Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland

(EKD-Datenschutzgesetz – DSG-EKD)
in der Bekanntgabe der Neufassung
vom 15. Januar 2025 (ABl. EKD S. 1).

Lfd. Nr.	Änderndes Recht	Datum	Fundstelle ABl. EKD	Paragrafen	Art der Änderung
1	Berichtigung	20.02.2025	2025 S. 42	§ 12 Satz 2 § 30 Abs. 7 Satz 2	Wort ersetzt Wörter ersetzt

Inhaltsübersicht

Präambel

Kapitel 1 Allgemeine Bestimmungen
§ 1 Zweck des Gesetzes
§ 2 Anwendungsbereich
§ 3 Seelsorgegeheimnis und Amtsverschwiegenheit
§ 4 Begriffsbestimmungen

Kapitel 2 Verarbeitung personenbezogener Daten
§ 5 Grundsätze
§ 6 Rechtmäßigkeit der Verarbeitung
§ 7 Rechtmäßigkeit der Zweckänderung
§ 8 Offenlegung an kirchliche oder öffentliche Stellen
§ 9 Offenlegung an sonstige Stellen
§ 10 Datenübermittlung an und in Drittländer oder an internationale Organisationen
§ 11 Einwilligung
§ 12 Einwilligung Minderjähriger
§ 13 Verarbeitung besonderer Kategorien personenbezogener Daten
§ 14 Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten
§ 15 Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist

Kapitel 3 Rechte der betroffenen Person
§ 16 Transparente Information, Kommunikation
§ 17 Informationspflicht bei unmittelbarer Datenerhebung

§ 18 Informationspflicht bei mittelbarer Datenerhebung
§ 19 Auskunftsrecht der betroffenen Person
§ 20 Recht auf Berichtigung
§ 21 Recht auf Löschung
§ 22 Recht auf Einschränkung der Verarbeitung
§ 23 Informationspflicht bei Berichtigung, Löschung oder Einschränkung der Verarbeitung
§ 24 Recht auf Datenübertragbarkeit
§ 25 Widerspruchsrecht
§ 25a Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

Kapitel 4 Pflichten der verantwortlichen Stellen und Auftragsverarbeiter
§ 26 Datengeheimnis
§ 27 Technische und organisatorische Maßnahmen, IT-Sicherheit
§ 28 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
§ 29 Gemeinsam verantwortliche Stellen
§ 30 Verarbeitung von personenbezogenen Daten im Auftrag
§ 30a Zentrale Verfahren
§ 31 Verzeichnis von Verarbeitungstätigkeiten
§ 32 Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde
§ 33 Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person
§ 34 Datenschutz-Folgenabschätzung
§ 35 Audit und Zertifizierung

Kapitel 5 Örtlich Beauftragte für den Datenschutz
§ 36 Bestellung von örtlich Beauftragten für den Datenschutz
§ 37 Stellung
§ 38 Aufgaben

Kapitel 6 Unabhängige Aufsichtsbehörden
§ 39 Errichtung der Aufsichtsbehörden und Bestellung der Beauftragten für den Datenschutz
§ 40 Unabhängigkeit
§ 41 Tätigkeitsbericht
§ 42 Rechtsstellung
§ 43 Aufgaben
§ 44 Befugnisse
§ 45 Geldbußen

Kapitel 7 Rechtsbehelfe und Schadensersatz
§ 46 Recht auf Beschwerde

§ 47 Rechtsweg
§ 48 Schadensersatz durch verantwortliche Stellen

Kapitel 8 Vorschriften für besondere Verarbeitungssituationen
§ 49 Verarbeitung personenbezogener Daten bei Dienst- und Arbeitsverhältnissen
§ 50 Verarbeitung personenbezogener Daten zu Archivzwecken, Forschungszwecken und zu statistischen Zwecken
§ 50a Verarbeitung personenbezogener Daten zur institutionellen Aufarbeitung sexualisierter Gewalt
§ 50b Mitgliederkommunikation
§ 51 Verarbeitung personenbezogener Daten durch die Medien
§ 52 Videoüberwachung öffentlich zugänglicher Räume
§ 53 Gottesdienste und kirchliche Veranstaltungen

Kapitel 9 Schlussbestimmungen
§ 54 Ergänzende Bestimmungen
§ 55 Übergangsregelungen
§ 56 Inkrafttreten, Außerkrafttreten

Präambel

[1]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. [2]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). [3]In Wahrnehmung dieses Rechts stellt dieses Kirchengesetz den Einklang mit der Datenschutz-Grundverordnung her und regelt die Datenverarbeitung im kirchlichen und diakonischen Bereich. [4]Die Datenverarbeitung dient der Erfüllung des kirchlichen Auftrags.

Kapitel 1
Allgemeine Bestimmungen

§ 1
Zweck des Gesetzes

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) [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). [2]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 erlassenen weiteren Bestimmungen Anwendung finden. [3]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. [4]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 kirchliche oder staatliche Rechtsvorschriften, die kirchliche Stellen anzuwenden haben, die Verarbeitung personenbezogener Daten regeln, gehen sie diesem Kirchengesetz vor.

§ 3
Seelsorgegeheimnis und Amtsverschwiegenheit

[1]Aufzeichnungen, die in Wahrnehmung eines kirchlichen Seelsorgeauftrages erstellt werden, dürfen Dritten nicht zugänglich sein. [2]Die besonderen Bestimmungen über den Schutz des Beicht- und Seelsorgegeheimnisses bleiben unberührt. [3]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 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, Behörde, Einrichtung oder andere 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, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag der verantwortlichen Stelle verarbeitet;

11. „Empfänger“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere 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, Behörde, Einrichtung oder andere 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;

19a. „Unternehmensgruppe“ eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht;

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;

22. „institutionelle Aufarbeitung sexualisierter Gewalt“ jede systematische, nicht auf den Einzelfall bezogene Untersuchung von Vorkommnissen sexualisierter Gewalt, insbesondere betreffend deren Ursachen, Rahmenbedingungen und Folgen.

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 oder öffentlichen 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 Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter 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 kirchliche oder staatliche 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 zur Wahrung der berechtigten Interessen der verantwortlichen Stelle oder eines Dritten erforderlich, sofern nicht die Interessen der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn diese minderjährig ist;
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.

§ 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 oder staatliche Rechtsvorschrift dies erlaubt oder anordnet;
2. sie erforderlich ist
   a) zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten oder
   b) zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche,

   sofern nicht die Interessen der betroffenen Person an dem Ausschluss der Verarbeitung überwiegen;
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. es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder

8. sie zur institutionellen Aufarbeitung sexualisierter Gewalt gemäß § 50a erforderlich ist.

(2) [1]In anderen Fällen muss die kirchliche Stelle feststellen, ob die Zweckänderung mit dem Zweck, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist. [2]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) [1]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. [2]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) [1]Die Verantwortung für die Zulässigkeit der Offenlegung nach §§ 6 und 7 an kirchliche Stellen trägt die offenlegende verantwortliche Stelle. [2]Erfolgt die Offenlegung auf Ersuchen der empfangenden kirchlichen Stelle, trägt diese die Verantwortung. [3]In diesem Fall prüft die offenlegende verantwortliche Stelle nur, ob das Ersuchen im Rahmen der Auf-

gaben der datenempfangenden kirchlichen Stelle liegt, es sei denn, dass besonderer Anlass zur Prüfung der Rechtmäßigkeit der Offenlegung besteht.

(2) [1]Die datenempfangende kirchliche Stelle darf die offengelegten Daten für den Zweck verarbeiten, zu dessen Erfüllung sie ihr offengelegt werden. [2]Eine Verarbeitung für andere Zwecke ist nur unter den Voraussetzungen des § 7 zulässig.

(3) Sind mit personenbezogenen Daten, die nach §§ 6 und 7 an kirchliche Stellen offengelegt werden, 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.

(4) Absatz 3 gilt entsprechend, wenn personenbezogene Daten innerhalb einer kirchlichen Stelle weitergegeben werden.

(5) Für die Offenlegung personenbezogener Daten gegenüber öffentlichen Stellen nach § 2 des Bundesdatenschutzgesetzes in der jeweils geltenden Fassung gelten die Absätze 1 bis 3 entsprechend.

§ 9
Offenlegung an sonstige Stellen

(1) Die Verantwortung für die Zulässigkeit der Offenlegung nach §§ 6 und 7 an sonstige Stellen oder Personen trägt die offenlegende kirchliche Stelle.

(2) [1]Die datenempfangenden Stellen und Personen dürfen die offengelegten Daten nur für den Zweck verarbeiten, zu dessen Erfüllung sie ihnen offengelegt werden. [2]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 oder
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 vorvertraglichen 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 öffentlichen oder 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) $_1$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. $_2$Soweit die Erklärung unter Umständen abgegeben worden ist, die gegen dieses Kirchengesetz verstoßen, ist sie unwirksam.

(3) $_1$Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. $_2$Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. $_3$Die betroffene Person wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt. $_4$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

[1]Minderjährige, denen insbesondere elektronische Angebote von kirchlichen Stellen gemacht werden, können in die Verarbeitung ihrer Daten wirksam einwilligen, wenn sie religionsmündig sind. [2]Sind die Minderjährigen noch nicht religionsmündig, ist die Verarbeitung nur rechtmäßig, wenn die Sorgeberechtigten die Einwilligung erteilt oder der Einwilligung zugestimmt haben. [3]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 kirchliche Stelle im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung erfolgt, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der kirchlichen 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 oder staatlichen 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 öffentlichen oder 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;
10. die Verarbeitung für im kirchlichen oder im öffentlichen 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,
11. die Verarbeitung für Zwecke der institutionellen Aufarbeitung sexualisierter Gewalt gemäß § 50a erforderlich ist und die Interessen der betroffenen Person durch angemessene Maßnahmen gewahrt sind oder
12. die Verarbeitung aus Gründen eines erheblichen öffentlichen Interesses zwingend erforderlich ist.

(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) [1]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. [2]In diesen Fällen finden die § 19 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 unverzüglich, in jedem Fall innerhalb von drei Monaten nach Eingang des Antrags zur Verfügung.

(4) Wird die verantwortliche Stelle auf den Antrag der betroffenen Person hin nicht tätig, so unterrichtet sie die betroffene Person unverzüglich, 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 eröffnet die verantwortliche Stelle der betroffenen Person zum Zeitpunkt der Erhebung in geeigneter und angemessener Weise Zugang zu folgenden Informationen:

1. den Namen und die Kontaktdaten der verantwortlichen Stelle;
2. gegebenenfalls die Kontaktdaten der 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 folgende weitere Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:

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 mögliche Folgen die Nichtbereitstellung hätte;
5. das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß § 25a Absatz 1 und 4 und – zumindest in diesen Fällen – aussagekräftige

Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

(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 3 und 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.

§ 19
Auskunftsrecht der betroffenen Person

(1) Die betroffene Person hat das Recht, von der verantwortlichen Stelle eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf folgende Informationen:

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;
8. das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß § 25a Absatz 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

(2) Werden personenbezogene Daten an ein Drittland oder an eine internationale Organisation übermittelt, so hat die betroffene Person zusätzlich das Recht, über die geeigneten Garantien gemäß § 10 im Zusammenhang mit der Übermittlung unterrichtet zu werden.

(3) $_1$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. $_2$Die Ablehnung der Auskunftserteilung ist gegenüber der betroffenen Person zu begründen.

(4) $_1$Die verantwortliche Stelle stellt eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung. $_2$Für alle weiteren Kopien, die die betroffene Person beantragt, kann die verantwortliche Stelle ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen. $_3$Stellt die betroffene Person den Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sie nichts anderes angibt.

(5) Das Recht auf Erhalt einer Kopie gemäß Absatz 4 darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

(6) Verarbeitet die verantwortliche Stelle eine große Menge von Informationen über die betroffene Person, so kann sie verlangen, dass die betroffene Person präzisiert, auf welche Information oder welche Verarbeitungsvorgänge sich ihr Auskunftsersuchen bezieht.

(7) Das Auskunftsrecht findet in den Fällen des § 50 Absatz 1 keine Anwendung, soweit die Auskunft einen unverhältnismäßigen Aufwand erfordern würde.

§ 20
Recht auf Berichtigung

(1) $_1$Die betroffene Person hat das Recht, von der verantwortlichen Stelle die unverzügliche Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. $_2$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) [1]Das Recht auf Berichtigung besteht nicht, wenn die personenbezogenen Daten zu Archivzwecken im kirchlichen Interesse verarbeitet werden. [2]Bestreitet die betroffene Person die Richtigkeit der personenbezogenen Daten, ist ihr die Möglichkeit einer Gegendarstellung einzuräumen. [3]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;
3. aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß § 13 Absatz 2 Nummer 8 bis 9;
4. für im kirchlichen oder öffentlichen 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 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

[1]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. [2]Die verantwortliche Stelle unterrichtet die betroffene Person über diese Empfänger, wenn die betroffene Person dies verlangt.

§ 24
Recht auf Datenübertragbarkeit

(1) [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.

[2]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 in Ausübung kirchlicher Aufsicht erfolgt.

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

§ 25
Widerspruchsrecht

(1) [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 3 oder Nummer 4 Widerspruch einzulegen. [2]Die verantwortliche Stelle verarbeitet die personenbezogenen Daten nicht mehr, es sei denn, sie kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Rechte und berechtigten Interessen der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

(2) [1]Werden personenbezogene Daten von Unternehmen im Sinne von § 4 Nummer 19 verarbeitet, um Direktwerbung zu betreiben, so hat die betroffene Person das Recht, je-

derzeit Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten zum Zwecke derartiger Werbung einzulegen; dies gilt auch für das Profiling, soweit es mit solcher Direktwerbung in Verbindung steht. [2]Die verantwortliche Stelle muss die betroffene Person spätestens zum Zeitpunkt der ersten Kommunikation mit ihr ausdrücklich auf dieses Widerspruchsrecht hinweisen. [3]Dieser Hinweis hat in einer verständlichen und von anderen Informationen getrennten Form zu erfolgen. [4]Widerspricht die betroffene Person der Verarbeitung für Zwecke der Direktwerbung, so werden die personenbezogenen Daten nicht mehr für diese Zwecke verarbeitet.

§ 25a
Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

(1) Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

(2) Absatz 1 gilt nicht, wenn die Entscheidung

a) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und der verantwortlichen Stelle erforderlich ist,

b) aufgrund einer staatlichen oder kirchlichen Rechtsvorschrift, denen die verantwortliche Stelle unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte sowie der berechtigten Interessen der betroffenen Person enthalten oder

c) mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

(3) In den in Absatz 2 Buchstaben a und c genannten Fällen trifft die verantwortliche Stelle angemessene Maßnahmen, um die Rechte sowie die berechtigten Interessen der betroffenen Person zu wahren, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens der verantwortlichen Stelle, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört.

(4) Entscheidungen nach Absatz 2 dürfen nicht auf besonderen Kategorien personenbezogener Daten nach § 4 Nummer 2 beruhen, sofern nicht § 13 Absatz 2 Nummer 1 oder Nummer 7 gilt und angemessene Maßnahmen zum Schutz der Rechte sowie der berechtigten Interessen der betroffenen Person getroffen wurden.

Kapitel 4
Pflichten der verantwortlichen Stellen und Auftragsverarbeiter

§ 26
Datengeheimnis

[1]Den bei der Datenverarbeitung tätigen Personen ist untersagt, personenbezogene Daten unbefugt zu verarbeiten (Datengeheimnis). [2]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. [3]Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

§ 27
Technische und organisatorische Maßnahmen, IT-Sicherheit

(1) [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. [2]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) [1]Verantwortliche Stellen und Auftragsverarbeiter sind verpflichtet, IT-Sicherheit zu gewährleisten. [2]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 Risiken 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) [1]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. [2]Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. [3]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 Kir-

chengesetz erfüllt, soweit die jeweiligen Aufgaben der verantwortlichen Stellen nicht durch Rechtsvorschriften festgelegt sind.

(2) [1]In der Vereinbarung kann eine Anlaufstelle für die betroffenen Personen angegeben werden. [2]Das Wesentliche der Vereinbarung wird der betroffenen Person 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) [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. [2]Die in Kapitel 3 genannten Rechte sind ihr gegenüber geltend zu machen. [3]Zuständig für die Aufsicht ist die Aufsichtsbehörde der beauftragenden kirchlichen Stelle.

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

(3) [1]Der Auftragsverarbeiter ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. [2]Der Auftrag ist in Textform 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 Einschränkung der Verarbeitung 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.

[3]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. [4]Das Ergebnis ist zu dokumentieren.

(4) [1]Der Auftragsverarbeiter darf die Daten nur im Rahmen der Weisungen der verantwortlichen Stelle verarbeiten. [2]Ist er der Ansicht, dass eine Weisung der verantwortlichen Stelle gegen dieses Kirchengesetz oder andere Vorschriften über den Datenschutz verstößt, hat er die verantwortliche Stelle unverzüglich darauf hinzuweisen.

(5) Sofern die kirchlichen Datenschutzbestimmungen auf den Auftragsverarbeiter keine Anwendung finden, dürfen sich abweichend von Absatz 3 die Vertragsinhalte an Artikel 28 EU-Datenschutz-Grundverordnung orientieren.

(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) [1]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. [2]Bei der Beauftragung anderer kirchlicher Stellen kann von Absatz 3 Satz 2 Nummer 3 Alternative 2, Nummer 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.

§ 30a
Zentrale Verfahren

Das Recht der Evangelischen Kirche in Deutschland, der Gliedkirchen oder der gliedkirchlichen Zusammenschlüsse kann für zentrale Verfahren, an denen mehrere verantwortliche Stellen beteiligt sind, abweichend von § 29 oder § 30 die Verteilung der datenschutzrechtlichen Aufgaben, Befugnisse und Verantwortlichkeiten zwischen den beteiligten verantwortlichen Stellen festlegen.

§ 31
Verzeichnis von Verarbeitungstätigkeiten

(1) [1]Jede verantwortliche Stelle führt ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. [2]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 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) [1]Die in den Absätzen 1 und 2 genannten Pflichten gelten nicht für verantwortliche Stellen, die weniger als 250 Beschäftigte haben. [2]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 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) [1]Die verantwortliche Stelle hat Verletzungen des Schutzes personenbezogener Daten zu dokumentieren. [2]Die Dokumentation hat alle mit den Vorfällen zusammenhängenden

Tatsachen, deren Auswirkungen und die ergriffenen Abhilfemaßnahmen zu umfassen. [3]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) [1]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. [2]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) [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. [2]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 örtlich Beauftragten ein, sofern eine Bestellung erfolgt ist.

(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

[1]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. [2]Näheres kann der Rat der Evangelischen Kirche in Deutschland durch Rechtsverordnung regeln.

Kapitel 5
Örtlich Beauftragte für den Datenschutz

§ 36
Bestellung von örtlich Beauftragten für den Datenschutz

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

1. bei ihnen in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten betraut sind, oder
2. die Kerntätigkeit der verantwortlichen Stelle in der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten besteht.

[2]Die Vertretung ist zu regeln.

(2) [1]Die Bestellung kann sich auf mehrere verantwortliche Stellen erstrecken. [2]Das Recht der Evangelischen Kirche in Deutschland, der Gliedkirchen und der gliedkirchlichen Zusammenschlüsse kann bestimmen, dass für mehrere verantwortliche Stellen gemeinsame örtlich Beauftragte bestellt werden. [3]Eine Unternehmensgruppe darf gemeinsam eine Person örtlich beauftragen.

(3) [1]Zu örtlich Beauftragten dürfen nur Personen bestellt werden, die die zur Erfüllung ihrer Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzen. [2]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) [1]Die Bestellung von örtlich Beauftragten erfolgt in Textform und ist der Aufsichtsbehörde und der nach dem jeweiligen Recht für die allgemeine Aufsicht zuständigen Stelle

anzuzeigen; die Kontaktdaten sind zu veröffentlichen. 2Sind örtlich Beauftragte nicht Beschäftigte einer verantwortlichen Stelle, sind ihre 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) 1Die örtlich Beauftragten sind den gesetzlich oder verfassungsmäßig berufenen Organen der verantwortlichen Stellen unmittelbar zu unterstellen. 2Sie sind im Rahmen ihrer Aufgaben weisungsfrei. 3Sie dürfen wegen dieser Tätigkeit nicht benachteiligt werden. 4Sie können Auskünfte verlangen, Einsicht in Unterlagen nehmen und erhalten Zugang zu personenbezogenen Daten und den Verarbeitungsvorgängen. 5Die verantwortliche Stelle unterstützt die örtlich Beauftragten bei der Erfüllung ihrer Aufgaben und stellt die notwendigen Mittel zur Verfügung. 6§ 42 Absatz 6 und 7 gilt entsprechend.

(2) 1Die Abberufung der örtlich Beauftragten ist nur in entsprechender Anwendung des § 626 des Bürgerlichen Gesetzbuches zulässig. 2Die Kündigung eines Arbeitsverhältnisses ist nur zulässig, wenn Tatsachen vorliegen, die zur Kündigung aus wichtigem Grund berechtigen. 3Gleiches gilt für den Zeitraum eines Jahres nach Beendigung der Bestellung.

(3) 1Zur 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. 2Die dazu notwendige Freistellung hat ohne Minderung der Bezüge oder des Erholungsurlaubes zu erfolgen. 3Im 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

1Die örtlich Beauftragten wirken auf die Einhaltung der Bestimmungen für den Datenschutz hin und unterstützen die verantwortlichen Stellen bei der Sicherstellung des Datenschutzes. 2Sie 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) [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). [2]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) [1]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. [2]Die Gliedkirchen können für die ihnen zugeordneten diakonischen Dienste, Einrichtungen und Werke eigene Aufsichtsbehörden errichten. [3]Der Rat der Evangelischen Kirche in Deutschland legt auf Vorschlag des Finanzbeirates der Evangelischen Kirche in Deutschland die jährlichen Beiträge für die Wahrnehmung der Aufsicht nach Satz 1 zweiter Halbsatz fest.

(4) [1]Beauftragte für den Datenschutz sollen für mindestens vier, höchstens acht Jahre bestellt werden. [2]Das Amt endet mit dem Amtsantritt einer Nachfolgerin oder eines Nachfolgers. [3]Die erneute Bestellung ist zulässig. [4]Das Amt ist hauptamtlich auszuüben. [5]Nebentätigkeiten sind nur zulässig, soweit dadurch das Vertrauen in die Unabhängigkeit und Unparteilichkeit nicht gefährdet wird und sie genehmigt sind.

(5) [1]Zu Beauftragten für den Datenschutz dürfen nur Personen bestellt werden, welche die zur Erfüllung ihrer Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzen. [2]Sie müssen die Befähigung zum Richteramt oder zum höheren Dienst besitzen und einer Gliedkirche der Evangelischen Kirche in Deutschland angehören. [3]Sie sind auf die gewissenhafte Erfüllung ihrer Amtspflichten und die Einhaltung der kirchlichen Ordnung zu verpflichten.

§ 40
Unabhängigkeit

(1) [1]Die Aufsichtsbehörden handeln bei der Erfüllung ihrer Aufgaben und bei der Ausübung ihrer Befugnisse völlig unabhängig. [2]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

[1]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. [2]Sie übermitteln den Bericht den jeweiligen kirchenleitenden Organen oder den jeweiligen Leitungsorganen der Diakonischen Werke und veröffentlichen ihn. [3]Auf dieser Grundlage können sie den leitenden Organen berichten.

§ 42
Rechtsstellung

(1) [1]Den Aufsichtsbehörden werden die Finanzmittel zur Verfügung gestellt, die sie benötigen, um ihre Aufgaben und Befugnisse effektiv wahrnehmen zu können. [2]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) [1]Die Aufsichtsbehörden können Aufgaben der Personalverwaltung und Personalwirtschaft auf andere Kirchenbehörden übertragen. [2]Diesen kirchlichen Stellen dürfen personenbezogene Daten der Beschäftigten offengelegt werden, soweit deren Kenntnis zur Erfüllung der übertragenen Aufgaben erforderlich ist.

(6) [1]Beauftragte für den Datenschutz und ihre Mitarbeitenden sind verpflichtet, über die ihnen amtlich bekanntgewordenen Angelegenheiten Verschwiegenheit zu bewahren. [2]Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. [3]Die Verpflichtung besteht auch nach Beendigung des Dienst- oder Arbeitsverhältnisses.

(7) [1]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. [2]Die Entscheidung über Aussagegenehmigungen treffen die Beauftragten für den Datenschutz für sich und ihre Mitarbeitenden in eigener Verantwortung. [3]Die Beauftragten für den Datenschutz gelten als oberste Aufsichtsbehörde im Sinne des § 99 Verwaltungsgerichtsordnung.

(8) [1]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. [2]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 dieses Gesetzes und sonstiger Vorschriften über den Datenschutz zu überwachen und durchzusetzen.

(2) [1]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. [2]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 Arztgeheimnis unterliegen, sofern die betroffene Person nicht eingewilligt hat, sowie
3. personenbezogene Daten in Personalakten, wenn die betroffene Person der Prüfung der auf sie bezogenen Daten im Einzelfall widerspricht.

(9) 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.

(10) [1]Die Beauftragten für den Datenschutz arbeiten zusammen und bilden eine Datenschutzkonferenz, auf der gemeinsame Stellungnahmen und Handreichungen zu Datenschutz- und Kohärenzfragen beschlossen werden können. [2]Sie tauschen mit den staatlichen Aufsichtsbehörden für den Datenschutz Erfahrungen und zweckdienliche Informationen aus und geben im Bedarfsfall Stellungnahmen ab.

§ 44
Befugnisse

(1) [1]Die Aufsichtsbehörden können verlangen, dass die verantwortlichen Stellen sie bei der Erfüllung ihrer Aufgaben unterstützen. [2]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. [3]Ihnen ist jederzeit Zutritt zu allen Diensträumen, einschließlich aller Verarbeitungsanlagen und -geräte zu gewähren, um Untersuchungen und Überprüfungen vorzunehmen. [4]Stellen Aufsichts-

behörden fest, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen dieses Kirchengesetz verstoßen, können sie Hinweise geben.

(2) [1]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. [2]Von einer Beanstandung kann abgesehen werden, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt. [3]Mit der Aufforderung zur Stellungnahme können Vorschläge zur Beseitigung der Mängel oder zur sonstigen Verbesserung des Datenschutzes verbunden werden. [4]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 löschen oder die Verarbeitung einzuschränken;
5. die von einer Verletzung des Schutzes personenbezogener Daten betroffene Person entsprechend zu benachrichtigen;
6. dem Antrag der betroffenen Person zu entsprechen.

(4) [1]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. [2]Soweit nicht Besonderheiten der kirchlichen Verwaltungsgerichtsordnung entgegenstehen, finden die Regelungen des § 21 des Bundesdatenschutzgesetzes entsprechende Anwendung.

§ 45
Geldbußen

(1) [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. [2]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) [1]Geldbußen werden je nach den Umständen des Einzelfalls verhängt. [2]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 kirchlicher 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 sechs Millionen 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) [1]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. [2]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) [1]Die Zuständigkeit für Klagen gegen die Aufsichtsbehörde nach § 39 Absatz 2 richtet sich nach § 5 des Kirchengerichtsgesetzes der Evangelischen Kirche in Deutschland in der jeweils geltenden Fassung. [2]Vor der Erhebung einer solchen Klage ist kein Vorverfahren durchzuführen.

§ 48
Schadensersatz durch verantwortliche Stellen

(1) [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 oder den kirchlichen Auftragsverarbeiter. [2]Wegen eines Schadens, der nicht Vermögensschaden ist, kann die betroffene Person eine angemessene Entschädigung in Geld verlangen.

(2) Eine verantwortliche Stelle oder ein kirchlicher Auftragsverarbeiter wird von der Haftung gemäß Absatz 1 befreit, wenn sie oder er nachweist, für den eingetretenen Schaden nicht verantwortlich zu sein.

(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) [1]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. [2]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. [3]Die Einwilligung bedarf der Textform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. [4]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;
4. sie zur Aufdeckung einer Straftat oder Amtspflichtverletzung oder zum Schutz möglicher Betroffener erforderlich erscheint oder
5. die Offenlegung zur institutionellen Aufarbeitung sexualisierter Gewalt gemäß § 50a erforderlich ist.

(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) [1]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. [2]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. [3]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) [1]Personenbezogene Daten, die vor Begründung eines Beschäftigungsverhältnisses erhoben wurden, sind unverzüglich zu löschen, sobald feststeht, dass ein solches nicht zustande kommt. [2]Dies gilt nicht, soweit überwiegende berechtigte Interessen der verantwortlichen Stelle der Löschung entgegenstehen oder die betroffene Person in die weitere Speicherung einwilligt. [3]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 zu Archivzwecken, Forschungszwecken und zu statistischen Zwecken

(1) Personenbezogene Daten dürfen zu im kirchlichen oder öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeitet werden, soweit geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorgesehen werden.

(2) Die Offenlegung personenbezogener Daten an andere als kirchliche Stellen für die Zwecke der Forschung oder 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.

(3) [1]Für Zwecke der Forschung oder Statistik erhobene oder gespeicherte personenbezogene Daten sind zu anonymisieren, sobald dies möglich ist. [2]Bis dahin sind die Merkmale gesondert zu verarbeiten, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer identifizierten oder identifizierbaren Person zugeordnet werden können. [3]Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Zweck dies erfordert.

(4) [1]Die Veröffentlichung personenbezogener Daten, die für Zwecke der Forschung oder Statistik übermittelt wurden, ist nur mit Zustimmung der übermittelnden Stelle zulässig. [2]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.

(5) Die ordnungsgemäße Archivierung von anzubietenden und zu übergebenden Unterlagen durch das zuständige Archiv ersetzt die nach kirchlichen oder staatlichen Rechts-

vorschriften erforderliche Löschung, wenn die Archivierung so erfolgt, dass Persönlichkeitsrechte der betroffenen Person oder Dritter nicht beeinträchtigt werden.

(6) Soweit kirchliche Stellen verpflichtet sind, Unterlagen dem zuständigen Archiv zur Übernahme anzubieten, ist eine Löschung erst zulässig, nachdem die Unterlagen angeboten worden und nicht als archivwürdig übernommen worden sind.

§ 50a
Verarbeitung personenbezogener Daten zur institutionellen Aufarbeitung sexualisierter Gewalt

(1) [1]An der institutionellen Aufarbeitung sexualisierter Gewalt besteht ein überragendes kirchliches Interesse. [2]Personenbezogene Daten dürfen zum Zwecke der institutionellen Aufarbeitung sexualisierter Gewalt verarbeitet werden.

(2) [1]Ihre Offenlegung ist ohne Einwilligung der Betroffenen im Sinne dieses Kirchengesetzes durch die Bereitstellung von Unterlagen, die Informationen über Vorgänge sexualisierter Gewalt enthalten oder von denen dieses aufgrund tatsächlicher Anhaltspunkte anzunehmen ist, zum Zwecke der institutionellen Aufarbeitung sexualisierter Gewalt gegenüber Wissenschaftlerinnen und Wissenschaftlern oder von der zuständigen kirchlichen Stelle Beauftragten zulässig,

1. wenn die Datenempfangenden ein Datenschutzkonzept vorlegen, das den Anforderungen dieses Kirchengesetzes entspricht und
2. sie auf das Datengeheimnis gemäß § 26 und darauf verpflichtet wurden, die Daten ausschließlich für die bestimmten Zwecke zu verarbeiten.

[2]§ 50 Absatz 3 gilt entsprechend.

(3) § 17 Absatz 3 findet keine Anwendung.

(4) [1]Die Veröffentlichung personenbezogener Daten, die für Zwecke der institutionellen Aufarbeitung sexualisierter Gewalt offengelegt wurden, ist nur mit Zustimmung der offenlegenden Stelle zulässig. [2]Die Zustimmung ist zu erteilen, wenn

1. die Veröffentlichung für die institutionelle Aufarbeitung sexualisierter Gewalt aufgrund der Stellung als Person der Zeitgeschichte unerlässlich ist oder
2. die betroffene Person in die Veröffentlichung eingewilligt hat.

[3]Vor Erteilung der Zustimmung nach Satz 2 Nummer 1 ist die betroffene Person anzuhören. [4]Personenbezogene Daten von Betroffenen sexualisierter Gewalt werden ausschließlich nach Satz 2 Nummer 2 veröffentlicht.

(5) Der Rat der Evangelischen Kirche in Deutschland kann durch Rechtsverordnung mit Zustimmung der Kirchenkonferenz das Nähere regeln.

§ 50b
Mitgliederkommunikation

(1) [1]Die kirchlichen juristischen Personen des öffentlichen Rechts verarbeiten Meldedaten und kirchliche Daten des Gemeindegliederverzeichnisses zur Erfüllung ihrer Aufgaben, insbesondere um gruppen- oder personenbezogen mit den Mitgliedern zu kommunizieren. [2]Dies schließt die Nutzung von Kommunikationsdaten ein, soweit ein Widerspruch dem nicht entgegensteht.

(2) Die gemeindebezogene Offenlegung personenbezogener Daten anlässlich von Amtshandlungen und Jubiläen ist zulässig, soweit ein Widerspruch dem nicht entgegensteht.

(3) Die Verarbeitung nach Absatz 1 kann mit dem Werben um persönlichen und finanziellen Einsatz für kirchliche und diakonische Zwecke (Fundraising) verbunden werden, soweit ein Widerspruch dem nicht entgegensteht.

§ 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) [1]Wird jemand durch eine Berichterstattung in seinem Persönlichkeitsrecht beeinträchtigt, so kann er Auskunft über die der Berichterstattung zugrundeliegenden, zu seiner Person gespeicherten Daten verlangen. [2]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. [3]Die betroffene Person kann die Berichtigung unrichtiger Daten verlangen.

§ 52
Videoüberwachung öffentlich zugänglicher Räume

(1) [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. 2Das 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 Verarbeitung 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) 1Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet und verarbeitet, so ist diese über die jeweilige Verarbeitung zu benachrichtigen. 2Von 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 Verarbeitung entgegenstehen.

§ 53
Gottesdienste und kirchliche Veranstaltungen

Die Aufzeichnung oder Übertragung von Gottesdiensten oder kirchlichen Veranstaltungen einschließlich ihrer Veröffentlichung ist datenschutzrechtlich zulässig, wenn die betroffenen Personen vor der Teilnahme durch geeignete Maßnahmen über Art und Umfang der Verarbeitung 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) [1]Soweit personenbezogene Daten von Sozialleistungsträgern offengelegt werden, gelten zum Schutz dieser Daten ergänzend die staatlichen Bestimmungen entsprechend. [2]Werden hierzu Bestimmungen gemäß Absatz 1 erlassen, ist vorher das Evangelische Werk für Diakonie und Entwicklung anzuhören.

§ 55
Übergangsregelungen

(1) [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. [2]Für diese Bestellungen gelten die Regelungen der §§ 39 bis 45 mit Inkrafttreten dieses Kirchengesetzes.

(2) [1]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. [2]Für diese Bestellungen gelten die Regelungen der §§ 36 bis 38 mit Inkrafttreten dieses Kirchengesetzes.

§ 56
Inkrafttreten, Außerkrafttreten

[1]§ 55 Absatz 4 tritt am Tag nach der Verkündung in Kraft. [2]Im Übrigen tritt dieses Kirchengesetz am 24. Mai 2018 in Kraft. [3]Gleichzeitig tritt das EKD-Datenschutzgesetz in der Fassung der Bekanntmachung vom 1. Januar 2013 (ABl. EKD S. 2, S. 34) außer Kraft.