Werke und Einrichtungen und bestellt den Beauftragten oder die Beauftragte für den Datenschutz der Evangelischen Kirche in Deutschland.

(3) Die Gliedkirchen und die gliedkirchlichen Zusammenschlüsse errichten die Aufsichtsbehörde für ihren Bereich einzeln oder gemeinschaftlich, soweit sie die Aufgaben nicht der Aufsichtsbehörde der Evangelischen Kirche in Deutschland übertragen. Die Gliedkirchen können für die ihnen zugeordneten diakonischen Dienste, Einrichtungen und Werke eigene Aufsichtsbehörden errichten.

(4) Beauftragte für den Datenschutz sollen für mindestens vier, höchstens acht Jahre bestellt werden. Das Amt endet mit dem Amtsantritt einer Nachfolgerin oder eines Nachfolgers. Die erneute Bestellung ist

zulässig. Das Amt ist hauptamtlich auszuüben. Nebentätigkeiten sind nur zulässig, soweit dadurch das Vertrauen in die Unabhängigkeit und Unparteilichkeit nicht gefährdet wird und sie genehmigt sind.

(5) Zu Beauftragten für den Datenschutz dürfen nur Personen bestellt werden, welche die zur Erfüllung ihrer Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzen. Sie müssen die Befähigung zum Richteramt oder zum höheren Dienst besitzen und einer Gliedkirche der Evangelischen Kirche in Deutschland angehören. Sie sind auf die gewissenhafte Erfüllung ihrer Amtspflichten und die Einhaltung der kirchlichen Ordnung zu verpflichten.

§ 40

Unabhängigkeit

(1) Die Aufsichtsbehörden handeln bei der Erfüllung ihrer Aufgaben und bei der Ausübung ihrer Befugnisse völlig unabhängig. Sie unterliegen weder direkter noch indirekter Beeinflussung von außen und ersuchen weder um Weisung noch nehmen sie Weisungen entgegen.

(2) Die Aufsichtsbehörden unterliegen der Rechnungsprüfung, soweit hierdurch die Unabhängigkeit nicht beeinträchtigt wird.

§ 41

Tätigkeitsbericht

Die Aufsichtsbehörden erstellen mindestens alle zwei Jahre einen Tätigkeitsbericht, der eine Liste der Arten der gemeldeten Verstöße und der Arten der getroffenen Maßnahmen enthalten kann. Sie übermitteln den Bericht den jeweiligen kirchenleitenden Organen oder den jeweiligen Leitungsorganen der Diakonischen Werke und veröffentlichen ihn. Auf dieser Grundlage können sie den leitenden Organen berichten.

§ 42

Rechtsstellung

(1) Den Aufsichtsbehörden werden die Finanzmittel zur Verfügung gestellt, die sie benötigen, um ihre Aufgaben und Befugnisse effektiv wahrnehmen zu können. Die Finanzmittel sind in einem eigenen Haushaltsplan oder als Teil eines Gesamthaushaltes gesondert auszuweisen und zu verwalten.

(2) Die Aufsichtsbehörden wählen ihr Personal aus und besetzen die Personalstellen.

(3) Die Beauftragten für den Datenschutz sind die Vorgesetzten der Mitarbeitenden in den Aufsichtsbehörden.

(4) Die Beauftragten für den Datenschutz bestellen aus dem Kreis ihrer Mitarbeitenden in den Aufsichtsbehörden einen Vertreter oder eine Vertreterin. Vertreter oder Vertreterin können auch Beauftragte für den Datenschutz anderer Gliedkirchen oder der oder die Beauftragte für den Datenschutz der Evangelischen Kirche in Deutschland sein.

(5) Die Aufsichtsbehörden können Aufgaben der Personalverwaltung und Personalwirtschaft auf andere Kirchenbehörden übertragen. Diesen kirchlichen Stellen dürfen personenbezogene Daten der Beschäftigten offengelegt werden, soweit deren Kenntnis zur Erfüllung der übertragenen Aufgaben erforderlich ist.

(6) Beauftragte für den Datenschutz und ihre Mitarbeitenden sind verpflichtet, über die ihnen amtlich bekanntgewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Die Verpflichtung besteht auch nach Beendigung des Dienst- oder Arbeitsverhältnisses.

(7) Beauftragte für den Datenschutz und ihre Mitarbeitenden dürfen, auch wenn sie nicht mehr im Amt sind, über Angelegenheiten, die der Verschwiegenheit unterliegen, ohne Genehmigung weder vor Gericht noch außergerichtlich aussagen oder Erklärungen abgeben. Die Entscheidung über Aussagegenehmigungen treffen die Beauftragten für den Datenschutz für sich und ihre Mitarbeitenden in eigener Verantwortung. Die Beauftragten für den Datenschutz gelten als oberste Aufsichtsbehörde im Sinne des § 99 Verwaltungsgerichtsordnung.

(8) Eine Kündigung von Beauftragten für den Datenschutz im Arbeitsverhältnis ist während der Amtszeit nur zulässig, soweit Tatsachen vorliegen, die zu einer Kündigung aus wichtigem Grund berechtigen. Dies gilt für den Zeitraum von einem Jahr nach Beendigung des Amtes entsprechend.

(9) Beauftragte für den Datenschutz im Kirchenbeamtenverhältnis scheiden während der Amtszeit aus dem Dienst aus, wenn nach den Bestimmungen der §§ 76, 77, 79 oder 80 des Kirchenbeamtengesetzes der EKD die Voraussetzungen einer Entlassung oder Gründe nach

§ 24 des Deutschen Richtergesetzes vorliegen, die bei einem Richter auf Lebenszeit dessen Entlassung aus dem Dienst rechtfertigen, oder wenn ein Disziplinargericht auf Entfernung aus dem Dienst erkennt.

§ 43

Aufgaben

(1) Die Aufsichtsbehörden haben insbesondere die einheitliche Anwendung und Durchsetzung des kirchlichen Datenschutzrechtes in ihrem Zuständigkeitsbereich zu überwachen und sicherzustellen.

(2) Sie sensibilisieren, informieren und beraten die kirchliche Öffentlichkeit sowie die verantwortlichen Stellen und kirchlichen Auftragsverarbeiter über Fragen und maßgebliche Entwicklungen des Datenschutzes sowie über die Vermeidung von Risiken. Sie unterrichten betroffene Personen auf Anfrage über deren persönliche Rechte aus diesem Kirchengesetz, wobei spezifische Maßnahmen für Minderjährige besondere Beachtung finden.

(3) Sie schulen die örtlich Beauftragten und bilden sie fort.

(4) Werden personenbezogene Daten in Drittländern verarbeitet, prüfen die Aufsichtsbehörden die Einhaltung der datenschutzrechtlichen Vorgaben und beraten über Möglichkeiten einer gesetzeskonformen Verarbeitung.

(5) Die Aufsichtsbehörden können auf Anregung der kirchenleitenden Organe oder von Amts wegen Gutachten und Stellungnahmen zu Rechtssetzungsvorhaben, die sich auf den Schutz von personenbezogenen Daten auswirken, abgeben.

(6) Die Aufsichtsbehörden können auf Anregung der kirchenleitenden Organe oder von Amts wegen Musterverträge und Standards zur Verarbeitung personenbezogener Daten erstellen, deren Einsatz und Umsetzung überprüfen und die Ergebnisse veröffentlichen; sie sollen Listen gemäß § 34 Absatz 5 bereitstellen.

(7) Kirchliche Gerichte unterliegen der Prüfung durch die Aufsichtsbehörden nur, soweit sie in eigenen Angelegenheiten als Verwaltung tätig werden.

(8) Der Prüfung durch die Aufsichtsbehörden unterliegen nicht:

1. Aufzeichnungen gemäß § 3 Satz 1;
2. personenbezogene Daten, die dem Post- und Fernmeldegeheimnis oder dem Arztgeheimnis unterliegen, sowie personenbezogene

Daten in Personalakten, wenn die betroffene Person der Prüfung der auf sie bezogenen Daten im Einzelfall zulässigerweise gegenüber den Beauftragten für den Datenschutz widerspricht.

Die Aufsichtsbehörden teilen die Ergebnisse ihrer Prüfungen den verantwortlichen Stellen mit. Damit können Vorschläge zur Verbesserung des Datenschutzes, insbesondere zur Beseitigung von festgestellten Mängeln bei der Verarbeitung personenbezogener Daten, verbunden sein.

(9) Die Beauftragten für den Datenschutz arbeiten zusammen und bilden eine Datenschutzkonferenz, auf der gemeinsame Stellungnahmen und Handreichungen zu Datenschutz- und Kohärenzfragen beschlossen werden können. Sie tauschen mit den staatlichen Aufsichtsbehörden für den Datenschutz Erfahrungen und zweckdienliche Informationen aus und geben im Bedarfsfall Stellungnahmen ab.

§ 44

Befugnisse

(1) Die Aufsichtsbehörden können verlangen, dass die verantwortlichen Stellen sie bei der Erfüllung ihrer Aufgaben unterstützen. Auf Verlangen ist ihnen Auskunft sowie Einsicht in alle Unterlagen und Akten über die Verarbeitung personenbezogener Daten zu geben, alle diesbezüglichen Informationen bereitzustellen, insbesondere über die gespeicherten Daten und über die eingesetzten Datenverarbeitungsprogramme. Ihnen ist jederzeit Zutritt zu allen Diensträumen, einschließlich aller Verarbeitungsanlagen und -geräte zu gewähren, um Untersuchungen und Überprüfungen vorzunehmen. Stellen Aufsichtsbehörden fest, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen dieses Kirchengesetz verstoßen, können sie Hinweise geben.

(2) Stellen die Aufsichtsbehörden Verstöße gegen die Datenschutzbestimmungen oder sonstige Mängel bei der Verarbeitung personenbezogener Daten fest, so beanstanden sie dies gegenüber der verantwortlichen Stelle oder gegenüber dem Auftragsverarbeiter und fordern zur Stellungnahme innerhalb einer gesetzten Frist auf. Von einer Beanstandung kann abgesehen werden, wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt. Mit der Aufforderung zur Stellungnahme können Vorschläge zur Beseitigung der Mängel oder zur sonstigen Verbesserung des Datenschutzes verbunden werden. Die Stellungnahme soll eine Darstellung der Maßnahmen enthalten, die aufgrund der Mitteilung der Aufsichtsbehörde getroffen worden sind.

(3) Um einen rechtmäßigen Zustand wiederherzustellen oder eine drohende Verletzung des Schutzes personenbezogener Daten abzuwenden, sind die Aufsichtsbehörden befugt, anzuordnen:

1. Verarbeitungsvorgänge auf bestimmte Weise und in einem bestimmten Zeitraum mit diesem Kirchengesetz in Einklang zu bringen;
2. Verarbeitungsvorgänge vorübergehend oder dauerhaft zu beschränken oder zu unterlassen;
3. die Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation auszusetzen;
4. personenbezogene Daten zu berichtigen, zu sperren oder zu löschen;
5. die von einer Verletzung des Schutzes personenbezogener Daten betroffene Person entsprechend zu benachrichtigen;
6. dem Antrag der betroffenen Person zu entsprechen.

(4) Halten die Aufsichtsbehörden einen Angemessenheitsbeschluss der Europäischen Kommission nach § 10 Absatz 1 Nummer 1 oder eine von der Europäischen Kommission erlassene oder genehmigte Standarddatenschutzklausel nach § 10 Absatz 1 Nummer 2, auf deren Gültigkeit es bei der Entscheidung der Aufsichtsbehörden ankommt, für rechtswidrig, so können sie ihr Verfahren aussetzen und einen Antrag auf gerichtliche Entscheidung stellen. Soweit nicht Besonderheiten der kirchlichen Verwaltungsgerichtsordnung entgegenstehen, finden die Regelungen des § 21 des Bundesdatenschutzgesetzes entsprechende Anwendung.

§ 45

Geldbußen

(1) Verstößt eine verantwortliche Stelle oder ein kirchlicher Auftragsverarbeiter vorsätzlich oder fahrlässig gegen Bestimmungen dieses Kirchengesetzes, so können die Aufsichtsbehörden Geldbußen verhängen oder für den Wiederholungsfall androhen. Gegen verantwortliche Stellen sind Geldbußen nur zu verhängen, soweit sie als Unternehmen im Sinne des § 4 Nummer 19 am Wettbewerb teilnehmen.

(2) Die Aufsichtsbehörden stellen sicher, dass die Verhängung von Geldbußen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

(3) Geldbußen werden je nach den Umständen des Einzelfalls verhängt. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall Folgendes gebührend berücksichtigt:

1. Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;
2. Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;
3. jegliche von der verantwortlichen Stelle oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;
4. der Grad der Verantwortung der verantwortlichen Stelle oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß § 27 getroffenen technischen und organisatorischen Maßnahmen;
5. etwaige einschlägige frühere Verstöße der verantwortlichen Stelle oder des Auftragsverarbeiters;
6. die Bereitschaft zur Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern;
7. die Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind;
8. die Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang die verantwortliche Stelle oder der Auftragsverarbeiter den Verstoß mitgeteilt hat;
9. die Einhaltung der früher gegen die verantwortliche Stelle oder den Auftragsverarbeiter in Bezug auf denselben Gegenstand angeordneten Maßnahmen, sofern solche Maßnahmen angeordnet wurden;
10. jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.

(4) Verstößt eine verantwortliche Stelle oder ein Auftragsverarbeiter bei gleichen oder miteinander verbundenen Verarbeitungsvorgängen vorsätzlich oder fahrlässig gegen mehrere Bestimmungen dieses Kirchengesetzes, so übersteigt der Gesamtbetrag der Geldbuße nicht den Betrag für den schwerwiegendsten Verstoß.

(5) Bei Verstößen werden im Einklang mit Absatz 3 Geldbußen von bis zu 500.000 Euro verhängt.

(6) Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich oder anstelle von Maßnahmen nach § 44 Absatz 3 verhängt.

Kapitel 7 – Rechtsbehelfe und Schadensersatz

§ 46

Recht auf Beschwerde

(1) Jede Person kann sich unbeschadet anderweitiger Rechtsbehelfe mit einer Beschwerde an die Aufsichtsbehörde wenden, wenn sie der Ansicht ist, bei der Verarbeitung ihrer personenbezogenen Daten in ihren Rechten verletzt worden zu sein.

(2) Die Aufsichtsbehörde unterrichtet die betroffene Person über den Stand und das Ergebnis der Beschwerde und weist auf die Möglichkeit gerichtlichen Rechtsschutzes gemäß § 47 hin.

(3) Niemand darf wegen der Mitteilung von Tatsachen, die geeignet sind, den Verdacht aufkommen zu lassen, dieses Kirchengesetz oder eine andere Rechtsvorschrift über den Datenschutz sei verletzt worden, gemaßregelt oder benachteiligt werden. Mitarbeitende müssen für Mitteilungen an die Aufsichtsbehörde nicht den Dienstweg einhalten.

§ 47

Rechtsweg

(1) Der Rechtsweg zu den kirchlichen Verwaltungsgerichten ist eröffnet

1. für Klagen gegen Verwaltungsakte und andere Entscheidungen der Aufsichtsbehörden,
2. für Klagen in Fällen, in denen sich die Aufsichtsbehörde nicht mit einer Beschwerde gemäß § 46 befasst oder die betroffene Person nicht innerhalb von drei Monaten über den Stand oder das Ergebnis der erhobenen Beschwerde in Kenntnis gesetzt hat,
3. für Klagen betroffener Personen gegen kirchliche Stellen und Auftragsverarbeiter wegen einer Verletzung ihrer Rechte aus diesem Kirchengesetz,

4. für Klagen der Aufsichtsbehörden gegen kirchliche Stellen und Auftragsverarbeiter, soweit dies zur Durchsetzung ihrer Befugnisse erforderlich ist.

(2) Vor Erhebung einer Klage nach Absatz 1 Nummer 1 oder 3 ist nach Maßgabe des jeweils anwendbaren Rechts ein Vorverfahren durchzuführen.

§ 48

Schadensersatz durch verantwortliche Stellen

(1) Jede Person, der wegen einer Verletzung der Regelungen über den kirchlichen Datenschutz ein Schaden entstanden ist, hat nach diesem Kirchengesetz Anspruch auf Schadensersatz gegen die verantwortliche Stelle. Wegen eines Schadens, der nicht Vermögensschaden ist, kann die betroffene Person eine angemessene Entschädigung in Geld verlangen.

(2) Eine verantwortliche Stelle wird von der Haftung gemäß Absatz 1 befreit, wenn sie nachweist, dass sie für den eingetretenen Schaden nicht verantwortlich ist.

(3) Auf das Mitverschulden der betroffenen Person ist § 254 des Bürgerlichen Gesetzbuches und auf die Verjährung sind die Verjährungsfristen für unerlaubte Handlungen des Bürgerlichen Gesetzbuches entsprechend anzuwenden.

(4) Mehrere Ersatzpflichtige haften als Gesamtschuldner im Sinne des Bürgerlichen Gesetzbuches.

(5) Vorschriften, nach denen Ersatzpflichtige in weiterem Umfang als nach dieser Vorschrift haften oder nach denen andere für den Schaden verantwortlich sind, bleiben unberührt.

Kapitel 8 Vorschriften für besondere Verarbeitungssituationen

§ 49

Verarbeitung personenbezogener Daten bei Dienst- und Arbeitsverhältnissen

(1) Daten von Beschäftigten dürfen nur verarbeitet werden, soweit dies zur Begründung, Durchführung, Beendigung oder Abwicklung des

Beschäftigungsverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch für Zwecke der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht.

(2) Im Zusammenhang mit dem Verdacht auf Straftaten und Amtspflichtverletzungen, die durch Beschäftigte begangen wurden, insbesondere zum Schutz möglicher Betroffener, dürfen unter Beachtung des Verhältnismäßigkeitsgrundsatzes personenbezogene Daten von Beschäftigten verarbeitet werden, solange der Verdacht nicht ausgeräumt ist und die Interessen von möglichen Betroffenen dies erfordern.

(3) Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder die verantwortliche Stelle und die beschäftigte Person gleichgelagerte Interessen verfolgen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Die verantwortliche Stelle hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht aufzuklären.

(4) Eine Offenlegung der Daten von Beschäftigten an Personen und Stellen außerhalb des kirchlichen Bereichs ist nur zulässig, wenn kirchliche Interessen nicht entgegenstehen und

1. die empfangende Person oder Stelle ein überwiegendes rechtliches Interesse darlegt;
2. Art oder Zielsetzung der dem oder der Beschäftigten übertragenen Aufgaben die Offenlegung erfordert;
3. offensichtlich ist, dass die Offenlegung im Interesse der betroffenen Person liegt und keine Anhaltspunkte vorliegen, dass sie in Kenntnis des Zwecks der Offenlegung ihre Einwilligung nicht erteilen würde oder
4. sie zur Aufdeckung einer Straftat oder Amtspflichtverletzung oder zum Schutz möglicher Betroffener erforderlich erscheint.

(5) Die Offenlegung an künftige Dienstherren, Dienst- oder Arbeitgeber ist nur mit Einwilligung der betroffenen Person zulässig, es sei denn, dass eine Abordnung oder Versetzung vorbereitet wird, die der Zustimmung der oder des Beschäftigten nicht bedarf, oder dass diese zur Verhütung möglicher Straftaten oder Amtspflichtverletzungen erforderlich erscheint.

(6) Verlangt die verantwortliche Stelle zur Begründung oder im Rahmen eines Beschäftigungsverhältnisses medizinische oder psychologische Untersuchungen und Tests, hat sie Anlass und Zweck der Begutachtung möglichst tätigkeitsbezogen zu bezeichnen. Ergeben sich keine medizinischen oder psychologischen Bedenken, darf die verantwortliche Stelle lediglich die Offenlegung des Ergebnisses der Begutachtung verlangen; ergeben sich Bedenken, darf auch die Offenlegung der festgestellten möglichst tätigkeitsbezogenen Risikofaktoren verlangt werden. Im Übrigen ist eine Weiterverarbeitung der bei den Untersuchungen oder Tests erhobenen Daten ohne schriftliche Einwilligung der betroffenen Person nur für den Zweck zulässig, für den sie erhoben worden sind.

(7) Personenbezogene Daten, die vor Begründung eines Beschäftigungsverhältnisses erhoben wurden, sind unverzüglich zu löschen, sobald feststeht, dass ein solches nicht zustande kommt. Dies gilt nicht, soweit überwiegende berechtigte Interessen der verantwortlichen Stelle der Löschung entgegenstehen oder die betroffene Person in die weitere Speicherung einwilligt. Nach Beendigung eines Beschäftigungsverhältnisses sind personenbezogene Daten zu löschen, soweit diese Daten nicht mehr benötigt werden.

(8) Die Ergebnisse medizinischer oder psychologischer Untersuchungen und Tests der Beschäftigten dürfen automatisiert nur verarbeitet werden, wenn dies dem Schutz der oder des Beschäftigten dient.

(9) Soweit Daten der Beschäftigten im Rahmen der Maßnahmen zur Datensicherung gespeichert werden, dürfen sie nicht für andere Zwecke, insbesondere nicht für Zwecke der Verhaltens- oder Leistungskontrolle, genutzt werden.

§ 50

Verarbeitung personenbezogener Daten für wissenschaftliche und statistische Zwecke

(1) Für Zwecke der wissenschaftlichen Forschung und der Statistik erhobene oder gespeicherte personenbezogene Daten dürfen nur für diese Zwecke verarbeitet werden.

(2) Die Offenlegung personenbezogener Daten an andere als kirchliche Stellen für Zwecke der wissenschaftlichen Forschung und der Statistik ist nur zulässig, wenn diese sich verpflichten, die offengelegten Daten nicht für andere Zwecke zu verarbeiten und die Vorschriften der Absätze 3 und 4 einzuhalten. Der kirchliche Auftrag darf durch die Offenlegung nicht gefährdet werden.

(3) Die personenbezogenen Daten sind zu anonymisieren, sobald dies möglich ist. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Zweck dies erfordert.

(4) Die Veröffentlichung personenbezogener Daten, die für Zwecke wissenschaftlicher oder historischer Forschung sowie der Statistik übermittelt wurden, ist nur mit Zustimmung der übermittelnden Stelle zulässig. Die Zustimmung kann erteilt werden, wenn

1. die betroffene Person eingewilligt hat oder
2. dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist, es sei denn, dass Grund zu der Annahme besteht, dass durch die Veröffentlichung der Auftrag der Kirche gefährdet würde.

§ 51

Verarbeitung personenbezogener Daten durch die Medien

(1) Soweit personenbezogene Daten von verantwortlichen Stellen ausschließlich für eigene journalistisch-redaktionelle oder literarische Zwecke verarbeitet werden, gelten von den Vorschriften dieses Kirchengesetzes nur die §§ 8, 22, 25, 26 und 48. Hierunter fällt die Herausgabe von Adressen-, Telefon- oder vergleichbaren Verzeichnissen nur, wenn mit ihr zugleich eine journalistisch-redaktionelle oder literarische Tätigkeit verbunden ist.

(2) Führt die journalistisch-redaktionelle Verarbeitung personenbezogener Daten zur Veröffentlichung von Gegendarstellungen der betroffenen Person, so sind diese Gegendarstellungen zu den gespeicherten Daten zu nehmen und für dieselbe Zeitdauer aufzubewahren wie die Daten selbst.

(3) Wird jemand durch eine Berichterstattung in seinem Persönlichkeitsrecht beeinträchtigt, so kann er Auskunft über die der Berichterstat-

tung zugrundeliegenden, zu seiner Person gespeicherten Daten verlangen. Die Auskunft kann verweigert werden, soweit aus den Daten auf die berichtenden oder einsendenden Personen oder die Gewährsleute von Beiträgen, Unterlagen und Mitteilungen für den redaktionellen Teil geschlossen werden kann. Die betroffene Person kann die Berichtigung unrichtiger Daten verlangen.

§ 52

Videoüberwachung öffentlich zugänglicher Räume

(1) Die Beobachtung öffentlich zugänglicher Bereiche innerhalb und außerhalb von Dienstgebäuden mit optisch-elektronischen Einrichtungen ist nur zulässig, soweit sie

1. in Ausübung des Hausrechts der kirchlichen Stelle oder
2. zum Schutz von Personen und Sachen erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Das Interesse an der nicht überwachten Teilnahme am Gottesdienst ist besonders schutzwürdig.

(2) Der Umstand der Beobachtung und der Name und die Kontaktdaten der verantwortlichen Stelle sind durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen.

(3) Die Speicherung oder Verwendung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zweckes erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet und verarbeitet, so ist diese über die jeweilige Verarbeitung zu benachrichtigen. Von der Benachrichtigung kann abgesehen werden,

1. solange das öffentliche Interesse an der Strafverfolgung das Recht auf Benachrichtigung der betroffenen Person erheblich überwiegt oder
2. wenn die Benachrichtigung im Einzelfall einen unverhältnismäßigen Aufwand erfordert.

(5) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

§ 53

Gottesdienste und kirchliche Veranstaltungen

Die Aufzeichnung oder Übertragung von Gottesdiensten oder kirchlichen Veranstaltungen ist datenschutzrechtlich zulässig, wenn die Teilnehmenden durch geeignete Maßnahmen über Art und Umfang der Aufzeichnung oder Übertragung informiert werden.

Kapitel 9 – Schlussbestimmungen

§ 54

Ergänzende Bestimmungen

(1) Der Rat der Evangelischen Kirche in Deutschland kann durch Rechtsverordnung mit Zustimmung der Kirchenkonferenz Durchführungsbestimmungen zu diesem Kirchengesetz und ergänzende Bestimmungen zum Datenschutz erlassen.

(2) Die Gliedkirchen können für ihren Bereich Durchführungsbestimmungen zu diesem Kirchengesetz und ergänzende Bestimmungen zum Datenschutz erlassen, soweit sie dem Recht der Evangelischen Kirche in Deutschland nicht widersprechen.

(3) Soweit personenbezogene Daten von Sozialleistungsträgern offengelegt werden, gelten zum Schutz dieser Daten ergänzend die staatlichen Bestimmungen entsprechend. Werden hierzu Bestimmungen gemäß Absatz 1 erlassen, ist vorher das Evangelische Werk für Diakonie und Entwicklung anzuhören.

(4) Dieses Kirchengesetz soll innerhalb von fünf Jahren überprüft werden.

§ 55

Übergangsregelungen

(1) Bisherige Bestellungen der Beauftragten für den Datenschutz gemäß den §§ 18 bis 18b des EKD-Datenschutzgesetzes in der Fassung der Bekanntmachung vom 1. Januar 2013 (ABl. EKD S. 2, S. 34) gelten fort. Für diese Bestellungen gelten die Regelungen der §§ 39 bis 45 mit Inkrafttreten dieses Kirchengesetzes.

(2) Bisherige Bestellungen der Betriebsbeauftragten und örtlichen Beauftragten für den Datenschutz gemäß § 22 des EKD-Datenschutzgesetzes in der Fassung der Bekanntmachung vom 1. Januar 2013 (ABl. EKD S. 2, S. 34) gelten fort. Für diese Bestellungen gelten die Regelungen der §§ 36 bis 38 mit Inkrafttreten dieses Kirchengesetzes.

(3) Vereinbarungen nach § 11 des EKD-Datenschutzgesetzes in der Fassung der Bekanntmachung vom 1. Januar 2013 (ABl. EKD S. 2, S. 34), gelten fort und sind spätestens bis zum 31. Dezember 2019 an dieses Kirchengesetz anzupassen.

(4) Verfahrensverzeichnisse betreffend die Videoüberwachung gemäß § 52 sind bis zum 24. Mai 2018 zu erstellen. Die Erstellung der Verfahrensverzeichnisse nach § 31 dieses Kirchengesetzes hat bis zum 30. Juni 2019 zu erfolgen.

§ 56

Inkrafttreten, Außerkraftreten

§ 55 Absatz 4 tritt am Tag nach der Verkündung in Kraft. Im Übrigen tritt dieses Kirchengesetz am 24. Mai 2018 in Kraft. Gleichzeitig tritt das EKD-Datenschutzgesetz in der Fassung der Bekanntmachung vom 1. Januar 2013 (ABl. EKD S. 2, S. 34) außer Kraft.

Kirchengesetz zur Ergänzung und Durchführung des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (Datenschutz-Anwendungsgesetz – DSAG) vom 18. Dezember 2018 (Kirchl. Amtsbl. S. 116)

Zur Durchführung und Ergänzung des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz – DSG-EKD) vom 15. November 2017 (ABl. EKD S. 353) hat die Landessynode mit Zustimmung des Kirchensenates das folgende Kirchengesetz beschlossen:

§ 1

Anwendungsbereich

Kirchliche Stellen gemäß § 2 Absatz 1 Satz 1 DSG-EKD sind die Landeskirche, die Kirchenkreise und ihre Verbände, die Kirchengemeinden und ihre Verbände, die Klöster Loccum und Amelungsborn, die Norddeutsche Kirchliche Versorgungskasse für Pfarrer und Kirchenbeamte, alle der Landeskirche zugeordneten Werke und Einrichtungen ohne Rücksicht auf deren Rechtsform sowie die der Aufsicht der Landeskirche unterstehenden rechtsfähigen Stiftungen.

§ 2

Errichtung der Aufsichtsbehörde für den Datenschutz

Die Aufgaben der Aufsichtsbehörde werden für die Landeskirche und die ihr zugeordneten diakonischen Werke und Einrichtungen durch die Aufsichtsbehörde der Evangelischen Kirche in Deutschland wahrgenommen. Mit Zustimmung des Landessynodalausschusses kann das Landeskirchenamt eine eigene Aufsichtsbehörde für die Landeskirche oder das Diakonische Werk evangelischer Kirchen in Niedersachsen e. V. errichten. Die Entscheidung über die Errichtung einer eigenen Aufsichtsbehörde für das Diakonische Werk evangelischer Kirchen in Niedersachsen e. V. bedarf des Einvernehmens der beteiligten Kirchen.

§ 3

Diakonisches Werk evangelischer Kirchen in Niedersachsen e. V.

Das Diakonische Werk evangelischer Kirchen in Niedersachsen e. V. verpflichtet seine Mitglieder zur Beachtung dieses Kirchengesetzes und der zu diesem Gesetz erlassenen Rechtsvorschriften in seiner Satzung.

§ 4

Örtlich Beauftragte für den Datenschutz

Für einen oder mehrere Kirchenkreise und die zu ihrem jeweiligen Bereich gehörenden kirchlichen Körperschaften sind gemeinsame örtlich Beauftragte für den Datenschutz zu bestellen. Das Nähere wird durch Rechtsverordnung geregelt.

§ 5

Verantwortliche Stelle

(1) Verantwortliche Stelle für die Einhaltung und Umsetzung der Bestimmungen zum Datenschutz sind für den Bereich der Landeskirche das Landeskirchenamt, für die Kirchenkreise, Kirchengemeinden und die anderen kirchlichen Körperschaften das jeweils für die Vertretung im Rechtsverkehr zuständige Organ.

(2) Für unselbständige Einrichtungen der kirchlichen Körperschaften kann die Aufgabe der verantwortlichen Stelle auf die jeweilige Leitung der Einrichtung übertragen werden.

(3) Verantwortliche Stelle für die Einhaltung und Umsetzung der Bestimmungen zum Datenschutz in den kirchlichen Diensten, Werken und Einrichtungen mit eigener Rechtspersönlichkeit ist das durch Kirchengesetz, Satzung, Vereinbarung oder Stiftungsurkunde mit der Geschäftsführung beauftragte Organ.

§ 6

Übersicht über die kirchlichen Werke und Einrichtungen mit eigener Rechtspersönlichkeit

Die Übersicht gemäß § 2 Absatz 1 Satz 3 DSG-EKD führt das Landeskirchenamt.

§ 7

Auftragsverarbeitung

Bei der Beauftragung anderer kirchlicher Stellen im Bereich der Landeskirche kann von den Bestimmungen des § 30 Absatz 3 Satz 2 Nummer 3, 5, 7 und 9 und Satz 4 DSG-EKD abgesehen werden.

§ 8

Verzeichnis von Verarbeitungstätigkeiten

Für Verarbeitungstätigkeiten gemäß § 31 Absatz 1 DSG-EKD, die einheitlich in der Landeskirche durchgeführt werden, wird das Verarbeitungsverzeichnis zentral im Landeskirchenamt geführt.

§ 9

Automatisierte Abrufverfahren und gemeinsame Dateien

Die Einrichtung eines automatisierten Abrufverfahrens oder einer gemeinsamen automatisierten Datei, in oder aus der mehrere verantwortliche Stellen personenbezogene Daten verarbeiten, ist zulässig, soweit dies unter Berücksichtigung der Rechte und Freiheiten der betroffenen Personen und der Aufgaben der beteiligten Stellen angemessen ist und durch technische und organisatorische Maßnahmen Risiken für die Rechte und Freiheiten der betroffenen Personen vermieden werden können.

§ 10

Weitere Regelungen

(1) Das Nähere zu den Grundsätzen des Datenschutzes, insbesondere in den Aufgabenbereichen der Verkündigung, Seelsorge, Bildung, Diakonie und Mission sowie in den Aufgaben der Leitung und Verwaltung wird durch Rechtsverordnung geregelt.

(2) Das Landeskirchenamt und das Diakonische Werk evangelischer Kirchen in Niedersachsen e. V. können für die Umsetzung der aus dem DSG-EKD resultierenden Verpflichtungen der kirchlichen Stellen, insbesondere für die Informationspflichten, die Verpflichtung auf das Datengeheimnis, das Verzeichnis von Verarbeitungstätigkeiten, die

Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde sowie für die Datenschutzfolgenabschätzung Formblätter, Muster und andere Vordrucke empfehlen oder für verbindlich erklären.

§ 11

Inkrafttreten

(1) Dieses Kirchengesetz tritt am 1. Januar 2019 in Kraft.

(2) Gleichzeitig tritt das Kirchengesetz der Konföderation evangelischer Kirchen in Niedersachsen zur Ergänzung und Durchführung des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland vom 23. November 1995 (Kirchl. Amtsbl. S. 166), das zuletzt durch das Kirchengesetz vom 9. März 2013 (Kirchl. Amtsbl. S. 46) geändert worden ist, außer Kraft.

Kirchengesetz über die digitale Kommunikation in der Evangelisch-lutherischen Landeskirche Hannovers (Digitalgesetz – DigitalG) vom 12. Dezember 2019 (Kirchl. Amtsbl. S. 315)

Die Landessynode hat mit Zustimmung des Kirchensenates das folgende Kirchengesetz beschlossen:

§ 1

Geltungsbereich

(1) Dieses Kirchengesetz gilt für die Evangelisch-lutherische Landeskirche Hannovers und deren unselbständige Einrichtungen sowie alle Körperschaften und Anstalten des öffentlichen Rechts und deren unselbstständige Einrichtungen, die unter der Aufsicht der Landeskirche stehen (kirchliche Körperschaften). Andere Körperschaften können mit Zustimmung des Landeskirchenamtes beschließen, dieses Kirchengesetz für sich anzuwenden.

(2) Dieses Kirchengesetz gilt für alle Personen, die digitale Anwendungen in den in Absatz 1 genannten Körperschaften nutzen.

(3) Mit Genehmigung des Landeskirchenamtes können kirchliche Körperschaften natürlichen oder juristischen Personen außerhalb des Geltungsbereichs nach Absatz 1 (Dritten) einen Zugriff auf Daten kirchlicher Körperschaften ermöglichen. Mit Dritten sind Vereinbarungen zu treffen, die die Einhaltung der Vorschriften dieses Gesetzes regeln.

(4) Bei einer Datenverarbeitung im Auftrag gilt Absatz 3 entsprechend. Die Bestimmungen des Datenschutzrechts bleiben unberührt.

§ 2

Grundsätze

(1) Die Nutzung der digitalen Kommunikation und der Einsatz von Informationstechnik und Software (IT) soll die Arbeit der beruflich und ehrenamtlich Mitarbeitenden zur Erfüllung des kirchlichen Auftrags unterstützen. Der Kreis der zur Nutzung berechtigten Mitarbeitenden (Nutzende) wird durch Rechtsverordnung geregelt.

(2) Das Landeskirchenamt definiert ein Konzept für die Infrastruktur der IT zur digitalen Kommunikation und schreibt dieses regelmäßig fort.

(3) Das Landeskirchenamt kann einheitliche fachliche und technische Standards für die Bereitstellung und Nutzung von IT unter Berücksichtigung von Funktionalität, Sicherheit und Wirtschaftlichkeit erlassen, insbesondere um die Funktionsfähigkeit aller angebotenen Dienste und Services zu gewährleisten.

(4) Die Landeskirche stellt eine einheitliche IT zur digitalen Arbeit und Kommunikation für die kirchlichen Körperschaften zur Verfügung. Die Anbindung an die Infrastruktur und die Nutzung bestimmter Programme und Verfahren können für verbindlich erklärt werden (Anschluss- und Benutzungszwang). Das Nähere wird durch Rechtsverordnung geregelt.

(5) Für die Nutzung von IT kann durch das Landeskirchenamt von den kirchlichen Körperschaften eine Gebühr erhoben werden. Das Nähere wird durch Rechtsverordnung geregelt.

§ 3

Einheitliche digitale Kommunikation

(1) Die Nutzenden der digitalen Kommunikation (§ 2 Absatz 1) in den kirchlichen Körperschaften sind in einem einheitlichen, zentralen landeskirchlichen Verzeichnis zu führen. Für Mitarbeitende in den kirchenleitenden Organen der Landeskirche liegt die Pflege des Verzeichnisses beim Landeskirchenamt. Im Übrigen obliegt die Pflege des Verzeichnisses der jeweils zuständigen kirchlichen Verwaltungsstelle.

(2) Nutzende erhalten eine persönliche E-Mail-Adresse mit einer vom Landeskirchenamt festgelegten Domain.

(3) Das Verzeichnis nach Absatz 1 dient zur Authentisierung von Nutzenden und wird als internes Adressverzeichnis genutzt. Für die Richtigkeit der Angaben im Adressverzeichnis sind die Nutzenden selbst verantwortlich.

(4) Nutzername und Kennwort sowie weitere Authentifizierungsmechanismen sind persönlich und vertraulich. Eine Weitergabe ist nicht gestattet.

(5) Die digitale Kommunikation soll Vorrang vor einer papiergebundenen Kommunikation haben. Verwaltungsprozesse sollen vorrangig digital abgebildet werden. Dabei ist auf einen schonenden Umgang mit Ressourcen zu achten.

(6) Durch Rechtsverordnung sind einheitliche Nutzungsbedingungen für die Authentisierung, die E-Mailnutzung und das Adressverzeichnis festzulegen. Im Übrigen sind die Rechte und Pflichten der Nutzenden bei der Anwendung der digitalen Kommunikation und der IT durch die zuständige kirchliche Körperschaft zu regeln. Für beruflich Mitarbeitende kann eine Dienstanweisung erlassen werden.

§ 4

Zentrale Anwendungen und Standards

(1) Die Landeskirche stellt den kirchlichen Körperschaften folgende zentrale Anwendungen zur Verfügung:

a) Meldewesen

b) Haushalts- und Rechnungswesen

c) Personalabrechnung

d) E-Mail und Kalender (Groupware)

Die Nutzung dieser Anwendungen ist für alle Körperschaften verbindlich (Anschluss- und Benutzungszwang).

(2) Zur Nutzung der zentralen Anwendungen kann das Landeskirchenamt Mindeststandards für Software und Clients (Hardware, Betriebssystem, Sicherheitseinstellungen) sowie deren Anbindung herausgeben, um Nutzbarkeit und Sicherheit zu gewährleisten.

§ 5

Kirchennetz und IT-Verbünde

(1) Die Landeskirche stellt ein kirchliches Datennetz (Kirchennetz) zur Verfügung. Das Kirchennetz ist ein zentraler IT-Verbund mit verbindlichen Standards für Anbindung, Berechtigungen, Sicherheitsniveaus, Nomenklaturen sowie weiteren technischen und organisatorischen Standards.

(2) Für die Definition und Veränderung von Standards im Kirchennetz ist das Landeskirchenamt zuständig.

(3) Kirchliche Körperschaften können eine eigene Infrastruktur (Server) innerhalb des Kirchennetzes unter Beachtung der definierten Standards betreiben.

(4) Darüber hinaus können kirchliche Körperschaften einen eigenen IT-Verbund betreiben, wenn gewährleistet ist, dass

a) die Infrastruktur außerhalb des Kirchennetzes liegt,

b) eine technische und organisatorische Trennung zum Kirchennetz vorliegt,

c) Zuständigkeiten geregelt sind und die Wirtschaftlichkeit gegeben ist und

d) die Bestimmungen dieses Kirchengesetzes eingehalten werden.

(5) Für jeden IT-Verbund ist von der verantwortlichen Stelle eine Informationssicherheitsleitlinie zu erlassen.

§ 6

Informationssicherheit

Im Rahmen der geltenden Bestimmungen über den Datenschutz und die Informationssicherheit sind das Landeskirchenamt oder von ihm beauftragte Stellen berechtigt, innerhalb des Kirchennetzes zur Abwehr von Gefahren für die Informationssicherheit

a) den im Datennetz der IT-Verbünde anfallenden Datenverkehr an den Übergabe- und Knotenpunkten automatisiert zu erheben,

b) die in den IT-Verbünden anfallenden Inhaltsdaten automatisiert nach Hinweisen auf Schadprogramme oder Angriffe unverzüglich auszuwerten,

c) die gespeicherten Daten zum Erkennen und Nachverfolgen von Auffälligkeiten automatisiert auszuwerten,

d) bei aktuellem Anlass zur Abwehr von Bedrohungen weitere erforderliche Maßnahmen zu veranlassen, um die Sicherheit der Infrastruktur und der Daten zu gewährleisten.

Das gleiche gilt für die verantwortliche Stelle eines anderen IT-Verbundes.

§ 7

Verantwortung, Aufsicht

(1) Wer die IT im Kirchennetz nutzt, ist für einen regelgerechten Umgang mit den anvertrauten Daten, Inhalten sowie der Hard- und Software verantwortlich.

(2) Für die Einhaltung der Regelungen ist das Leitungsorgan der jeweiligen kirchlichen Körperschaft zuständig.

(3) Die Verantwortung für einen IT-Verbund trägt die kirchliche Körperschaft, die den IT-Verbund errichtet hat.

§ 8

Weitere Regelungen

(1) Nähere Regelungen können durch Rechtsverordnung getroffen werden.

(2) Für die Umsetzung der aus diesem Kirchengesetz resultierenden Verpflichtungen der kirchlichen Körperschaften kann das Landeskirchenamt Leitlinien und Muster empfehlen oder für verbindlich erklären.

§ 9

Inkrafttreten

Dieses Kirchengesetz tritt am 1. Januar 2020 in Kraft. Für die technische Apassung bestehender Systeme gilt eine Übergangsfrist bis zum 1. Januar 2021.

Rechtsverordnung zur Ergänzung und Durchführung datenschutzrechtlicher Vorschriften (Datenschutzdurchführungsverordnung – DATVO) vom 21. Februar 2019 (Kirchl. Amtsbl. S. 5), geändert durch Rechtsverordnung vom 15. September 2020 (Kirchl. Amtsbl. S. 116)

Aufgrund des § 10 Absatz 1 des Kirchengesetzes zur Ergänzung und Durchführung des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (Datenschutz-Anwendungsgesetz – DSAG) vom 18. Dezember 2018 (Kirchl. Amtsbl. S. 116) erlassen wir mit Zustimmung des Landessynodalausschusses die folgende Rechtsverordnung:

I. Prinzipien des Datenschutzes

§ 1

Rechtmäßigkeit, Grundsätze, Offenlegung

(1) Die Verarbeitung personenbezogener Daten ist rechtmäßig, wenn das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder soweit die betroffene Person eingewilligt hat (Grundsatz des Verbots mit Erlaubnisvorbehalt).

(2) Die Verarbeitung ist außerdem rechtmäßig, wenn die Datenkenntnis zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist. Maßgebend sind die durch das kirchliche Recht bestimmten oder herkömmlichen Aufgabenbereiche der Verkündigung, Seelsorge, Diakonie, Mission und Unterweisung, Finanzverwaltung, Melde- und Friedhofswesen und der übrigen Aufgaben der Verwaltung in kirchlichen Körperschaften, Behörden und Dienststellen sowie in kirchlichen Werken und Einrichtungen ohne Rücksicht auf deren Rechtsform.

(3) Im Übrigen ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn die Voraussetzungen des § 6 DSG-EKD vorliegen.

(4) Für die Grundsätze der Verarbeitung personenbezogener Daten, für die Rechtmäßigkeit der Verarbeitung, die Rechtmäßigkeit der Zweckänderung, die Offenlegung an andere Stellen, die Datenübermittlung an Stellen außerhalb der Europäischen Union, für die Ein-

willigung, für die Verarbeitung besonderer Kategorien personenbezogener Daten und für die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten gelten die Vorschriften in Kapitel 2 des DSG-EKD.

(5) Die Begriffsbestimmungen für den kirchlichen Datenschutz sind in § 4 DSG-EKD erläutert.

(6) Soweit kirchlichen Stellen personenbezogene Daten von Sozialleistungsträgern offengelegt werden, sind die besonderen Bestimmungen der Sozialgesetzbücher, insbesondere über das Sozialgeheimnis (§ 35 SGB I) und den Schutz der Sozialdaten (§§ 67 ff. SGB X) sowie über bereichsbezogene Datenschutzbestimmungen der gesetzlichen Krankenversicherung (SGB V) und der sozialen Pflegeversicherung (SGB XI), zu beachten.

§ 2

Grundsätzliche Schutzmaßnahmen

(1) Für den Schutz personenbezogener Daten gelten neben den Bestimmungen des DSG-EKD, der Verordnung zur Sicherheit der Informationstechnik (ITSVO), und des DSAG die nachfolgenden Grundsätze.

(2) Die Umsetzung der Verpflichtungen aus der ITSVO, insbesondere die Informationssicherheitsorganisation und die kontinuierliche Weiterentwicklung von Informationssicherheitsstandards regelt das Landeskirchenamt im Rahmen von Richtlinien.

(3) Die verantwortlichen Stellen im Sinne von § 4 Nummer 9 DSG-EKD sind verpflichtet, unter Beachtung der in § 27 DSG-EKD genannten Grundsätze für die Einhaltung der Datenschutzbestimmungen für ihren Bereich zu sorgen und geeignete technische und organisatorische Maßnahmen zu treffen.

(4) Der Personenkreis, der Zugang zu personenbezogenen Daten hat, ist auf das unbedingt notwendige Maß zu beschränken und auf die Einhaltung der Datenschutzbestimmungen gemäß § 26 Satz 2 DSG-EKD zu verpflichten. Diese Verpflichtung besteht auch nach Beendigung des Dienstverhältnisses oder der ehrenamtlichen Tätigkeit. Näheres hierzu regelt das Landeskirchenamt durch Verwaltungsvorschrift.

(5) Verstöße gegen das Datengeheimnis sind Pflichtverletzungen und können bei beruflichen und ehrenamtlichen Mitarbeitenden rechtliche Konsequenzen oder Haftungstatbestände auslösen. Bei beruflichen Mitarbeitenden können diese Verstöße dienstrechtlich und disziplinarrechtlich oder arbeitsrechtlich geahndet werden.

(6) Die Vorschriften über die Amtsverschwiegenheit der kirchlichen Mitarbeitenden (z. B. §§ 30, 31 Pfarrdienstgesetz der EKD, § 24 Kirchenbeamtengesetz der EKD) und über sonstige Geheimhaltungspflichten (z. B. Steuergeheimnis) bleiben unberührt.

(7) Für die Nutzung privater Endgeräte im dienstlichen Bereich sind die Regelungen gemäß § 2 Absatz 2 ITSVO anzuwenden. Die Nutzung dienstlicher Endgeräte für private Zwecke soll durch Dienstvereinbarung oder Dienstanweisung geregelt werden.

(8) Analoge und digitale Daten, die nicht mehr benötigt werden, sind in einer Weise zu vernichten oder zu löschen, die jede Weiterverwendung und jeden Missbrauch der Daten ausschließt.

§ 3

Auftragsverarbeitung

(1) Werden personenbezogene Daten im Auftrag durch andere kirchliche oder sonstige Stellen oder Personen verarbeitet, ist § 30 DSG-EKD zu beachten. Die Speicherung der personenbezogenen Daten hat mandantenbezogen zu erfolgen. Mandant ist, in dessen Auftrag oder zu dessen Gunsten die Auftragsverarbeitung durchgeführt wird.

(2) Eine Weitergabe der personenbezogenen Daten an Dritte durch den Auftragnehmer ist auszuschließen.

(3) Örtlich Beauftragte für den Datenschutz sind frühzeitig bei der Auftragsverarbeitung zu beteiligen.

II. Gemeindegliederverzeichnis, Kirchenbuch, Gemeindegliederdaten

§ 4

Gemeindegliederverzeichnis

(1) Unbeschadet der Vorschriften des Kirchengesetzes der Evangelischen Kirche in Deutschland über die Kirchenmitgliedschaft und die zur Ergänzung und Durchführung ergangenen Vorschriften gelten für die Führung und Fortschreibung des Gemeindegliederverzeichnisses die Bestimmungen der Absätze 2 bis 4.

(2) Die zuständigen kirchlichen Stellen dürfen zur Erfüllung ihrer Aufgaben personenbezogene Daten, die ihnen nach dem staatlichen Melderecht übermittelt werden und die im Gemeindegliederverzeichnis gespeichert sind oder gespeichert werden sollen, aufgrund dieser Verordnung oder einer anderen Rechtsvorschrift verarbeiten.

(3) Das Recht und die Pflicht, das Gemeindegliederverzeichnis von Amts wegen fortzuschreiben, wenn gespeicherte Daten sich geändert haben oder wenn Daten zu speichern sind, erstrecken sich auch auf die von den Meldebehörden aus dem Melderegister übermittelten Daten der Kirchenmitglieder. Dies gilt insbesondere für die Berichtigung von Fehlern und für die Vervollständigung von Datenangaben aufgrund von kirchlichen Amtshandlungen oder Umgemeindungen.

(4) Daten aus dem Kirchenbuchwesen und der Kirchgeldhebung dürfen mit Meldewesendaten wechselseitig verknüpft werden. Insbesondere dürfen die Angaben über kirchlich beurkundete Amtshandlungen für Einladungen zu Jubiläen dieser Amtshandlungen und zu anderen kirchlichen Veranstaltungen verarbeitet werden. Widersprüche sind aufzunehmen und zu beachten.

(5) Kirchenbuchdaten und Daten aus dem kirchlichen Meldewesen dürfen verarbeitet werden, um Kirchenmitglieder zur Taufe ihrer noch ungetauften Kinder einzuladen. Widersprüche sind aufzunehmen und zu beachten.

§ 5

Veröffentlichung von Gemeindegliederdaten und Amtshandlungsdaten

(1) Die Kirchengemeinden dürfen Alters- und Ehejubiläen 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 hinzuweisen. Bei regelmäßigen Veröffentlichungen ist es ausreichend, wenn ein Hinweis auf das Widerspruchsrecht regelmäßig an derselben Stelle wie die Veröffentlichung erfolgt.

(2) Die Kirchengemeinden dürfen Amtshandlungen in Gottesdiensten bekannt geben und in Gemeindebriefen und anderen örtlichen kirchlichen Publikationen mit Namen sowie Tag und Ort der Amtshandlung veröffentlichen sowie Auskünfte zu Amtshandlungen erteilen. In Gottesdiensten und Gemeindebriefen dürfen zusätzlich Geburts-

und Sterbedaten sowie Lebensalter von verstorbenen und kirchlich bestatteten Personen bekannt gegeben werden. Die Bekanntgabe, Veröffentlichung und Auskunft unterbleibt, wenn hierfür von den Betroffenen ein überwiegendes schutzwürdiges Interesse am Ausschluss der Veröffentlichung geltend gemacht wird.

(3) Die aus den kommunalen Melderegistern übermittelten Auskunfts- und Übermittlungssperren sowie Widersprüche nach den Absätzen 1 und 2 sind in die kirchlichen Gemeindegliederverzeichnisse aufzunehmen und zu beachten. Personenbezogene Daten von Personen, für die Auskunftssperren nach § 51 Bundesmeldegesetz (BMG), ein bedingter Sperrvermerk nach § 52 BMG oder Maßnahmen des Zeugenschutzes nach § 53 BMG bestehen, dürfen für Veröffentlichungen nur genutzt werden, wenn vorher das schriftliche Einverständnis der betroffenen Personen eingeholt wurde. Dies gilt auch für die Familienangehörigen der betroffenen Personen.

(4) Die Veröffentlichung von Namen von Gemeindegliedern, ihrer Alters- und Ehejubiläen sowie von kirchlichen Amtshandlungsdaten im Internet ist nur zulässig, wenn die Einwilligung der betroffenen Personen vorher schriftlich eingeholt wurde.

(5) Sind durch verbindliche Regelungen über die regionale Zusammenarbeit von Kirchengemeinden nach dem Regionalgesetz oder durch eine Zusammenarbeit von Kirchenkreisen sachliche oder örtliche Zuständigkeiten begründet worden, die den Zugang zu den Gemeindegliederverzeichnissen mehrerer Kirchengemeinden erfordern, so dürfen die in diesen Strukturen nach § 4 Absatz 2 zuständigen kirchlichen Stellen die Gemeindegliederdaten aus den Gemeindegliederverzeichnissen der an der Zusammenarbeit beteiligten Kirchengemeinden verarbeiten, soweit dieses für die Erfüllung der gemeinsamen Aufgaben erforderlich ist. Nach einer insoweit erforderlichen Ergänzung der technischen und organisatorischen Maßnahmen (§ 27 DSG-EKD) und nach einer Bestimmung des berechtigten Personenkreises ist der Zugang zu den Gemeindegliederverzeichnissen durch das Kirchenamt zu ermöglichen.

III. Verkündigungsdienste

§ 6

Angehörige der im Verkündigungsdienst Tätigen

Die zuständige kirchliche Stelle kann für die in § 49 Absatz 1 und 2 DSG-EKD genannten Zwecke personenbezogene Daten der Angehörigen von Pastoren, Pastorinnen, Vikaren, Vikarinnen, Kandidaten und Kandidatinnen des Predigtamtes sowie von Pfarrverwaltern und Pfarrverwalterinnen verarbeiten, soweit dies im Rahmen der Aufgabenerfüllung erforderlich ist.

§ 7

Ehrenamtliche

(1) Personenbezogene Daten der in der kirchlichen oder in der diakonischen Arbeit ehrenamtlich Mitarbeitenden können von der verantwortlichen Stelle oder dem Diakonischen Werk verarbeitet werden, soweit dies im Rahmen der Aufgabenerfüllung erforderlich ist.

(2) Die zuständigen kirchlichen Stellen dürfen Namen, Vornamen, Geburtsdaten, Adressen sowie kirchliche Ämter und Funktionen von ehrenamtlichen Mitarbeitenden zur Erfüllung kirchlicher Aufgaben an die aufsichtsführenden Stellen, diakonische Stellen an das Diakonische Werk sowie die jeweiligen Fachverbände offenlegen, soweit dies im Rahmen der Aufgabenerfüllung erforderlich ist.

§ 8

Theologiestudierende

Die zuständigen kirchlichen Stellen dürfen personenbezogene Daten der in die Liste der Studierenden der Theologie eingetragenen Studierenden verarbeiten, soweit dies zur Förderung des Studiums, zur Begleitung und Beratung bei der Ausbildung, zu Prüfungszwecken sowie zur Durchführung der in § 49 Absatz 1 DSG-EKD genannten Maßnahmen erforderlich ist.

IV. Bildungswesen sowie Ausbildung und Fortbildung

§ 9

Daten der Schüler und Schülerinnen

(1) Schulen in kirchlicher und in diakonischer Trägerschaft dürfen personenbezogene Daten ihrer Schüler und Schülerinnen und der Erziehungsberechtigten verarbeiten, soweit dies zur Erfüllung der Aufgaben erforderlich ist. Das Gleiche gilt für ein der Schule angegliedertes Internat. Die zuständige kirchliche Stelle sowie deren Diakonisches Werk haben neben der Schule die Befugnisse nach Satz 1.

(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.

§ 10

Lehrer und Lehrerinnen

(1) Schulen und deren kirchliche oder diakonische Träger dürfen personenbezogene Daten von Lehrerinnen und Lehrern, Lehramtsanwärterinnen und Lehramtsanwärtern sowie Studienreferendaren und Studienreferendarinnen verarbeiten, 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.

§ 11

Kirchliche Bestätigung von Religionslehrkräften

(1) Die zuständigen kirchlichen Stellen dürfen von den Personen, die eine kirchliche Bestätigung für die Erteilung von evangelischem Religionsunterricht beantragen, die für die Bearbeitung des Antrages und die Teilnahme an Vokationstagungen erforderlichen personen-

bezogenen Daten im Rahmen der Erfüllung der Aufgaben verarbeiten und an kirchliche Stellen weiterleiten.

(2) Die in Absatz 1 genannten personenbezogenen Daten dürfen an staatliche Schulaufsichtsbehörden, Schulen und andere kirchliche Stellen offengelegt werden, soweit dies zur Aufgabenerfüllung dieser Stellen erforderlich ist. Eine Veröffentlichung der personenbezogenen Daten bedarf der Einwilligung der Betroffenen.

§ 12

Religionspädagogische Einrichtungen

(1) Die religionspädagogischen Einrichtungen dürfen von den Personen, die Lehrgänge als Lehrende oder Teilnehmende besuchen, die für die Veranstaltungen, Kurse und Prüfungen erforderlichen personenbezogenen Daten verarbeiten, soweit dies im Rahmen der Erfüllung der Aufgaben erforderlich ist.

(2) Die religionspädagogischen Einrichtungen dürfen die zur auftragsgemäßen Betreuung, Unterrichtung und Fortbildung der evangelischen Religionslehrer und Religionslehrerinnen erforderlichen personenbezogenen Daten dieses Personenkreises verarbeiten.

(3) Die in den Absätzen 1 und 2 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 Einwilligung der Betroffenen.

§ 13

Ausbildung des kirchlichen Verwaltungsnachwuchses

(1) Die zuständigen kirchlichen Stellen sind berechtigt, Daten der Ausbildung des kirchlichen Verwaltungsnachwuchses, die nach dem Berufsbildungsgesetz des Bundes erhoben werden, für Lehrgänge und Prüfungen der Ausbilder und Ausbilderinnen an die zuständigen Stellen des Berufsbildungsgesetzes zu übermitteln.

(2) Die für die Ausbildung erforderlichen personenbezogenen Daten der Kirchenbeamten und Kirchenbeamtinnen auf Widerruf im Vorbereitungsdienst können die zuständigen Stellen der Kirchen den Ausbildungsstätten bei Anmeldung zu Studium und Prüfung sowie bei Zuweisung zur theoretischen Ausbildung übermitteln. Das Gleiche

gilt hinsichtlich der Verwaltungsstellen, denen die Kirchenbeamten und Kirchenbeamtinnen zur berufspraktischen Ausbildung zugewiesen werden. Für die Anmeldung der Teilnehmenden bei Verwaltungslehrgängen gilt Satz 1 entsprechend.

§ 14

Listen der Teilnehmenden von Fortbildungen und Veranstaltungen

(1) Kirchliche Stellen können bei ihren Fortbildungen und Veranstaltungen personenbezogene Daten der Mitwirkenden und der Teilnehmenden verarbeiten, soweit dies für die Durchführung der Fortbildung oder Veranstaltung notwendig ist.

(2) Die Listen von Teilnehmenden bei Fortbildungen und Veranstaltungen dürfen allen Teilnehmenden übermittelt werden. Auf das Widerspruchsrecht ist hinzuweisen. Bei Widersprüchen ist die Liste der Teilnehmenden entsprechend anzupassen.

(3) Die personenbezogenen Daten von Teilnehmenden der Fortbildungen und Veranstaltungen dürfen mit Einwilligung der Betroffenen verarbeitet 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 Fortbildungen und Veranstaltungen ermöglichen wollen. Die Einwilligung kann jederzeit widerrufen werden.

V. Kirchliche Abgaben, Finanzwesen, kirchliche Gerichte

§ 15

Steuerdaten der Kirchenmitglieder

(1) 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 verarbeitet werden.

(2) Die Übermittlung der Steuerdaten der Kirchenmitglieder zwischen den steuererhebenden Körperschaften, den kirchlichen Verwaltungsstellen und den zuständigen kirchlichen Stellen ist zulässig, soweit dies im Rahmen einer ordnungsgemäßen Besteuerung erforderlich ist.

§ 16

Steuergeheimnis

Die Wahrung des Steuergeheimnisses geht den Regelungen des Datenschutzes vor.

§ 17

Kirchenbeiträge

Soweit die Kirchengemeinden, auch mit Hilfe der kirchlichen Verwaltungsstellen und automatisierter Verfahren, von den Kirchenmitgliedern anstelle der Ortskirchensteuer freiwillige Beiträge erheben, gelten die §§ 15 und 16 entsprechend. Die für die Beitragserhebung benötigten personenbezogenen Daten dürfen aus dem Gemeindegliederverzeichnis im Übrigen nur bei den betroffenen Kirchenmitgliedern erhoben und zu diesem Zweck verarbeitet werden.

§ 18

Dienstwohnungsinhaber und -inhaberinnen

(1) Die zuständigen kirchlichen Stellen können, sofern sie Dienstwohnungen an Mitarbeitende überlassen, die personenbezogenen Daten der Dienstwohnungsinhaber und -inhaberinnen verarbeiten, die zur Durchführung der dienstlichen Nutzungsverhältnisse einschließlich der Abrechnung der Dienstwohnungsvergütung erforderlich sind. Diese Daten können, soweit es zur ordnungsgemäßen Abwicklung der laufenden Vorgänge und zur Überprüfung erforderlich ist, zwischen den zuständigen kirchlichen Stellen ausgetauscht werden.

(2) Die steuerrechtlich geregelten Mitteilungspflichten bleiben unberührt.

§ 19

Nutzung von Grundstücken und Gebäuden

Die zuständigen kirchlichen Stellen und von ihnen Beauftragte können, sofern sie Dritten Grundstücke, grundstücksgleiche Rechte, Gebäude, Gebäudeteile und Wohnraum zur Miete oder sonst zur Nutzung überlassen oder daran Rechte einräumen oder Dritte ihnen solche Nutzungen und Rechte einräumen, die zur verwaltungsmäßigen Abwicklung und Überprüfung erforderlichen personenbezogenen Daten der Berechtigten oder Verpflichteten verarbeiten.

§ 20

Wohnungsbewerbungen, Mietbeihilfen

Die zuständigen kirchlichen Stellen und von ihnen Beauftragte können die Daten von Bewerberinnen und Bewerbern für Wohnungen und von Antragstellerinnen und Antragstellern auf Mietbeihilfen und ähnliche Leistungen sowie von deren Familienangehörigen verarbeiten. Eine Offenlegung dieser Daten ist nur mit Einwilligung der Betroffenen zulässig.

§ 21

Darlehen, Gehaltsvorschüsse, Unterstützungen

Die zuständigen kirchlichen Stellen und die von ihnen Beauftragten können die für die Gewährung von Darlehen, Gehaltsvorschüssen und Unterstützungen an kirchliche Mitarbeitende und Studierende sowie in besonderen anderen Fällen zur Sicherung und Tilgung der entsprechenden Forderungen und zur Vorlage von Verwendungsnachweisen notwendigen personenbezogenen Daten der Empfänger und Empfängerinnen der Beträge sowie deren dafür mithaftenden Familienangehörigen und der Bürgen verarbeiten.

§ 22

Friedhöfe

(1) Zur Bewirtschaftung und Verwaltung der Friedhöfe und ihrer Einrichtungen sowie zur Festsetzung und Einziehung von Gebühren dürfen von den Friedhofsträgern oder in ihrem Auftrage die zu den vorgenannten Zwecken erforderlichen personenbezogenen Daten der Verstorbenen und der Nutzungsberechtigten verarbeitet werden.

(2) Im Rahmen der Zulassung und Überwachung der auf den Friedhöfen tätigen Gewerbetreibenden des Friedhofs- und Bestattungsgewerbes dürfen von den Friedhofsträgern die erforderlichen personenbezogenen Daten verarbeitet werden.

(3) Der Friedhofsträger darf zum Zwecke der Bestattung die notwendigen Daten der oder des Verstorbenen sowie von Angehörigen an den Pastor oder die Pastorin übermitteln, der oder die die Bestattung vornimmt.

(4) Bei der Umbettung von Leichen dürfen den zuständigen Gesundheitsbehörden die notwendigen 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 die notwendigen personenbezogenen Daten zur Prüfung der vorgelegten Anträge übermittelt werden.

(6) Ist beim Betrieb von Grabstätten, Friedhöfen oder Friedhofsteilen die Einschaltung von Sachverständigen erforderlich, so dürfen den Sachverständigen die notwendigen personenbezogenen Daten offengelegt werden.

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

(8) 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 nicht beeinträchtigt werden.

(9) Zum Gedenken und zur Fürbitte dürfen in Sterbe- oder Totenbücher, die in Kirchen oder sonstigen kirchlichen Gebäuden allgemein zugänglich sind, Namen und Vornamen der verstorbenen Personen sowie Geburts- und Sterbedaten eingetragen werden.

§ 23

Kirchliche Gerichte

(1) Die kirchlichen Stellen dürfen gespeicherte Daten an die kirchlichen Gerichte offenlegen, soweit dies zur Erfüllung von deren Aufgaben erforderlich ist.

(2) Die nach Absatz 1 gespeicherten Daten dürfen nach vorheriger Anonymisierung oder Pseudonymisierung auch für wissenschaftliche Zwecke an kirchliche Forschungseinrichtungen offengelegt werden.

VI. Fundraising

§ 24

Fundraising

(1) Fundraising als kirchliche Aufgabe wahrgenommen verbindet die Beziehungspflege mit dem Werben um persönlichen und finanziellen Einsatz für kirchliche und diakonische Zwecke.

(2) Kirchliche Stellen dürfen personenbezogene Daten von Gemeindegliedern und deren Angehörigen, von den in der kirchlichen oder in der diakonischen Arbeit ehrenamtlich oder beruflich Tätigen und von an der kirchlichen und diakonischen Arbeit interessierten Personen für das Fundraising verarbeiten, soweit dies für die Durchführung des Fundraisings erforderlich ist.

(3) Die kirchlichen Stellen dürfen für das Fundraising ihre im Gemeindegliederverzeichnis und in den Kirchenbüchern enthaltenen Daten von Kirchenmitgliedern und Familienangehörigen nutzen, soweit kein melderechtlicher Sperrvermerk diese Nutzung ausschließt.

(4) Kirchliche Stellen dürfen für das Fundraising Daten nutzen, die aus allgemein zugänglichen Quellen entnommen oder zu diesem Zweck erworben werden.

(5) Personenbezogene Daten der von diakonischen Einrichtungen betreuten oder behandelten Personen (Patientendaten), ihrer Angehörigen, Bevollmächtigten sowie ihrer rechtlichen Betreuer und Betreuerinnen dürfen nur mit deren Einwilligung verarbeitet werden.

(6) Die für das Fundraising erhobenen personenbezogenen Daten sind zu löschen, soweit der Löschung ein konkreter kirchlicher Auftrag, Rechtsvorschriften oder Aufbewahrungsfristen nicht entgegenstehen.

§ 25

Datenübermittlung an andere kirchliche Stellen im Rahmen des Fundraisings

(1) Personenbezogene Daten können an kirchliche Stellen offengelegt 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 Fundraisings mit der übermittelnden kirchlichen Stelle abgestimmt werden,
3. die datenempfangende kirchliche Stelle sicherstellt, dass Widersprüche von betroffenen Personen gegen die Datennutzung im Rahmen des Fundraisings beachtet und der übermittelnden kirchlichen Stelle mitgeteilt werden und
4. ausreichende technische und organisatorische Datenschutzmaßnahmen unter Beachtung des Schutzbedarfs der Anforderungen gemäß § 27 DSG-EKD vorliegen, von denen sich die übermittelnde kirchliche Stelle im Zweifelsfall zu überzeugen hat.

(2) Für das Fundraising kirchlicher Stellen dürfen nur folgende Daten von Kirchenmitgliedern und ihren Familienangehörigen aus dem kirchlichen Meldewesen verarbeitet werden:

1. Name, Vorname 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.

(3) Weitere Daten von Kirchenmitgliedern dürfen von den zuständigen kirchlichen Stellen für das Fundraising verarbeitet werden, soweit dies für die Durchführung der Maßnahme erforderlich ist, insbesondere:

1. Name, Vorname und Anschrift von Spenderinnen und 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.

Entsprechendes gilt für Personen, die mit der kirchlichen und diakonischen Arbeit in Beziehung getreten sind.

(4) Spenden anlässlich von Jubiläen, Geburtstagen und Trauerfällen, die auf Veranlassung der Jubilarin oder des Jubilars sowie von Familienangehörigen für einen kirchlichen Zweck gesammelt werden, dürfen der veranlassenden Person mit Namen und Spendenhöhe bekannt gegeben werden.

§ 26

Ausschluss der Nutzung

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

VII. Daten von Beschäftigten und Verzeichnisse über Personen und Dienste

§ 27

Personenangaben im Dienstbetrieb

(1) Soweit in Ausübung von Dienst- und Arbeitsverhältnissen personenbezogene Daten verarbeitet werden, ist § 49 DSG-EKD anzuwenden.

(2) Die Weitergabe der Daten gemäß Absatz 1 ist insbesondere an Sozialversicherungsträger, Träger betrieblicher Altersversorgung und Finanzbehörden zulässig.

(3) Die in Anträgen auf die Gewährung von Beihilfen in Krankheits-, Pflege-, Geburts- und Todesfällen enthaltenen personenbezogenen Daten von Familienangehörigen der Antragstellenden dürfen nur von der für die Gewährung der Beihilfe zuständigen Stelle verarbeitet werden.

(4) Dienst- und mitarbeiterrechtliche Regelungen, insbesondere die Bestimmungen des Mitarbeiter- und Mitarbeitervertretungsrechts und des Pfarrdienstrechts bleiben unberührt.

§ 28

Wahl zu kirchlichen Leitungsämtern und Organen

Personenbezogene Daten der Kandidaten und Kandidatinnen für durch Wahl zu besetzende kirchliche Leitungsämter und für Sitze in kirchlichen Leitungsorganen dürfen für die öffentliche Bekanntgabe in folgendem Umfang verarbeitet werden: Name, Vorname, akademischer Titel, Anschrift, Beruf und Lebensalter. Die öffentliche Bekanntgabe kann durch andere Arten der Bekanntmachung ergänzt werden.

§ 29

Mitglieder von Organen und Ausschüssen

Personenbezogene Daten von Mitgliedern der Leitungsorgane kirchlicher Stellen sowie von diesen gebildeten Ausschüssen und Arbeitsgruppen können verarbeitet werden, soweit dies für die Arbeit der genannten Gremien erforderlich ist. Die Daten dürfen in einer gemeinsamen Datei geführt werden, wenn der begrenzte Zugriff auf die Daten geregelt ist.

§ 30

Anschriftenverzeichnisse der verantwortlichen Stellen, Kirchliches Amtsblatt

(1) Anschriftenverzeichnisse und digitale Adressbücher, die Namen, Dienst- oder Amtsbezeichnungen, dienstliche Anschriften, Stellenbesetzungs-, Geburts- und Ordinationsdaten von kirchlichen Mitarbeitenden und sonstigen Inhaberinnen und Inhabern kirchlicher Ämter und Ehrenämter enthalten, dürfen für die kirchliche und diakonische Arbeit unter Verwendung der vorliegenden Personendaten verarbeitet werden. Privatanschriften können erhoben und für Anschriftenverzeichnisse genutzt werden, soweit dies für die Erreichbarkeit erforderlich ist. Die Daten der Pastoren und Pastorinnen im Ruhestand dürfen mit Namen, Dienstbezeichnungen, letzten Tätigkeiten, Geburtsdaten und Privatanschriften in Anschriftenverzeichnisse aufgenommen werden.

(2) Die Offenlegung dieser Daten an andere kirchliche oder öffentliche Stellen richtet sich nach § 8 DSG-EKD, die Offenlegung an sonstige Stellen richtet sich nach § 9 DSG-EKD.

(3) Im Kirchlichen Amtsblatt dürfen folgende Personalnachrichten der Pastoren und Pastorinnen, Prädikanten und Prädikantinnen, Pasto-

ren und Pastorinnen im Ehrenamt sowie der Kirchenbeamten und Kirchenbeamtinnen in Leitungsämtern veröffentlicht werden, auch soweit das Amtsblatt mit Datum im Internet veröffentlicht wird:

1. Name und die Tatsache der bestandenen Ersten oder Zweiten theologischen Prüfung, Ordination oder Beauftragung sowie deren Aberkennung, Ernennung, Einweisung, Versetzung, Entlassung, Ruhestand;
2. im Zusammenhang mit dem Versterben auch den Geburtsort, das Geburtsdatum, Ordinationsort und -datum, Tätigkeitsorte und Beginn des Ruhestands.

   Entsprechendes gilt für die Personalnachrichten von Mitgliedern kirchlicher Leitungsorgane.

(4) Für den Verlust der Rechte aus der Ordination gilt darüber hinaus § 5 Absatz 3 des Pfarrdienstgesetzes der EKD.

§ 31

Einheitliche Datenverwaltungssysteme, Intranet

(1) Personenbezogene Daten aus den Bereichen Ausbildungs-, Prüfungs-, Personal-, Stellen-, Gremien-, Finanz- und Liegenschaftsverwaltung, aus diakonischen Arbeitsbereichen und sonstigen kirchlichen Bereichen sowie Anschriftenverzeichnisse und digitale Adressbücher dürfen, soweit dies aus organisatorischen Gründen erforderlich ist, im Rahmen eines einheitlichen Datenverwaltungsprogramms verarbeitet werden.

(2) Ein Zugriff auf die Daten ist auch zulässig, wenn es sich um einen Zugriff aus dem Intranet oder eine verschlüsselte Verbindung aus dem Internet handelt.

(3) Es ist sicherzustellen, dass die gespeicherten personenbezogenen Daten in der jeweiligen kirchlichen Stelle nur den Personen zugänglich gemacht werden, die sie für die Erfüllung ihrer Aufgaben benötigen. Durch technische und organisatorische Maßnahmen ist sicherzustellen, dass der Schutz der verarbeiteten personenbezogenen Daten gemäß § 27 DSG-EKD gewährleistet ist und die Löschungsbestimmungen eingehalten werden.

§ 32

Versorgungskassen

Die kirchlichen Versorgungskassen sind berechtigt, zur Bearbeitung und zur Zahlung von Alters- und Hinterbliebenenbezügen sowie von Beihilfen in Krankheits-, Pflege-, Geburts- und Todesfällen diejenigen personenbezogenen Daten der kirchlichen Mitarbeitenden und der Empfänger und Empfängerinnen von Versorgungsbezügen sowie deren Familienangehörigen zu verarbeiten, die für die Hebung der Beiträge und für die Berechnung und Zahlung der Versorgungsbezüge sowie für die Gewährung von Beihilfen notwendig sind.

VIII. Personenbezogene Daten in der Öffentlichkeitsarbeit

§ 33

Gemeindebriefe, kirchliche Publikationen

(1) Für Redakteure und Redakteurinnen von Gemeindebriefen, kirchlichen Publikationen, Presseerklärungen und ähnlichen Verlautbarungen gilt § 51 DSG-EKD.

(2) Stellen, die kirchliche Publikationen herstellen oder verbreiten, dürfen personenbezogene Daten nur verarbeiten, soweit dies für die Erfüllung ihres Auftrags erforderlich ist.

§ 34

Soziale Netzwerke

(1) Soziale Netzwerke können von kirchlichen Stellen zur Information über die kirchliche und diakonische Arbeit und zur Beziehungspflege mit Gemeindegliedern und deren Angehörigen, den in der kirchlichen oder in der diakonischen Arbeit ehrenamtlich oder beruflich Mitarbeitenden und den an der kirchlichen und diakonischen Arbeit interessierten Personen genutzt werden.

(2) Mitarbeitende, die seitens der kirchlichen Stelle mit der Wahrnehmung der Kommunikation in sozialen Netzwerken beauftragt sind, haben die für die dienstliche Nutzung erlassenen Verhaltensregeln (Social-Media-Leitlinien), die datenschutzrechtlichen Regelungen,

das Urheberrecht sowie weitere rechtliche Bestimmungen insbesondere zur Verschwiegenheit zu beachten.

(3) Kirchliche Stellen können eigene soziale Netzwerke einrichten und betreiben.

§ 35

Kirchliche und öffentliche Auszeichnungen und Ehrungen

(1) Zur Vorbereitung kirchlicher und öffentlicher Auszeichnungen und Ehrungen dürfen die zuständigen kirchlichen Stellen die dazu erforderlichen personenbezogenen Daten einschließlich besonderer Kategorien personenbezogener Daten im Sinne des § 13 DSG-EKD verarbeiten, es sei denn, dass der zuständigen Stelle bekannt ist, dass die betroffene Person ihrer kirchlichen oder öffentlichen Auszeichnung oder Ehrung oder der damit verbundenen Datenverarbeitung widersprochen hat. Auf Anforderung der in Satz 1 genannten Stellen dürfen kirchliche Stellen die erforderlichen Daten übermitteln. Gleiches gilt auf Anforderung der zuständigen öffentlichen Stellen. Eine Verarbeitung der personenbezogenen Daten für andere Zwecke ist nur mit Einwilligung der betroffenen Person zulässig.

(2) Die §§ 17 bis 19 und 23 DSG-EKD finden keine Anwendung.

IX. Diakonische Arbeitsbereiche

§ 36

Sozialgeheimnis

Mitarbeitende, die Sozialdaten verarbeiten, sind neben der Verpflichtung auf das Datengeheimnis gemäß § 26 DSG-EKD auch auf die Einhaltung des Sozialgeheimnisses (§ 35 SGB I) hinzuweisen.

§ 37

Tageseinrichtungen für Kinder, Einrichtungen der Jugendhilfe

(1) Soweit für den Betrieb von Einrichtungen der Jugendhilfe, insbesondere Tageseinrichtungen für Kinder, durch den Träger die Verarbeitung personenbezogener Daten erforderlich ist, sind die Vorschrif-

ten über den Schutz personenbezogener Daten des SGB VIII und des SGB X entsprechend anzuwenden.

(2) Kirchliche und kommunale Stellen dürfen personenbezogene Daten im Rahmen der Platzvergabe gemeinsam verarbeiten.

(3) Tageseinrichtungen für Kinder und Einrichtungen der Jugendhilfe dürfen personenbezogene Daten der Kinder, Jugendlichen und Erziehungsberechtigen verarbeiten, soweit dies zur Erfüllung ihres Erziehungs-, Bildungs- und Betreuungsauftrags erforderlich ist.

(4) Personenbezogene Daten, die für die Festsetzung der Elternbeiträge erforderlich sind, dürfen die Träger ausschließlich zu diesem Zweck verarbeiten. 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, Erhebung, Überprüfung oder Vollstreckung der Beiträge. Unterlagen dürfen nur im erforderlichen Umfang erhoben und offengelegt werden.

(5) Personenbezogene Daten der Kinder und Jugendlichen sowie deren Erziehungsberechtigten dürfen mit Einwilligung der Erziehungsberechtigten für Zwecke der örtlichen Kirchengemeindearbeit verarbeitet werden. Dies gilt für Zwecke des Schulwesens entsprechend.

(6) Personaldaten dürfen vom Träger nur zu Zwecken der Abrechnung der Finanzhilfe von staatlichen Stellen verarbeitet werden.

§ 38

Diakoniestationen

(1) Soweit für den Betrieb von Einrichtungen der Diakonie- und Sozialstationen in Trägerschaft oder in Mitverantwortung kirchlicher Stellen die Verarbeitung personenbezogener Daten erforderlich ist, sind die Vorschriften über den Schutz personenbezogener Daten des SGB X sowie die Vorschriften über die Pflichten der Leistungserbringer des SGB V entsprechend anzuwenden.

(2) Die Verarbeitung von durch Diakonie- und Sozialstationen gespeicherten personenbezogenen Daten der Kirchenmitglieder für Zwecke der Kirchengemeinde und für die pfarramtliche Betreuung zur Erfüllung des seelsorgerischen Auftrags ist nur mit Einwilligung zulässig.

§ 39

Beratungsstellen

Kirchliche Beratungsstellen dürfen diejenigen personenbezogenen Daten verarbeiten, die für die jeweils beantragte Beratung erforderlich sind. Personenbezogene Daten dürfen mit Einwilligung der betroffenen Person für andere Beratungszwecke in derselben Einrichtung verwandt werden.

§ 40

Bewohner-, Patienten- und Klientendaten

(1) Bewohner-, Patienten- und Klientendaten dürfen in kirchlichen und diakonischen Einrichtungen, insbesondere in Krankenhäusern, Einrichtungen der Behinderten-, Suchtkranken-, Alten- und Wohnungslosenhilfe sowie Arbeitslosenprojekten, nur verarbeitet werden, soweit dieses im Rahmen der Vertragsbeziehung, zur verwaltungsmäßigen Abwicklung, zur Leistungsberechnung, zur Erfüllung bestehender Dokumentationspflichten oder wegen eines damit im Zusammenhang stehenden Rechtsstreites erforderlich ist.

(2) Die personenbezogenen Daten der in Absatz 1 genannten Personen dürfen mit Einwilligung der betroffenen Person an den Krankenhausseelsorger und den jeweils örtlich zuständigen Seelsorger übermittelt werden. Die Einwilligung soll bereits bei der Aufnahme in eine der in Absatz 1 genannten Einrichtungen eingeholt werden.

X. Schlussbestimmungen

§ 41

Inkrafttreten, Außerkrafttreten

Diese Rechtsverordnung tritt am 1. März 2019 in Kraft. Gleichzeitig tritt die Verordnung des Rates der Konförderation evangelischer Kirchen in Niedersachsen zur Ergänzung und Durchführung datenschutzrechtlicher Vorschriften vom 12. Dezember 1995 (Kirchl. Amtsbl. S. 190), die zuletzt durch Rechtsverordnung vom 10. Dezember 2013 (Kirchl. Amtsbl. S. 182) geändert worden ist, außer Kraft.

Rechtsverordnung über die Bestellung von örtlich Beauftragten für den Datenschutz (RVO-DS-Beauftragte) vom 25. Juni 2015 (Kirchl. Amtsbl. S. 58), zuletzt geändert durch Rechtsverordnung vom 12. Dezember 2019 (Kirchl. Amtsbl. S. 319)

Aufgrund des § 27 Absatz 2 des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz – DSG-EKD) in der Bekanntmachung der Neufassung vom 1. Januar 2013 (ABl. EKD S. 2, berichtigt S. 34) und des § 7 des Kirchengesetzes der Konföderation evangelischer Kirchen in Niedersachsen zur Ergänzung und Durchführung des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (Gemeinsames Datenschutz-Anwendungsgesetz – DSAG) vom 23. November 1995 (Kirchl. Amtsbl. S. 166), zuletzt geändert durch Kirchengesetz vom 9. März 2013 (Kirchl. Amtsbl. S. 46), erlassen wir mit Zustimmung des Landessynodalausschusses die folgende Rechtsverordnung:

§ 1

Verpflichtung kirchlicher Stellen

(1) Gemäß § 36 des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetzes – DSG-EKD) sind bei kirchlichen Stellen örtlich Beauftragte für den Datenschutz schriftlich zu bestellen. Nach den Bestimmungen des DSG-EKD unterstützen die örtlich Beauftragten für den Datenschutz die verantwortlichen Stellen bei der Sicherstellung des Datenschutzes (§ 38 Satz 1 DSG-EKD). Unabhängig davon verbleibt die Verantwortung für die Sicherstellung des Datenschutzes bei der Dienststellenleitung.

(2) § 36 DSG-EKD ist nach Maßgabe der nachfolgenden Bestimmungen anzuwenden.

§ 2

Bestellung, Zuständigkeit

(1) Die Kirchenkreise bestellen eine örtlich Beauftragte oder einen örtlich Beauftragten für den Datenschutz. Die örtlich Beauftragten sollen für den Zuständigkeitsbereich eines Kirchenamtes oder Kirchenkreisamtes gemeinsam bestellt werden. Sie können unabhängig von der Sprengelzuordnung auch für den Zuständigkeitsbereich mehrerer Kirchenämter oder Kirchenkreisämter gemeinsam bestellt werden. Die Bestellung kann befristet für mindestens drei Jahre erfolgen.

(2) Zum oder zur örtlich Beauftragten für den Datenschutz darf nur bestellt werden, wer Mitarbeiter oder Mitarbeiterin einer der in Absatz 5 genannten kirchlichen Körperschaften ist. Nicht bestellt werden dürfen Personen, die mit der Leitung der Datenverarbeitung beauftragt sind oder denen die Leitung der kirchlichen Stelle obliegt.

(3) Die Bestellung kann befristet oder unbefristet erfolgen und ist nach dem Muster der Anlage 1 zu dieser Rechtsverordnung vorzunehmen.

(4) Es ist eine Vertretung zu bestellen, die nach dem Muster der Anlage 1 zu dieser Rechtsverordnung vorzunehmen ist. Die Vertretung kann auch einem oder einer örtlich Beauftragten für den Datenschutz aus einem anderen Zuständigkeitsbereich übertragen werden.

(5) Die Zuständigkeit der oder des örtlich Beauftragten für den Datenschutz nach Absatz 1 erstreckt sich auf alle kirchlichen Körperschaften und deren rechtlich unselbständigen Einrichtungen im Bereich des Kirchenkreises oder der Kirchenkreise, für die sie bestellt wurden. § 36 Absatz 1 Nummer 1 DSG-EKD findet insoweit keine Anwendung.

§ 3

Qualifikation und Aufgaben

(1) Die örtlich Beauftragten für den Datenschutz müssen über die zur Erfüllung ihrer Aufgaben erforderliche Fachkunde und Zuverlässigkeit verfügen.

(2) Sie sind in dieser Eigenschaft weisungsfrei. Sie können sich unmittelbar an die jeweils verantwortliche Dienststellenleitung wenden. Sie dürfen wegen der Erfüllung ihrer Aufgaben nicht benachteiligt werden. Sie können Auskünfte verlangen und Einsicht in Unterlagen nehmen. Hiervon ausgenommen sind personenbezogene Daten nach § 43 Absatz 8 Satz 1 DSG-EKD.

(3) Sie sind bei der Erfüllung ihrer Aufgaben zu unterstützen. In Zweifelsfällen können sie sich an die für die Datenschutzaufsicht zuständige Stelle wenden.

(4) Die örtlich Beauftragten für den Datenschutz wirken auf die Einhaltung der Bestimmungen für den Datenschutz hin. Hierzu haben sie insbesondere

1. die verantwortliche Stelle und die Mitarbeitenden zu beraten;
2. die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen;

3. die bei der Verarbeitung personenbezogener Daten tätigen Personen zu informieren und zu schulen;
4. mit der Aufsichtsbehörde zusammenzuarbeiten;
5. die verantwortliche Stelle bei der Datenschutz-Folgenabschätzung, insbesondere im Zusammenhang mit der Videoüberwachung öffentlich zugänglicher Räume, zu beraten und deren Durchführung zu überwachen.

(5) Beim Abschluss von Vereinbarungen mit Auftragsverarbeitern gemäß § 30 DSG-EKD sind die örtlich Beauftragten für den Datenschutz frühzeitig zu beteiligen.

(6) Die örtlich Beauftragten für den Datenschutz sind verpflichtet, über die in dieser Eigenschaft bekannt gewordenen Angelegenheiten Verschwiegenheit zu wahren. Die Verpflichtung besteht auch nach Beendigung der Bestellung fort.

§ 4

Rechtliche Stellung

(1) Die örtlich Beauftragten für den Datenschutz sind zur Wahrnehmung ihrer Aufgaben von ihren sonstigen dienstlichen Tätigkeiten in erforderlichem Umfang unter Fortzahlung des Entgelts freizustellen. Für den zeitlichen Umfang der Wahrnehmung der Aufgaben wird folgender Aufwand zugrunde gelegt:

1 Stunde/Woche	je 60.000 Gemeindeglieder
2 Stunden/Woche	je 400 Beschäftigte

(2) Den örtlich Beauftragten für den Datenschutz ist Auslagenersatz im Rahmen des geltenden Rechts zu gewähren. Sie sind mit den zur Erfüllung ihrer Aufgaben notwendigen räumlichen, personellen und sachlichen Mitteln auszustatten.

(3) Ihnen ist die Teilnahme an Fort- und Weiterbildungsveranstaltungen entsprechend dem Aufgabenbereich zu ermöglichen. Die erforderlichen Kosten sind zu übernehmen. Im Konfliktfall kann die Aufsichtsbehörde angerufen werden.

(4) Die Abberufung der örtlich Beauftragten für den Datenschutz ist nur in entsprechender Anwendung des § 626 des Bürgerlichen Gesetzbuches zulässig. Die Kündigung des Arbeitsverhältnisses der oder des örtlich Beauftragten für den Datenschutz ist nur zulässig, wenn Tatsachen vorliegen, die zur Kündigung aus wichtigem Grund berechti-

gen. Gleiches gilt für eine Kündigung binnen eines Jahres nach Beendigung der Bestellung.

§ 5

Bekanntmachung, Mitteilung

(1) Die Bestellung von örtlich Beauftragten für den Datenschutz ist den Mitarbeitenden der jeweiligen kirchlichen Stellen nach dem Muster der Anlage 2 zu dieser Rechtsverordnung bekannt zu machen.

(2) Die Mitarbeitenden können sich in allen Angelegenheiten des Datenschutzes ohne Einhaltung des Dienstweges an die örtlich Beauftragten für den Datenschutz wenden.

(3) Name und Dienstadresse der jeweils bestellten Personen sind dem Landeskirchenamt mitzuteilen.

§ 6

Inkrafttreten

Diese Rechtsverordnung tritt am 1. Juli 2015 in Kraft.

Anlage 1
zu § 2 Absätze 3 und 4

Bestellung von Beauftragten und deren Stellvertretung gemäß § 36 Absatz 1 DSG-EKD i. V. m. § 2 Absätze 3 und 4 RVO-DS-Beauftragte

Frau / Herr .....
(Vorname, Name)

wird mit Wirkung vom .....

für .....
(Namen und Adressen der kirchlichen Stelle, bei gemeinsamen örtlichen Beauftragten alle beteiligten kirchlichen Stellen aufführen)

☐ zum/zur örtlich Beauftragten für den Datenschutz

☐ 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. Die Aufgaben ergeben sich aus dem kirchlichen Datenschutzrecht und werden in dem ausgehändigten Merkblatt: „Örtlich Beauftragte für den Datenschutz" näher beschrieben.

Im Rahmen dieser Tätigkeit sind Sie arbeitsrechtlich unmittelbar

.....
unterstellt.

Ihre Zuständigkeit erstreckt sich auf:

Ev.-luth. Kirchenkreis ..... ,

Ev.-luth. Kirchenkreis ..... ,

Ev.-luth. Kirchenkreis ..... ,

Kirchenkreisverband .....

sowie auf die Körperschaften, die der Aufsicht der vorgenannten Kirchenkreise unterstehen.

.....
Ort, Datum, Unterschrift (Leitung)

Empfangsbestätigung

Die Bestellung zum/zur örtlich Beauftragten für den Datenschutz sowie ein Exemplar des Merkblatts „Örtlich Beauftragte für den Datenschutz“ habe ich erhalten.

.....

Ort, Datum, Unterschrift der bestellten Person

☐ Exemplar an Mitarbeiterin/Mitarbeiter

☐ Exemplar zur Personalakte

☐ Exemplar an das Landeskirchenamt Hannover

☐ Exemplar an

☐ Exemplar an

Anlage 2
zu § 5 Absatz 1

Bekanntmachung über die Bestellung von örtlichen Beauftragten für den Datenschutz und deren Stellvertretung gemäß § 36 Absatz 1 DSG-EKD

Frau/Herr .....
(Vorname, Name, ggf. Organisationseinheit / Arbeitsbereich)

ist mit Wirkung vom .....

☐ zum / zur örtlich Beauftragten für den Datenschutz

☐ zur Vertretung der / des örtlich Beauftragten für den Datenschutz

bestellt und ist in dieser Eigenschaft unmittelbar ..... unterstellt.

Die Zuständigkeit der/des örtlich Beauftragten für Datenschutz erstreckt sich auf:

Ev.-luth. Kirchenkreis ..... ,

Ev.-luth. Kirchenkreis ..... ,

Ev.-luth. Kirchenkreis ..... ,

Kirchenkreisverband .....
sowie auf die Körperschaften, die der Aufsicht der vorgenannten Kirchenkreise unterstehen.

Zu den Aufgaben gehören insbesondere die Beratung der Mitarbeitenden in allen Fragen des Datenschutzes sowie die Information und Schulung der Mitarbeitenden, die personenbezogene Daten verarbeiten. Darüber hinaus überwachen sie die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen und beraten die verantwortliche Stelle bei der Datenschutz-Folgenabschätzung.

Frau/Herr .....
ist bei der Erfüllung der Aufgaben zu unterstützen:

- Die notwendigen Auskünfte sind zu erteilen,
- die Einsicht in Unterlagen ist zu gestatten, soweit dies zur Aufgabenerfüllung erforderlich ist,
- Informationen über neue oder geänderte Datenverarbeitungs-Verfahren sowie über die Einführung oder Änderung von Regelungen und Maßnahmen zur Verarbeitung personenbezogener Daten sind frühzeitig bekannt zu geben, damit eine Beratung aus Sicht des Datenschutzes ermöglicht wird.

Betroffene Personen und Mitarbeitende können sich in Angelegenheiten des Datenschutzes jederzeit ohne Einhaltung des Dienstweges an die örtlich Beauftragte oder den örtlich Beauftragten sowie im Verhinderungsfall an die Vertretung wenden.

.....

(Ort, Datum, Unterschrift)

Merkblatt Örtlich Beauftragte für den Datenschutz

1. Verantwortung, Kontrolle und Unterstützung

Die Verantwortung für den Datenschutz in einer kirchlichen Stelle (Kirchengemeinden, Kirchenkreise und alle anderen kirchlichen Körperschaften) trägt die Dienststellenleitung. Sie hat die Einhaltung der allgemeinen und bereichsspezifischen Datenschutzbestimmungen und die Rechtmäßigkeit der Verarbeitung personenbezogener Daten sicherzustellen. Das bedeutet, dass sie auch Vorsorge für die Einhaltung oder Maßnahmen zur Umsetzung datenschutzrechtlicher Bestimmungen treffen muss.

Die oder der örtlich Beauftragte für den Datenschutz unterstützt die Leitung in dieser Aufgabe und prüft die Umsetzung des Datenschutzes in der Praxis.

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

Die örtlich Beauftragten für den Datenschutz können Verstöße gegen datenschutzrechtliche Bestimmungen feststellen und Abhilfe verlangen, und sie können datenschutzkonforme Verfahren anregen. Sie haben jedoch keine Befugnis, ihre Forderungen gegenüber den einzelnen Mitarbeitenden durchzusetzen. Diese Aufgabe obliegt der Leitung der jeweiligen kirchlichen Stelle.

Die Leitung ist verantwortlich dafür, dass die Mitarbeitenden in ihrem Zuständigkeitsbereich in einer datenschutzgerechten Art und Weise arbeiten.

Eine Leitung, die aktiv Datenschutz betreibt, erfüllt den berechtigten Anspruch, den die betroffenen Personen, wie z.B. Gemeindeglieder, Eltern von Kindern in Kindertagesstätten, Mitarbeitende in den Kirchengemeinden und Kirchenkreisen, Klienten von Beratungsstellen o.a. haben.

2. Bestellung von örtlichen Datenschutzbeauftragten

Nach § 36 Abs. 1 DSG-EKD müssen bei allen kirchlichen Stellen örtlich Beauftragte für den Datenschutz bestellt werden. Die Landeskirche hat durch Rechtsverordnung (RVO-DS-Beauftragte) festgelegt, dass die Kirchenkreise für die Bestellung zuständig sind. Dabei soll allerdings

angestrebt werden, dass die Beauftragten zumindest für den Zuständigkeitsbereich eines Kirchen(kreis)amtes gemeinsam bestellt werden. Unabhängig von der Sprengelzuordnung kann der oder die Beauftragte aber auch für den Zuständigkeitsbereich mehrerer Kirchen(kreis)ämter bestellt werden. Die oder der örtlich Beauftragte muss Mitarbeiterin oder Mitarbeiter einer kirchlichen Körperschaft sein, die zu ihrem oder seinem Zuständigkeitsbereich gehört.

Ebenso ist in der RVO-DS-Beauftragte festgelegt, dass der oder die Beauftragte in erforderlichem Umfang von den sonstigen dienstlichen Tätigkeiten freigestellt wird. Für den zeitlichen Umfang wird ein Aufwand von 1 Stunde/Woche je 60.000 Gemeindeglieder und 2 Stunden/ Woche je 400 Beschäftigte zugrunde gelegt.

Werden größere Einheiten gebildet, werden die Stundenumfänge kumuliert, der Anteil der Tätigkeit als örtlich Beauftragte oder örtlich Beauftragter erhöht sich entsprechend. Hierüber sind entsprechende Vereinbarungen nach dem Muster der Anlage 1 zu § 2 Absätze 3 und 4 RVO-DS-Beauftragte zu treffen.

In den Vorschriften des DSG-EKD ist vorgesehen, dass die Abwesenheitsvertretung der örtlichen Beauftragten für den Datenschutz zu regeln ist. In den meisten Fällen dürfte es sich anbieten, dass die Vertretung durch einen anderen örtlich Beauftragten in örtlicher Nähe wahrgenommen wird. Nach § 2 Abs. 5 RVO-DS-Beauftragte ist es zulässig, dass die Vertretung aus dem Zuständigkeitsbereich eines anderen Kirchen(kreis)amtes kommt.

3. Anforderungen an örtliche Datenschutzbeauftragte

Nach den gesetzlichen Vorgaben dürfen zu örtlich Beauftragten nur Personen bestellt werden, die die zur Erfüllung ihrer Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzen (§ 36 Abs. 3 DSG-EKD). Die oder der örtlich Beauftragte für den Datenschutz muss danach in fachlicher und persönlicher Hinsicht für die Aufgabe geeignet sein.

Sollte die Fachkunde bei der Bestellung noch nicht vorliegen, so ist dafür Sorge zu tragen, dass sie zeitnah erworben wird. Gerade zu Beginn der Tätigkeit soll Gelegenheit zur Teilnahme an geeigneter Fortbildung gegeben werden. Hierzu gehören insbesondere die vom Beauftragten für den Datenschutz der EKD (BfD-EKD) angebotenen Fortbildungsveranstaltungen.

Zur Fachkunde gehört die Kenntnis der datenschutzrechtlichen Grundlagen. Dies sind insbesondere die Datenschutzbestimmungen

– im Kirchengesetz über den Datenschutz in der Evangelischen Kirche in Deutschland (DSG-EKD),

– im Datenschutz-Anwendungsgesetz (DSAG),
– in der Datenschutzdurchführungsverordnung (DATVO),
– in der IT-Sicherheitsverordnung (ITSVO-EKD).

Örtlich Beauftragte müssen über IT-Grundkenntnisse verfügen. Darüber hinaus richten sich die weiteren konkreten IT-Anforderungen nach der Aufgabe der jeweiligen kirchlichen Stelle, der vorhandenen IT und der Art der verarbeiteten Daten.

Außerdem müssen die Beauftragten Kenntnisse über die Organisation und Arbeitsabläufe der von ihnen jeweils betreuten kirchlichen Stelle haben.

Im Hinblick auf die persönliche Zuverlässigkeit werden Kompetenzen wie Konfliktfähigkeit, Urteilsvermögen und (Selbst-)Organisation gefordert.

Örtlich Beauftragte unterliegen der Verschwiegenheit gemäß § 36 Abs. 1 i. V. m. §§ 42 Abs. 6 und 7 DSG-EKD. Die Verpflichtung zur Verschwiegenheit besteht auch nach Beendigung der Tätigkeit fort. Ohne Genehmigung des Dienstherrn dürfen örtlich Beauftragte über diese Angelegenheiten weder vor Gericht noch außergerichtlich aussagen oder Erklärungen abgeben.

Die Verschwiegenheitspflicht gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Offenkundig sind z. B. Tatsachen, wenn sie auch unbeteiligten Dritten z.B. durch Presse, Rundfunk oder sonstige Veröffentlichungen bekannt geworden sind.

4. Vermeidung von Interessenkollisionen

Die örtlich Beauftragten für den Datenschutz dürfen während ihrer Tätigkeit nicht mit Aufgaben betraut sein, deren Wahrnehmung zu Interessenkollisionen führen könnten. So sollen sie beispielsweise nicht gleichzeitig mit der Leitung der Datenverarbeitung beauftragt sein oder die Leitung der kirchlichen Stelle wahrnehmen.

5. Bestellung, Bekanntmachung, Kündigungsschutz, Ausscheiden aus dem Dienst, Befristung

Örtlich Beauftragte sind gemäß § 36 Abs. 5 Satz 1 DSG-EKD schriftlich zu bestellen. Hierfür ist das Muster der Anlage 1 zu verwenden. In der Bestellung müssen die einzelnen Kirchenkreise und die bestehenden Kirchen-

kreisverbände genannt werden, für die der oder die örtlich Beauftragte für den Datenschutz zuständig ist.

Damit die örtlich Beauftragten ihre Aufgabe im vollen Umfang erfüllen können, muss ihre Bestellung den Beschäftigten bekannt gemacht werden. Die RVO-DS-Beauftragte sieht hierfür in der Anlage 2 einen entsprechenden Vordruck vor. Die Kontaktdaten der oder des örtlich Beauftragten sind gemäß § 36 Abs. 5 Satz 1, 2. Halbsatz DSG-EKD zu veröffentlichen.

Eine unabhängige und organisatorisch besondere Stellung ist für eine wirkungsvolle Tätigkeit der örtlich Beauftragten von entscheidender Bedeutung. Deshalb können sich die örtlich Beauftragten jederzeit unmittelbar an die Leitung der jeweiligen kirchlichen Stelle wenden und sind nur ihr gegenüber rechenschaftspflichtig. Dies ermöglicht es der Leitung, dass sie frühzeitig über Beeinträchtigungen der Datensicherheit, Gesetzesverstöße oder Verbesserungsvorschläge unterrichtet wird und entsprechend schnell reagieren kann.

Arbeitsrechtlich sind die örtlich Beauftragten unmittelbar nur der Leitung ihrer Anstellungskörperschaft unterstellt. Bei der Bestellung für die Zuständigkeitsbereiche mehrerer Kirchen(kreis)ämter sind entsprechende Regelungen in den Vereinbarungen zwischen den Kirchenkreisen zu treffen.

Die örtlich Beauftragten sind in der Wahrnehmung ihrer Aufgabe gemäß § 37 Abs. 1 Satz 2 DSG-EKD weisungsfrei. Die Erledigung ihrer Aufgaben organisieren sie selbst. Die Ergebnisse teilen sie – soweit sie es für erforderlich halten – der verantwortlichen Dienststellenleitung mit.

Eine Benachteiligung der örtlich Beauftragten wegen dieser Tätigkeit ist gemäß § 37 Abs. 1 DSG-EKD verboten. Dieses Benachteiligungsverbot ist weit gefasst. Es richtet sich nicht nur an die Leitung, sondern auch an die Mitarbeitenden und die Mitarbeitervertretung. Auch darf die Tätigkeit als örtlich Beauftragte oder Beauftragter keine negativen Auswirkungen auf die berufliche Entwicklung derjenigen haben, die diese Funktion ausüben.

Der oder die örtlich Beauftragte unterliegt einem besonderen Kündigungsschutz. Gemäß § 37 Abs. 2 Satz 2 DSG-EKD ist die Kündigung des Arbeitsverhältnisses einer oder eines örtlich Beauftragten nur zulässig, wenn Tatsachen vorliegen, die zur Kündigung aus wichtigem Grund berechtigen. Dieser Kündigungsschutz gilt auch für Kündigungen binnen eines Jahres nach Beendigung der Bestellung fort. Eine Abberufung der örtlichen Beauftragten ist nur unter den Voraussetzungen des § 626 BGB möglich (§ 37 Abs. 2 Satz 1 DSG-EKD).

Mit dem Ausscheiden der oder des örtlich Beauftragten aus dem Dienst- oder Arbeitsverhältnis einer kirchlichen Stelle endet auch die Bestellung. Es ist möglich, die Bestellung von vornherein zeitlich zu befristen. Es gilt

eine Mindestfrist von drei Jahren gemäß § 36 Abs. 3 Satz 2 DSG-EKD. Eine einvernehmliche Beendigung der Bestellung ist jederzeit möglich.

6. Aufgaben der örtlich Beauftragten für den Datenschutz

Die örtlich Beauftragten beraten und unterstützen die Leitung der kirchlichen Stelle und die Arbeitsbereiche, die personenbezogene Daten verarbeiten, in allen Fragen des Datenschutzes und der Datensicherheit sowie der datenschutzgerechten Organisation. Hierzu gehört auch die frühzeitige Beteiligung bei der Erstellung und der kontinuierlichen Fortschreibung eines IT-Sicherheitskonzeptes für die in der kirchlichen Stelle eingesetzte Informationstechnik. Insoweit arbeiten die örtlich Beauftragten mit dem Arbeitsbereich IT zusammen.

Die konkreten Beteiligungsrechte hierzu ergeben sich auch aus der IT-Sicherheitsverordnung der EKD (§§ 3, 5 Abs. 3 Nr. 8 IT-Sicherheitsverordnung). In diesem Zusammenhang obliegt den Datenschutzbeauftragten auch die Prüfung der getroffenen technischen und organisatorischen Maßnahmen gemäß § 27 Abs. 1 DSG-EKD. Allerdings sind die örtlich Beauftragten für den Datenschutz selbst nicht verantwortlich für die Gewährleistung von IT-Sicherheit.

Eine enge Zusammenarbeit mit der Leitung der kirchlichen Stelle kann dadurch gefördert werden, dass regelmäßig Gespräche darüber geführt werden, wie ein angemessener Datenschutz umgesetzt wird, welche Schwachpunkte in der jeweiligen kirchlichen Stelle bestehen und wie diese auszuräumen sind.

Die örtlich Beauftragten stellen Informationen zu datenschutzrechtlichen Themen über geeignete Kanäle und Medien bereit. Sie führen Schulungen im Rahmen der allgemeinen Aus- und Fortbildung durch (§ 38 Nr. 3 DSG-EKD). Denkbar sind auch Berichte in Gremien und bei Mitarbeiterversammlungen.

Darüber hinaus sollen sie bei Projekten mit datenschutzrelevanten Komponenten beteiligt werden. Verantwortliche Stellen müssen gemäß § 37 Abs. 6 DSG-EKD sicherstellen, dass örtlich Beauftragte ordnungsgemäß und frühzeitig bei allen mit dem Schutz personenbezogener Daten zusammenhängenden Fragen beteiligt werden, insbesondere bei der Planung und Entwicklung von IT-Verfahren zur Verarbeitung personenbezogener Daten.

Örtlich Beauftragte überwachen insbesondere die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen (§ 38 Satz 2 Nr. 2 DSG-EKD). Gemäß § 38 Satz 2 Nr. 5 DSG-EKD haben die örtlich Beauftragten die verantwortliche Stelle bei der Datenschutz-Folgenabschätzung zu beraten und deren Durchführung zu überwachen.

Örtlich Beauftragte sind zu beteiligen bei

- dem Erstellen von Satzungen, Dienstvereinbarungen, Geschäftsordnungen, Richtlinien und Rundschreiben;
- der Entwicklung von Formularen, Makros und Datenbanken, mit denen personenbezogene Daten verarbeitet werden;
- der Einführung und dem Betrieb von IT-Verfahren zur Verarbeitung personenbezogener Daten (z. B. Beratung und Mitarbeit bei der Erstellung einer Risikoanalyse, Abschätzung der Folgen und der Prüfung der rechtlichen Zulässigkeit des Verfahrens);
- der Formulierung von Verträgen, deren Gegenstand die Verarbeitung personenbezogener Daten ist (vgl. § 3 Abs. 3 DATVO).

Im Rahmen der Auftragsverarbeitung können die örtlich Beauftragten auch mit der Überwachung der Auftragnehmer gemäß § 30 Abs. 3 Satz 3 beauftragt werden. Bei einer Videoüberwachung sind die Datenschutzbeauftragten nach § 34 Abs. 2 DSG-EKD zur Beratung heranzuziehen.

Örtlich Beauftragte müssen mit der Aufsichtsbehörde zusammenarbeiten (§ 38 Satz 2 Nr. 4 DSG-EKD).

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

Um den örtlich Beauftragten eine sachgerechte Aufgabenerfüllung zu ermöglichen, sind sie durch das Gesetz mit verschiedenen Kompetenzen ausgestattet. Gemäß § 37 Abs. 1 Satz 3 DSG-EKD kann die oder der örtlich Beauftragte für den Datenschutz Auskünfte verlangen und Einsicht in Unterlagen nehmen, soweit dies zur Erfüllung der Aufgaben erforderlich ist.

Verordnung zur Sicherheit der Informationstechnik (IT-Sicherheitsverordnung – ITSVO-EKD) vom 29. Mai 2015 (ABl. EKD S. 146)

Der Rat der Evangelischen Kirche in Deutschland hat auf Grund des § 9 Absatz 2 Satz 2 des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) in der Fassung der Neubekanntmachung vom 1. Januar 2013 (ABl. EKD 2013, S. 2 und S. 34) mit Zustimmung der Kirchenkonferenz folgende Rechtsverordnung erlassen:

§ 1

IT-Sicherheit

(1) Die mit der Informationstechnik (IT) erhobenen oder verarbeiteten Daten sind insbesondere vor unberechtigtem Zugriff, vor unerlaubten Änderungen und vor der Gefahr des Verlustes zu schützen (IT-Sicherheit), um deren Vertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten.

(2) Zur Umsetzung der IT-Sicherheit haben die Evangelische Kirche in Deutschland, ihre Gliedkirchen und ihre gliedkirchlichen Zusammenschlüsse sowie die ihnen zugeordneten kirchlichen und diakonischen Werke und Einrichtungen ohne Rücksicht auf deren Rechtsform und rechtsfähige evangelische Stiftungen des bürgerlichen Rechts (kirchliche Stellen) sicherzustellen, dass ein IT-Sicherheitskonzept erstellt und kontinuierlich fortgeschrieben wird. Dabei ist den unterschiedlichen Gegebenheiten der kirchlichen Stellen Rechnung zu tragen.

(3) Der für die Umsetzung des IT-Sicherheitskonzeptes erforderliche Sicherheitsstandard orientiert sich an den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur Informationssicherheit und zum IT-Grundschutz. Andere vergleichbare Sicherheitsstandards können zu Grunde gelegt werden. Das IT-Sicherheitskonzept muss den Schutzbedarf der Daten, die Art der eingesetzten IT und die örtlichen Gegebenheiten der jeweiligen kirchlichen Stelle berücksichtigen.

(4) Die Evangelische Kirche in Deutschland stellt Muster-IT-Sicherheitskonzepte nach Maßgabe des Absatzes 3 zur Verfügung.

§ 2

Einsatz von IT

(1) Mindestvoraussetzungen für den Einsatz von IT sind, dass

1. ein Anforderungsprofil und eine Dokumentation vorliegen,
2. die datenschutzrechtlichen Anforderungen eingehalten werden,
3. die Systeme vor ihrem Einsatz getestet wurden.

(2) Für die mit IT-Sicherheit verarbeiteten Daten soll dienstliche IT genutzt werden. Private IT-Geräte dürfen zugelassen werden, wenn durch Vereinbarung insbesondere sichergestellt ist, dass

1. eine Rechtsgrundlage für die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten gegeben ist,
2. das kirchliche Datenschutzrecht Anwendung findet,
3. die notwendigen technischen und organisatorischen Maßnahmen zur IT-Sicherheit und zum Datenschutz getroffen und Regelungen zur Verantwortung vereinbart worden sind und
4. eine Haftung des Dienstgebers ausgeschlossen ist, wenn im Zusammenhang mit dienstlichen Anwendungen Schäden auf privaten IT-Geräten, insbesondere Datenverlust, entstehen.

Die Zulassung ist zu widerrufen, wenn ein Verstoß gegen Satz 2 festgestellt oder die IT-Sicherheit durch den Einsatz privater IT gefährdet oder beeinträchtigt wird und andere Maßnahmen nicht zur Behebung ausreichen.

§ 3

Beteiligung

Bei der Erstellung und der kontinuierlichen Fortschreibung des IT-Sicherheitskonzeptes und bei der Entscheidung zur Auswahl über IT, mit der personenbezogene Daten verarbeitet werden, sind Betriebsbeauftragte oder örtlich Beauftragte für den Datenschutz frühzeitig zu beteiligen.

§ 4

Einhaltung der IT-Sicherheit

(1) Kirchliche Stellen haben durch angemessene Schulungs- und Fortbildungsmöglichkeiten den qualifizierten Umgang mit IT zu ermöglichen.

(2) Die Verantwortung für die IT-Sicherheit liegt beim Leitungsorgan der jeweiligen kirchlichen Stelle. Die aufsichtführenden Stellen oder Personen überwachen die Einhaltung dieser Verordnung. Bei Verstößen sind geeignete Maßnahmen zu ergreifen. § 5 bleibt unberührt.

(3) Maßnahmen der oder des Beauftragten für den Datenschutz nach § 20 DSG-EKD bleiben unberührt.

§ 5

IT-Sicherheitsbeauftragte

(1) Mit der Wahrnehmung der IT-Sicherheit können kirchliche Stellen besondere Personen beauftragen (IT-Sicherheitsbeauftragte). Die Beauftragung kann mehrere kirchliche Stellen umfassen.

(2) Zu Beauftragten sollen nur Personen bestellt werden, die die zur Erfüllung ihrer Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzen.

(3) Zu den Aufgaben der die IT-Sicherheit wahrnehmenden Person zählen insbesondere:

1. den IT-Sicherheitsprozess beratend zu begleiten und bei allen damit zusammenhängenden Aufgaben mitzuwirken,
2. die Erstellung und kontinuierliche Fortschreibung eines IT-Sicherheitskonzeptes zu koordinieren,
3. Regelungen zur IT-Sicherheit vorzuschlagen,
4. die Durchführung von IT-Sicherheitsmaßnahmen zu empfehlen und zu überprüfen,
5. IT-Sicherheitsvorfälle zu untersuchen und Handlungsempfehlungen auszusprechen,
6. IT-Schulungen zu initiieren und zu koordinieren,
7. dem Leitungsorgan der jeweiligen kirchlichen Stelle regelmäßig über den Stand der IT-Sicherheit sowie über ihre Tätigkeiten zu berichten und
8. mit den Betriebsbeauftragten oder den örtlich Beauftragten für den Datenschutz zusammenzuarbeiten.

(4) Die die Aufgaben der IT-Sicherheit wahrnehmende Person ist über IT-Sicherheitsvorfälle zu informieren und informiert bei Gefahr im Verzug unverzüglich das zuständige Leitungsorgan.

§ 6

Durchführungs- und Ergänzungsbestimmungen

(1) Die Evangelische Kirche in Deutschland, die Gliedkirchen und die gliedkirchlichen Zusammenschlüsse können jeweils für ihren Bereich Durchführungsbestimmungen zu dieser Verordnung und ergänzende Bestimmungen zur IT-Sicherheit erlassen, soweit sie dieser Verordnung nicht widersprechen.

(2) Bestehende Regelungen bleiben unberührt, soweit sie dieser Verordnung nicht widersprechen. Anderenfalls sind diese Regelungen innerhalb eines Jahres anzupassen.

§ 7

Übergangsbestimmungen

Die erstmalige Erstellung des IT-Sicherheitskonzeptes gemäß § 1 Absatz 2 hat in ihren Grundzügen spätestens bis zum 31. Dezember 2015 zu erfolgen und deren vollständige Umsetzung bis zum 31. Dezember 2017.

§ 8

Inkrafttreten

Diese Verordnung tritt am Tage nach der Verkündung in Kraft.

Verpflichtung von Mitarbeitenden auf das Datengeheimnis

Frau/Herr

_____

wird mit Aushändigung und unter Hinweis auf das anliegende Merkblatt wie folgt auf das Datengeheimnis gemäß § 26 DSG-EKD verpflichtet:

Es ist untersagt, personenbezogene Daten unbefugt zu verarbeiten (Datengeheimnis).

Das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.

Verstöße gegen das Datengeheimnis sind Pflichtverletzungen und können dienstrechtlich, arbeitsrechtlich, urheberrechtlich, strafrechtlich und disziplinarrechtlich geahndet werden sowie Haftungstatbestände auslösen.

_____

Ort, Datum

_____

Unterschrift der/des Mitarbeitenden

_____

Unterschrift der Vertreterin/des Vertreters der kirchlichen Stelle

Original zur Akte

Kopie an den Mitarbeitenden

Merkblatt über den Datenschutz für Mitarbeitende in der evangelisch-lutherischen Landeskirche Hannovers

In diesem Merkblatt erhalten Sie Informationen über den wesentlichen Inhalt des Datengeheimnisses und den Sinn der Verpflichtungserklärung. Die Erläuterungen und Hinweise müssen im jeweiligen Zusammenhang, der sich aus Anwendungsfragen der täglichen Arbeit sowie den jeweils geltenden Rechtsvorschriften ergibt, gesehen werden.

Welche rechtlichen Grundlagen gelten für den Datenschutz?

Zunächst gelten die allgemeinen Datenschutzbestimmungen. Dies sind jeweils in ihrer geltenden Fassung:

- das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD),
- die IT-Sicherheitsverordnung der Evangelischen Kirche in Deutschland (ITSVO-EKD),
- das Kirchengesetz zur Ergänzung und Durchführung des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (DSAG),
- die Rechtsverordnung zur Ergänzung und Durchführung datenschutzrechtlicher Vorschriften (DATVO),
- die Rechtsverordnung über die Bestellung von örtlich Beauftragten für den Datenschutz (RVO-DS-Beauftragte).

Außerdem gelten Bestimmungen, die den allgemeinen Regelungen zum Datenschutz vorgehen, wie etwa die besonderen Regelungen über den Schutz des Beicht- und Seelsorgegeheimnisses, die Amtsverschwiegenheit sowie sonstige gesetzliche Geheimhaltungs- und Verschwiegenheitspflichten oder von Berufs- bzw. besonderen Amtsgeheimnissen, die nicht auf gesetzliche Vorschriften beruhen sowie andere Rechtsvorschriften wie etwa das Digitalgesetz, die die Verarbeitung personenbezogener Daten regeln.

Sie finden die kirchlichen Datenschutzvorschriften in der Rechtssammlung der hannoverschen Landeskirche unter **www.kirchenrecht-evlka.de**. In gleicher Weise sind künftige Rechts- und Verwaltungsvorschriften sowie Veröffentlichungen der evangelisch-lutherischen Landeskirche Hannovers und der Evangelischen Kirche in Deutschland zu den Bereichen Datenschutz und IT-Sicherheit zu beachten.

Warum ist Datenschutz wichtig?

Niemand darf durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt werden. Jeder hat das Recht, über den Umgang mit seinen personenbezogenen Daten grundsätzlich selbst zu bestimmen. Das Ziel des Datenschutzes ist es, den Einzelnen vor einer Beeinträchtigung zu schützen.

Was sind personenbezogene Daten?

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; identifizierbar ist eine natürliche Person, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Personenbezogene Daten sind z. B. Geburtsdatum, Anschrift, Konfession, Beruf, Familienstand, Gesundheitszustand, Fotos, Videoaufzeichnungen, Grundbesitz, Einkommen oder Rechtsbeziehungen zu Dritten.

Nach § 2 Absatz 2 DSG-EKD können sie in Akten und Aktensammlungen enthalten sein oder bei automatisierten Verarbeitungen anfallen. Beispiele für automatisierte Verarbeitungen sind Programme aus den Bereichen Textverarbeitung, Tabellenkalkulation und Datenbanken.

Zu beachten ist, dass personenbezogene Daten auch beim Einsatz von mobilen Endgeräten, Videoüberwachungen, automatischen Schließsystemen und weiteren technischen Anwendungen anfallen.

Welche grundsätzlichen Regelungen gelten für den Datenschutz?

Die Verarbeitung personenbezogener Daten ist nur rechtmäßig, wenn das DSG-EKD oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder soweit die betroffene Person eingewilligt hat (Grundsatz des Verbots mit Erlaubnisvorbehalt).

Personenbezogene Daten dürfen für die Erfüllung kirchlicher Aufgaben verarbeitet werden. Maßgebend sind die herkömmlichen oder durch das kirchliche Recht bestimmten Aufgaben auf dem Gebiet der Verkündigung, Seelsorge, Diakonie und Unterweisung sowie der kirchlichen Verwaltung (einschließlich Gemeinde- und Pfarrbüro).

Personenbezogene Daten sind gemäß § 5 DSG-EKD nach folgenden Grundsätzen zu verarbeiten:

- Rechtmäßigkeit, Verhältnismäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz;
- Zweckbindung: Personenbezogene Daten werden für festgelegte, eindeutige und legitime Zwecke erhoben. Sie dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Eine Weiterverarbeitung für im kirchlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszecke oder für statistische Zwecke gilt als vereinbar mit den ursprünglichen Zwecken;
- Datenminimierung: Die Verarbeitung personenbezogener Daten wird auf das dem Zweck angemessene und notwendige Maß beschränkt; personenbezogene Daten sind zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert;
- Richtigkeit: Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden;
- Speicherbegrenzung: Personenbezogene Daten werden in einer Form gespeichert, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Personenbezogene Daten dürfen länger gespeichert werden, soweit sie für die Zwecke des Archivs, der wissenschaftlichen und historischen Forschung sowie der Statistik verarbeitet werden;
- Integrität und Vertraulichkeit: Personenbezogene Daten werden in einer Weise verarbeitet, die eine angemessene Sicherheit gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Zerstörung oder unbeabsichtigter Schädigung.

Die verantwortliche Stelle muss die Einhaltung der Grundsätze nachweisen können (Rechenschaftspflicht).

Mündliche, elektronische und schriftliche Auskünfte aus Akten oder Datenbanken sowie die Offenlegung von personenbezogenen Daten (z. B. Kopien von Listen, Datenträgern und Akten) sind zulässig an kirchliche Stellen, andere öffentlich-rechtliche Religionsgesellschaften sowie

an Behörden und sonstige öffentliche Stellen des Bundes, der Länder, der Gemeinden etc., soweit eine Rechtsgrundlage für die Offenlegung der Daten vorhanden ist und sie zur Erfüllung kirchlicher Aufgaben erforderlich sind (siehe auch § 8 DSG-EKD).

Die Offenlegung der Daten an sonstige Stellen oder Personen ist nur in Ausnahmefällen statthaft (siehe auch § 9 DSG-EKD). Auskünfte zur geschäftlichen oder gewerblichen Verwendung der Daten dürfen ohne Einwilligung der betroffenen Person in keinem Fall gegeben werden.

Widersprüche von betroffenen Personen, die sich gegen die Verarbeitung ihrer personenbezogenen Daten richten, sind zu beachten – Ausnahmen regeln die kirchlichen Vorschriften sowie § 25 DSG-EKD.

Alle Informationen, die Mitarbeitende auf Grund ihrer Arbeit an und mit Akten, Dateien und Listen erhalten, sind vertraulich zu behandeln. Diese Pflicht besteht auch nach Beendigung der Tätigkeit fort. Personenbezogene Daten dürfen nur kirchlichen Mitarbeitenden zugänglich gemacht werden, die auf Grund ihrer dienstlichen Aufgaben zum Empfang der Daten berechtigt sind.

Die Mitarbeitenden sind für die datenschutzrechtlich korrekte Ausübung ihrer Tätigkeit verantwortlich. Die sorgsame und vertrauliche Behandlung von Daten ist ein wichtiges Gebot im Rahmen der kirchlichen Arbeit.

Sofern Sie im Zusammenhang mit Ihrer Tätigkeit Zugang zu Sozialdaten haben, ist das Sozialgeheimnis zu wahren (§ 35 SGB I). Sozialdaten sind personenbezogene Daten, die von einem Sozialleistungsträger, etwa der Renten-, Pflege- oder Krankenversicherung oder einem Jugendhilfeträger, im Hinblick auf deren Aufgaben verarbeitet werden (§ 67 Abs. 2 SGB X).

Eine Übermittlung von Sozialdaten an eine nicht-öffentliche Stelle ist auf deren Ersuchen hin nur zulässig, wenn diese sich gegenüber der übermittelnden Stelle verpflichtet hat, die Daten nur für den Zweck zu verarbeiten, zu dem sie ihr übermittelt werden. Die Dritten haben die Daten in demselben Umfang geheim zu halten wie die übermittelnde Stelle.

In § 78 Abs. 2 SGB X ist bestimmt, dass die in den nicht-öffentlichen Stellen beschäftigten Personen, die diese Daten speichern, verändern, nutzen, übermitteln, in der Verarbeitung einschränken oder löschen, von dieser Stelle auf die Einhaltung dieser Pflichten hinzuweisen sind (siehe auch § 36 DATVO).

Was ist aus Sicht des technischen und organisatorischen Datenschutzes zu beachten?

Wenn personenbezogene Daten verarbeitet werden, sind die technischen und organisatorischen Maßnahmen gemäß §§ 27, 28 DSG-EKD zu beachten.

Landeskirchliche Bestimmungen sowie Regelungen und Hinweise zum Datenschutz und zur Datensicherheit aus bestehenden Dienst- und Organisationsanweisungen sind zu befolgen.

Eigenmächtige Änderungen der dienstlichen Hardware und deren Konfiguration – insbesondere der Einbau von Karten und der Anschluss von Druckern oder anderen Zusatzgeräten – sind ebenso wie das unbefugte Einspielen von privater Software nicht gestattet. Wenn der Einsatz privater IT-Geräte durch Vereinbarung mit der kirchlichen Stelle zugelassen ist, dürfen diese eingesetzt werden (§ 2 Absatz 2 ITSVO-EKD).

Soweit aus Gründen der Aufgabenerfüllung Daten mittels eines Datenträgers auf einen PC übertragen werden, ist durch geeignete Maßnahmen sicherzustellen, dass die auf dem Datenträger enthaltenen Daten nicht mit Schadsoftware befallen sind.

Es ist untersagt, Passwörter und Hardwaretoken (z. B. USB-Stick und Chipkarten) sowie Benutzerkennungen weiterzugeben.

Daten (z. B. Belege, EDV Listen), Datenträger (z. B. Festplatten, USB-Sticks, DVDs) und Zubehör (z. B. Schlüssel) sind stets sicher und verschlossen zu verwahren und vor jeder Einsicht oder sonstigen Nutzung durch Unbefugte zu schützen.

Analoge und digitale Daten, die nicht mehr benötigt werden, müssen in einer Weise vernichtet oder gelöscht werden, die jeden Missbrauch der Daten ausschließt.

Mängel, die bei der Datenverarbeitung auffallen, müssen dem Dienstvorgesetzten gemeldet werden. Dies gilt auch für den Fall, dass in den Bereichen Datenschutz und Datensicherheit unzureichende technische und organisatorische Maßnahmen ergriffen wurden. Es wird empfohlen, die örtlich Beauftragten für den Datenschutz zu beteiligen. Unabhängig davon können sich Mitarbeitende auch ohne Einhaltung des Dienstweges vertraulich an den Beauftragten für den Datenschutz der EKD wenden.

Welche strafrechtlichen Konsequenzen können mir im Einzelfall drohen?

Bestimmte Handlungen, die einen Verstoß gegen das Datengeheimnis beinhalten, stellen Straftatbestände dar. Danach kann mit Freiheitsstrafe oder mit Geldstrafe beispielsweise bestraft werden, wer

- unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft (§ 202a StGB „Ausspähen von Daten“),
- Passwörter Dritten verkauft oder überlässt oder entsprechende Computerprogramme installiert (§ 202c StGB „Vorbereiten des Ausspähens und Abfangens von Daten“),
- unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihr oder ihm anvertraut wurde in Ausübung der Berufe Ärztin oder Arzt (oder Angehörige oder Angehöriger eines anderen Heilberufs), Psychologin oder Psychologe, Ehe-, Familien-, Erziehungs- oder Jugendberaterin und -berater sowie Beraterinnen und Berater für Suchtfragen in einer Beratungsstelle, Mitglieder einer anerkannten Beratungsstelle nach dem Schwangerschaftskonfliktgesetz, Sozialarbeiterinnen und Sozialarbeiter (§ 203 StGB „Verletzung von Privatgeheimnissen“),
- rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert (§ 303a StGB „Datenveränderung“).

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

Wo erhält man weitere Auskünfte?

Wenn Sie weitere Fragen zum Datenschutz haben oder in einem Einzelfall eine Rechtsauskunft benötigen, wenden Sie sich an die Dienstvorgesetzten oder an die örtlich Beauftragte oder den örtlich Beauftragten für den Datenschutz. Eine Liste der in der evangelisch-lutherischen Landeskirche Hannovers bestellten örtlichen Datenschutzbeauftragten finden Sie unter:

www.landeskirche-hannovers.de/evlka-de/meta/service/datenschutz.

Die Aufgabe der Aufsichtsbehörde obliegt der oder dem Beauftragten für den Datenschutz der EKD. Weitere Informationen und die Kontaktdaten erhalten Sie im Internet unter:

https://datenschutz.ekd.de.

Verpflichtung von Ehrenamtlichen auf das Datengeheimnis

Frau/Herr

_____

wird als Ehrenamtliche/Ehrenamtlicher mit Aushändigung und unter Hinweis auf das anliegende Merkblatt wie folgt auf das Datengeheimnis gemäß § 26 DSG EKD verpflichtet:

Es ist untersagt, personenbezogene Daten unbefugt zu verarbeiten (Datengeheimnis).

Das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.

Verstöße gegen das Datengeheimnis sind Pflichtverletzungen und können rechtliche Konsequenzen haben.

_____

Ort, Datum

_____

Unterschrift der/des Ehrenamtlichen

_____

Unterschrift der Vertreterin/des Vertreters der kirchlichen Stelle

Original zur Akte

Kopie an die Ehrenamtliche/den Ehrenamtlichen

Merkblatt über den Datenschutz für Ehrenamtliche

Wenn Sie als Ehrenamtliche oder Ehrenamtlicher in Kirche oder Diakonie regelmäßig mit personenbezogenen Daten umgehen, muss diejenige Stelle, für die Sie tätig sind, Sie auf das Datengeheimnis verpflichten. In diesem Merkblatt erhalten Sie einige Informationen über den wesentlichen Inhalt des Datengeheimnisses und den Sinn der Verpflichtungserklärung.

Welchen Grund hat die Verpflichtung auf das Datengeheimnis?

Wer seine persönlichen Daten einer kirchlichen Stelle oder diakonischen Einrichtung anvertraut, hat einen Anspruch darauf, dass mit diesen Daten verantwortlich umgegangen wird. Dies gilt etwa für den Umgang mit den Daten von Mitgliedern der Kirchengemeinde oder Hilfesuchenden im diakonischen Bereich, aber auch für den Umgang mit den Inhalten eines vertraulich geführten Gesprächs. Beruflich Mitarbeitende in Kirche und Diakonie sind zumeist durch Kirchengesetz, Arbeitsrechtsregelung, Dienst- oder Arbeitsvertrag zur Verschwiegenheit verpflichtet. Für Ehrenamtliche gelten diese Bestimmungen in der Regel nicht. Deshalb sind auch Ehrenamtliche auf das Datengeheimnis zu verpflichten.

Die Verpflichtungserklärung sollte nicht als Ausdruck eines grundsätzlichen Misstrauens gegenüber Ehrenamtlichen missverstanden werden. Sie ist vielmehr ein Qualitätsmerkmal für die ehrenamtlich geleistete Arbeit! Denn für die betroffene Person (z. B. Mitglied der Kirchengemeinde, Klient) ist es oft sehr wichtig, darüber Gewissheit zu haben, dass über ihre Daten Verschwiegenheit gewahrt wird. Ein vertrauliches Gespräch wird ohne diese Gewissheit nicht zustande kommen. Dabei macht es aus Sicht der betroffenen Person keinen Unterschied, ob das Gespräch mit einer Pastorin, einem Pastor oder mit Ehrenamtlichen geführt wird.

Alle personenbezogenen Informationen, die Sie im Rahmen Ihrer Tätigkeit an und mit Akten, Dateien, Listen und Karteien oder über Gespräche erhalten, sind grundsätzlich vertraulich zu behandeln. Diese Pflicht besteht auch nach Beendigung Ihrer Tätigkeit fort.

Weshalb ist Datenschutz notwendig?

Ziel des Datenschutzes ist es, jede einzelne Person davor zu schützen, dass sie durch den Umgang mit ihren personenbezogenen Daten in ihrem Persönlichkeitsrecht beeinträchtigt wird.

Auf dieser Grundlage regelt das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG EKD), unter welchen Voraussetzungen Daten verwendet werden dürfen. Die Rechte der betroffenen

Personen sind in diesem Gesetz näher beschrieben. Ebenso ist festgelegt, wer über die Einhaltung der Datenschutzvorschriften wacht.

Was sind personenbezogene Daten?

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen. Dazu gehören z. B. Name, Geburtsdatum, Anschrift, Beruf, Familienstand, Konfession, Gesundheitszustand sowie Fotos und Videoaufzeichnungen. Wenn Sie etwa als Mitglied eines Besuchskreises Gespräche mit einem Gemeindemitglied führen, handelt es sich bei dem, was Ihre Gesprächspartner*innen Ihnen über sich selbst oder über eine andere Person erzählt, um personenbezogene Daten. Diese Daten werden durch die Datenschutzregelungen besonders geschützt.

Welche rechtlichen Grundlagen gelten für den kirchlichen Datenschutz?

Durch das Datengeheimnis wird es denjenigen, die mit personenbezogenen Daten umgehen, untersagt, diese Daten unbefugt zu verarbeiten. Was dies im Einzelnen bedeutet, wird durch die jeweils geltenden Datenschutzbestimmungen festgelegt. Es sind insbesondere die folgenden grundlegenden Bestimmungen zum Datenschutz zu beachten:

a) das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG EKD),

b) die IT-Sicherheitsverordnung der Evangelischen Kirche in Deutschland (ITSVO-EKD)

c) das Kirchengesetz zur Ergänzung und Durchführung des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (DSAG),

d) die Rechtsverordnung zur Ergänzung und Durchführung datenschutzrechtlicher Vorschriften (DATVO)

e) die Rechtsverordnung über die Bestellung von örtlich Beauftragten für den Datenschutz (RVO-DS-Beauftragte).

Sie finden diese Vorschriften in der Online-Rechtssammlung der Landeskirche unter: **www.kirchenrecht-evlka.de**.

Was bedeutet die Verarbeitung von personenbezogenen Daten?

Die Verarbeitung personenbezogener Daten umfasst jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Spei-

cherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung von Daten. Auch die Einschränkung der Verarbeitung, das Löschen oder die Vernichtung von Daten gehören dazu.

Wann ist die Verarbeitung von personenbezogenen Daten zulässig?

Die Verarbeitung personenbezogener Daten ist nur zulässig,

- wenn das kirchliche Datenschutzrecht oder
- wenn eine andere Rechtsvorschrift dies erlaubt oder anordnet oder
- soweit die betroffene Person eingewilligt hat.

Das kirchliche Recht sieht vor, dass

- Daten nur in dem Umfang verarbeitet werden dürfen, wie dies zur Wahrnehmung Ihrer ehrenamtlichen Tätigkeit erforderlich ist,
- Daten grundsätzlich nur zu dem Zweck verarbeitet werden dürfen, für den sie erhoben worden sind,
- Daten auch innerhalb der verantwortlichen Stelle nur solchen Personen bekannt gegeben werden dürfen, die diese zur Erfüllung ihrer Aufgaben benötigen und zur Verschwiegenheit verpflichtet sind,
- Auskünfte aus oder Kopien von Datensammlungen an Dritte außerhalb der eigenen verantwortlichen Stelle nur erteilt bzw. angefertigt werden dürfen, wenn eine Rechtsvorschrift dies erlaubt oder die betroffene Person eingewilligt hat.

Grundsätzlich haben Sie über alle personenbezogenen Daten, die Sie auf Grund ihrer Tätigkeit erfahren, Verschwiegenheit zu wahren. So ist es nicht zulässig, Familienmitglieder oder andere Personen über das Erfahrene zu informieren. Dies gilt nur dann nicht, wenn die betroffene Person diese Daten selbst öffentlich gemacht hat. Unabhängig davon dürfen Daten in keinem Fall zum Zwecke der Werbung an Versicherungen, Zeitungen oder Firmen herausgegeben werden.

Sofern Sie im Zusammenhang mit Ihrer Tätigkeit Zugang zu Sozialdaten haben, ist das Sozialgeheimnis zu wahren. Sozialdaten sind personenbezogene Daten, die von einem Sozialleistungsträger im Hinblick auf seine Aufgaben verarbeitet werden. Zu Sozialdaten gehören u.a. der Pflegegrad einer Person oder personenbezogene Daten der Renten-, Pflege- oder Krankenversicherung.

Welche Maßnahmen sind aus Gründen des Datenschutzes und der Datensicherheit zu treffen?

Um den Anforderungen des kirchlichen Datenschutzes zu genügen, sind auch technische und organisatorische Maßnahmen zu treffen. Bitte bewahren Sie deshalb alle Informationen mit personenbezogenen Daten (z. B. Notizzettel, Karteikarten, USB-Sticks) stets sicher und verschlossen auf, damit ein unbefugter Zugriff Dritter nach Möglichkeit ausgeschlossen ist.

Falls Sie personenbezogene Daten auf Ihren privaten Endgeräten (z. B. Laptop, Smartphone, Tablet) speichern wollen, müssen Sie dies vorher mit der verantwortlichen Stelle absprechen. Dadurch soll sichergestellt werden, dass alle rechtlichen und technischen Vorgaben eingehalten werden. Folgende Maßnahmen sind mindestens notwendig:

- Benutzerkennung und Passwortschutz,
- Familienangehörige oder andere Personen dürfen keinen Zugriff auf die kirchlichen Daten haben (so können z. B. separate Benutzerkonten eingerichtet werden),
- Programm- und Browserversionen sind stets aktuell zu halten,
- Virenschutzprogramme sind regelmäßig zu aktualisieren,
- der Einsatz einer Firewall ist zu empfehlen,
- nur für Ihre Arbeit erforderliche Daten dürfen gespeichert werden,
- nicht mehr benötigte Datenbestände sind sicher zu löschen,
- Datensicherungen sind regelmäßig durchzuführen,
- Mail-Anhänge mit personenbezogenen Daten sind vor dem Versand zu verschlüsseln,
- sensible personenbezogene Daten auf privaten Endgeräten sind stets verschlüsselt zu speichern. Dies gilt auch für Datensicherungen.

Wo erhält man weitere Auskünfte?

Wenn Sie weitere Fragen zum Datenschutz haben oder in einem Einzelfall eine Rechtsauskunft benötigen, wenden Sie sich an die hauptamtlichen Mitarbeitenden oder an die örtlich Beauftragte oder den örtlich Beauftragten für den Datenschutz. Den Namen und die Kontaktdaten erhalten Sie über die verantwortliche Stelle, die Sie für Ihre Aufgabe beauftragt.

Die Aufgabe der Datenschutzaufsicht obliegt der oder dem Beauftragten für den Datenschutz der EKD. Weitere Informationen und die Kontaktdaten erhalten Sie über das Internet unter **https://datenschutz.ekd.de**.

Vereinbarung zur Auftragsverarbeitung personenbezogener Daten durch eine andere kirchliche Stelle

Diese Vereinbarung ist nur abzuschließen, soweit die Auftragsverarbeitung nicht bereits durch Satzung oder aufgrund einer sonstigen Rechtsgrundlage geregelt ist. Dieses Muster ist nicht abschließend und kann für den Einzelfall angepasst werden.

zwischen

Bezeichnung der auftraggebenden kirchlichen Stelle

Straße Hausnummer

Postleitzahl Ort

– nachfolgend bezeichnet als Auftraggeberin –

und

Bezeichnung der auftragnehmenden kirchlichen Stelle

Straße Hausnummer

Postleitzahl Ort

– nachfolgend bezeichnet als Auftragnehmerin –

Vorbemerkung

Sofern ein Vertrag über die zu erbringende Leistung und Abrechnung der Auftragsverarbeitung zwischen den kirchlichen Stellen geschlossen wurde, gilt diese Vereinbarung zusätzlich zum Hauptvertrag. Fehlt ein schriftlicher Hauptvertrag, konkretisiert diese Vereinbarung die Auftragsinhalte und dokumentiert insbesondere die datenschutzrechtlichen Verpflichtungen beider kirchlicher Stellen bei der Durchführung der Auftragsverarbeitung. Dieses Muster kann für den Einzelfall angepasst werden.

§ 1 Gegenstand und Dauer der Vereinbarung

(1) Ein Hauptvertrag wurde geschlossen am [Datum].

(2) Sofern kein schriftlicher Hauptvertrag geschlossen wurde, bzw. die Inhalte der Auftragsverarbeitung dort nicht näher beschrieben sind, werden folgende Aufgaben vereinbart:

[Beschreibung der Aufgaben, z.B. Druckaufträge, IT-Administration, Botendienste]

(3) Diese Vereinbarung gilt ab dem [Datum] und endet nach der Beendigung des Hauptvertrages (sofern vorhanden). Soweit kein schriftlicher Hauptvertrag besteht, wird diese Vereinbarung auf unbestimmte Zeit mit einer Kündigungsfrist von [Fristangabe] zum Ende eines Monats/Quartals/Jahres geschlossen.

(4) Die Vereinbarung gilt sowohl für die Verarbeitung von Daten, welche die Auftraggeberin an die Auftragnehmerin übergibt, als auch für Daten, die im Auftrag der Auftraggeberin erstmalig durch die Auftragnehmerin verarbeitet werden.

§ 2 Umfang, Art und Zweck der Datenverarbeitung

Die Auftraggeberin bleibt im datenschutzrechtlichen Sinn verantwortliche Stelle gemäß § 30 Abs. 1 Satz 1 DSG-EKD. Die zu verarbeitenden Daten werden wie folgt festgelegt:

a) Art der personenbezogenen Daten bzw. der Datenkategorien

[z.B. Personenstammdaten, Kommunikationsdaten (Telefonnummern, E-Mail-Adressen), Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse, Kundenhistorie, Abrechnungs- und Zahlungsdaten), Planungs- und Steuerungsdaten, Buchhaltung: Rechnungsdaten, Lieferantendaten, Debitor*innen, Kreditor*innen, Adressdaten, Bankverbindungen, Gläubiger-ID, Ansprechpartner*innen bei Lieferant*innen, Steuernummern]

b) Umfang, Art und Zweck der Verarbeitung von Daten

[z.B. Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung]

c) Kreis der betroffenen Personen bzw. der Personenkategorien

[z.B. Gemeindemitglieder, Mitarbeitende, Patient*innen, Ehrenamtliche, Abonnent*innen, Lieferant*innen, Pächter*innen, Mieter*innen, Ansprechpersonen, Teilnehmende]

§ 3 Rechte und Pflichten sowie Weisungsbefugnis der Auftraggeberin

(1) Die Verarbeitung der Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung der Auftraggeberin. Die Auftragnehmerin wird die Weisungen der Auftraggeberin beach-

ten und befolgen. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren.

(2) Die Auftraggeberin erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem elektronischen Format zu bestätigen.

(3) Zur Erteilung und zum Empfang von Weisungen sind ausschließlich die im Anhang genannten Personen berechtigt. Die Kontaktdaten der/s örtlich Beauftragten für den Datenschutz bei der Auftraggeberin und die Kontaktdaten der/s örtlich Beauftragten für den Datenschutz bei der Auftragnehmerin sind im Anhang dieser Vereinbarung anzugeben.

(4) Bei einer Änderung, einem Wechsel oder einer dauerhaften Verhinderung einer benannten Person ist dies der anderen Partei unverzüglich schriftlich unter Benennung einer Nachfolge bzw. einer Vertretung mitzuteilen.

§ 4 Pflichten der Auftragnehmerin

(1) Die Auftragnehmerin darf die Daten nur im Rahmen der Weisungen der Auftraggeberin verarbeiten. Ist sie der Ansicht, dass eine Weisung der Auftraggeberin gegen das EKD-Datenschutzgesetz oder andere Vorschriften über den Datenschutz verstößt, hat sie die Auftraggeberin unverzüglich darauf hinzuweisen. Die Auftragnehmerin ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch die Auftraggeberin nach Überprüfung bestätigt oder geändert wird.

(2) Auskünfte an Dritte oder betroffene Personen darf die Auftragnehmerin nur nach vorheriger Zustimmung durch die Auftraggeberin erteilen. Soweit sich eine betroffene Person unmittelbar an die Auftragnehmerin wendet, wird die Auftragnehmerin die betroffene Person an die Auftraggeberin verweisen und das Ersuchen unverzüglich an die Auftraggeberin weiterleiten.

(3) Ist die Auftraggeberin gegenüber einer betroffenen Person verpflichtet, Auskünfte zur Auftragsverarbeitung zu erteilen, so unterstützt die Auftragnehmerin die Auftraggeberin auf eigene Kosten.

(4) Die Auftragnehmerin verwendet die Daten ausschließlich für die festgelegten Zwecke. Die Auftragnehmerin stellt sicher, dass weder Inhalte noch Arbeitsergebnisse Unbefugten zur Kenntnis gelangen. Diese Verpflichtung besteht auch nach Beendigung der Auftragsver-

arbeitung fort. Kopien dürfen nur mit Zustimmung der Auftraggeberin erstellt werden. Davon ausgenommen sind Sicherheitskopien zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung, sowie Daten zur Erfüllung gesetzlicher Aufbewahrungspflichten.

(5) Die Auftragnehmerin hat die konkreten Orte der Leistungserbringung stets aktuell zu dokumentieren und auf Verlangen der Auftraggeberin nachzuweisen. Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Eine Verlagerung der Datenverarbeitung in ein Drittland ist der Auftraggeberin anzuzeigen. Sind die Voraussetzungen gemäß § 10 DSG-EKD nicht gegeben, steht der Auftraggeberin ein außerordentliches Kündigungsrecht zu.

(6) Die Auftraggeberin kann während der Laufzeit der Vereinbarung jederzeit die Herausgabe ihrer Daten verlangen. Die Auftragnehmerin stellt bei der Übermittlung einen angemessenen Schutz durch geeignete technische und organisatorische Maßnahmen sicher.

(7) Eine Datenverarbeitung in Privatwohnungen ist nur mit schriftlicher Zustimmung der Auftraggeberin zulässig. Soll dies erfolgen, sind geeignete technische und organisatorische Maßnahmen zum Schutz der Daten vorab festzulegen. Es ist sicherzustellen, dass der Auftraggeberin und der/dem Beauftragten für den Datenschutz der EKD Zugang zur Wohnung gewährt wird. Die Auftragnehmerin sichert zu, dass auch die anderen Bewohner*innen dieser Privatwohnung mit der Regelung einverstanden sind.

§ 5 Mitteilungs- und Unterstützungspflichten der Auftragnehmerin

(1) Die Auftragnehmerin wird die Auftraggeberin unverzüglich benachrichtigen, wenn Hinweise auf Verletzung des Schutzes personenbezogener Daten (Datenpanne) durch die Auftragnehmerin oder ihre Unterauftragnehmerinnen oder durch die bei der Auftragnehmerin oder ihren Unterauftragnehmerinnen beschäftigten Personen oder ein entsprechender Verdacht bekannt werden. Die Benachrichtigungspflicht gilt auch bei schwerwiegenden Betriebsstörungen (technischer oder organisatorischer Art) oder anderen Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten. Die Benachrichtigung hat unverzüglich zu erfolgen.

(2) Die Auftragnehmerin hat in diesen Fällen angemessene Maßnahmen zur Sicherung der Daten und zur Minderung möglicher Schäden für betroffene Personen zu ergreifen. Die Auftraggeberin ist über

die getroffenen Maßnahmen zu informieren. Die Auftragnehmerin unterstützt die Auftraggeberin kostenfrei bei einer eventuell erforderlichen Benachrichtigung der betroffenen Personen.

(3) Bei der Erfüllung der Rechte der betroffenen Personen nach §§ 16 bis 25 DSG-EKD durch die Auftraggeberin, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgenabschätzungen der Auftraggeberin hat die Auftragnehmerin im notwendigen Umfang mitzuwirken und die Auftraggeberin soweit möglich angemessen zu unterstützen.

(4) Über Kontrollen und Maßnahmen der oder des Beauftragten für den Datenschutz der EKD informiert die Auftragnehmerin die Auftraggeberin unaufgefordert und unverzüglich, sofern hierdurch die Datenverarbeitung der Auftraggeberin betroffen ist.

§ 6 Unterauftragsverhältnisse

(1) Die Auftragnehmerin erbringt die vertraglichen Leistungen ausschließlich durch folgende Unterauftragnehmerinnen:

[Art der Leistung, Name und Kontaktdaten]

(2) Die Beauftragung weiterer Unterauftragnehmerinnen zur Verarbeitung von Daten der Auftraggeberin ist der Auftragnehmerin nur mit Zustimmung der Auftraggeberin gestattet. Erfolgt eine Unterbeauftragung ohne vorherige Zustimmung, so steht der Auftraggeberin ein außerordentliches Kündigungsrecht zu.

(3) Die Auftragnehmerin informiert die Auftraggeberin über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Unterbeauftragungen, wodurch die Auftraggeberin die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Eine Beauftragung von Unterauftragnehmerinnen in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen des § 10 Abs. 1 DSG-EKD erfüllt sind (Angemessenheitsbeschluss der EU-Kommission, Standarddatenschutzklauseln).

(4) Die Verträge der Auftragnehmerin mit den Unterauftragnehmerinnen sind so zu gestalten, dass sie den Anforderungen gesetzlicher Datenschutzbestimmungen genügen und dass die Unterauftragnehmerinnen dieselben Verpflichtungen übernehmen, die der Auftragnehmerin obliegen.

(5) Die Auftragnehmerin haftet für das Handeln der Unterauftragnehmerinnen wie für eigenes Handeln.

(6) Die Verträge und Auftragsvereinbarungen sind auf Verlangen der Auftraggeberin in Kopie zu übergeben.

(7) Dienstleistungen Dritter, die als Nebenleistungen zur Auftragsdurchführung in Anspruch genommen werden, gelten nicht als Unterauftragsverhältnisse. Dazu zählen z. B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungspersonal, Rechnungs- oder Wirtschaftsprüfung, Entsorgung von Datenträgern. Die Auftragnehmerin ist jedoch bei derartiger Inanspruchnahme verpflichtet, angemessene Vereinbarungen zum Schutz der Daten zu treffen und auch Kontrollmaßnahmen durchzuführen.

§ 7 Rückgabe von Datenträgern, Löschung gespeicherter Daten und Dokumentation

(1) Nach Abschluss der vereinbarten Arbeiten oder mit der Beendigung des Hauptvertrages oder dieser Vereinbarung haben die Auftragnehmerin sowie alle Unterauftragnehmerinnen die in ihrem Besitz befindlichen Unterlagen, Verarbeitungsergebnisse und Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, der Auftraggeberin auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu löschen bzw. zu vernichten.

(2) Gleiches gilt für Daten in Archivierungs- und Sicherungsdateien in allen Systemen der Auftragnehmerin und der Unterauftragnehmerinnen sowie für Test- und Ausschussmaterial.

(3) Die datenschutzgerechte Löschung ist zu protokollieren und das Löschprotokoll ist vorzulegen.

§ 8 Haftung

Es gelten die Regelungen zum Schadensersatz gemäß § 48 DSG-EKD.

§ 9 Schlussbestimmungen

(1) Änderungen oder Ergänzungen der Vereinbarung, die unmittelbar den Inhalt oder den Umfang der geschuldeten Leistung beeinflussen, bedürfen der Schriftform.

(2) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind von der Auftragnehmerin entsprechend den jeweiligen gesetzlichen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Die Auftragnehmerin kann diese zu ihrer Entlastung bei Vertragsende der Auftraggeberin aushändigen.

(3) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für die Auftraggeberin verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(4) Sollte eine der Regelungen oder eine mit Bezug hierauf geschlossene weitere Vereinbarung, gleich wann und aus welchem Grund, unwirksam sein oder werden oder eine nach übereinstimmender Auffassung der Parteien regelungsbedürftige Lücke enthalten, berührt dies die Wirksamkeit der übrigen Regelungen nicht. Anstelle der unwirksamen Regelung oder in Ausfüllung der Lücke gelten die gesetzlichen Bestimmungen.

Auftraggeberin	Auftragnehmerin
(Ort, Datum)	(Ort, Datum)
(Unterschriften mit Amts-/Funktionsbezeichnungen)	(Unterschriften mit Amts-/Funktionsbezeichnungen)

Anhang

Berechtigte Weisungsgeber/in, Weisungsempfänger/in, Datenschutzbeauftragte

1. Zur Erteilung von Weisungen für die Auftraggeberin ist folgende Person berechtigt:

   [Name, Funktion, Anschrift, Telefon, Fax, E-Mail]

   Als örtlich Beauftragte/r für den Datenschutz bei der Auftraggeberin ist bestellt:

   [Name, Anschrift, Telefon, Fax, E-Mail]

2. Zum Empfang von Weisungen für die Auftragnehmerin ist folgende Person berechtigt:

   [Name, Funktion, Anschrift, Telefon, Fax, E-Mail]

   Als örtlich Beauftragte/r für den Datenschutz bei der Auftragnehmerin ist bestellt:

   [Name, Anschrift, Telefon, Fax, E-Mail]

Vereinbarung zur Auftragsverarbeitung personenbezogener Daten durch eine nicht kirchliche Stelle

Diese Vereinbarung ist nicht abzuschließen, soweit es sich um die Inanspruchnahme fremder Fachleistungen handelt, bei denen die Datenverarbeitung nicht im Vordergrund steht (Beispiele hierzu siehe Webseite der Landeskirche zum Datenschutz). Dieses Muster ist nicht abschließend und kann für den Einzelfall angepasst werden.

zwischen

Bezeichnung der auftraggebenden kirchlichen Stelle

Straße Hausnummer

Postleitzahl Ort

– nachfolgend bezeichnet als Auftraggeberin –

und

Bezeichnung der auftragnehmenden kirchlichen Stelle

Straße Hausnummer

Postleitzahl Ort

– nachfolgend bezeichnet als Auftragnehmerin –

§ 1 Gegenstand und Dauer der Vereinbarung

(1) Ein Hauptvertrag wurde geschlossen am [Datum].

(2) Diese Vereinbarung gilt ab dem [Datum] und endet nach der Beendigung des Hauptvertrages mit der Übergabe oder der Vernichtung aller personenbezogenen Daten der auftraggebenden kirchliche Stelle gemäß dieser Vereinbarung, ohne dass es einer gesonderten Kündigung dieser Vereinbarung bedarf.

(3) Die Vereinbarung wird wirksam am [Datum] und endet am [Datum].

oder:

Die Vereinbarung wird auf unbestimmte Zeit mit einer Kündigungsfrist von [Fristangabe] zum Ende eines Monats/Quartals/Jahres geschlossen.

(4) Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung der verantwortlichen Stelle und darf nur erfolgen, wenn die besonderen Voraussetzungen des § 10 DSG-EKD erfüllt sind (z. B. Angemessenheitsbeschluss der EU-Kommission, Verwendung von Standarddatenschutzklauseln).

(5) Die Auftraggeberin kann die Vereinbarung und den Hauptvertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß der Auftragnehmerin gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegen.

(6) Die Vereinbarung gilt sowohl für die Verarbeitung von Daten, welche die Auftraggeberin an die Auftragnehmerin übergibt, als auch für Daten, die im Auftrag der Auftraggeberin erstmalig durch die Auftragnehmerin verarbeitet werden.

§ 2 Umfang, Art und Zweck der Datenverarbeitung

(1) Die Auftraggeberin bleibt im datenschutzrechtlichen Sinn verantwortliche Stelle gemäß § 30 Abs. 1 Satz 1 DSG-EKD.

a) Art der personenbezogenen Daten bzw. Datenkategorien

[z.B. Personenstammdaten, Kommunikationsdaten (Telefonnummern, E-Mail-Adressen), Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse, Kundenhistorie, Abrechnungs- und Zahlungsdaten), Planungs- und Steuerungsdaten, Buchhaltung: Rechnungsdaten, Lieferantendaten, Debitor*innen, Kreditor*innen, Adressdaten, Bankverbindungen, Gläubiger-ID, Ansprechpartner*innen bei Lieferant*innen, Steuernummern]

b) Umfang, Art und Zweck der Verarbeitung von Daten

[z.B. Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung]

c) Kreis der betroffenen Personen bzw. der Personenkategorien

[z.B. Gemeindemitglieder, Mitarbeitende, Patient*innen, Ehrenamtliche, Abonnent*innen, Lieferant*innen, Pächter*innen, Mieter*innen, Ansprechpersonen, Teilnehmende]

§ 3 Rechte und Pflichten sowie Weisungsbefugnis der Auftraggeberin

(1) Die Verarbeitung der Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung der Auftraggeberin. Die Auftraggeberin behält sich ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung im Rahmen der gemäß der Vereinbarung durchgeführten Auftragsverarbeitung vor, das sie durch Einzelweisungen konkretisieren kann. Die Auftragnehmerin wird die Weisungen der Auftraggeberin einer angemessenen Nachkontrolle auf Richtigkeit und Plausibilität unterziehen. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren.

(2) Die Auftraggeberin erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem elektronischen Format zu bestätigen.

(3) Die Auftraggeberin hat das Recht, die nach § 30 Abs. 3 Satz 3 DSG-EKD vorgesehene Überprüfung durchzuführen oder durch im Einzelfall zu benennende Personen durchführen zu lassen. Sie hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch die Auftragnehmerin in deren Geschäftsbetrieben zu überzeugen. Die Auftragnehmerin verpflichtet sich, der Auftraggeberin auf Anforderung die zur Wahrung ihrer Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen. Die Prüfungs-, Zutritts- und Auskunftsrechte stehen auch der oder dem Beauftragten für den Datenschutz der EKD zu.

(4) Die Auftraggeberin verpflichtet sich, alle im Rahmen dieser Vereinbarung erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der Auftragnehmerin vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieser Vereinbarung bestehen.

(5) Zur Erteilung und zum Empfang von Weisungen sind ausschließlich die im Anhang genannten Personen berechtigt. Die Kontaktdaten der/s örtlich Beauftragten für den Datenschutz der Auftraggeberin und der/s Datenschutzbeauftragten der Auftragnehmerin sind im Anhang dieser Vereinbarung anzugeben.

(6) Bei einer Änderung, einem Wechsel oder einer dauerhaften Verhinderung einer benannten Person ist dies der anderen Partei unverzüg-

lich schriftlich unter Benennung einer Nachfolge bzw. einer Vertretung mitzuteilen.

§ 4 Pflichten der Auftragnehmerin

(1) Die Auftragnehmerin darf die Daten nur im Rahmen der Weisungen der Auftraggeberin verarbeiten. Ist sie der Ansicht, dass eine Weisung der Auftraggeberin gegen das EKD-Datenschutzgesetz oder andere Vorschriften über den Datenschutz verstößt, hat sie die Auftraggeberin unverzüglich darauf hinzuweisen. Die Auftragnehmerin ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch die Auftraggeberin nach Überprüfung bestätigt oder geändert wird.

(2) Auskünfte an Dritte oder betroffene Personen darf die Auftragnehmerin nur nach vorheriger Zustimmung durch die Auftraggeberin erteilen. Soweit sich eine betroffene Person unmittelbar an die Auftragnehmerin wendet, wird die Auftragnehmerin die betroffene Person an die Auftraggeberin verweisen und das Ersuchen unverzüglich an die Auftraggeberin weiterleiten.

(3) Ist die Auftraggeberin gegenüber einer betroffenen Person verpflichtet, Auskünfte zur Auftragsverarbeitung zu erteilen, so unterstützt die Auftragnehmerin die Auftraggeberin auf eigene Kosten.

(4) Im Hinblick auf die Kontrollverpflichtungen der Auftraggeberin nach § 30 Abs. 3 Satz 3 DSG-EKD und im Wege der Datenschutz-Folgenabschätzung nach § 34 DSG-EKD stellt die Auftragnehmerin sicher, dass sich die Auftraggeberin von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist die Auftragnehmerin der Auftraggeberin auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß § 27 DSG-EKD nach.

(5) Die Auftragnehmerin verpflichtet sich, das Datengeheimnis zu wahren und für die Datenverarbeitung nur solche Beschäftigten oder sonstigen Personen einzusetzen, die auf das Datengeheimnis verpflichtet worden sind. Die Verpflichtung von Beschäftigten oder sonstigen Personen auf das Datengeheimnis hat unter Hinweis auf die möglichen Folgen des Verstoßes gegen datenschutzrechtliche Pflichten zu erfolgen. Auf Verlangen der Auftraggeberin weist die Auftragnehmerin die Verpflichtung der Beschäftigten und sonstigen Personen nach.

(6) Die Auftragnehmerin verwendet die Daten ausschließlich für die festgelegten Zwecke. Die Auftragnehmerin stellt sicher, dass weder Inhalte noch Arbeitsergebnisse Unbefugten zur Kenntnis gelangen. Diese Verpflichtung besteht auch nach Beendigung der Auftragsver-

arbeitung fort. Kopien dürfen nur mit Zustimmung der Auftraggeberin erstellt werden. Davon ausgenommen sind Sicherheitskopien zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung, sowie Daten zur Erfüllung gesetzlicher Aufbewahrungspflichten.

(7) Die Auftragnehmerin sichert für ihren Verantwortungsbereich zu, dass die nach § 1 dieser Vereinbarung durchzuführenden Tätigkeiten sämtliche datenschutzrechtlichen Vorschriften, denen die Auftraggeberin unterliegt, eingehalten werden. Die Auftragnehmerin ist verpflichtet, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch von der Auftraggeberin beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort.

(8) Die Auftragnehmerin unterstellt sich der Kontrolle der zuständigen kirchlichen Datenschutzaufsichtsbehörde. Diese Behörde nimmt insbesondere die Aufgaben nach § 43 DSG-EKD sowie die Befugnisse nach § 44 DSG-EKD unmittelbar gegenüber dem nichtkirchlichen Auftragsverarbeiter wahr.

(9) Die Auftragnehmerin hat die konkreten Orte der Leistungserbringung stets aktuell zu dokumentieren und auf Verlangen der Auftraggeberin nachzuweisen. Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Eine Verlagerung der Datenverarbeitung in ein Drittland ist der Auftraggeberin anzuzeigen. Sind die Voraussetzungen gemäß § 10 DSG-EKD nicht gegeben, steht der Auftraggeberin ein außerordentliches Kündigungsrecht zu.

(10) Die Auftraggeberin kann während der Laufzeit der Vereinbarung jederzeit die Herausgabe ihrer Daten verlangen. Die Auftragnehmerin stellt bei der Übermittlung einen angemessenen Schutz durch geeignete technische und organisatorische Maßnahmen sicher.

(11) Eine Datenverarbeitung in Privatwohnungen ist nur mit schriftlicher Zustimmung der Auftraggeberin zulässig. Soll dies erfolgen, sind geeignete technische und organisatorische Maßnahmen zum Schutz der Daten vorab festzulegen. Es ist sicherzustellen, dass der Auftraggeberin und der/dem Beauftragten für den Datenschutz der EKD Zugang zur Wohnung gewährt wird. Die Auftragnehmerin sichert zu, dass auch die anderen Bewohner*innen dieser Privatwohnung mit der Regelung einverstanden sind.

§ 5 Mitteilungs- und Unterstützungspflichten der Auftragnehmerin

(1) Die Auftragnehmerin wird die Auftraggeberin unverzüglich benachrichtigen, wenn Hinweise auf Verletzung des Schutzes personenbezogener Daten (Datenpanne) durch die Auftragnehmerin oder ihre Unterauftragnehmerinnen oder durch die bei der Auftragnehmerin oder ihren Unterauftragnehmerinnen beschäftigten Personen oder ein entsprechender Verdacht bekannt werden. Die Benachrichtigungspflicht gilt auch bei schwerwiegenden Betriebsstörungen (technischer oder organisatorischer Art) oder anderen Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten. Die Benachrichtigung hat unverzüglich zu erfolgen.

(2) Die Auftragnehmerin hat in diesen Fällen angemessene Maßnahmen zur Sicherung der Daten und zur Minderung möglicher Schäden für betroffene Personen zu ergreifen. Die Auftraggeberin ist über die getroffenen Maßnahmen zu informieren. Die Auftragnehmerin unterstützt die Auftraggeberin kostenfrei bei einer eventuell erforderlichen Benachrichtigung der betroffenen Personen.

(3) Ist die Auftraggeberin gegenüber einer betroffenen Person verpflichtet, Auskünfte zur Auftragsverarbeitung zu erteilen, so unterstützt die Auftragnehmerin die Auftraggeberin auf eigene Kosten.

(4) Die Auftragnehmerin wird die Auftraggeberin bei der Einhaltung der in den §§ 27, 31, 32, 33 und 34 DSG-EKD genannten Pflichten unterstützen. Die Auftragnehmerin wird die Auftraggeberin auch mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, dass die Auftraggeberin ihren Pflichten der in §§ 16 bis 25 DSG-EKD geregelten Rechte der betroffenen Person nachkommen kann.

(5) Über Kontrollen und Maßnahmen der oder des Beauftragten für den Datenschutz der EKD oder der staatlichen Datenschutzaufsichtsbehörden informiert die Auftragnehmerin die Auftraggeberin unaufgefordert und unverzüglich, sofern hierdurch die Datenverarbeitung der Auftraggeberin betroffen ist.

(6) Über Maßnahmen von Strafverfolgungsbehörden benachrichtigt die Auftragnehmerin die Auftraggeberin unaufgefordert und unverzüglich, soweit hierdurch die Datenverarbeitung für die Auftraggeberin betroffen ist oder sein kann. Die Benachrichtigungspflicht besteht nicht, soweit die Auftragnehmerin durch ihre Benachrichtigung gegen ein gesetzliches Verbot verstoßen würde.

§ 6 Unterauftragsverhältnisse

(1) Die Auftragnehmerin erbringt die vertraglichen Leistungen ausschließlich durch folgende Unterauftragnehmerinnen:

[Art der Leistung, Name und Kontaktdaten]

(2) Die Beauftragung weiterer Unterauftragnehmerinnen zur Verarbeitung von Daten der Auftraggeberin ist der Auftragnehmerin nur mit Zustimmung der Auftraggeberin gestattet. Erfolgt eine Unterbeauftragung ohne vorherige Zustimmung, so steht der Auftraggeberin ein außerordentliches Kündigungsrecht zu.

(3) Die Auftragnehmerin informiert die Auftraggeberin über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Unterbeauftragungen, wodurch die Auftraggeberin die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Eine Beauftragung von Unterauftragnehmerinnen in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen des § 10 Abs. 1 DSG-EKD erfüllt sind (Angemessenheitsbeschluss der EU-Kommission, Standarddatenschutzklauseln).

(4) Die Verträge der Auftragnehmerin mit ihren Unterauftragnehmerinnen sind so zu gestalten, dass sie den Anforderungen gesetzlicher Datenschutzbestimmungen genügen und dass die Unterauftragnehmerinnen dieselben Verpflichtungen übernehmen, die der Auftragnehmerin obliegen.

(5) Die Auftragnehmerin haftet für das Handeln von Unterauftragnehmerinnen wie für eigenes Handeln.

(6) Die Verträge und Auftragsvereinbarungen sind auf Verlangen der Auftraggeberin in Kopie zu übergeben.

(7) Dienstleistungen Dritter, die als Nebenleistungen zur Auftragsdurchführung in Anspruch genommen werden, gelten nicht als Unterauftragsverhältnisse. Dazu zählen z. B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungspersonal, Rechnungs- oder Wirtschaftsprüfung, Entsorgung von Datenträgern. Die Auftragnehmerin ist jedoch bei derartiger Inanspruchnahme verpflichtet, angemessene Vereinbarungen zum Schutz der Daten zu treffen und auch Kontrollmaßnahmen durchzuführen.

§ 7 Rückgabe von Datenträgern, Löschung gespeicherter Daten und Dokumentation

(1) Nach Abschluss der vereinbarten Arbeiten oder mit der Beendigung des Hauptvertrages oder dieser Vereinbarung haben die Auftrag-

nehmerin sowie alle Unterauftragnehmerinnen die in ihrem Besitz befindlichen Unterlagen, Verarbeitungsergebnisse und Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, der Auftraggeberin auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu löschen bzw. zu vernichten.

(2) Gleiches gilt für Daten in Archivierungs- und Sicherungsdateien in allen Systemen der Auftragnehmerin und der Unterauftragnehmerinnen sowie für Test- und Ausschussmaterial.

(3) Die datenschutzgerechte Löschung ist zu protokollieren und das Löschprotokoll ist vorzulegen.

§ 8 Haftung

Es gelten die Regelungen zum Schadensersatz gemäß § 48 DSG-EKD.

9. Schlussbestimmungen

(1) Änderungen oder Ergänzungen der Vereinbarung, die unmittelbar den Inhalt oder den Umfang der geschuldeten Leistung beeinflussen, bedürfen der Schriftform.

(2) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind von der Auftragnehmerin entsprechend den jeweiligen gesetzlichen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Die Auftragnehmerin kann diese zu ihrer Entlastung bei Vertragsende der Auftraggeberin aushändigen.

(3) Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten der Auftraggeberin bei der Auftragnehmerin durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat die Auftragnehmerin die Auftraggeberin unverzüglich zu verständigen.

(4) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für die Auftraggeberin verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(5) Sollte eine der Regelungen oder eine mit Bezug hierauf geschlossene weitere Vereinbarung, gleich wann und aus welchem Grund, unwirksam sein oder werden oder eine nach übereinstimmender Auffassung der Parteien regelungsbedürftige Lücke enthalten, berührt dies die Wirksamkeit der übrigen Regelungen nicht. Anstelle der unwirksamen Regelung oder in Ausfüllung der Lücke gelten die gesetzlichen Bestimmungen.

Auftraggeberin	Auftragnehmerin
(Ort, Datum)	(Ort, Datum)
(Unterschriften mit Amts-/Funktionsbezeichnungen)	(Firmenstempel)

Anhang

Berechtigte Weisungsgeber/in, Weisungsempfänger/in, Datenschutzbeauftragte

1. Zur Erteilung von Weisungen für die Auftraggeberin ist folgende Person berechtigt:

   [Name, Funktion, Anschrift, Telefon, Fax, E-Mail]

   Als örtlich Beauftragte/r für den Datenschutz bei der Auftraggeberin ist bestellt:

   [Name, Anschrift, Telefon, Fax, E-Mail]

2. Zum Empfang von Weisungen für die Auftragnehmerin ist folgende Person berechtigt:

   [Name, Funktion, Anschrift, Telefon, Fax, E-Mail]

   Als Datenschutzbeauftragte/r bei der Auftragnehmerin ist bestellt:

   [Name, Anschrift, Telefon, Fax, E-Mail]

Dokumentation der Einhaltung der bei der Auftragnehmerin getroffenen technischen und organisatorischen Maßnahmen

Dieses ist eine mögliche Checkliste für den Nachweis gemäß § 30 Abs. 2 S. 4 DSG-EKD. Das Muster ist nicht abschließend und kann für den Einzelfall angepasst werden.

1. Maßnahmen zur Sicherstellung der Vertraulichkeit

1.1. Maßnahmen, die Unbefugten den räumlichen Zutritt zu Datenverarbeitungsanlagen verwehren, mit denen personenbezogene Daten verarbeitet werden

a) Vorhandene Zutrittskontrollen zum Gebäude und den Büroräumen:

ja / nein

☐ / ☐ Personenkontrolle durch Pförtner / Empfang am Eingang

☐ / ☐ Besucherregelung mit Ausgabe von Besucherausweisen

☐ / ☐ Videoüberwachung aller Gebäudezugänge

☐ / ☐ Einbruchsmeldeanlage, informiert wird: .....

☐ / ☐ Schließsystem mit Berechtigungsregelung

☐ / ☐ Chipkarten-/Transponder-Schließsystem (z.B. RFID)

Protokollierung erfolgt für die Dauer von: .....

☐ / ☐ Regelungen zur Nachvollziehbarkeit der Schlüsselausgabe

☐ / ☐ Sonstiges:.....

b) Vorhandene Zutrittskontrollen zum Serverraum:

ja / nein

☐ / ☐ Personenbezogene Daten werden auf Server gespeichert

☐ / ☐ Gesonderte Zutrittsregelung für autorisiertes Personal

☐ / ☐ Der oder die Server befinden sich in der Dienststelle

Folgende Personen haben Zutritt: .....

☐ / ☐ Wird der Serverraum auch für andere Zwecke genutzt?

Wenn ja, welche:.....

☐ / ☐ Der oder die Server sind ausgelagert / angemietet:

1. Standort / Firma: .....

2. Standort / Firma: .....

☐ / ☐ Sonstiges: .....

1.2. Maßnahmen, die Unbefugten die Nutzung der Datenverarbeitungssysteme und die Verarbeitung von personenbezogenen Daten verwehren

a) Vorhandene Zugangskontrollen zu den Datenverarbeitungssystemen:

ja / nein

☐ / ☐ Die Systeme sind durch eine Firewall geschützt

☐ / ☐ Die Firewall wird regelmäßig aktualisiert

Durch: ☐ eigene IT ☐ Dienstleister

☐ / ☐ Der Zugriff von außen erfolgt über eine VPN-Verbindung

Zugang wird nach ..... erfolglosen Anmeldeversuchen

für ..... Min. gesperrt

☐ / ☐ Authentifizierung erfolgt durch Benutzername und Kennwort

Vorgaben sind:

mindestens: ☐ 6 Zeichen ☐ 8 Zeichen ☐ 10 Zeichen

zu verwenden sind:

☐ Sonderzeichen ☐ Ziffern ☐ Groß-/Kleinschreibung

Gültigkeitsdauer:

☐ 90 Tage ☐ bis 180 Tage ☐ mehr als 180 Tage

☐ / ☐ Das IT System zwingt zur Einhaltung der o. a. Vorgaben

☐ / ☐ Authentifizierung mit biometrischen Verfahren

☐ / ☐ Datenträger werden verschlüsselt. Verschlüsselung erfolgt bei:

☐ Notebooks ☐ mobilen Datenträgern ☐ Smartphones

☐ / ☐ Externe Schnittstellen (z.B. USB) werden auf mobilen Geräten gesperrt

☐ / ☐ Smartphones können durch zentrale Admin-Software zurückgesetzt werden

☐ / ☐ Einsatz von Anti-Viren-Software

☐ / ☐ Automatische Sperrmechanismen bei unautorisiertem Zugang

☐ / ☐ Protokollierung des Zugangs

☐ / ☐ Sonstiges: .....

b) Vorhandene Zugriffskontrollen zu personenbezogenen Daten:

ja / nein

☐ / ☐ Ein Berechtigungskonzept kommt zur Anwendung

☐ / ☐ Die Rechtevergabe wird nachvollziehbar protokolliert

Die Verwaltung der Rechte erfolgt durch: .....

☐ / ☐ Physisches Löschen von Datenträgern vor Weiterverwendung

☐ / ☐ Vernichtung von Datenträgern nach DIN 66399 (ggf. über zertifizierte Dienstleister)

☐ / ☐ Protokollierung der Vernichtung

☐ / ☐ Sonstiges: .....

1.3 Maßnahmen, die sicherstellen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennungskontrolle)

ja / nein

☐ / ☐ Trennung von Produktiv- und Testsystemen

☐ / ☐ Mandantentrennung

- ☐ / ☐ Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ☐ / ☐ Logische Mandantentrennung (softwareseitig)

☐ / ☐ Nutzung von Berechtigungskonzepten

☐ / ☐ Sonstiges: .....

2. Maßnahmen zur Sicherstellung der Integrität (Unversehrtheit von Daten)

Maßnahmen zur nachträglichen Feststellung, ob und von wem Daten eingegeben, verändert oder entfernt worden sind (Eingabekontrolle)

ja / nein

☐ / ☐ Vergabe und Dokumentation von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts inklusive Vererbungslogik

☐ / ☐ Protokollierung der Eingabe, der Änderung und der Löschung von Daten auf Basis individueller Benutzernamen

☐ / ☐ Sonstiges: .....

3. Maßnahmen zur Sicherstellung der Verfügbarkeit

Maßnahmen, die eine Zerstörung personenbezogener Daten verhindern, bzw. eine Wiederherstellung sicherstellen (Verfügbarkeitskontrolle)

ja / nein

☐ / ☐ Serverraum ist hochwassergeschützt

☐ / ☐ Serverraum befindet sich nicht unter sanitären Anlagen

☐ / ☐ Serverraum ist klimatisiert

☐ / ☐ Temperatur und Feuchtigkeit im Serverraum werden überwacht

☐ / ☐ Brandmeldeanlage ist vorhanden

☐ / ☐ Überspannungsschutz ist vorhanden

☐ / ☐ Unterbrechungsfreie Stromversorgung (USV) ist vorhanden

☐ / ☐ Notstromaggregat ist vorhanden

☐ / ☐ Alarmmeldung bei unberechtigten Zutritten zum Serverraum

☐ / ☐ Festplattenspiegelung (RAID System) ist eingerichtet

☐ / ☐ Backup- & Wiederherstellungskonzept ist vorhanden

Backup erfolgt: ☐ täglich ☐ wöchentlich ☐ monatlich

☐ / ☐ Test einer Datenwiederherstellung erfolgt regelmäßig

☐ / ☐ Backup-Datei/en ist/sind verschlüsselt

☐ / ☐ Datensicherung wird von den Servern räumlich getrennt aufbewahrt:

☐ Separater Brandabschnitt

☐ Anderer Standort

☐ / ☐ Prozesse für Software- und Patchmaßnahmen sind vorhanden

- ☐ werden regelmäßig durchgeführt
- ☐ werden dokumentiert
- ☐ werden durch eigene IT durchgeführt
- ☐ werden von einem Dienstleister durchgeführt

☐ / ☐ Notfallplan ist vorhanden (z.B. bei Brand, Hardwaredefekt)

☐ / ☐ Sonstiges: .....

4. Maßnahmen zur sicheren Datenübertragung

Maßnahmen, die sicherstellen, dass bei Übertragungen Unbefugte die Daten nicht lesen, kopieren, verändern oder entfernen können (Weitergabekontrolle)

ja / nein

☐ / ☐ Die Datenübertragung erfolgt für alle in diesem Auftrag relevanten Vorgänge elektronisch und zwar verschlüsselt per:

- ☐ Transportverschlüsselung
  - ☐ VPN-Tunnel (Virtual Private Network)
  - ☐ TLS/SSL (Transport Layer Security / Secure Sockets Layer)
  - ☐ SFTP (Secure File Transfer Protocol)
- ☐ Ende-zu-Ende-Verschlüsselung
  - ☐ SMime (Secure Multipurpose Internet Mail Extensions)
  - ☐ PGP (Pretty Good Privacy)
  - ☐ WinZip-Dateianhang an einer E-Mail

  .....

☐ / ☐ Abruf- und Übermittlungsvorgänge werden nachvollziehbar protokolliert und aufbewahrt:

- ☐ dauerhaft ☐ bis Auftragsende ☐ bis .....

☐ / ☐ Transport erfolgt physisch sicher verpackt auf einem Datenträger

☐ / ☐ Sonstiges: .....

**Zusatzvereinbarung zum Vertrag nach
Artikel 28 EU-Datenschutz-Grundverordnung (DSGVO)
zur Verarbeitung von personenbezogenen Daten im Auftrag**

zwischen

Bezeichnung der verantwortlichen kirchlichen Stelle

Straße Hausnummer

Postleitzahl Ort

– nachfolgend bezeichnet als Auftraggeberin –

und

Bezeichnung des Auftragsverarbeiters

Straße Hausnummer

Postleitzahl Ort

– nachfolgend bezeichnet als Auftragnehmerin –

In Ergänzung des zwischen den Parteien am [Datum] geschlossenen Vertrages zur Auftragsverarbeitung gemäß Artikel 28 EU-Datenschutz-Grundverordnung (DSGVO) erkennt die Auftragnehmerin gemäß § 30 Absatz 5 Satz 3 Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) die kirchliche Datenschutzaufsicht als zuständige Behörde an. Die Anerkenntnis erstreckt sich auch auf die Aufgaben und Befugnisse der kirchlichen Datenschutzaufsicht nach §§ 43, 44 DSG-EKD. Die Kontaktdaten der für die Auftraggeberin zuständigen Aufsichtsbehörde sind:

Der Beauftragte für den Datenschutz der EKD
Außenstelle Hannover
Lange Laube 20
30159 Hannover

Auftraggeberin	Auftragnehmerin
(Ort, Datum)	(Ort, Datum)
(Unterschriften mit Amts-/Funktionsbezeichnungen)	(Unterschriften mit Amts-/Funktionsbezeichnungen)

Erläuterung

Wenn eine kirchliche Stelle einen Vertrag zur Durchführung einer Auftragsverarbeitung (kurz: AVV) mit einer anderen Stelle abschließt, die nicht den kirchlichen Datenschutzbestimmungen unterliegt, so muss gemäß § 30 Absatz 5 Satz 1 EKD-Datenschutzgesetz (DSG-EKD) sichergestellt sein, dass der Auftragsverarbeiter die Vorgaben des § 30 DSG-EKD oder gleichwertige Bestimmungen beachtet und sich der kirchlichen Datenschutzaufsicht unterwirft.

Als gleichwertige Bestimmungen sind die Regelungen des Artikel 28 EU-Datenschutz-Grundverordnung (DSGVO) zu verstehen. Mit dem Abschluss der Zusatzvereinbarung ist zudem die Voraussetzung des § 30 Absatz 5 Satz 3 DSG-EKD erfüllt.

Die Zusatzvereinbarung ist ergänzend zum Vertrag nach Art. 28 DSGVO abzuschließen.

Meldung einer Verletzung des Schutzes personenbezogener Daten an die Aufsichtsbehörde (Datenpanne)

Ev.-luth. Kirchengemeinde .....

Straße

PLZ Ort

Der Beauftragte für den Datenschutz der EKD
– Außenstelle Hannover –
Lange Laube 20
30159 Hannover

Betreff: Meldung einer Datenpanne

1. Art der Meldung	
☐ Neumeldung	☐ Folgemeldung

2. Verantwortliche Stelle – Wo ist der Vorfall passiert	
Bezeichnung der Organisation:	Name der betroffenen organisatorischen Einheit
Anschrift:	Straße und Hausnummer
PLZ und Ort:	PLZ und Ort
Webseite:	Webadresse / URL der Website

3. Meldende Person

Name:	Ihr Name
Funktion:	Wählen Sie ein Element aus
Telefonnummer:	Telefonnummer
E-mail-Adresse:	Ihre E-Mail-Adresse

4. Örtlich Beauftragte/r für den Datenschutz oder sonstige Anlaufstelle

Name und Kontaktdaten (Postanschrift, Telefonnummer, E-Mail-Adresse) des oder der örtlich Beauftragten für den Datenschutz oder eine sonstige Anlaufstelle für weitere Informationen oder Verweis nach oben, wenn meldende Person und Ansprechpartner/-in identisch sind.

5. Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten

Was ist passiert?	Wählen Sie ein Element aus.

Nähere Beschreibung des Vorfalls:

Bitte beschreiben Sie den Vorfall möglichst präzise. Wo ist der Vorfall passiert? Wer war beteiligt? Wie haben Sie davon erfahren? Ist die verantwortliche Organisation schon informiert? Welche Dritte haben Kenntnis erlangt oder hatten die Möglichkeit zur Kenntnisnahme?

Zeitraum oder Zeitpunkt des Vorfalls:	Möglichst exakte Zeitangabe
Zeitpunkt der Feststellung des Vorfalls:	Möglichst exakte Zeitangabe

Art der betroffenen Daten:

☐ Religiose oder weltanschauliche Überzeugungen	☐ Genetische Daten
☐ Rassische und ethnische Herkunft	☐ Biometrische Daten
☐ Politische Meinungen	☐ Gesundheitsdaten
☐ Gewerkschaftszugehörigkeit	☐ Daten zum Sexualleben oder zur sexuellen Orientierung
☐ Geburtsdatum	☐ Personalausweisnummer
☐ Postalische Adressen	☐ Andere Identifikationsnummer
☐ E-Mail-Adressen	☐ Andere Ausweise
☐ Fotos/Videos	☐ Steuernummer
☐ Passwörter	☐ Angaben zu Straftaten
☐ Wirtschaftliche Verhältnisse	☐ Standort
☐ Bank- oder Kreditbereich	☐ Sonstige personenbezogene Daten
☐ Unbekannte Daten	

Anzahl der betroffenen Personen:
Wie viele Personen sind vom Vorfall betroffen? (ggf. Schätzung)

Anzahl der betroffenen personenbezogenen Datensätze:
Wie viele Datensätze sind betroffen? (ggf. Schätzung)

Kategorien der betroffenen Personen	
☐ Mitarbeitende	☐ besonders schutzwürdige Personen (z.B. Behinderte, Pflegebedürftige)
☐ Kunden/Kundinnen	☐ Nutzer/Nutzerinnen
☐ Klienten/Klientinnen	☐ Patienten/Patientinnen
☐ Kinder/Minderjährige	☐ Sonstige
Weitere Erläuterungen:	
Weitere Erläuterungen sind v.a. erforderlich, wenn „besonders schutzwürdige Personen“ oder „Sonstige“ angekreuzt wurde.	

6. Wahrscheinliche Folgen der Datenschutzverletzung	
☐ Diskriminierung	☐ Verlust des Arbeitsplatzes
☐ Identitätsdiebstahl oder -betrug	☐ Geheimnisoffenbarung
☐ Lebensgefährdung	☐ Bloßstellung
☐ Finanzieller Schaden	☐ Gesellschaftliche Nachteile
☐ Rufschädigung	☐ Wirtschaftliche Nachteile
☐ Existenzgefährdung	☐ Sonstiges
☐ Unbefugte Aufhebung von Pseudonymisierung	
Weitere Erläuterungen:	
Weitere Erläuterungen sind v.a. erforderlich, wenn „Lebensgefährdung“ oder „Sonstiges“ angekreuzt wurde.	

7. Abhilfemaßnahmen
Welche Maßnahmen wurden von der verantwortlichen Stelle nach Bekanntwerden des Vorfalls ergriffen, um die Verletzung des Schutzes personenbezogener Daten zu beheben und ihre möglichen nachteiligen Auswirkungen abzumildern? Welche weiteren Maßnahmen sind geplant oder werden vorgeschlagen?

8. Vollständigkeit

☐ Die vorliegende Meldung ist vollständig und umfasst alle gemäß § 32 Absatz 3 DSG-EKD der Aufsichtsbehörde mitzuteilenden Informationen.

☐ Die vorliegende Meldung ist noch unvollständig, da nicht alle Informationen unverzüglich bereitgestellt werden können.

Begründung:
Bitte nennen Sie hier den Grund, aus dem eine vollständige Bereitstellung der Informationen zum aktuellen Zeitpunkt noch nicht möglich ist.

Noch fehlende Informationen werden der Aufsichtsbehörde in Form einer Folgemeldung unverzüglich zur Verfügung gestellt.

☐ Die vorliegende Meldung ergänzt oder korrigiert eine vorherige Meldung.

Datum der vorherigen Meldung: Datum

Aktenzeichen der vorherigen Meldung: Aktenzeichen

(Ort, Datum)

(Unterschriften mit Amts-/Funktionsbezeichnungen)

Nutzung von Homeoffice oder Telearbeit

Das Datenschutzrecht gilt grundsätzlich auch für das Arbeiten im Homeoffice. Jeder Einzelfall ist zu prüfen und unter Beachtung des Schutzbedarfs der zu verarbeitenden Daten zu beurteilen, ob die Bearbeitung im Homeoffice datenschutzrechtlich vertretbar ist. Zu entscheiden hat das die datenschutzrechtlich verantwortliche Stelle.

Risiken lassen sich weder bei der Arbeit im Büro, noch im Homeoffice gänzlich vermeiden. Mit der Verlagerung der Arbeitsstätte in den häuslichen oder gar in den öffentlichen Bereich steigen jedoch die Risiken, da die Kontroll- und Einflussmöglichkeiten der verantwortlichen Stelle eingeschränkt sind. Vertretbar ist die Verarbeitung personenbezogener Daten, wenn deren Schutz durch angemessene technische und organisatorische Maßnahmen gewährleistet ist. Kann aber z.B. der erhöhte Schutzbedarf für Sozialdaten oder Beschäftigtendaten nicht gewährleistet werden, dürfen derartige Daten auch nicht im Homeoffice verarbeitet werden.

Bei der Beurteilung, ob personenbezogene Daten außerhalb der Diensträume verarbeitet werden dürfen, sind auch Arbeitsabläufe und Kommunikationswege zu berücksichtigen. Kann die Aufgaben– und Ergebnisübermittlung durchgängig automatisiert auf elektronischem Weg erfolgen oder muss ein physischer Transport von Unterlagen durchgeführt werden? Bei Letzterem kann das Risiko eines Verlustes steigen und unbefugte Dritte können auf personenbezogene Daten zugreifen. Gleiches gilt bei Verlust eines Notebooks oder Smartphones, wenn die Geräte nicht verschlüsselt und gesperrt sind.

Allgemeingültige Regelungen für eine rechtssichere Gestaltung von Homeoffice lassen sich nur begrenzt treffen. Die folgende Checkliste führt mögliche Regelungsbereiche und Einzelhinweise auf, die bei einer individuellen Gestaltung von technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten zu bedenken sind. Weitere Informationen zu technischen Fragen rund um das Home Office finden Sie unter: **https://it.landeskirche-hannovers.de/homeoffice**

1. Organisatorische Regelungen

- Datenschutzgrundsätze sind in einer Dienstvereinbarung zu regeln und mit den Mitarbeitenden bzw. der Mitarbeitervertretung vertraglich zu vereinbaren.
- Die zu verarbeitenden Daten sind zu klassifizieren und die einzuhaltenden Sicherheitsmaßnahmen zu beschreiben.

- Allgemeine Sicherheitsanforderungen für z.B. Datensicherung, Virenschutz, Firewall, Verschlüsselung von Datenträgern, Komplexität von Passworten, abschließbare Schränke sind festzulegen.
- Eine private Nutzung dienstlicher Geräte oder dienstliche Nutzung privater Geräte ist zu regeln oder auszuschließen.
- Regelungen zur Datenübermittlung oder Fernzugriffe über Virtual Private Network (VPN), sowie Umgang mit mobilen Datenträgern (z.B. USB) oder Ausdrucken sind zu regeln.
- Die Vorgehensweise bei evtl. Datenpannen im Homeoffice ist zu bestimmen.
- Zu nutzende Kommunikationsarten und -wege (E-Mail, Internet, Mobiltelefon) sind vorzugeben.
- Regelungen zur Datenträgervernichtung (Papier und elektronische) sind abzustimmen.
- Ausgabe und Rücknahme dienstlicher Geräte (z. B. Notebook, Smartphone) und Akten sind zu dokumentieren.
- Ein Zutrittsrecht der verantwortlichen Stelle zum Heimarbeitsplatz oder der dazu beauftragten Personen zwecks Kontrolle und Zugriff auf dienstliche Dokumente ist zu vereinbaren. Dazu gehört auch die Zustimmung der in der häuslichen Gemeinschaft lebenden Personen.
- Durchführung regelmäßiger Schulungen zum sicheren und datenschutzgerechten Umgang mit PCs und mobilen Geräten.
- Örtliche Datenschutzbeauftragte sollten in die Erstellung der Regelungen zum Homeoffice/Telearbeit einbezogen werden.
- Alle Regelungen zum Homeoffice/Telearbeit sind den betroffenen Mitarbeitenden bekanntzugeben.

2. Arbeitsabläufe

- Transport mobiler Geräte erfolgt ausschließlich im gesperrten Zustand.
- Papierunterlagen und dienstlich genutzte Geräte dürfen nicht unbeaufsichtigt gelassen werden, sodass Dritte keine Möglichkeit der Einsichtnahme bekommen. Dies gilt auch für den Transport.
- Drucker nur anbinden, wenn Dritte keine Kenntnis von den Ausdrucken erlangen können.

- Dienstliche Telefonate sollen nur geführt werden, wenn keine unbefugten Dritten mithören können.
- Bei Nutzung privater Telefone müssen automatisch gespeicherte Anrufkontakte regelmäßig gelöscht werden. Die eigene private Rufnummer sollte unterdrückt sein.
- Bei Nutzung von Smartphones dürfen Dritte (z.B. über installierte Apps) nicht auf berufliche Kontakte des Telefonbuchspeichers zugreifen können.
- Dienstliche E-Mails dürfen nicht auf private Postfächer umgeleitet werden.

3. Zugriffskontrolle

- Für eine sichere Authentisierung sind Passwort (ausreichend komplex) oder PIN zu verwenden.
- Authentisierung, Zugriffe, Änderungen und Administratortätigkeiten werden protokolliert.
- Benutzerrechte für Mitarbeitende einschränken (keine Administratorenrechte).
- Verbindung zur Dienststelle nur über dienstlich bereitgestelltes Virtual Private Network (VPN).
- Der Umgang mit USB-Anschlüssen muss geregelt werden, z.B. Verbot des Anschlusses von USB-Sticks.

4. Datensicherheit (Verschlüsselung)

- Daten auf mobilen Geräten (Notebook, Smartphone, USB-Stick) sind stets zu verschlüsseln.
- Mail-Anhänge mit personenbezogenen Daten sind zu verschlüsseln.
- Die Verbindung zum häuslichen W-LAN muss verschlüsselt sein oder kabelgebunden erfolgen.

5. Umgebungssicherheit

- Geeignete häusliche Räumlichkeiten und Arbeitsmittel für die sichere Aufbewahrung von Unterlagen, Geräten und Datenträgern müssen vorhanden sein.

- Die in der häuslichen Gemeinschaft lebenden Personen haben keinen Zugriff auf dienstliche Geräte und Unterlagen.
- Clean-Desk-Methode wird eingehalten (Dokumente vor Einsicht Dritter schützen).
- Eine automatische Bildschirmsperre beim Verlassen des Computers ist einzurichten.
- Blickschutzfolie für den Bildschirm schützt vor Blicken Unbefugter (z.B. Besucher, Familienangehörige).

6. Betriebssicherheit

- Mitarbeitende im Homeoffice sollten sicher mit mobilen Geräten umgehen können.
- Updates werden zeitnah installiert und sind stets aktuell.
- Eine Firewall ist aktiviert.
- Ein Virenschutz ist installiert und immer aktuell.
- Die Aktivierung eines zusätzlichen Bot-Schutzes ist wünschenswert.
- Dienstliche Daten sollten auf zentralen Systemen der Dienststelle gespeichert werden (Netzlaufwerke, DMS usw.). Bei lokaler Speicherung ist regelmäßig eine verschlüsselte Datensicherung durchzuführen, inkl. einer Kontrolle der Wiederherstellung.

7. Kommunikationssicherheit

- Sicherstellung des Zugriffs auf dienstliche E-Mail-Postfächer. Dienstliche E-Mails dürfen nicht auf private Postfächer umgeleitet werden.
- Vertrauliche Dokumente dürfen nicht unverschlüsselt einer E-Mail angehängt werden.
- Bei Videokonferenzen ist die Nutzung eines Headsets empfehlenswert.
- Die Nutzung öffentlicher Netzzugänge ist nur unter Verwendung von VPN gestattet.
- Ein Mobile Device Management zur zentralen Administration der Endgeräte ist anzustreben (ermöglicht nachträgliches Löschen der Daten eines verlorenen oder gestohlenen Gerätes).

An der Herausgabe der Rechtssammlung zum Datenschutz waren die Mitglieder der Arbeitsgruppe „Datenschutzmuster“ und folgende Autorinnen und Autoren beteiligt:

J. Arkenberg (Örtliche Datenschutzbeauftragte)

C. Buchwald (Örtlicher Datenschutzbeauftragter)

R. Burmeister (Örtlicher Datenschutzbeauftragter)

A. v. Collande (Landeskirchenamt)

G. Eichhorn (Örtlicher Datenschutzbeauftragter)

S. Guhl (Örtlicher Datenschutzbeauftragter)

A. Holzmann (Landeskirchenamt)

C. Marquardt (Örtliche Datenschutzbeauftragte)

S. Schierding (Landeskirchenamt)

H. Schulze (Örtlicher Datenschutzbeauftragter)

K. Tancredi (Örtliche Datenschutzbeauftragte)

W. Volkhardt (Landeskirchenamt)