Gesetz über den Kirchlichen Datenschutz (KDG)

Durchführungsverordnung zum KDG (KDG-DVO)

in der Fassung der VDD Vollversammlung vom 24. November 2025

Katholisches Datenschutzzentrum

Gesetz über den Kirchlichen Datenschutz (KDG)

Gesetz über den Kirchlichen Datenschutz (KDG) in der Fassung des Beschlusses der Vollversammlung des Verbandes der Diözesen Deutschlands vom 20. November 2017, geändert durch Beschluss der Vollversammlung des Verbandes der Diözesen Deutschlands vom 24. November 2025

Seiten 3-45

Durchführungsverordnung zum KDG (KDG-DVO)

Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO} in der Fassung des Beschlusses der Vollversammlung des Verbandes der Diözesen Deutschlands vom 19. November 2018, geändert durch Beschluss der Vollversammlung des Verbandes der Diözesen Deutschlands vom 24. November 2025

Seiten 46-58

nichtamtliche Lesefassungen

Inkraftsetzung zum 01.03.2026, veröffentlicht in den Gesetz- und Mitteilungsblättern der nordrhein-westfälischen (Erz-)Diözesen:

Erzdiözese Paderborn
Kirchliches Amtsblatt 1 Januar 2026, Gesetz vom 22.12.2025

Erzdiözese Köln
Amtsblatt Stück 3 März 2026, Gesetz vom 05.02.2026

Diözese Aachen
Kirchliches Amtsblatt Nr. 3 März 2026, Gesetz vom 03.02.2026

Diözese Essen
Kirchliches Amtsblatt Stück 2 Februar 2026, Gesetz vom 05.02.2026

Diözese Münster
Kirchliches Amtsblatt Nr. 3 März 2026, Gesetz vom 04.02.2026

Herausgegeben vom Diözesandatenschutzbeauftragten der nordrhein-westfälischen (Erz-)Diözesen

So erreichen Sie uns:
Katholisches Datenschutzzentrum (KdöR)
Brackeler Hellweg 144
44309 Dortmund
Tel. 0231 / 13 89 85 – 0
Fax 0231 / 13 89 85 – 22
E-Mail: info@kdsz.de
www.katholisches-datenschutzzentrum.de

Revision 2.0 / 19.11.2026

Gesetz über den Kirchlichen Datenschutz (KDG) in der Fassung des Beschlusses der Vollversammlung des Verbandes der Diözesen Deutschlands vom 20. November 2017, geändert durch Beschluss der Vollversammlung des Verbandes der Diözesen Deutschlands vom 24. November 2025

Inhaltsübersicht

Präambel

Kapitel 1
Allgemeine Bestimmungen

§ 1 Zweck
§ 2 Sachlicher Anwendungsbereich
§ 3 Organisatorischer Anwendungsbereich
§ 4 Begriffsbestimmungen

Kapitel 2
Grundsätze

§ 5 Datengeheimnis
§ 6 Rechtmäßigkeit der Verarbeitung personenbezogener Daten
§ 7 Grundsätze für die Verarbeitung personenbezogener Daten
§ 8 Einwilligung
§ 9 - nicht belegt -
§ 10 - nicht belegt -
§ 11 Verarbeitung besonderer Kategorien personenbezogener Daten
§ 12 Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten
§ 13 Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist

Kapitel 3
Informationspflichten des Verantwortlichen und Rechte der betroffenen Person

Abschnitt 1
Informationspflichten des Verantwortlichen

§ 14 Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person
§ 15 Informationspflicht bei unmittelbarer Datenerhebung
§ 16 Informationspflicht bei mittelbarer Datenerhebung

Abschnitt 2
Rechte der betroffenen Person

§ 17 Auskunftsrecht der betroffenen Person
§ 18 Recht auf Berichtigung
§ 19 Recht auf Löschung
§ 20 Recht auf Einschränkung der Verarbeitung
§ 21 Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung
§ 22 Recht auf Datenübertragbarkeit
§ 23 Widerspruchsrecht
§ 24 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling
§ 25 Unabdingbare Rechte der betroffenen Person

Kapitel 4
Verantwortlicher und Auftragsverarbeiter

Abschnitt 1

Technik und Organisation; Auftragsverarbeitung

§ 26 Technische und organisatorische Maßnahmen
§ 27 Technikgestaltung und Voreinstellungen
§ 28 Gemeinsam Verantwortliche
§ 29 Verarbeitung personenbezogener Daten im Auftrag
§ 30 Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters

Abschnitt 2
Pflichten des Verantwortlichen

§ 31 Verzeichnis von Verarbeitungstätigkeiten
§ 32 Zusammenarbeit mit der Datenschutzaufsicht
§ 33 Meldung an die Datenschutzaufsicht
§ 34 Benachrichtigung der betroffenen Person
§ 35 Datenschutz-Folgenabschätzung und vorherige Konsultation

Abschnitt 3
Betrieblicher Datenschutzbeauftragter

§ 36 Benennung von betrieblichen Datenschutzbeauftragten
§ 37 Rechtsstellung des betrieblichen Datenschutzbeauftragten
§ 38 Aufgaben des betrieblichen Datenschutzbeauftragten

Kapitel 5
Übermittlung personenbezogener Daten an Drittländer, internationale Organisationen oder nichtstaatliche Völkerrechtssubjekte

§ 39 Allgemeine Grundsätze
§ 40 Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses oder bei geeigneten Garantien
§ 41 Ausnahmen für bestimmte Fälle

Kapitel 6
Unabhängige Datenschutzaufsicht

§ 42 Datenschutzaufsicht
§ 43 Der oder die Diözesandatenschutzbeauftragte und seine oder ihre Vertretung
§ 44 Aufgaben der Datenschutzaufsicht
§ 45 Zuständigkeit der Datenschutzaufsicht bei über- oder mehrdiözesanen Rechtsträgern sowie bei gemeinsamer Verantwortlichkeit
§ 46 Zusammenarbeit kirchlicher Stellen mit den Datenschutzaufsichten
§ 47 Befugnisse der Datenschutzaufsicht

Kapitel 7
Beschwerde, gerichtlicher Rechtsbehelf, Haftung und Sanktionen

§ 48 Beschwerde bei einer Datenschutzaufsicht
§ 49 Recht auf gerichtlichen Rechtsbehelf gegen einen Bescheid der Datenschutzaufsicht
§ 49a Recht auf gerichtlichen Rechtsbehelf gegen Verantwortliche oder kirchliche Auftragsverarbeiter
§ 49b Zuständigkeit der Datenschutzgerichte
§ 50 Haftung und Schadenersatz
§ 51 Geldbußen

Kapitel 8
Vorschriften für besondere Verarbeitungssituationen

§ 52 Videoüberwachung
§ 52a Gottesdienste und kirchliche Veranstaltungen
§ 53 Verarbeitung personenbezogener Daten für Zwecke des Beschäftigungsverhältnisses
§ 54 Verarbeitung personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken, zu Archivzwecken oder zu statistischen Zwecken
§ 54a Verarbeitung personenbezogener Daten zur institutionellen Aufarbeitung sexualisierter Gewalt und anderer Formen des Missbrauchs
§ 55 Verarbeitung personenbezogener Daten durch die Medien

Kapitel 9
Übergangs- und Schlussbestimmungen

§ 56 Ermächtigungen
§ 57 Übergangsbestimmungen
§ 58 Inkrafttreten

Präambel

[1]Aufgabe des Datenschutzes ist es, die Grundrechte und Grundfreiheiten natürlicher Personenund insbesondere deren Recht auf Schutz personenbezogener Daten bei der Verarbeitung dieser Daten zu schützen. [2]Für die katholische Kirche ist der Schutz der personenbezogenen Daten ein unerlässlicher Bestandteil der in can. 220 des Codex Iuris Canonici (CIC) anerkannten Rechte.
[3]Zur Erfüllung des kirchlichen Auftrages ist die Verarbeitung personenbezogener Daten durch kirchliche Stellen erforderlich.

[4]Dieses Gesetz über den Kirchlichen Datenschutz (KDG) wird erlassen aufgrund des verfassungsrechtlich garantierten Rechts der Katholischen Kirche, ihre Angelegenheiten selbstständig innerhalb der Schranken des für alle geltenden Gesetzes zu ordnen und zu verwalten. [5]Dieses Recht ist auch europarechtlich geachtet und festgeschrieben in Art. 91 und Erwägungsgrund 165 der 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 – EU-DSGVO) sowie in Art. 17 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV). [6]In Wahrnehmung dieses Rechts stellt dieses Gesetz den Einklang mit der EUDSGVO her.

Kapitel 1
Allgemeine Bestimmungen

§ 1
Zweck

Zweck dieses Gesetzes ist es, betroffene Personen davor zu schützen, dass sie durch die Verarbeitung ihrer personenbezogenen Daten in ihrem Persönlichkeitsrecht beeinträchtigt werden, und den freien Verkehr solcher Daten zu ermöglichen.

§ 2
Sachlicher Anwendungsbereich

(1) [1]Dieses Gesetz gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. [2]§ 53 Absatz 3 bleibt unberührt.

(2) Soweit besondere kirchliche oder besondere staatliche Rechtsvorschriften auf Verarbeitungen personenbezogener Daten anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor, sofern sie das Datenschutzniveau dieses Gesetzes nicht unterschreiten.

(3) Die Verpflichtung zur Wahrung des Beicht- und Seelsorgegeheimnisses, anderer gesetzlicher Geheimhaltungspflichten oder anderer Berufs- oder besonderer Amtsgeheimnisse, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

§ 3
Organisatorischer Anwendungsbereich

(1) Dieses Gesetz gilt für die Verarbeitung personenbezogener Daten durch folgende kirchliche Stellen:

a) die Diözese, die Kirchengemeinden, die Kirchenstiftungen und die Kirchengemeindeverbände,
b) den Deutschen Caritasverband, die Diözesan-Caritasverbände, ihre Untergliederungen und ihre Fachverbände ohne Rücksicht auf ihre Rechtsform,
c) die kirchlichen Körperschaften, Stiftungen, Anstalten, Werke, Einrichtungen und die sonstigen kirchlichen Rechtsträger ohne Rücksicht auf ihre Rechtsform.

(2) Dieses Gesetz findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten eines kirchlichen Verantwortlichen oder Auftragsverarbeiters erfolgt, unabhängig davon, wo die Verarbeitung stattfindet.

§ 4
Begriffsbestimmungen

Im Sinne dieses Gesetzes bezeichnet der Ausdruck:

1. „personenbezogene Daten" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, 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, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

2. „besondere Kategorien personenbezogener Daten" personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Die Zugehörigkeit zu einer Kirche oder Religionsgemeinschaft ist keine besondere Kategorie personenbezogener Daten.

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, wirtschaftliche Lage, Gesundheit, persönliche 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 großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen 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. „Verantwortlicher“ 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; sind die Zwecke und Mittel dieser Verarbeitung durch kirchliches, staatliches oder europäisches Recht vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach diesem Recht vorgesehen werden.

10. „Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen 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, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;

13. „Einwilligung“ der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung 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 beziehungsweise 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“ ein Land außerhalb der Europäischen Union oder des europäischen Wirtschaftsraums;

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

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

21. „Datenschutzaufsicht“ die von einem oder mehreren Diözesanbischöfen gemäß §§ 42 ff. errichtete unabhängige, mit der Datenschutzaufsicht beauftragte kirchliche Behörde;

22. „Diözesandatenschutzbeauftragter“ oder „Diözesandatenschutzbeauftragte“ den Leiter oder die Leiterin der Datenschutzaufsicht;

23. „Betrieblicher Datenschutzbeauftragter“ oder „Betriebliche Datenschutzbeauftragte“ den vom Verantwortlichen oder vom Auftragsverarbeiter benannten Datenschutzbeauftragten oder die vom Verantwortlichen oder vom Auftragsverarbeiter benannte Datenschutzbeauftragte;

24. „Beschäftigte“ insbesondere

    a) Kleriker und Kandidaten für das Weiheamt,
    b) Ordensangehörige, soweit sie auf einer Planstelle in einer Einrichtung der eigenen Ordensgemeinschaft oder aufgrund eines Gestellungsvertrages tätig sind,
    c) in einem Beschäftigungsverhältnis oder in einem kirchlichen Beamtenverhältnis stehende Personen,
    d) zu ihrer Berufsbildung tätige Personen mit Ausnahme der Postulanten und Novizen,
    e) Teilnehmende an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobungen (Rehabilitanden),
    f) in anerkannten Werkstätten für Menschen mit Behinderungen tätige Personen,
    g) nach dem Bundesfreiwilligendienstgesetz oder dem Jugendfreiwilligendienstegesetz oder in vergleichbaren Diensten tätige Personen sowie Praktikanten oder Praktikantinnen,
    h) Personen, die wegen ihrer wirtschaftlichen Unselbstständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,
    i) sich für ein Beschäftigungsverhältnis Bewerbende sowie Personen, deren Beschäftigungsverhältnis beendet ist.
    j) Leiharbeitnehmerinnen und Leiharbeitnehmer, soweit sie zu einem kirchlichen Arbeitgeber entsandt sind.

Kapitel 2
Grundsätze

§ 5
Datengeheimnis

(1) [1]Den bei der Verarbeitung personenbezogener Daten tätigen Personen ist untersagt, diese unbefugt zu verarbeiten (Datengeheimnis). [2]Diese Personen sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis und die Einhaltung der einschlägigen Datenschutzregelungen schriftlich zu verpflichten. [3]Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

(2) Absatz 1 gilt auch für ehrenamtlich tätige Personen, sofern sie personenbezogene Daten verarbeiten.

§ 6
Rechtmäßigkeit der Verarbeitung personenbezogener Daten

(1) Die Verarbeitung personenbezogener Daten ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) Dieses Gesetz oder eine andere kirchliche oder eine staatliche Rechtsvorschrift erlaubt sie oder ordnet sie an;
b) die betroffene Person hat in die Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke eingewilligt;
c) 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 erfolgen;
d) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
e) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
f) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im kirchlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
g) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um einen Minderjährigen handelt. Lit. g) gilt nicht für die von öffentlich-rechtlich organisierten kirchlichen Stellen in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

(2) Die Verarbeitung für einen anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, ist nur rechtmäßig, wenn

a) eine Rechtsvorschrift dies erlaubt oder anordnet und kirchliche Interessen nicht entgegenstehen;
b) die betroffene Person eingewilligt hat,
c) offensichtlich ist, dass es im Interesse der betroffenen Person liegt, und kein Grund zu der Annahme besteht, dass sie in Kenntnis des anderen Zwecks ihre Einwilligung verweigern würde,
d) Angaben der betroffenen Person überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
e) die Daten allgemein zugänglich sind oder der Verantwortliche sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Zweckänderung offensichtlich überwiegt,
f) sie zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist, sofern

nicht die Interessen der betroffenen Person an dem Ausschluss der Verarbeitung überwiegen;

g) es zur Verfolgung oder Aufklärung von Straftaten oder Ordnungswidrigkeiten oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist;
h) es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte eines Dritten erforderlich ist,
i) es zur institutionellen Aufarbeitung von sexualisierter Gewalt und anderen Formen es Missbrauchs auf der Grundlage kirchlichen Rechts erforderlich ist und die Interessen der betroffenen Person (§ 4 Nr. 1) durch angemessene Maßnahmen gewahrt sind;
j) der Auftrag der Kirche oder die Glaubwürdigkeit ihres Dienstes dies erfordert oder
k) es zur Vorbereitung, Durchführung und Nachbereitung von kirchlichen Wahlen insbesondere zu diözesanen, pfarrlichen oder kirchengemeindlichen Gremien erforderlich ist; hierzu gehören auch die Kandidatenwerbung und -ansprache sowie nachgelagerte Maßnahmen zu Information und Schulung.

(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 den Verantwortlichen dient. [2]Das gilt auch für die Verarbeitung zu Ausbildungs- und Prüfungszwecken durch den Verantwortlichen, soweit nicht überwiegende schutzwürdige Interessen der betroffenen Person entgegenstehen.

(4) Beruht die Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, nicht auf der Einwilligung der betroffenen Person oder auf einer kirchlichen oder staatlichen Rechtsvorschrift, so berücksichtigt der Verantwortliche – um festzustellen, ob die Verarbeitung zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist – unter anderem

a) jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung;
b) den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen;
c) die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß § 12 verarbeitet werden;
d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen;
e) das Vorhandensein geeigneter Garantien, zu denen die Verschlüsselung, die Pseudonymisierung oder die Anonymisierung gehören können.

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

§ 7
Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);
b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit

diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung"); eine Weiterverarbeitung für im kirchlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt als vereinbar mit den ursprünglichen Zwecken;

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung"); insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und der Aufwand nicht außer Verhältnis zum angestrebten Schutzzweck steht;
d) 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 („Richtigkeit");
e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist („Speicherbegrenzung");
f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit").

(2) Der Verantwortliche ist für die Einhaltung der Grundsätze des Absatzes 1 verantwortlich und muss dies nachweisen können („Rechenschaftspflicht").

§ 8
Einwilligung

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

(2) [1]Wird die Einwilligung bei der betroffenen Person eingeholt, ist diese auf den Zweck der Verarbeitung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. [2]Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung der betroffenen Person beruht.

(3) [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 so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. [2]Teile der Erklärung sind dann nicht verbindlich, wenn sie einen Verstoß gegen dieses Gesetz darstellen.

(4) [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.

(5) Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand 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.

(6) [1]Personenbezogene Daten eines oder einer Minderjährigen, dem oder der elektronisch eine Dienst-

leistung oder ein vergleichbares anderes Angebot von einer kirchlichen Stelle unterbreitet wird, dürfen nur verarbeitet werden, wenn der oder die Minderjährige das sechzehnte Lebensjahr vollendet hat. [2]Hat der oder die Minderjährige das sechzehnte Lebensjahr noch nicht vollendet, ist die Verarbeitung nur rechtmäßig, sofern und soweit eine Einwilligung durch die Personensorgeberechtigten erteilt wird. [3]Der für die Verarbeitung Verantwortliche unternimmt unter Berücksichtigung der verfügbaren Technik angemessene Anstrengungen, um sich in solchen Fällen zu vergewissern, dass die Einwilligung durch die Personensorgeberechtigten oder mit deren Zustimmung erteilt wurde. [4]Die Einwilligung der Personensorgeberechtigten ist nicht erforderlich, wenn kirchliche Präventions- oder Beratungsdienste einem oder einer Minderjährigen elektronisch oder nichtelektronisch unmittelbar und kostenfrei angeboten werden und die Einholung einer Einwilligung der Personensorgeberechtigten voraussichtlich die Zielsetzung des Präventions- oder Beratungsangebots gefährden oder dieser zuwiderlaufen würde.

§ 9
- weggefallen -

§ 10
- weggefallen -

§ 11
Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Die Verarbeitung besonderer Kategorien personenbezogener Daten ist untersagt.

(2) Absatz 1 gilt nicht in folgenden Fällen:

a) Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt, es sei denn, nach kirchlichem, staatlichem oder europäischem Recht kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden,
b) die Verarbeitung ist erforderlich, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach kirchlichem, staatlichem oder europäischem Recht oder nach einer Dienstvereinbarung nach der Mitarbeitervertretungsordnung, die geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsehen, zulässig ist,
c) die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben,
d) die Verarbeitung erfolgt durch eine kirchliche Stelle im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der kirchlichen Einrichtung 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,
e) die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat,
f) die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der kirchlichen Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich,
g) die Verarbeitung ist auf der Grundlage kirchlichen Rechts, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vor-

sieht, aus Gründen eines erheblichen kirchlichen Interesses erforderlich,

h) die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des oder der Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheitsoder Sozialbereich auf der Grundlage des kirchlichen oder staatlichen Rechts oder aufgrund eines Vertrags mit einem oder einer Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Absatz 3 genannten Bedingungen und Garantien erforderlich,
i) die Verarbeitung ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten, auf der Grundlage kirchlichen oder staatlichen Rechts, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsieht, erforderlich,
j) die Verarbeitung ist auf der Grundlage des 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, für im kirchlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke erforderlich,
k) die Verarbeitung ist für Zwecke der institutionellen Aufarbeitung von sexualisierter Gewalt und anderen Formen des Missbrauchs auf der Grundlage kirchlichen Rechts erforderlich und die Interessen der betroffenen Person (§ 4 Nr. 1) sind durch angemessene Maßnahmen gewahrt oder
l) die Verarbeitung ist aus Gründen eines erheblichen kirchlichen oder öffentlichen Interesses zwingend erforderlich.

(3) Die in Absatz 1 genannten personenbezogenen Daten dürfen zu den in Absatz 2 lit. h) genannten Zwecken verarbeitet werden, wenn diese Daten von Fachpersonal oder unter dessen Verantwortung verarbeitet werden und dieses Fachpersonal nach dem kirchlichen oder staatlichen Recht dem Berufsgeheimnis unterliegt, oder wenn die Verarbeitung durch eine andere Person erfolgt, die ebenfalls nach kirchlichem oder staatlichem Recht einer Geheimhaltungspflicht unterliegt.

(4) In den Fällen des Absatzes 2 sind unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen.

(5) Eine Verarbeitung von besonderen Kategorien personenbezogener Daten zu anderen Zwecken ist zulässig, wenn die Voraussetzungen der Absätze 2 bis 4 und ein Ausnahmetatbestand nach § 6 Absätze 2 bis 5 vorliegen.

§ 12
Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten

Die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln aufgrund von § 6 Absatz 1 ist nur zulässig, wenn dies nach kirchlichem oder staatlichem Recht, welches geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht, zulässig ist.

§ 13
Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist

(1) Ist für die Zwecke, für die ein Verantwortlicher personenbezogene Daten verarbeitet, die Identifizierung der betroffenen Person durch den Verantwortlichen nicht oder nicht mehr erforderlich, so ist dieser nicht verpflichtet, zur bloßen Einhaltung dieses Gesetzes zusätzliche Informationen aufzubewahren, einzuholen oder zu verarbeiten, um die betroffene Person zu identifizieren.

(2) Kann der Verantwortliche in Fällen gemäß Absatz 1 nachweisen, dass er nicht in der Lage ist, die betroffene Person zu identifizieren, so unterrichtet er die betroffene Person hierüber, sofern möglich. In diesen Fällen finden die §§ 17 bis 22 keine Anwendung, es sei denn, die betroffene Person stellt zur Ausübung ihrer in diesen Bestimmungen niedergelegten Rechte zusätzliche Informationen bereit, die ihre Identifizierung ermöglichen.

Kapitel 3
Informationspflichten des Verantwortlichen und Rechte der betroffenen Person

Abschnitt 1
Informationspflichten des Verantwortlichen

§ 14
Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person

(1) [1]Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person innerhalb einer angemessenen Frist alle Informationen gemäß den §§ 15 und 16 und alle Mitteilungen gemäß den §§ 17 bis 24 und 34, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache, ggf. auch mit standardisierten Bildsymbolen, zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Minderjährige richten. [2]Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch. [3]Falls von der betroffenen Person verlangt, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde.

(2) [1]Der Verantwortliche erleichtert der betroffenen Person die Ausübung ihrer Rechte gemäß den §§ 17 bis 24. [2]In den Fällen des § 13 Absatz 2 darf sich der Verantwortliche nur dann weigern, aufgrund des Antrags der betroffenen Person auf Wahrnehmung ihrer Rechte gemäß den §§ 17 bis 24 tätig zu werden, wenn er glaubhaft macht, dass er nicht in der Lage ist, die betroffene Person zu identifizieren.

(3) [1]Der Verantwortliche stellt der betroffenen Person Informationen über die auf Antrag gemäß den §§ 17 bis 24 ergriffenen Maßnahmen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung. [2]Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. [3]Der Verantwortliche unterrichtet die betroffene Person innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung. [4]Stellt die betroffene Person den Antrag elektronisch, so ist sie nach Möglichkeit auf elektronischem Weg zu unterrichten, sofern sie nichts anderes angibt.

(4) Wird der Verantwortliche auf den Antrag der betroffenen Person hin nicht tätig, so unterrichtet er die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, bei der Datenschutzaufsicht Beschwerde zu erheben oder einen gerichtlichen Rechtsbehelf einzulegen.

(5) [1]Informationen gemäß den §§ 15 und 16 sowie alle Mitteilungen und Maßnahmen gemäß den §§ 17 bis 24 und 34 werden unentgeltlich zur Verfügung gestellt. [2]Bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person kann der Verantwortliche

a) ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder
b) sich weigern, aufgrund des Antrags tätig zu werden.

[3]Der Verantwortliche hat den Nachweis für den offenkundig unbegründeten oder exzessiven harakter des Antrags zu erbringen.

(6) Hat der Verantwortliche begründete Zweifel an der Identität der natürlichen Person, die den Antrag gemäß den §§ 17 bis 23 stellt, so kann er unbeschadet des § 13 zusätzliche Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind.

§ 15
Informationspflicht bei unmittelbarer Datenerhebung

(1) Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:

a) den Namen und die Kontaktdaten des Verantwortlichen;
b) gegebenenfalls die Kontaktdaten des oder der betrieblichen Datenschutzbeauftragten;
c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
d) wenn die Verarbeitung auf § 6 Absatz 1 lit. g) beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und
f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an oder in ein Drittland oder an eine internationale Organisation zu übermitteln sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Europäischen Kommission oder im Falle von Übermittlungen gemäß § 40 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist oder wo sie verfügbar sind.

(2) Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche 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:

a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
b) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
c) wenn die Verarbeitung auf § 6 Absatz 1 lit. b) oder § 11 Absatz 2 lit. a) beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
d) das Bestehen eines Beschwerderechts bei der Datenschutzaufsicht;

e) ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte und
f) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß § 24 Absätze 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 der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so stellt er 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 bis 3 finden keine Anwendung, wenn und soweit die betroffene Person bereits über die Informationen verfügt oder die Informationserteilung an die betroffene Person einen unverhältnismäßigen Aufwand erfordern würde und das Interesse der betroffenen Person an der Informationserteilung nach den Umständen des Einzelfalls, insbesondere wegen des Zusammenhangs, in dem die Daten erhoben wurden, als gering anzusehen ist.

(5) Die Absätze 1 bis 3 finden auch dann keine Anwendung,

a) wenn und 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,
b) wenn die Erteilung der Information die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche beeinträchtigen würde und die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen oder
c) wenn durch die Information die Wahrnehmung des Auftrags der Kirche gefährdet wird.

§ 16
Informationspflicht bei mittelbarer Datenerhebung

(1) Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person über die in § 15 Absätze 1 und 2 genannten Informationen hinaus mit

a) die zu ihr verarbeiteten Daten und
b) aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls, ob sie aus öffentlich zugänglichen Quellen stammen.

(2) Der Verantwortliche erteilt die Informationen

a) unter Berücksichtigung der spezifischen Umstände der Verarbeitung der personenbezogenen Daten innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats,
b) falls die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden sollen, spätestens zum Zeitpunkt der ersten Mitteilung an sie, oder,
c) falls die Offenlegung an einen anderen Empfänger beabsichtigt ist, spätestens zum Zeitpunkt der ersten Offenlegung.

(3) Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erlangt wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß Absatz 1 zur Verfügung.

(4) Die Absätze 1 bis 3 finden keine Anwendung, wenn und soweit

a) die betroffene Person bereits über die Informationen verfügt,
b) die Erteilung dieser Informationen sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde; dies gilt insbesondere für die Verarbeitung für im kirchlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke oder soweit die in Absatz 1 genannte Pflicht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt. In diesen Fällen ergreift der Verantwortliche geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung dieser Informationen für die Öffentlichkeit,
c) die Erlangung oder Offenlegung durch kirchliche, staatliche oder europäische Rechtsvorschriften, denen der Verantwortliche unterliegt und die geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsehen, ausdrücklich geregelt ist oder
d) die personenbezogenen Daten gemäß dem kirchlichen, staatlichen oder europäischen Recht dem Berufsgeheimnis, einschließlich einer satzungsmäßigen Geheimhaltungspflicht, unterliegen und daher vertraulich behandelt werden müssen.

(5) Die Absätze 1 bis 3 finden keine Anwendung, wenn die Erteilung der Information

a) im Falle einer kirchlichen Stelle im Sinne des § 3 Abs. 1 lit. a)

(aa) die ordnungsgemäße Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgaben gefährden würde oder
(bb) die Information dem kirchlichen Wohl erhebliche Nachteile bereiten würde

b) im Fall einer kirchlichen Stelle im Sinne des § 3 Absatz 1 lit. b) oder c) die Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche beeinträchtigen würde und nicht das Interesse der betroffenen Person an der Informationserteilung überwiegt.

(6) [1]Unterbleibt eine Information der betroffenen Person nach Maßgabe des Absatzes 1, ergreift der Verantwortliche geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person. [2]Der Verantwortliche hält schriftlich fest, aus welchen Gründen er von einer Information abgesehen hat.

Abschnitt 2
Rechte der betroffenen Person

§ 17
Auskunftsrecht der betroffenen Person

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen eine Auskunft 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:

a) die Verarbeitungszwecke;
b) die Kategorien personenbezogener Daten, die verarbeitet werden;

c) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;
d) 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;
e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;
f) das Bestehen eines Beschwerderechts bei der Datenschutzaufsicht;
g) wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;
h) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß § 24 Absätze 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 oder in ein Drittland oder an eine internationale Organisation übermittelt, so hat die betroffene Person das Recht, über die geeigneten Garantien gemäß § 40 im Zusammenhang mit der Übermittlung unterrichtet zu werden.

(3) [1]Der Verantwortliche stellt eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung. [2]Für alle weiteren Kopien, die die betroffene Person beantragt, kann der Verantwortliche 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.

(4) Das Recht auf Erhalt einer Kopie gemäß Absatz 3 darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

(5) Das Recht auf Auskunft der betroffenen Person gegenüber einem kirchlichen Archiv besteht nicht, wenn das Archivgut nicht durch den Namen der Person erschlossen ist oder keine Angaben gemacht werden, die das Auffinden des betreffenden Archivguts mit vertretbarem Verwaltungsaufwand ermöglichen.

(6) Das Recht auf Auskunft der betroffenen Person besteht ergänzend zu Absatz 5 nicht, wenn

a) die betroffene Person nach § 15 Absatz 4 oder 5 oder nach § 16 Absatz 4 lit. d) nicht zu informieren ist oder
b) die Daten

(aa) nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher oder satzungsmäßiger Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder
(bb) ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen

und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde sowie eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist.

(7) [1]Die Gründe der Auskunftsverweigerung sind zu dokumentieren. [2]Die Ablehnung der Auskunftserteilung ist gegenüber der betroffenen Person zu begründen, soweit nicht durch die Mitteilung der tatsächlichen oder rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. [3]Die zum Zweck der Auskunftserteilung an die betroffene Person und zu deren Vorbereitung gespeicherte Daten dürfen nur für diesen Zweck sowie für Zwecke der Datenschutzkontrolle verarbeitet werden; für andere Zwecke ist die Verarbeitung nach Maßgabe des § 20 einzuschränken.

(8) [1]Wird der betroffenen Person durch eine kirchliche Stelle im Sinne des § 3 Absatz 1 lit. a) keine Auskunft erteilt, so ist sie auf Verlangen der betroffenen Person dem oder der Diözesandatenschutzbeauftragten zu erteilen, soweit nicht die Bischöfliche Behörde im Einzelfall feststellt, dass dadurch kirchliche Interessen erheblich beeinträchtigt würden. [2]Die Mitteilung des oder der Diözesandatenschutzbeauftragten an die betroffene Person über das Ergebnis der datenschutzrechtlichen Prüfung darf keine Rückschlüsse auf den Erkenntnisstand des Verantwortlichen zulassen, sofern dieser nicht einer weitergehenden Auskunft zustimmt.

(9) Das Recht der betroffenen Person auf Auskunft über personenbezogene Daten, die durch eine kirchliche Stelle im Sinne des § 3 Absatz 1 lit. a) weder automatisiert verarbeitet noch nicht automatisiert verarbeitet und in einem Dateisystem gespeichert werden, besteht nur, soweit die betroffene Person Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse steht.

§ 18
Recht auf Berichtigung

(1) [1]Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die 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.

§ 19
Recht auf Löschung

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:

a) die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig;
b) die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß § 6 Absatz 1 lit. b) oder § 11 Absatz 2 lit. a) stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung;
c) die betroffene Person legt gemäß § 23 Absatz 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß § 23 Absatz 2 Widerspruch gegen die Verarbeitung ein;
d) die personenbezogenen Daten wurden unrechtmäßig verarbeitet;
e) die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem staatlichen oder dem kirchlichen Recht erforderlich, dem der Verantwortliche unterliegt.

(2) Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er gemäß Absatz 1 zu deren Löschung verpflichtet, so trifft er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, um für die Datenverarbeitung Verantwortliche, 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

a) zur Ausübung des Rechts auf freie Meinungsäußerung und Information;
b) zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach kirchlichem oder staatlichem Recht, dem der Verantwortliche unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im kirchlichen Interesse liegt oder in Ausübung hoheitlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
c) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß § 11 Absatz 2 lit. h) und i) sowie § 11 Absatz 3;
d) für im kirchlichem Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke, soweit das in Absatz 1 genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, oder
e) zur Geltendmachung von Rechtsansprüchen sowie zur Ausübung oder Verteidigung von Rechten oder
f) zum Erhalt und zur Gewährleistung der Nachvollziehbarkeit von Amtshandlungen sowie von Urkunden und vergleichbaren Dokumenten; hierzu gehören insbesondere die durch kirchliche Rechtsvorschriften vorgesehenen Eintragungen in die Kirchenbücher (insbesondere Taufen, Trauungen, Todesfälle) sowie Dekrete, Beschlüsse von Gremien der Diözesen und Kirchengemeinden und sonstige Urkunden.

(4) [1]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 § 20. [2]Dies gilt nicht, wenn die personenbezogenen Daten unrechtmäßig verarbeitet wurden. [3]Als Einschränkung der Verarbeitung gelten auch die Sperrung und die Eintragung eines Sperrvermerks.

§ 20
Recht auf Einschränkung der Verarbeitung

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, wenn eine der folgenden Voraussetzungen gegeben ist:

a) die Richtigkeit der personenbezogenen Daten wird von der betroffenen Person bestritten, und zwar für eine Dauer, die es dem Verantwortlichen ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen;
b) die Verarbeitung ist unrechtmäßig und die betroffene Person lehnt die Löschung der personenbezogenen Daten ab und verlangt stattdessen die Einschränkung der Nutzung der personenbezogenen Daten;
c) der Verantwortliche benötigt die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger, die betroffene Person benötigt sie jedoch zur Geltendmachung von Rechtsansprüchen oder zur Ausübung oder Verteidigung von Rechten oder
d) die betroffene Person hat Widerspruch gegen die Verarbeitung gemäß § 23 eingelegt und es steht noch nicht fest, ob die berechtigten Gründe des Verantwortlichen 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 von Rechtsansprüchen oder zur Ausübung oder Verteidigung von Rechten oder zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen kirchlichen Interesses verarbeitet werden.

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

(4) Die in Absatz 1 lit. a), b) und d) vorgesehenen Rechte bestehen nicht, soweit diese Rechte voraussichtlich die Verwirklichung der im kirchlichen Interesse liegenden Archivzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Ausnahmen für die Erfüllung dieser Zwecke erforderlich sind.

§ 21
Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung

[1]Der Verantwortliche teilt allen Empfängern, denen personenbezogene Daten offengelegt wurden, jede Berichtigung oder Löschung der personenbezogenen Daten oder eine Einschränkung der Verarbeitung nach §§ 18, 19 Absatz 1 und 20 mit, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. [2]Der Verantwortliche unterrichtet die betroffene Person über diese Empfänger, wenn die betroffene Person dies verlangt.

§ 22
Recht auf Datenübertragbarkeit

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

a) die Verarbeitung auf einer Einwilligung gemäß § 6 Absatz 1 lit. b) oder § 11 Absatz 2 lit. a) oder auf einem Vertrag gemäß § 6 Absatz 1 lit. c) beruht und
b) die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

(2) Bei der Ausübung ihres Rechts auf Datenübertragbarkeit gemäß Absatz 1 hat die betroffene Person das Recht zu erwirken, dass die personenbezogenen Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist.

(3) [1]Die Ausübung des Rechts nach Absatz 1 lässt § 19 unberührt. [2]Dieses Recht gilt nicht für eine Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im kirchlichen Interesse liegt oder in Ausübung hoheitlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

(4) Das Recht gemäß Absatz 2 darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

(5) Das Recht auf Datenübertragbarkeit besteht nicht, soweit dieses Recht voraussichtlich die Verwirklichung der im kirchlichen Interesse liegenden Archivzwecke unmöglich macht oder ernsthaft beeinträchtigt und die Ausnahmen für die Erfüllung dieser Zwecke erforderlich sind.

§ 23
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, die aufgrund von § 6 Absatz 1 lit. f) oder g) erfolgt, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmungen gestütztes Profiling. [2]Der Verantwortliche verarbeitet die personenbezogenen Daten nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung von Rechtsansprüchen oder der Ausübung oder Verteidigung von Rechten.

(2) Werden personenbezogene Daten verarbeitet, um Direktwerbung oder Fundraising zu betreiben, so hat die betroffene Person das Recht, jederzeit 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.

(3) Widerspricht die betroffene Person der Verarbeitung für Zwecke der Direktwerbung, so werden die personenbezogenen Daten nicht mehr für diese Zwecke verarbeitet.

(4) Die betroffene Person muss spätestens zum Zeitpunkt der ersten Kommunikation mit ihr ausdrücklich auf das in den Absätzen 1 und 2 genannte Recht hingewiesen werden; dieser Hinweis hat in einer verständlichen und von anderen Informationen getrennten Form zu erfolgen.

(5) [1]Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, gegen die sie betreffende Verarbeitung sie betreffender personenbezogener Daten, die zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken erfolgt, Widerspruch einzulegen. [2]Das Recht auf Widerspruch besteht nicht, soweit an der Verarbeitung ein zwingendes kirchliches oder öffentliches Interesse besteht, das die Interessen der betroffenen Person überwiegt, oder eine Rechtsvorschrift zur Verarbeitung verpflichtet.

§ 24
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 dem Verantwortlichen erforderlich ist,
b) aufgrund von kirchlichen Rechtsvorschriften, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder
c) mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

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

(4) Entscheidungen nach Absatz 2 dürfen nicht auf besonderen Kategorien personenbezogener Daten beruhen, sofern nicht § 11 Absatz 2 lit. a) oder g) gilt und angemessene Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person getroffen wurden.

§ 25
Unabdingbare Rechte der betroffenen Person

(1) Die Rechte der betroffenen Person auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit oder Widerspruch können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.

(2) 1Sind die Daten der betroffenen Person automatisiert in einer Weise gespeichert, dass mehrere Verantwortliche speicherungsberechtigt sind, und ist die betroffene Person nicht in der Lage, festzustellen, welcher Verantwortliche die Daten gespeichert hat, so kann sie sich an jeden dieser Verantwortlichen wenden. 2Dieser Verantwortliche ist verpflichtet, das Vorbringen der betroffenen Person an den Verantwortlichen, der die Daten gespeichert hat, weiterzuleiten. 3Die betroffene Person ist über die Weiterleitung und den Verantwortlichen, an den weitergeleitet wurde, zu unterrichten.

Kapitel 4
Verantwortlicher und Auftragsverarbeiter

Abschnitt 1
Technik und Organisation;
Auftragsverarbeitung

§ 26
Technische und organisatorische Maßnahmen

(1) [1]Der Verantwortliche und der Auftragsverarbeiter haben unter Berücksichtigung unter anderem 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:

a) die Pseudonymisierung, die Anonymisierung und die Verschlüsselung personenbezogener Daten;
b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
d) 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 erücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung, unbefugte Offenlegung on 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 Faktor herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen gemäß Absatz 1 nachzuweisen.

(5) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte um sicherzustellen, dass ihnen unterstellte Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach kirchlichem oder staatlichem Recht zur Verarbeitung verpflichtet.

§ 27
Technikgestaltung und Voreinstellungen

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche 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 Gesetzes zu genügen und die Rechte der betroffenen Personen zu schützen.

(1) [1]Der Verantwortliche 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 durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

(2) Ein nach dem europäischen Recht genehmigtes Zertifizierungsverfahren kann als Faktor erangezogen werden, um die Erfüllung der in den Absätzen 1 und 2 genannten Anforderungen nachzuweisen.

§ 28
Gemeinsam Verantwortliche

(1) [1]Legen mehrere Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. [2]Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtungen gemäß diesem Gesetz erfüllt, insbesondere wer den Informationspflichten gemäß den §§ 15 und 16 nachkommt.

(2) [1]Die Verarbeitung in gemeinsamer Verantwortung erfolgt auf der Grundlage der Vereinbarung gemäß Absatz 1 Satz 2 oder eines anderen Rechtsinstruments nach dem kirchlichen Recht, an die bzw. an das die gemeinsam Verantwortlichen gebunden sind. [2]Die Vereinbarung gemäß Absatz 1 Satz 2 oder das Rechtsinstrument gemäß Satz 1 enthält insbesondere die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber der betroffenen Person. [3]Die betroffene Person wird über den wesentlichen, die Verarbeitung personenbezogener Daten betreffenden Inhalt der Vereinbarung bzw. des Rechtsinstruments informiert.

(3) Ungeachtet der Einzelheiten der Vereinbarung bzw. des Rechtsinstruments kann die betroffene Person ihre Rechte im Rahmen dieses Gesetzes bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen.

§ 29
Verarbeitung personenbezogener Daten im Auftrag

(1) Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieses Gesetzes erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

(2) [1]Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. [2]Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

(3) Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem kirchlichen, dem staatlichen oder dem europäischen Recht, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem

a) Gegenstand der Verarbeitung
b) Dauer der Verarbeitung,
c) Art und Zweck der Verarbeitung,
d) die Art der personenbezogenen Daten,
e) die Kategorien betroffener Personen und
f) die Pflichten und Rechte des Verantwortlichen

festgelegt sind.

(4) Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter

a) die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeitet, sofern er nicht durch das kirchliche, das staatliche oder das europäische Recht, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen kirchlichen Interesses verbietet;
b) gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
c) alle gemäß § 26 erforderlichen Maßnahmen ergreift;
d) die in den Absätzen 2 und 5 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;
e) angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in den §§ 15 bis 25 genannten Rechte der betroffenen Person nachzukommen;
f) unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den §§ 26, 33 bis 35 genannten Pflichten unterstützt;

g) nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen aten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt, sofern nicht nach dem kirchlichen, dem staatlichen oder dem europäischen Recht eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht;
h) dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Paragraphen niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen dieses Gesetz oder gegen andere kirchliche Datenschutzbestimmungen oder Datenschutzbestimmungen der Europäischen Union oder ihrer Mitgliedstaaten verstößt.

(5) [1]Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem kirchlichen, dem staatlichen oder dem europäischen Recht dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemäß den Absätzen 3 und 4 festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieses Gesetzes erfolgt. [2]Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen ür die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

(6) Die Einhaltung nach europäischem Recht genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahrens durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um hinreichende Garantien im Sinne der Absätze 1 und 5 nachzuweisen.

(7) Unbeschadet eines individuellen Vertrags zwischen dem Verantwortlichen und dem Auftragsverarbeiter kann der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3, 4 und 5 ganz oder teilweise auf den in den Absatz 8 genannten Standardvertragsklauseln beruhen, auch wenn diese Bestandteil einer dem Verantwortlichen oder dem Auftragsverarbeiter erteilten Zertifizierung sind.

(8) Die Datenschutzaufsicht kann Standardvertragsklauseln zur Regelung der in den Absätzen 3 bis 5 genannten Fragen festlegen.

(9) [1]Der Vertrag im Sinne der Absätze 3 bis 5 bedarf der Schriftform. [2]Maßgeblich für die rsetzung der Schriftform durch die elektronische Form oder die Textform sind die jeweils geltenden staatlichen Regelungen.

(10) Ein Auftragsverarbeiter, der unter Verstoß gegen dieses Gesetz die Zwecke und Mittel der Verarbeitung bestimmt, gilt in Bezug auf diese Verarbeitung als Verantwortlicher.

§ 30
Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters

Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach kirchlichem, staatlichem oder europäischem Recht zur Verarbeitung verpflichtet sind.

Abschnitt 2
Pflichten des Verantwortlichen

§ 31
Verzeichnis von Verarbeitungstätigkeiten

(1) [1]Jeder Verantwortliche führt ein Verzeichnis aller Verarbeitungstätigkeiten, die seiner uständigkeit unterliegen. [2]Dieses Verzeichnis hat die folgenden Angaben zu enthalten:

a) den Namen und die Kon
taktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen sowie des betrieblichen Datenschutzbeauftragten, sofern ein solcher zu benennen ist;
b) die Zwecke der Verarbeitung;
c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
d) gegebenenfalls die Verwendung von Profiling;
e) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;
f) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland, an in nichtstaatliches Völkerrechtssubjekt oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands, des betreffenden nichtstaatlichen Völkerrechtssubjektes oder der betreffenden internationalen Organisation sowie bei den in § 40 Absatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
g) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
h) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 26 dieses Gesetzes.

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

a) den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie eines betrieblichen Datenschutzbeauftragten, sofern ein solcher zu benennen ist;
b) die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;
c) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland, ein nichtstaatliches Völkerrechtssubjekt oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands, des betreffenden nichtstaatlichen Völkerrechtssubjekts oder der betreffenden internationalen Organisation sowie bei den in § 40 Absatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
d) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 26 dieses Gesetzes.

(3) Das in den Absätzen 1 und 2 genannte Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.

(4) Der Verantwortliche und der Auftragsverarbeiter stellen dem oder der betrieblichen Datenschutzbeauftragten und auf Anfrage der Datenschutzaufsicht das in den Absätzen 1 und 2 genannte Verzeichnis zur Verfügung.

(5) [1]Die in den Absätzen 1 und 2 genannten Pflichten gelten für Unternehmen oder Einrichtungen, die 250 oder mehr Beschäftigte haben. [2]Sie gilt darüber hinaus für Unternehmen oder Einrichtungen mit weniger als 250 Beschäftigten, wenn durch die Verarbeitung die Rechte und Freiheiten der betroffenen Personen gefährdet werden, die Verarbeitung nicht nur gelegentlich erfolgt oder die Verarbeitung besondere Datenkategorien gemäß § 11 bzw. personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des § 12 beinhaltet.

§ 32
Zusammenarbeit mit der Datenschutzaufsicht

Der Verantwortliche und der Auftragsverarbeiter arbeiten auf Anfrage der Datenschutzaufsicht mit dieser bei der Erfüllung ihrer Aufgaben zusammen.

§ 33
Meldung an die Datenschutzaufsicht

(1) [1]Der Verantwortliche meldet der Datenschutzaufsicht unverzüglich die Verletzung des Schutzes personenbezogener Daten, wenn diese Verletzung ein Risiko für die Rechte und Freiheiten natürlicher Personen darstellt. [2]Erfolgt die Meldung nicht binnen 72 Stunden, nachdem die Verletzung des Schutzes personenbezogener Daten bekannt wurde, so ist ihr eine Begründung für die Verzögerung beizufügen.

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

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

a) 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;
b) den Namen und die Kontaktdaten des betrieblichen Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
d) eine Beschreibung der von dem Verantwortlichen 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 nach Absatz 3 nicht zeitgleich bereitgestellt werden können, stellt der Verantwortliche diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung.

(5) [1]Der Verantwortliche dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich aller damit im Zusammenhang stehenden Tatsachen, deren Auswirkungen und die ergriffenen Abhilfemaßnahmen. [2]Diese Dokumentation muss der Datenschutzaufsicht die Überprüfung der Einhaltung der Bestimmungen der Absätze 1 bis 4 ermöglichen.

§ 34
Benachrichtigung der betroffenen Person

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

(2) Die in Absatz 1 genannte Benachrichtigung der betroffenen Person beschreibt in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten und enthält zumindest die in § 33 Absatz 3 lit. b), c) und d) genannten Informationen und Maßnahmen.

(3) Die Benachrichtigung der betroffenen Person gemäß Absatz 1 ist nicht erforderlich, wenn eine der folgenden Bedingungen erfüllt ist:

a) Der Verantwortliche hat geeignete technische und organisatorische Maßnahmen getroffen und auf die von der Verletzung betroffenen personenbezogenen Daten angewandt, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung;
b) der Verantwortliche hat durch nachträglich getroffene Maßnahmen sichergestellt, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 aller Wahrscheinlichkeit nach nicht mehr besteht;
c) die Benachrichtigung erfordert einen unverhältnismäßigen Aufwand. In diesem Fall hat ersatzweise eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

(4) Wenn der Verantwortliche die betroffene Person nicht bereits über die Verletzung des Schutzes personenbezogener Daten benachrichtigt hat, kann die Datenschutzaufsicht unter Berücksichtigung der Wahrscheinlichkeit, mit der die Verletzung des Schutzes personenbezogener Daten zu einem hohen Risiko führt, von dem Verantwortlichen verlangen, dies nachzuholen, oder sie kann mit einem Beschluss feststellen, dass bestimmte der in Absatz 3 genannten Voraussetzungen erfüllt sind.

§ 35
Datenschutz-Folgenabschätzung und vorherige Konsultation

(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 und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche 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) Der Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des oder der betrieblichen Datenschutzbeauftragten ein, sofern ein solcher oder eine solche benannt wurde.

(3) Ist der Verantwortliche nach Anhörung des oder der betrieblichen Datenschutzbeauftragten der Ansicht, dass ohne Hinzuziehung der Datenschutzaufsicht eine Datenschutz-Folgenabschätzung nicht möglich ist, kann er der Datenschutzaufsicht den Sachverhalt zur Stellungnahme vorlegen.

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

a) 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;
b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß § 12 oder
c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

(5) [1]Die Datenschutzaufsicht soll eine Liste der Verarbeitungsvorgänge erstellen und veröffentlichen, für die eine Datenschutz-Folgenabschätzung gemäß Absatz 1 durchzuführen ist. [2]Sie kann ferner eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist.

(6) [1]Die Listen der Datenschutzaufsicht sollen sich an den Listen der Aufsichtsbehörden des Bundes und der Länder orientieren. [2]Gegebenenfalls ist der Austausch mit staatlichen Aufsichtsbehörden zu suchen.

(7) Die Datenschutz-Folgenabschätzung umfasst insbesondere:

a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;
b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und
d) 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 dieses Gesetz eingehalten wird.

(8) Der Verantwortliche holt gegebenenfalls die Stellungnahme der betroffenen Person zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder kirchlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge ein.

(9) Falls die Verarbeitung auf einer Rechtsgrundlage im kirchlichen, im staatlichen oder im europäischen Recht, dem der Verantwortliche 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.

(10) Erforderlichenfalls führt der Verantwortliche 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.

(11) Der Verantwortliche konsultiert vor der Verarbeitung die Datenschutzaufsicht, wenn aus der Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hat, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft.

Abschnitt 3
Betrieblicher Datenschutzbeauftragter

§ 36
Benennung von betrieblichen Datenschutzbeauftragten

(1) Kirchliche Stellen im Sinne des § 3 Absatz 1 lit. a) benennen schriftlich einen betrieblichen Datenschutzbeauftragten oder eine betriebliche Datenschutzbeauftragte.

(2) Kirchliche Stellen im Sinne des § 3 Absatz 1 lit. b) und c) benennen schriftlich einen betrieblichen Datenschutzbeauftragten oder eine betriebliche Datenschutzbeauftragte, wenn

a) sich bei ihnen in der Regel mindestens zwanzig Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigen,
b) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder
c) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß § 12 besteht.

(3) Für mehrere kirchliche Stellen im Sinne des § 3 Absatz 1 kann unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe ein gemeinsamer betrieblicher Datenschutzbeauftragter oder eine gemeinsame betriebliche Datenschutzbeauftragte benannt werden.

(4) [1]Der Verantwortliche oder der Auftragsverarbeiter veröffentlicht die Kontaktdaten des oder der betrieblichen Datenschutzbeauftragten. [2]Die Benennung von betrieblichen Datenschutzbeauftragten ist der Datenschutzaufsicht anzuzeigen.

(5) [1]Der oder die betriebliche Datenschutzbeauftragte kann eine natürliche oder eine juristische Person sein. [2]Er oder sie kann Beschäftigter oder Beschäftigte des Verantwortlichen oder des Auftragsverarbeiters sein oder seine oder ihre Aufgaben auf der Grundlage eines Dienstleistungsvertrags oder einer sonstigen Vereinbarung erfüllen. [3]Ist der oder die betriebliche Datenschutzbeauftragte Beschäftigter oder Beschäftigte des Verantwortlichen, finden § 43 Absatz 1 Satz 1 und 2 entsprechende Anwendung.

(6) Zum betrieblichen Datenschutzbeauftragten darf nur benannt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt.

(7) [1]Zum oder zur betrieblichen Datenschutzbeauftragten darf der- oder diejenige nicht benannt werden, der oder die mit der Leitung der Datenverarbeitung beauftragt ist oder dem oder der die Leitung der kirchlichen Stelle obliegt. [2]Andere Aufgaben und Pflichten des oder der Benannten dürfen im Übrigen nicht so ausgestaltet oder umfangreich sein, dass der oder die betriebliche Datenschutzbeauftragte seinen oder ihren Aufgaben nach diesem Gesetz nicht unabhängig bzw. umgehend nachkommen kann.

(8) Soweit keine Verpflichtung für die Benennung eines oder einer betrieblichen Datenschutzbeauftragten besteht, hat der Verantwortliche oder der Auftragsverarbeiter die Erfüllung der Aufgaben nach § 38 in anderer Weise sicherzustellen.

§ 37
Rechtsstellung des betrieblichen Datenschutzbeauftragten

(1) [1]Der oder die betriebliche Datenschutzbeauftragte ist dem Leiter oder der Leiterin der kirchlichen Stelle unmittelbar zu unterstellen. [2]Er oder sie ist bei der Erfüllung seiner oder ihrer Aufgaben auf dem Gebiet des Datenschutzes weisungsfrei. [3]Er oder sie darf wegen der Erfüllung seiner oder ihrer Aufgaben nicht benachteiligt werden.

(2) [1]Der Verantwortliche und der Auftragsverarbeiter stellen sicher, dass der oder die betriebliche Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird. [2]Sie unterstützen den betrieblichen Datenschutzbeauftragten oder die betriebliche Datenschutzbeauftragte bei der Erfüllung seiner oder ihrer Aufgaben, indem sie die für die Erfüllung dieser Aufgaben erforderlichen Mittel und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen zur Verfügung stellen.

[3]Zur Erhaltung der zur Erfüllung seiner oder ihrer Aufgaben erforderlichen Fachkunde haben der Verantwortliche oder der Auftragsverarbeiter dem oder der betrieblichen Datenschutzbeauftragten die Teilnahme an Fort- und Weiterbildungsveranstaltungen in angemessenem Umfang zu ermöglichen und deren Kosten zu übernehmen. § 43 Absätze 7 und 8 gelten entsprechend.

(3) Betroffene Personen können sich jederzeit und unmittelbar an den betrieblichen Datenschutzbeauftragten der die betriebliche Datenschutzbeauftragte wenden.

(4) [1]Ist ein betrieblicher Datenschutzbeauftragter oder eine betriebliche Datenschutzbeauftragte benannt worden, so ist die Kündigung seines oder ihres Arbeitsverhältnisses unzulässig, es sei denn, dass Tatsachen vorliegen, welche den Verantwortlichen oder den Auftragsverarbeiter ur Kündigung aus wichtigem Grund ohne Einhaltung der Kündigungsfrist berechtigen. [2]Nach der Abberufung als betrieblicher Datenschutzbeauftragter oder als betriebliche Datenschutzbeauftragte ist die Kündigung innerhalb eines Jahres nach der Beendigung der Bestellung unzulässig, es sei denn, dass der Verantwortliche oder der Auftragsverarbeiter zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigt ist.

(5) Der Verantwortliche und der Auftragsverarbeiter stellen sicher, dass die Wahrnehmung anderer Aufgaben und Pflichten durch den betrieblichen Datenschutzbeauftragten oder die betriebliche Datenschutzbeauftragte nicht zu einem Interessenkonflikt führt.

§ 38
Aufgaben des betrieblichen Datenschutzbeauftragten

[1]Betriebliche Datenschutzbeauftragte wirken auf die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz hin. [2]Zu diesem Zweck können sie sich in Zweifelsfällen an die Datenschutzaufsicht gemäß §§ 42 ff. wenden. [3]Sie haben insbesondere

a) die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen; zu diesem Zweck ist er über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten,
b) den Verantwortlichen oder den Auftragsverarbeiter zu unterrichten und zu beraten,
c) die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz und mit den jeweiligen besonderen Erfordernissen des Datenschutzes vertraut zu machen,
d) auf Anfrage des Verantwortlichen oder des Auftragsverarbeiters diesen bei der Durchführung einer Datenschutz-Folgenabschätzung zu beraten und bei der Überprüfung, ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung erfolgt, zu unterstützen und
e) mit der Datenschutzaufsicht zusammenzuarbeiten.

Kapitel 5
Übermittlung personenbezogener Daten an Drittländer, internationale Organisationen oder nichtstaatliche Völkerrechtssubjekte

§ 39
Allgemeine Grundsätze

[1]Jede Übermittlung personenbezogener Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland, an eine internationale Organisation oder an ein nichtstaatliches Völkerrechtssubjekt verarbeitet werden sollen, ist nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die in diesem Gesetz niedergelegten Bedingungen einhalten. [2]Dies gilt auch für die etwaige Weiterübermittlung personenbezogener Daten aus dem betreffenden Drittland, der betreffenden internationalen Organisation oder dem betreffenden nichtstaatlichen Völkerrechtssubjekt.

§ 40
Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses oder bei geeigneten Garantien

(1) Eine Übermittlung personenbezogener Daten an ein Drittland oder an eine internationale Organisation ist zulässig, wenn ein Angemessenheitsbeschluss der Europäischen Kommission vorliegt.

(2) Liegt ein Angemessenheitsbeschluss nicht vor, darf eine Übermittlung personenbezogener Daten an ein Drittland, an eine internationale Organisation oder an ein nichtstaatliches Völkerrechtssubjekt nur erfolgen, sofern der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen.

§ 41
Ausnahmen für bestimmte Fälle

(1) Falls weder ein Angemessenheitsbeschluss nach § 40 Absatz 1 noch geeignete Garantien ach § 40 Absatz 2 bestehen, ist eine Übermittlung personenbezogener Daten an ein Drittland oder an eine internationale Organisation oder an ein nichtstaatliches Völkerrechtssubjekt nur unter einer der folgenden Bedingungen zulässig:

a) die betroffene Person hat in die vorgeschlagene Übermittlung eingewilligt, nachdem sie über die für sie bestehenden möglichen Risiken derartiger Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien unterrichtet wurde;
b) die Übermittlung ist für die Erfüllung eines Vertrages zwischen der betroffenen Person und dem Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich;
c) die Übermittlung ist zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person von dem Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrages erforderlich;
d) die Übermittlung erfolgt aufgrund kirchenrechtlicher Vorschriften oder in Wahrnehmung kirchlicher Aufgaben an den Heiligen Stuhl oder an den Staat der Vatikanstadt oder ist aus anderen wichtigen Gründen des kirchlichen oder öffentlichen Interesses notwendig;
e) die Übermittlung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich;
f) die Übermittlung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen erforderlich, sofern die betroffene Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben.

(2) Der Verantwortliche oder der Auftragsverarbeiter erfasst die von ihm vorgenommene Beurteilung in der Dokumentation gemäß § 31.

Kapitel 6
Unabhängige Datenschutzaufsicht

§ 42
Datenschutzaufsicht

(1) Der Diözesanbischof richtet für den Bereich seiner Diözese eine Datenschutzaufsicht als unabhängige kirchliche Behörde ein.

(2) [1]Der Diözesanbischof bestellt für den Bereich seiner Diözese einen Diözesandatenschutzbeauftragten als Leiter oder eine Diözesandatenschutzbeauftragte als Leiterin der Datenschutzaufsicht. [2]Zum oder zur Diözesandatenschutzbeauftragten kann nur eine natürliche Person bestellt werden.

(3) [1]Der oder die Diözesandatenschutzbeauftragte handelt bei der Erfüllung seiner oder ihrer Aufgaben und bei der Ausübung seiner oder ihrer Befugnisse gemäß diesem Gesetz völlig unabhängig und ist nur dem kirchlichen Recht und dem für die Kirchen verbindlichen staatlichen oder europäischen Recht unterworfen. [2]Die Ausübung seiner oder ihrer Tätigkeit geschieht in organisatorischer und sachlicher Unabhängigkeit. [3]Die Dienstaufsicht ist so zu regeln, dass dadurch die Unabhängigkeit nicht beeinträchtigt wird.

(4) [1]Der oder die Diözesandatenschutzbeauftragte sieht von allen mit den Aufgaben seines oder ihres Amtes nicht zu vereinbarenden Handlungen ab und übt während seiner oder ihrer Amtszeit keine andere mit seinem oder ihrem Amt nicht zu vereinbarende entgeltliche oder unentgeltliche Tätigkeit aus. [2]Dem steht eine Bestellung als Diözesandatenschutzbeauftragter oder Diözesandatenschutzbeauftragte für mehrere Diözesen und/oder Ordensgemeinschaften nicht entgegen.

(5) [1]Dem oder der Diözesandatenschutzbeauftragten wird die Personal- und Sachausstattung zur Verfügung gestellt, die er oder sie benötigt, um seine oder ihre Aufgaben und Befugnisse wahrnehmen zu können. [2]Dies gilt auch für seine oder ihre Aufgaben im Bereich der Amtshilfe und der Zusammenarbeit mit anderen Datenschutzaufsichten im Sinne des § 44 Absatz 2 lit. f). [3]Er oder sie verfügt über einen eigenen jährlichen Haushalt, der gesondert auszuweisen ist und veröffentlicht wird, und unterliegt der Rechnungsprüfung durch die dafür von der Diözese bestimmte Stelle, soweit hierdurch seine oder ihre Unabhängigkeit nicht beeinträchtigt wird.

(6) [1]Der oder die Diözesandatenschutzbeauftragte wählt das notwendige Personal aus, das von der Datenschutzaufsicht selbst, ggf. einer anderen kirchlichen Stelle angestellt wird. [2]Die angestellten Mitarbeitenden unterstehen der Dienst- und Fachaufsicht des oder der Diözesandatenschutzbeauftragten und können, soweit sie bei einer anderen kirchlichen Stelle angestellt sind, nur mit seinem oder ihrem Einverständnis von der kirchlichen Stelle gekündigt, versetzt oder abgeordnet werden. [3]Die Mitarbeitenden sehen von allen mit den Aufgaben ihres Amtes nicht zu vereinbarenden Handlungen ab und üben während ihrer Amtszeit keine anderen mit ihrem Amt nicht zu vereinbarenden entgeltlichen oder unentgeltlichen Tätigkeiten aus.

(7) [1]Der oder die Diözesandatenschutzbeauftragte kann Aufgaben der Personalverwaltung und Personalwirtschaft auf andere kirchliche Stellen übertragen oder sich deren Hilfe bedienen. [2]Diesen dürfen personenbezogene Daten der Mitarbeitenden übermittelt werden, soweit deren Kenntnis zur Erfüllung der übertragenen Aufgaben erforderlich ist.

(8) [1]Die Datenschutzaufsicht ist oberste Dienstbehörde im Sinne des § 96 Strafprozessordnung. [2]Der oder die Diözesandatenschutzbeauftragte trifft die Entscheidung über Aussagegenehmigungen für sich und seinen oder ihren Bereich in eigener Verantwortung. [3]Die Datenschutzaufsicht ist oberste Aufsichtsbehörde im Sinne des § 99 Verwaltungsgerichtsordnung.

(9) [1]Der oder die Diözesandatenschutzbeauftragte ist berechtigt, über Personen, die ihm oder ihr in seiner oder ihrer Eigenschaft als Diözesandatenschutzbeauftragter oder Diözesandatenschutzbeauftragte Tatsachen anvertraut haben, sowie über diese Tatsachen selbst keine Auskunft zu geben. [2]Dies gilt auch für die Mitarbeitenden des oder der Diözesandatenschutzbeauftragten mit der Maßgabe, dass über die Ausübung dieses Rechts der oder die Diözesandatenschutzbeauftragte entscheidet. [3]Soweit diese Verschwiegenheit reicht, darf die Vorlegung oder Auslieferung von Akten oder anderen Dokumenten von ihm oder ihr nicht gefordert werden. [4]Im Verfahren vor den kirchlichen Datenschutzgerichten darf er oder sie entsprechende Angaben unkenntlich machen. 5§ 17 bleibt unberührt.

§ 43
Der oder die Diözesandatenschutzbeauftragte und seine oder ihre Vertretung

(1) [1]Die Bestellung des oder der Diözesandatenschutzbeauftragten durch den Diözesanbischof erfolgt für die Dauer von mindestens vier, höchstens sechs Jahren und gilt bis zur Aufnahme der Amtsgeschäfte durch den Nachfolger oder die Nachfolgerin. [2]Die mehrmalige erneute Bestellung ist zulässig. [3]Die Bestellung für mehrere Diözesen und/oder Ordensgemeinschaften ist zulässig. [4]Der oder die Diözesandatenschutzbeauftragte übt sein oder ihr Amt hauptamtlich aus.

(2) [1]Zum oder zur Diözesandatenschutzbeauftragten darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. [2]Er oder sie soll die Befähigung zum Richteramt gemäß dem Deutschen Richtergesetz haben. [3]Als Person, die das katholische Profil der Einrichtung inhaltlich prägt, mitverantwortet und nach außen repräsentiert, muss er oder sie der katholischen Kirche angehören. [4]Der oder die Diözesandatenschutzbeauftragte ist auf die gewissenhafte Erfüllung seiner oder ihrer Pflichten und die Einhaltung des kirchlichen und des für die Kirchen verbindlichen staatlichen Rechts zu verpflichten.

(3) [1]Die Bestellung kann vor Ablauf der Amtszeit widerrufen werden, wenn Gründe nach § 24 Deutsches Richtergesetz vorliegen, die bei einem Richter oder einer Richterin auf Lebenszeit dessen oder deren Entlassung aus dem Dienst rechtfertigen, oder Gründe vorliegen, die nach der Grundordnung des kirchlichen Dienstes in der jeweils geltenden Fassung eine Kündigung rechtfertigen. [2]Auf Antrag des oder der Diözesandatenschutzbeauftragten nimmt der Diözesanbischof die Bestellung zurück.

(4) [1]Das der Bestellung zum oder zur Diözesandatenschutzbeauftragten zugrunde liegende Dienstverhältnis kann während der Amtszeit nur unter den Voraussetzungen des Absatzes 3 beendet werden. [2]Dieser Kündigungsschutz wirkt für den Zeitraum von einem Jahr nach der Beendigung der Amtszeit entsprechend fort, soweit ein kirchliches Beschäftigungsverhältnis fortgeführt wird oder sich anschließt.

(5) Der oder die Diözesandatenschutzbeauftragte benennt aus dem Kreis seiner oder ihrer Mitarbeitenden einen Vertreter oder eine Vertreterin, der oder die im Fall seiner oder ihrer Verhinderung die unaufschiebbaren Entscheidungen trifft.

(6) [1]Ist der oder die Diözesandatenschutzbeauftragte an der Ausübung seines oder ihres Amtes dauerhaft verhindert oder endet sein oder ihr Amtsverhältnis vorzeitig und ist er oder sie nicht zur Weiterführung der Geschäfte verpflichtet, bestellt der Diözesanbischof bis zur Wiederaufnahme des Amtes durch den Diözesandatenschutzbeauftragten oder die Diözesandatenschutzbeauftragte oder die Bestellung eines oder einer neuen Diözesandatenschutzbeauftragten übergangsweise eine Leitung. [2]§ 43 Absatz 2 gilt entsprechend. [3]Die übergangsweise Leitung hat sämtliche Rechte und Pflichten, die nach diesem Gesetz dem oder der Diözesandatenschutzbeauftragten zukommen. [4]Sie tritt nicht in die laufende Amtszeit des oder der bisherigen Diözesandatenschutzbeauftragten ein. [5]Mit der Bestellung der übergangsweisen Leitung durch den Diözesanbischof endet die Vertretung nach Absatz 5.

(7) [1]Der oder die Diözesandatenschutzbeauftragte und seine Mitarbeitenden sind auch nach Beendigung ihrer Aufträge verpflichtet, über die ihnen in dieser Eigenschaft bekannt gewordenen 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.

(8) [1]Der oder die Diözesandatenschutzbeauftragte und seine Mitarbeitenden dürfen, wenn ihr Auftrag beendet ist, über solche Angelegenheiten ohne Genehmigung des oder der amtierenden Diözesandatenschutzbeauftragten weder vor Gericht noch außergerichtlich Aussagen oder Erklärungen abgeben. [2]Die Genehmigung, als Zeuge oder Zeugin auszusagen, wird in der Regel erteilt. [3]Unberührt bleibt die gesetzlich begründete Pflicht, Straftaten anzuzeigen.

(9) Die Absätze 7 und 8 gelten für die Vertretung oder eine übergangsweise Leitung entsprechend.

§ 44
Aufgaben der Datenschutzaufsicht

(1) Die Datenschutzaufsicht wacht über die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz und setzt diese durch.

(2) Darüber hinaus hat die Datenschutzaufsicht insbesondere folgende Aufgaben:

a) Die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung sensibilisieren und sie darüber aufklären. Besondere Beachtung finden dabei spezifische Maßnahmen für Minderjährige;
b) kirchliche Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung beraten;
c) die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus diesem Gesetz entstehenden Pflichten sensibilisieren;
d) auf Anfrage jeder betroffenen Person Informationen über die Ausübung ihrer echte aufgrund dieses Gesetzes zur Verfügung stellen und gegebenenfalls zu diesem Zweck mit den anderen Datenschutzaufsichten sowie staatlichen und sonstigen kirchlichen Aufsichtsbehörden zusammenarbeiten;
e) sich mit Beschwerden einer betroffenen Person befassen, den Gegenstand der Beschwerde in angemessenem Umfang untersuchen und den Beschwerdeführer innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Untersuchung unterrichten; zur Erleichterung der Einlegung von Beschwerden hält die Datenschutzaufsicht Musterformulare in digitaler und Papierform bereit.
f) mit anderen Datenschutzaufsichten zusammenarbeiten, auch durch Informationsaustausch, nd ihnen Amtshilfe leisten, um die einheitliche Anwendung und Durchsetzung dieses Gesetzes zu gewährleisten;
g) Untersuchungen über die Anwendung dieses Gesetzes durchführen, auch auf der Grundlage von Informationen einer anderen Datenschutzaufsicht oder einer anderen Behörde;
h) maßgebliche Entwicklungen verfolgen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie und der Geschäftspraktiken;
i) gegebenenfalls eine Liste der Verarbeitungsarten erstellen und führen, für die gemäß § 35 entweder keine oder für die eine Datenschutz-Folgenabschätzung durchzuführen ist;
j) Beratung in Bezug auf die in § 35 genannten Verarbeitungsvorgänge leisten;
k) interne Verzeichnisse über Verstöße gegen dieses Gesetz und die im Zusammenhang mit diesen Verstößen ergriffenen Maßnahmen führen und
l) jede sonstige Aufgabe im Zusammenhang mit dem Schutz personenbezogener Daten erfüllen.

(3) Die Datenschutzaufsicht kann im Rahmen ihrer Zuständigkeit Muster zur Verfügung stellen.

(4) [1]Die Tätigkeit der Datenschutzaufsicht ist für die betroffene Person unentgeltlich. [2]Bei offensichtlich unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anfragen kann jedoch die Datenschutzaufsicht ihre weitere Tätigkeit auf eine neuerliche Anfrage der betroffenen Person hin davon abhängig machen, dass eine angemessene Gebühr für den Verwaltungsaufwand entrichtet wird, oder sich weigern, aufgrund der Anfrage tätig zu werden.

[3]In diesem Fall trägt die Datenschutzaufsicht die Beweislast für den offenkundig unbegründeten oder exzessiven Charakter der Anfrage.

(5) [1]Die Datenschutzaufsicht erstellt jährlich einen Tätigkeitsbericht, der dem Diözesanbischof vorgelegt und der Öffentlichkeit zugänglich gemacht wird. [2]Der Tätigkeitsbericht soll auch eine Darstellung der wesentlichen Entwicklungen des Datenschutzes im nichtkirchlichen Bereich enthalten.

§ 45
Zuständigkeit der Datenschutzaufsicht bei über- oder mehrdiözesanen Rechtsträgern sowie bei gemeinsamer Verantwortlichkeit

(1) [1]Handelt es sich bei dem Rechtsträger einer kirchlichen Stelle im Sinne des § 3 Absatz 1 um einen über- oder mehrdiözesanen kirchlichen Rechtsträger, so gilt das Gesetz über den kirchlichen Datenschutz der Diözese und ist die Datenschutzaufsicht der Diözese zuständig, in der der Rechtsträger der kirchlichen Stelle seinen Sitz hat. [2]Bei Abgrenzungsfragen gegenüber dem Bereich der Ordensgemeinschaften erfolgt eine Abstimmung zwischen dem oder der Diözesandatenschutzbeauftragten und dem oder der Ordensdatenschutzbeauftragten.

(2) Verfügt der über- oder mehrdiözesane kirchliche Rechtsträger im Sinne des § 3 Absatz 1 über eine oder mehrere rechtlich unselbständige Einrichtungen, die in einer anderen Diözese als der Diözese ihren Sitz haben, in der der Rechtsträger seinen Sitz hat, so gilt das Gesetz über den kirchlichen Datenschutz der Diözese und ist die Datenschutzaufsicht der Diözese zuständig, in der der Rechtsträger seinen Sitz hat.

(3) In Fällen einer gemeinsamen Verantwortlichkeit im Sinne des § 28 verständigen sich die betroffenen Datenschutzaufsichten.

§ 46
Zusammenarbeit kirchlicher Stellen mit den Datenschutzaufsichten

Die in § 3 Absatz 1 genannten kirchlichen Stellen sind verpflichtet, im Rahmen ihrer Zuständigkeit

a) den Anweisungen der Datenschutzaufsicht Folge zu leisten,

b) die Datenschutzaufsicht bei der Erfüllung ihrer Aufgaben zu unterstützen; ihr ist dabei insbesondere Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen und Akten zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen, namentlich in die gespeicherten Daten und in die Datenverarbeitungsprogramme, und während der Dienstzeit zum Zwecke von Prüfungen Zutritt zu allen Diensträumen, die der Verarbeitung und Aufbewahrung automatisierter Dateien dienen, zu gewähren,

c) Untersuchungen in Form von Datenschutzüberprüfungen durch die Datenschutzaufsicht zuzulassen.

§ 47
Befugnisse der Datenschutzaufsicht

(1) Die Datenschutzaufsicht verfügt über sämtliche folgenden Untersuchungsbefugnisse, die es ihr gestatten,

a) den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, alle Informationen bereitzustellen, die für die Erfüllung der Aufgaben der Datenschutzaufsicht erforderlich sind;
b) Untersuchungen in Form von Datenschutzüberprüfungen durchzuführen;
c) den Verantwortlichen oder den Auftragsverarbeiter auf einen vermeintlichen Verstoß gegen dieses Gesetz hinzuweisen;

d) von dem Verantwortlichen und dem Auftragsverarbeiter Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung der Aufgaben der Datenschutzaufsicht notwendig sind, zu erhalten;
e) gemäß dem geltenden Verfahrensrecht Zugang zu den Räumlichkeiten, einschließlich aller Datenverarbeitungsanlagen und -geräte, des Verantwortlichen und des Auftragsverarbeiters zu erhalten.

(2) Die Datenschutzaufsicht verfügt über sämtliche folgenden Abhilfebefugnisse, die es ihr gestatten,
a) einen Verantwortlichen oder einen Auftragsverarbeiter zu warnen, dass beabsichtigte erarbeitungsvorgänge voraussichtlich gegen dieses Gesetz oder andere datenschutzrechtliche estimmungen verstoßen;
b) einen Verantwortlichen oder einen Auftragsverarbeiter zu verwarnen, wenn er mit Verarbeitungsvorgängen gegen dieses Gesetz oder andere datenschutzrechtliche Bestimmungen verstoßen hat;
c) den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, den Anträgen der etroffenen Person auf Ausübung der ihr nach diesem Gesetz zustehenden Rechte zu entsprechen;
d) den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge egebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit diesem Gesetz zu bringen;
e) den Verantwortlichen anzuweisen, die von einer Verletzung des Schutzes personenbezogener Daten betroffene Person entsprechend zu benachrichtigen;
f) eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen;
g) die Berichtigung oder Löschung von personenbezogenen Daten oder die Einschränkung der Verarbeitung gemäß den §§ 18, 19 und 20 und die Unterrichtung der Empfänger, an die diese personenbezogenen Daten gemäß §§ 19 Absatz 2 und 21 offengelegt wurden, über solche Maßnahmen anzuordnen;
h) eine Geldbuße gemäß § 51 zu verhängen, zusätzlich zu oder anstelle von in diesem Absatz genannten Maßnahmen, je nach den Umständen des Einzelfalls;
i) die Aussetzung der Übermittlung von Daten an einen Empfänger in einem Drittland der an eine internationale Organisation oder an ein nichtstaatliches Völkerrechtssubjekt nzuordnen.

(3) Hat die Datenschutzaufsicht die Feststellung getroffen, dass eine Datenschutzverletzung objektiv vorliegt, kann der betroffenen Person im Verfahren vor den staatlichen Zivilgerichten über den Schadensersatz das Fehlen einer solchen nicht entgegengehalten werden.

(4) [1]Werden Maßnahmen nach Absatz 2 nicht in der von der Datenschutzaufsicht bestimmten Frist befolgt, so verständigt die Datenschutzaufsicht die für die kirchliche Stelle zuständige Aufsicht und fordert sie zu einer Stellungnahme gegenüber der Datenschutzaufsicht auf. [2]Diese Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die getroffen worden sind.

(5) [1]Vor Abhilfemaßnahmen nach Absatz 2 ist dem Verantwortlichen oder dem Auftragsverarbeiter innerhalb einer angemessenen Frist Gelegenheit zu geben, sich zu den für die Entscheidung erheblichen Tatsachen zu äußern. [2]Von der Anhörung kann abgesehen werden, wenn sie nach den Umständen des Einzelfalls nicht geboten, insbesondere wenn eine sofortige Entscheidung wegen Gefahr im Verzug oder im kirchlichen Interesse notwendig erscheint.

Kapitel 7
Beschwerde, gerichtlicher Rechtsbehelf, Haftung und Sanktionen

§ 48
Beschwerde bei einer Datenschutzaufsicht

(1) [1]Jede betroffene Person hat unbeschadet eines anderweitigen Rechtsbehelfs das Recht auf Beschwerde bei einer Datenschutzaufsicht, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen Vorschriften dieses Gesetzes oder gegen andere Datenschutzvorschriften verstößt. [2]Die Einhaltung des Dienstwegs ist dabei nicht erforderlich.

(2) Auf ein solches Vorbringen hin prüft die Datenschutzaufsicht den Sachverhalt. Sie fordert den Verantwortlichen, den Empfänger oder die Empfängerin und/oder den Dritten oder die Dritte zur Stellungnahme auf, soweit der Inhalt des Vorbringens den Tatbestand einer Datenschutzverletzung erfüllt.

(3) Niemand darf gemaßregelt oder benachteiligt werden, weil er sich im Sinne des Absatz 1 an die Datenschutzaufsicht gewendet hat.

(4) Die Datenschutzaufsicht unterrichtet den Beschwerdeführer oder die Beschwerdeführerin über den Stand und die Ergebnisse der Beschwerde einschließlich der Möglichkeit eines gerichtlichen Rechtsbehelfs nach § 49.

§ 49
Recht auf gerichtlichen Rechtsbehelf
gegen einen Bescheid der Datenschutzaufsicht

[1]Jede natürliche oder juristische Person hat unbeschadet des Rechts auf Beschwerde bei einer Datenschutzaufsicht (§ 48) das Recht auf einen gerichtlichen Rechtsbehelf gegen einen sie betreffenden Bescheid der Datenschutzaufsicht. [2]Dies gilt auch dann, wenn sich die Datenschutzaufsicht nicht mit einer Beschwerde nach § 48 befasst oder die betroffene Person nicht innerhalb von drei Monaten über den Stand oder das Ergebnis der nach § 48 erhobenen Beschwerde in Kenntnis gesetzt hat.

§ 49a
Recht auf gerichtlichen Rechtsbehelf
gegen Verantwortliche oder kirchliche Auftragsverarbeiter

Jede betroffene Person hat unbeschadet eines Rechts auf Beschwerde bei einer Datenschutzaufsicht (§ 48) das Recht auf einen gerichtlichen Rechtsbehelf gegen einen Verantwortlichen oder einen kirchlichen Auftragsverarbeiter, wenn sie der Ansicht ist, dass die ihr aufgrund dieses Gesetzes zustehenden Rechte infolge einer nicht im Einklang mit diesem Gesetz stehenden Verarbeitung ihrer personenbezogenen Daten verletzt wurden.

§ 49 b
Zuständigkeit der Datenschutzgerichte

(1) Für gerichtliche Rechtsbehelfe nach den §§ 49 und 49 a ist das Interdiözesane Datenschutzgericht zuständig.

(2) Für Rechtsmittel gegen eine Entscheidung des Interdiözesanen Datenschutzgerichts ist das Datenschutzgericht der Deutschen Bischofskonferenz zuständig.

§ 50
Haftung und Schadenersatz

(1) Jede Person, der wegen eines Verstoßes gegen dieses Gesetz ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen die kirchliche Stelle als Verantwortlicher oder Auftragsverarbeiter.

(2) Ein Auftragsverarbeiter haftet für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus diesem Gesetz nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat.

(3) Ein Verantwortlicher oder ein Auftragsverarbeiter ist von der Haftung gemäß Absatz 1 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

(4) Wegen eines Schadens, der nicht Vermögensschaden ist, kann die betroffene Person eine angemessene Entschädigung in Geld verlangen.

(5) Lässt sich bei einer automatisierten Verarbeitung personenbezogener Daten nicht ermitteln, welche von mehreren beteiligten kirchlichen Stellen als Verantwortlicher oder Auftragsverarbeiter den Schaden verursacht hat, so haftet jede als Verantwortlicher für den gesamten Schaden.

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

(7) Hat bei der Entstehung des Schadens ein Verschulden der betroffenen Person mitgewirkt, ist § 254 des Bürgerlichen Gesetzbuchs entsprechend anzuwenden.

(8) Auf die Verjährung finden die für unerlaubte Handlungen geltenden Verjährungsvorschriften des Bürgerlichen Gesetzbuchs entsprechende Anwendung.

§ 51
Geldbußen

(1) Verstößt ein Verantwortlicher oder ein Auftragsverarbeiter vorsätzlich oder fahrlässig gegen Bestimmungen dieses Gesetzes, so kann die Datenschutzaufsicht eine Geldbuße verhängen.

(2) Die Datenschutzaufsicht stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Paragraphen für Verstöße gegen dieses Gesetz in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

(3) [1]Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach § 47 Absatz 2 lit. a) bis g) und i) verhängt. [2]Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall Folgendes gebührend berücksichtigt:

a) 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;
b) Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;
c) jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;
d) Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß § 26 getroffenen technischen und organisatorischen Maßnahmen;
e) etwaige einschlägige frühere Verstöße des Verantwortlichen oder des Auftragsverarbeiters;
f) Umfang der Zusammenarbeit mit der Datenschutzaufsicht, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern;
g) Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind;
h) Art und Weise, wie der Verstoß der Datenschutzaufsicht bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat;
i) Einhaltung der früher gegen den für den betreffenden Verantwortlichen oder Auftragsverarbeiter in Bezug auf denselben Gegenstand angeordneten Maßnahmen (§ 47 Absatz 2), wenn solche Maßnahmen angeordnet wurden;
j) jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.

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

(5) [1]Bei Verstößen werden im Einklang mit Absatz 3 Geldbußen innerhalb eines Rahmens von bis zu 1.000.000 € verhängt. [2]Für den Bereich kirchlicher Unternehmen im Sinne des § 4 Nummer 19., die am Wettbewerb teilnehmen, können im Einklang mit Absatz 2 Geldbußen von bis zu 4 Prozent des Jahresumsatzes, maximal in Höhe von 3.000.000 €, verhängt werden.

(6) Gegen kirchliche Stellen im Sinne des § 3 Absatz 1, soweit sie im weltlichen Rechtskreis öffentlich-rechtlich verfasst sind, werden keine Geldbußen verhängt; dies gilt nicht, soweit sie als Unternehmen am Wettbewerb teilnehmen.

(7) [1]Die Datenschutzaufsicht leitet einen Vorgang, in welchem sie einen objektiven Verstoß gegen dieses Gesetz festgestellt hat, einschließlich der von ihr verhängten Höhe der Geldbuße an die nach staatlichem Recht zuständige Vollstreckungsbehörde weiter. [2]Unbeschadet ihrer jeweiligen Rechtsform ist die Datenschutzaufsicht Inhaber der Bußgeldforderung und mithin Vollstreckungsgläubiger. [3]Die nach staatlichem Recht zuständige Vollstreckungsbehörde ist an die Feststellung der Datenschutzaufsicht hinsichtlich des Verstoßes und an die von dieser festgesetzten Höhe der Geldbuße gebunden. [4]Sofern das staatliche Recht die Zuständigkeit einer solchen Vollstreckungsbehörde nicht vorsieht, erfolgt die Vollstreckung auf dem Zivilrechtsweg.

(8) Eine Meldung nach § 33 oder eine Benachrichtigung nach § 34 Absatz 1 darf in einem Verfahren zur Verhängung eines Bußgeldes nach dieser Vorschrift gegen den Meldepflichtigen oder die Meldepflichtige oder den Benachrichtigenden oder die Benachrichtigende oder seine oder ihre in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung des oder der Meldepflichtigen oder des oder der Benachrichtigenden verwendet werden.

Kapitel 8
Vorschriften für besondere Verarbeitungssituationen

§ 52
Videoüberwachung

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie

a) zur Aufgabenerfüllung oder zur Wahrnehmung des Hausrechts oder
b) zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Person überwiegen.

(2) Der Umstand der Beobachtung und der Verantwortliche 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 Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Person überwiegen.

(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über eine Verarbeitung gemäß §§ 15 und 16 zu benachrichtigen.

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

§ 52a
Gottesdienste und kirchliche Veranstaltungen

(1) Die Aufzeichnung, Übertragung oder Veröffentlichung von Gottesdiensten oder Veranstaltungen gottesdienstähnlicher Art sind datenschutzrechtlich zulässig, wenn die betroffenen Personen vor der Teilnahme durch geeignete Maßnahmen über Art und Umfang der Aufzeichnung, Übertragung oder Veröffentlichung informiert werden.

(2) Besonderen schutzwürdigen Interessen - insbesondere von Minderjährigen - ist in angemessenem Umfang Rechnung zu tragen.

(3) Unbeschadet des Absatzes 2 sind von der Aufzeichnung, Übertragung oder Veröffentlichung nicht erfasste Plätze für Gottesdienstbesucher und -besucherinnen in angemessenerZahl vorzuhalten.

§ 53
Verarbeitung personenbezogener Daten für Zwecke des Beschäftigungsverhältnisses

(1) Personenbezogene Daten eines oder einer Beschäftigten einschließlich der Daten über die eligionszugehörigkeit, die religiöse Überzeugung und die Erfüllung von Loyalitätsobliegenheiten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist.

(2) Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines oder einer Beschäftigten dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des oder der Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind oder eine Rechtsvorschrift dies vorsieht.

(3) Absatz 1 ist auch anzuwenden, wenn personenbezogene Daten verarbeitet werden, ohne dass sie automatisiert verarbeitet oder in oder aus einer nicht automatisierten Datei verarbeitet oder für die Verarbeitung in einer solchen Datei erhoben werden.

(4) Die Beteiligungsrechte nach der jeweils geltenden Mitarbeitervertretungsordnung bleiben unberührt.

§ 54
Verarbeitung personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken, zu Archivzwecken oder zu statistischen Zwecken

(1) [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]Mit diesen Garantien wird sichergestellt, dass technische und organisatorische Maßnahmen bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird. [3]§ 11 Absatz 2 lit. h) bis j) bleiben unberührt.

(2) [1]Die Offenlegung personenbezogener Daten an andere als kirchliche Stellen für Zwecke der wissenschaftlichen oder historischen Forschung oder der Statistik ist nur zulässig, wenn diese sich verpflichten, die übermittelten Daten nicht für andere Zwecke zu verarbeiten und die Vorschriften der Absätze 3 und 4 einzuhalten. [2]Der kirchliche Auftrag darf durch die Offenlegung nicht gefährdet werden.

(3) [1]Personenbezogene Daten, die für Zwecke der Forschung oder Statistik verarbeitet werden, sind zu anonymisieren, sobald dies nach dem Forschungs- oder Statistikzweck möglich ist. Bis dahin sind die Merkmale gesondert zu verarbeiten, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer identifizierten oder identifizierbaren Person zugeordnet werden können. [2]Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungs- oder Statistikzweck dies erfordert.

(4) [1]Die Veröffentlichung personenbezogener Daten, die zum Zwecke wissenschaftlicher oder historischer Forschung oder der Statistik übermittelt wurden, ist nur mit Zustimmung der übermittelnden kirchlichen Stelle zulässig. [2]Die Zustimmung kann erteilt werden, wenn

a) die betroffene Person eingewilligt hat oder
b) dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist, es sei denn, dass Grund zu der Annahme besteht, dass durch die Veröffentlichung der Auftrag der Kirche gefährdet würde oder schutzwürdige Interessen der betroffenen Person überwiegen.

(5) Für die Archivierung von Unterlagen kirchlicher Stellen im Sinne des § 3 gilt die Anordnung über die kirchlichen Archive (KAO) in der jeweils geltenden Fassung.

§ 54a
Verarbeitung personenbezogener Daten zur institutionellen Aufarbeitung sexualisierter Gewalt und anderer Formen des Missbrauchs

[1]An der institutionellen Aufarbeitung sexualisierter Gewalt und anderer Formen des Missbrauchs besteht ein überragendes kirchliches Interesse. [2]Personenbezogene Daten dürfen zum Zwecke der institutionellen Aufarbeitung sexualisierter Gewalt nach Maßgabe dieses Gesetzes und auf Grundlage spezifischer diözesaner Bestimmungen verarbeitet werden, die die Offenlegung von personenbezogenen Daten von sexuellem Missbrauch betroffener Personen für Aufarbeitungs- und Forschungszwecke durch Auskunft oder Einsicht in Unterlagen ausdrücklich regeln, darunter auch Regelungen, die Auskunft oder Einsicht in Unterlagen lediglich im Falle einer Einwilligung betroffener Personen zulassen.

§ 55
Verarbeitung personenbezogener Daten durch die Medien

(1) [1]Soweit personenbezogene Daten von kirchlichen Stellen ausschließlich zu eigenen journalistisch-redaktionellen oder literarischen Zwecken verarbeitet werden, gelten von den Vorschriften dieses Gesetzes nur die §§ 5, 26 und 50. [2]Soweit personenbezogene Daten zur Herausgabe von Adressen-, Telefon- oder vergleichbaren Verzeichnissen verarbeitet werden, gilt Satz 1 nur, wenn mit der Herausgabe 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 oder sie Auskunft über die der Berichterstattung zugrunde liegenden, zu seiner Person gespeicherten Daten verlangen.

²Die 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. ³Die betroffene Person kann die Berichtigung unrichtiger Daten verlangen.

Kapitel 9
Übergangs- und Schlussbestimmungen

§ 56
Ermächtigungen

Die zur Durchführung dieses Gesetzes erforderlichen Regelungen trifft der Generalvikar. Er legt insbesondere fest:

a) den Inhalt eines Musters der schriftlichen Verpflichtungserklärung gemäß § 5 Satz 2 und

b) die technischen und organisatorischen Maßnahmen gemäß § 26.

§ 57
Übergangsbestimmungen

Bisherige Bestellungen der betrieblichen Datenschutzbeauftragten, deren Amtszeiten noch nicht abgelaufen sind, bleiben unberührt, soweit hierbei die Regelungen der §§ 36 ff. Beachtung finden.

§ 58
Inkrafttreten

Dieses Gesetz tritt am 24.05.2018 in Kraft.

Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO) in der Fassung des Beschlusses der Vollversammlung des Verbandes der Diözesen Deutschlands vom 19. November 2018, geändert durch Beschluss der Vollversammlung des Verbandes der Diözesen Deutschlands vom 24. November 2025

Inhaltsübersicht

Kapitel 1
Verarbeitungstätigkeiten

§ 1 Verzeichnis von Verarbeitungstätigkeiten

Kapitel 2
Datengeheimnis

§ 2 Belehrung und Verpflichtung auf das Datengeheimnis, Schulung
§ 3 Inhalt der Verpflichtungserklärung

Kapitel 3
Technische und organisatorische Maßnahmen

Abschnitt 1
Grundsätze und Maßnahmen

§ 4 Begriffsbestimmungen (IT-Systeme, Lesbarkeit)
§ 5 Grundsätze der Verarbeitung
§ 6 Technische und organisatorische Maßnahmen
§ 7 Überprüfung
§ 8 Verarbeitung von Meldedaten in kirchlichen Rechenzentren

Abschnitt 2
Schutzbedarf und Risikoanalyse

§ 9 Einordnung in Datenschutzklassen und Datenschutzniveau
§ 10 Risikoanalyse
§ 11 Datenschutzklasse I und Schutzniveau I
§ 12 Datenschutzklasse II und Schutzniveau II
§ 13 Datenschutzklasse III und Schutzniveau III
§ 14 Umgang mit personenbezogenen Daten, die dem Beichtgeheimnis oder dem Seelsorgegeheimnis unterliegen

Kapitel 4
Maßnahmen des Verantwortlichen und des oder der Mitarbeitenden

§ 15 Maßnahmen des Verantwortlichen
§ 16 Maßnahmen des Verantwortlichen zur Datensicherung
§ 17 Maßnahmen des oder der Mitarbeitenden

Kapitel 5
Besondere Gefahrenlagen

§ 18 Nutzung von Cloud-Diensten
§ 19 Autorisierte Programme
§ 20 Nutzung dienstlicher IT-Systeme zu auch privaten Zwecken
§ 21 Nutzung privater IT-Systeme zu dienstlichen Zwecken
§ 22 Externe Zugriffe, Auftragsverarbeitung
§ 23 Verschrottung und Vernichtung von IT-Systemen, Abgabe von IT-Systemen zur weiteren Nutzung
§ 24 Passwortlisten der Systemverwaltung
§ 25 Übermittlung personenbezogener Daten per Fax
§ 26 Sonstige Formen der Übermittlung personenbezogener Daten
§ 27 Kopier-/Scangeräte

Kapitel 6
Übergangs- und Schlussbestimmungen

§ 28 Inkrafttreten

Kapitel 1
Verarbeitungstätigkeiten

§ 1
Verzeichnis von Verarbeitungstätigkeiten

(1) Das vom Verantwortlichen gemäß § 31 Absatz 1 bis Absatz 3 KDG zu führende Verzeichnis von Verarbeitungstätigkeiten ist dem oder der betrieblichen Datenschutzbeauftragten, sofern ein solcher oder eine solche benannt wurde, vor Beginn der Verarbeitung von personenbezogenen Daten und auf entsprechende Anfrage der Datenschutzaufsicht auch dieser unverzüglich zur Verfügung zu stellen.

(2) Sofern die zuständige Datenschutzaufsicht ein Muster für ein Verzeichnis von Verarbeitungstätigkeiten gemäß § 31 KDG zur Verfügung stellt, bildet dieses grundsätzlich den Mindeststandard.

(3) [1]Das Verzeichnis ist bei jeder Veränderung eines Verfahrens zu aktualisieren. [2]Im Übrigen ist es in regelmäßigen Abständen von höchstens zwei Jahren einer Überprüfung durch den Verantwortlichen zu unterziehen und bei Bedarf zu aktualisieren. [3]Die Überprüfung sowie die Aktualisierung sind in geeigneter Weise zu dokumentieren.

Kapitel 2
Datengeheimnis

§ 2
Belehrung und Verpflichtung auf das Datengeheimnis, Schulung

(1) Zu den bei der Verarbeitung personenbezogener Daten tätigen Personen im Sinne des § 5 KDG gehören die in den Stellen gemäß § 3 Absatz 1 KDG Beschäftigten im Sinne des § 4 Ziffer 24. KDG sowie die dort ehrenamtlich tätigen Personen (Mitarbeitende im Sinne dieser Durchführungsverordnung, im Folgenden: Mitarbeitende).

(2) [1]Durch geeignete Maßnahmen sind die Mitarbeitenden mit den Vorschriften des KDG sowie den anderen für ihre Tätigkeit geltenden Datenschutzvorschriften vertraut zu machen.

[2]Dies geschieht im Wesentlichen durch Hinweis auf die für den Aufgabenbereich der Person wesentlichen Grundsätze und Erfordernisse und im Übrigen durch Bekanntgabe der entsprechenden Regelungstexte in der jeweils gültigen Fassung. [3]Das KDG und diese Durchführungsverordnung sowie die sonstigen Datenschutzvorschriften werden zur Einsichtnahme und etwaigen Ausleihe bereitgehalten oder elektronisch zur Verfügung gestellt; dies ist den Mitarbeitenden in geeigneter Weise mitzuteilen.

(3) Ferner sind die Mitarbeitenden zu belehren über

a) die Verpflichtung zur Beachtung der in Absatz 2 genannten Vorschriften bei der Verarbeitung personenbezogener Daten,
b) mögliche rechtliche Folgen eines Verstoßes gegen das KDG und andere für ihre Tätigkeit geltende Datenschutzvorschriften,
c) das Fortbestehen des Datengeheimnisses nach Beendigung der Tätigkeit bei der Datenverarbeitung.

(4) Bei einer wesentlichen Änderung des KDG oder anderer für die Tätigkeit der Mitarbeitenden geltender Datenschutzvorschriften sowie bei Aufnahme einer neuen Tätigkeit durch den Mitarbeitenden oder die Mitarbeitende hat insoweit eine erneute Belehrung zu erfolgen.

(5) [1]Die Mitarbeitenden haben in nachweisbar dokumentierter Form eine Verpflichtungserklärung gemäß § 3 abzugeben. [2]Diese Verpflichtungserklärung wird zu der Personalakte bzw. den Unterlagen des oder der jeweiligen Mitarbeitenden genommen. [3]Dieser oder diese erhält eine Ausfertigung der Erklärung.

(6) Die Verpflichtung auf das Datengeheimnis gemäß § 5 KDG erfolgt durch den Verantwortlichen oder einen von ihm Beauftragten.

(7) Die Mitarbeitenden sind regelmäßig zu schulen.

§ 3
Inhalt der Verpflichtungserklärung

(1) Die gemäß § 2 Absatz 5 nachweisbar zu dokumentierende Verpflichtungserklärung des oder der Mitarbeitenden gemäß § 5 Satz 2 KDG hat zum Inhalt

a) Angaben zur Identifizierung des oder der Mitarbeitenden (Vorname, Zuname, Beschäftigungsdienststelle, Personalnummer sowie, sofern Personalnummer nicht vorhanden, Geburtsdatum und Anschrift),
b) die Bestätigung, dass der oder die Mitarbeitende auf die für die Ausübung seiner oder ihrer Tätigkeit spezifisch geltenden Bestimmungen und im Übrigen auf die allgemeinen datenschutzrechtlichen Regelungen in den jeweils geltenden Fassungen sowie auf die Möglichkeit der Einsichtnahme und Ausleihe dieser Texte hingewiesen wurde,
c) die Verpflichtung des oder der Mitarbeitenden, das KDG und andere für seine Tätigkeit geltende Datenschutzvorschriften in den jeweils geltenden Fassungen sorgfältig einzuhalten,
d) die Bestätigung, dass der oder die Mitarbeitende über rechtliche Folgen eines Verstoßes gegen das KDG sowie gegen sonstige für die Ausübung seiner oder ihrer Tätigkeit spezifisch geltende Bestimmungen belehrt wurde.

(2) Die Verpflichtungserklärung ist von dem oder der Mitarbeitenden unter Angabe des Ortes und des Datums der Unterschriftsleistung zu unterzeichnen oder auf eine andere dem Verfahren angemessene Weise zu signieren.

(3) Sofern die zuständige Datenschutzaufsicht ein Muster einer Verpflichtungserklärung zur Verfügung stellt, bildet dieses den Mindeststandard.

Kapitel 3
Technische und organisatorische Maßnahmen

Abschnitt 1
Grundsätze und Maßnahmen

§ 4
Begriffsbestimmungen (IT-Systeme, Lesbarkeit)

(1) IT-Systeme im Sinne dieser Durchführungsverordnung sind sämtliche technischen Einrichtungen, mittels derer personenbezogene Daten automatisiert verarbeitet werden.

(2) IT-Systeme sind insbesondere

a) hardwarebasierte IT-Komponenten (elektronische Geräte wie Server, Arbeitsplatzrechner, mobile Endgeräte, eingebettete Systeme (z.B. IoT) oder vergleichbare technische Komponenten, die einzeln oder im Verbund betrieben werden können),
b) Softwarelösungen (lokal installierte oder netzwerkgestützte Programme und Anwendungen einschließlich betriebssystemnaher Software und Anwendungssoftware, die unmittelbar oder mittelbar an der Verarbeitung personenbezogener Daten beteiligt sind),
c) cloudbasierte Systeme und Dienste (Bereitstellungsformen wie Software as a Service (SaaS), Platform as a Service (PaaS) oder Infrastructure as a Service (IaaS), die über netzwerkbasierte Umgebungen (insbesondere Internet oder Intranet) zugänglich sind und zur Datenverarbeitung eingesetzt werden).

(3) Unter Lesbarkeit im Sinne dieser Durchführungsverordnung ist die Möglichkeit zur vollständigen oder teilweisen Wiedergabe des Informationsgehalts von personenbezogenen Daten zu verstehen.

§ 5
Grundsätze der Verarbeitung

(1) Der Verantwortliche hat sicher zu stellen, dass bei der Verarbeitung personenbezogener Daten durch innerbetriebliche Organisation und mittels technischer und organisatorischer Maßnahmen die Einhaltung des Datenschutzes gewährleistet wird.

(2) Die Verarbeitung personenbezogener Daten auf IT-Systemen darf erst erfolgen, wenn der Verantwortliche und der Auftragsverarbeiter die nach dem KDG und dieser Durchführungsverordnung erforderlichen technischen und organisatorischen Maßnahmen zum Schutz dieser Daten getroffen haben.

§ 6
Technische und organisatorische Maßnahmen

(1) Je nach der Art der zu schützenden personenbezogenen Daten sind unter Berücksichtigung von §§ 26 und 27 KDG angemessene technische und organisatorische Maßnahmen zu treffen, die geeignet sind,

a) zu verhindern, dass unberechtigt Rückschlüsse auf eine bestimmte Person gezogen werden können (z.B. durch Pseudonymisierung oder Anonymisierung personenbezogener Daten),
b) einen wirksamen Schutz gegen eine unberechtigte Verarbeitung personenbezogener Daten insbesondere während ihres Übertragungsvorgangs herzustellen (z. B. durch Verschlüsselung mit geeigneten Verschlüsselungsverfahren; das Verschlüsselungsverfahren ist dem aktuellen Stand der Technik und dem jeweiligen Sicherheitsbedarf entsprechend angemessen auszuwählen),

c) die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste zum Schutz vor unberechtigter Verarbeitung auf Dauer zu gewährleisten und dadurch Verletzungen des Schutzes personenbezogener Daten in angemessenem Umfang vorzubeugen,
d) im Fall eines physischen oder technischen Zwischenfalls die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen rasch wiederherzustellen (Wiederherstellung).

(2) Im Einzelnen sind für die Verarbeitung personenbezogener Daten in elektronischer Form unabhängig vom Ort der Verarbeitungstätigkeit insbesondere folgende Maßnahmen zu treffen:

a) Unbefugten ist der Zutritt zu IT-Systemen im Sinne des § 4 Absatz 2 Nr. 1, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Zutrittskontrolle).
b) 1Es ist zu verhindern, dass IT-Systeme und Benutzerzugänge von Unbefugten genutzt werden können (Zugangskontrolle). 2Zum Schutz personenbezogener Daten und zur Vermeidung von Identitätsdiebstahl sind geeignete technische und organisatorische Maßnahmen nach dem jeweiligen Stand der Technik zu ergreifen. 3Dies gilt insbesondere für Datenverarbeitungen außerhalb eines geschlossenen und gesicherten Netzwerks.
c) Die zur Benutzung eines IT- Systems Berechtigten dürfen ausschließlich auf die ihrer Zuständigkeit unterliegenden personenbezogenen Daten zugreifen können; personenbezogene Daten dürfen nicht unbefugt gelesen, kopiert, verändert oder entfernt werden (Zugriffskontrolle).
d) Personenbezogene Daten sind auch während ihrer elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern gegen unbefugtes Auslesen, Kopieren, Verändern oder Entfernen durch geeignete Maßnahmen zu schützen.
e) ¹Es muss überprüft und festgestellt werden können, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung erfolgt (Weitergabekontrolle). ²Werden personenbezogene Daten außerhalb der vorgesehenen Datenübertragung weitergegeben, ist dies zu protokollieren.
f) ¹Es ist grundsätzlich sicher zu stellen, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in IT-Systemen verarbeitet worden sind (Eingabekontrolle). ²Die Eingabekontrolle umfasst unbeschadet der gesetzlichen Aufbewahrungsfristen mindestens einen Zeitraum von sechs Monaten.
g) Personenbezogene Daten, die im Auftrag verarbeitet werden, dürfen nur entsprechend den Weisungen des Auftraggebers verarbeitet werden (Auftragskontrolle).
h) Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle).
i) Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden (Trennungsgebot).
j) Im Netzwerk- und im Einzelplatzbetrieb ist eine abgestufte Rechteverwaltung erforderlich. Anwender- und Administrationsrechte sind zu trennen.
k) Bei der Auswahl von IT-Systemen, insbesondere von Softwarelösungen, ist dem Grundsatz der Datenminimierung angemessen Rechnung zu tragen.

(3) Absatz 2 gilt entsprechend für die Verarbeitung personenbezogener Daten in nicht automatisierter Form.

§ 7
Überprüfung

(1) ¹Zur Gewährleistung der Sicherheit der Verarbeitung sind die getroffenen technischen und organisatorischen Maßnahmen durch den Verantwortlichen regelmäßig, mindestens jedoch im Abstand von jeweils zwei Jahren, auf ihre Wirksamkeit zu überprüfen. ²Zu diesem Zweck ist ein für die jeweilige kirchliche Stelle geeignetes und angemessenes Verfahren zu entwickeln, welches eine verlässliche Bewertung des Ist-Zustandes und eine zweckmäßige Anpassung an den aktuellen Stand der Technik erlaubt.

(2) [1]Insbesondere die Vorlage eines anerkannten Zertifikats gemäß § 26 Absatz 4 KDG durch den Verantwortlichen, welches sich an Veröffentlichungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) orientiert, ist als Nachweis zulässig. [2]Abweichend von Satz 1 kann auch eine Orientierung an anderen Regelungen erfolgen, die einen vergleichbaren Schutzstandard gewährleisten (insbesondere ISO/IEC 27001).

(3) Die Überprüfung nach Absatz 1 ist zu dokumentieren.

(4) Für den Fall der Auftragsverarbeitung gilt § 15 Absatz 5.

§ 8
Verarbeitung von Meldedaten in kirchlichen Rechenzentren

(1) Werden personenbezogene Daten aus den Melderegistern der kommunalen Meldebehörden in kirchlichen Rechenzentren verarbeitet, so orientieren sich die von diesen zu treffenden Schutzmaßnahmen an den jeweils geltenden BSI-IT-Grundschutzkatalogen oder vergleichbaren Veröffentlichungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Abweichend von Satz 1 kann auch eine Orientierung an anderen Regelungen erfolgen, die einen vergleichbaren Schutzstandard gewährleisten (insbesondere ISO 27001 auf Basis IT-Grundschutz).

(2) Rechenzentren im Sinne dieser Durchführungsverordnung sind die für den Betrieb von größeren, zentral in mehreren Dienststellen eingesetzten Informations- und Kommunikationssystemen erforderlichen Einrichtungen.

Abschnitt 2
Schutzbedarf und Risikoanalyse

§ 9
Einordnung in Datenschutzklassen und Datenschutzniveau

(1) Unter Berücksichtigung der Art der zu verarbeitenden personenbezogenen Daten und des Ausmaßes der möglichen Gefährdung personenbezogener Daten hat eine Einordnung in eine der in §§ 11 bis 13 genannten drei Datenschutzklassen zu erfolgen.

(2) Bei der Einordnung personenbezogener Daten in eine Datenschutzklasse sind auch der Zusammenhang mit anderen gespeicherten Daten, der Zweck ihrer Verarbeitung und das anzunehmende Interesse an einer missbräuchlichen Verwendung der Daten zu berücksichtigen.

(3) [1]Die Einordnung erfolgt durch den Verantwortlichen; sie soll in der Regel bei Erstellung des Verzeichnisses von Verarbeitungstätigkeiten vorgenommen werden. [2]Der oder die betriebliche Datenschutzbeauftragte soll angehört werden.

(4) [1]In begründeten Einzelfällen kann der Verantwortliche eine abweichende Einordnung vornehmen. [2]Die Gründe sind zu dokumentieren. [3]Erfolgt eine Einordnung in eine niedrigere Datenschutzklasse, ist zuvor der oder die betriebliche Datenschutzbeauftragte anzuhören.

(5) Erfolgt keine Einordnung, gilt automatisch die Datenschutzklasse III, sofern nicht die Voraussetzungen des § 14 vorliegen.

(6) Die Einordnung in eine der nachfolgend genannten Datenschutzklassen erfordert die Einhaltung des dieser Datenschutzklasse entsprechenden Schutzniveaus und die Einhaltung der dort beschriebenen Mindestmaßnahmen.

(7) Erfolgt die Verarbeitung durch einen Auftragsverarbeiter, ist der Verantwortliche verpflichtet, sich in geeigneter Weise, insbesondere durch persönliche Überprüfung oder Vorlage von Nachweisen, von dem Bestehen des der jeweiligen Datenschutzklasse entsprechenden Schutzniveaus zu überzeugen.

§ 10
Risikoanalyse

(1) Die den individuellen Gegebenheiten entspringenden Risiken sind vom Verantwortlichen anhand einer Risikoanalyse festzustellen.

(2) [1]Für eine Analyse der möglichen Risiken für die Rechte und Freiheiten natürlicher Personen, die mit der Verarbeitung personenbezogener Daten verbunden sind, sind objektive Kriterien zu entwickeln und anzuwenden. [2]Hierzu zählen insbesondere die Eintrittswahrscheinlichkeit und die Schwere eines Schadens für die betroffene Person. [3]Zu berücksichtigen sind auch Risiken, die durch – auch unbeabsichtigte oder unrechtmäßige – Vernichtung, durch Verlust, Veränderung, unbefugte Offenlegung von oder unbefugten Zugang zu personenbezogenen Daten entstehen.

(3) Die identifizierten Risiken sind durch entsprechende Maßnahmen im Einklang mit § 6 zu behandeln.

§ 11
Datenschutzklasse I und Schutzniveau I

(1) Der Datenschutzklasse I unterfallen personenbezogene Daten, deren missbräuchliche Verarbeitung keine besonders schwerwiegende Beeinträchtigung des Betroffenen erwarten lässt. Hierzu gehören insbesondere Namens- und Adressangaben ohne Sperrvermerke sowie Berufs-, Branchen- oder Geschäftsbezeichnungen.

(2) Zum Schutz der in die Datenschutzklasse I einzuordnenden Daten ist ein Schutzniveau I zu definieren. Dieses setzt voraus, dass mindestens folgende Voraussetzungen gegeben sind:

a) Das IT-System, auf dem die schützenswerten personenbezogenen Daten abgelegt sind, ist nicht frei zugänglich; es befindet sich z.B. in einem abschließbaren Gebäude oder unter ständiger Aufsicht.
b) [1]Die Anmeldung am IT-System ist nur nach Eingabe eines geeigneten benutzerdefinierten Passwortes oder unter Verwendung eines anderen, dem aktuellen Stand der Technik und dem jeweiligen Sicherheitsbedarf entsprechenden Authentifizierungsverfahrens zulässig. [2]In sicherheitskritischen Bereichen oder bei Zugriffen außerhalb gesicherter Netze ist insbesondere der Einsatz von Mehr-Faktor-Authentifizierungsverfahren (z. B. Kombination aus Passwort und Einmalcode, Hardware-Token oder biometrischen Verfahren) vorzusehen.
c) Sicherungskopien von Daten sind nach aktuellem Stand der Technik mit geeigneten Maßnahmen vor unbefugtem Zugriff zu schützen.
d) Vor der Weitergabe eines IT-Systems, insbesondere eines Datenträgers für einen anderen Einsatzzweck sind die auf ihm befindlichen Daten so zu löschen, dass ihre Lesbarkeit und ihre Wiederherstellung ausgeschlossen sind.
e) Nicht öffentlich verfügbare Daten werden nur dann weitergegeben, wenn sie durch geeignete Schutzmaßnahmen geschützt sind. Die Art und Weise des Schutzes ist vor Ort zu definieren.

§ 12
Datenschutzklasse II und Schutzniveau II

(1) Der Datenschutzklasse II unterfallen personenbezogene Daten, deren missbräuchliche Verarbeitung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann. Hierzu gehören z.B. Daten über Mietverhältnisse, Geschäftsbeziehungen sowie Geburts- und Jubiläumsdaten.

(2) Zum Schutz der in die Datenschutzklasse II einzuordnenden Daten ist ein Schutzniveau II zu definieren. Dieses setzt voraus, dass neben dem Schutzniveau I mindestens folgende Voraussetzungen gegeben sind:

a) [1]Die Anmeldung am IT-System ist nur nach Eingabe eines geeigneten benutzerdefinierten Passwortes zulässig, das ausreichend komplex gewählt werden muss und dessen Erneuerung nach dem jeweiligen Sicherheitsbedarf erfolgt. [2]Alternativ ist die Verwendung eines anderen, dem aktuellen Stand der Technik und dem jeweiligen Sicherheitsbedarf entsprechenden Authentifizierungsverfahrens zulässig.
b) [1]Das Starten des IT-Systems darf nur mit dem dafür bereit gestellten Betriebssystem erfolgen. [2]Zu diesem Zweck sind geeignete technische Maßnahmen wie beispielsweise ein Boot-Schutz umzusetzen.
c) Sicherungskopien und Ausdrucke der Datenbestände sind vor Fremdzugriff und vor der gleichzeitigen Vernichtung mit den Originaldaten zu schützen.
d) [1]Die Daten der Schutzklasse II sind auf zentralen Systemen in besonders gegen unbefugten Zutritt gesicherten Räumen zu speichern, sofern keine begründeten Ausnahmefälle gegeben sind. [2]Diese sind schriftlich dem oder der betrieblichen Datenschutzbeauftragten zu melden. [3]Die jeweils beteiligten IT-Systeme sind dem aktuellen Stand der Technik und dem jeweiligen Sicherheitsbedarf entsprechend angemessen zu schützen. [4]Eine Speicherung auf anderen IT-Systemen darf nur erfolgen, wenn diese mit einem geeigneten Zugriffsschutz ausgestattet sind.
e) [1]Die Übermittlung personenbezogener Daten außerhalb eines geschlossenen und gesicherten Netzwerks (auch über automatisierte Schnittstellen) hat grundsätzlich verschlüsselt zu erfolgen. [2]Das Verschlüsselungsverfahren ist dem aktuellen Stand der Technik und dem jeweiligen Sicherheitsbedarf entsprechend angemessen auszuwählen.

§ 13
Datenschutzklasse III und Schutzniveau III

(1) [1]Der Datenschutzklasse III unterfallen personenbezogene Daten, deren missbräuchliche Verarbeitung die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen erheblich beeinträchtigen kann. [2]Hierzu gehören insbesondere die besonderen Kategorien personenbezogener Daten gemäß § 4 Ziffer 2. KDG sowie Daten über strafbare Handlungen, arbeitsrechtliche Rechtsverhältnisse, Disziplinarentscheidungen und Namens- und Adressangaben mit Sperrvermerken.

(2) [1]Zum Schutz der in die Datenschutzklasse III einzuordnenden Daten ist ein Schutzniveau III zu definieren. [2]Dieses setzt voraus, dass neben dem Schutzniveau II mindestens folgende Voraussetzungen gegeben sind:

a) [1]Ist es aus dienstlichen Gründen zwingend erforderlich, dass Daten der Datenschutzklasse III auf mobilen Geräten im Sinne des § 4 Absatz 2 oder Datenträgern gespeichert werden, sind diese Daten nur verschlüsselt abzuspeichern. [2]Das Verschlüsselungsverfahren ist dem aktuellen Stand der Technik und dem jeweiligen Sicherheitsbedarf entsprechend angemessen auszuwählen.
b) [1]Eine langfristige Lesbarkeit der zu speichernden Daten ist sicher zu stellen. [2]So müssen z.B. bei verschlüsselten Daten die Sicherheit des Schlüssels und die erforderliche Entschlüsselung auch in dem nach § 16 Absatz 1 zu erstellenden Datensicherungskonzept berücksichtigt werden.

§ 14
Umgang mit personenbezogenen Daten, die dem Beichtgeheimnis oder dem Seelsorgegeheimnis unterliegen

(1) [1]Personenbezogene Daten, die dem Beichtgeheimnis oder dem Seelsorgegeheimnis unterliegen, sind in besonders hohem Maße schutzbedürftig. [2]Ihre Ausspähung oder Verlautbarung würde dem Vertrauen in die Verschwiegenheit katholischer Dienststellen und Einrichtungen schweren Schaden zufügen.

(2) Das Beichtgeheimnis nach cc. 983 ff. CIC ist zu wahren; personenbezogene Daten, die dem Beichtgeheimnis unterliegen, dürfen nicht verarbeitet werden.

(3) Personenbezogene Daten, die, ohne Gegenstand eines Beichtgeheimnisses nach cc. 983 ff. CIC zu sein, dem Seelsorgegeheimnis unterliegen, dürfen nur verarbeitet werden, wenn dem besonderen Schutzniveau angepasste, erforderlichenfalls über das Schutzniveau der Datenschutzklasse III hinausgehende technische und organisatorische Maßnahmen ergriffen werden.

(4) [1]Eine Maßnahme im Sinne des Absatz 3 kann, wenn die Verarbeitung auf IT-Systemen erfolgt, insbesondere die Unterhaltung eines eigenen Servers bzw. einer eigenen Datenablage in einem Netzwerk ohne externe Datenverbindung sein. [2]Auch die verschlüsselte Abspeicherung der personenbezogenen Daten auf einem externen Datenträger, der außerhalb der Dienstzeiten in einem abgeschlossenen Tresor gelagert wird, kann eine geeignete technische und organisatorische Maßnahme darstellen.

(5) Erfolgt die Seelsorge außerhalb eines geschlossenen Netzwerkes, sind geeignete, erforderlichenfalls über das Schutzniveau der Datenschutzklasse III hinausgehende, technische und organisatorische Maßnahmen nach dem aktuellen Stand der Technik zu treffen.

(6) Die Absätze 3 bis 5 gelten auch für personenbezogene Daten, die in vergleichbarer Weise schutzbedürftig sind.

Kapitel 4
Maßnahmen des Verantwortlichen und des oder der Mitarbeitenden

§ 15
Maßnahmen des Verantwortlichen

(1) Verantwortlicher ist gemäß § 4 Nr. 9. KDG 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.

(2) Ihm obliegt die Risikoanalyse zur Feststellung des Schutzbedarfs (§ 9 Absatz 1) sowie die zutreffende Einordnung der jeweiligen Daten in die Datenschutzklassen (§ 9 Absatz 6).

(3) Der Verantwortliche klärt die Mitarbeitenden über Gefahren und Risiken auf, die insbesondere aus der Nutzung eines IT-Systems erwachsen können.

(4) Der Verantwortliche stellt sicher, dass ein Konzept zur datenschutzrechtlichen Ausgestaltung der IT-Systeme erstellt und umgesetzt wird.

(5) [1]Erfolgt die Verarbeitung personenbezogener Daten durch einen Auftragsverarbeiter, so ist der Verantwortliche verpflichtet, die technischen und organisatorischen Maßnahmen des Auftragsverarbeiters regelmäßig, mindestens jedoch im Abstand von jeweils zwei Jahren auf ihre Wirksamkeit zu überprüfen und dies zu dokumentieren. [2]Bei Vorlage eines anerkannten Zertifikats durch den Auftragsverarbeiter gemäß § 29 Absatz 6 KDG kann auf eine Prüfung verzichtet werden.

(6) [1]Der Verantwortliche kann, unbeschadet seiner Verantwortlichkeit, seine Aufgaben und Befugnisse nach dieser Durchführungsverordnung durch schriftliche Anordnung auf geeignete Mitarbeitende übertragen. [2]Eine Übertragung auf den betrieblichen Datenschutzbeauftragten oder die betriebliche Datenschutzbeauftragte ist ausgeschlossen.

§ 16
Maßnahmen des Verantwortlichen zur Datensicherung

(1) [1]Der Verantwortliche hat ein Datensicherungskonzept zu erstellen und entsprechend umzusetzen. [2]Dabei ist die langfristige Lesbarkeit der zu speichernden Daten in der Datensicherung anzustreben.

(2) [1]Zum Schutz personenbezogener Daten vor Verlust sind regelmäßige Datensicherungen erforderlich. [2]Dabei sind u.a. folgende Aspekte mit zu berücksichtigen:

a) Soweit eine dauerhafte Lesbarkeit der Daten im Sinne des § 4 Absatz 3 nicht auf andere Weise sichergestellt werden kann, sind Sicherungskopien der verwendeten Programme in allen verwendeten Versionen anzulegen und von den Originaldatenträgern der Programme und den übrigen Datenträgern getrennt aufzubewahren.
b) Die Datensicherung soll in Umfang und Zeitabstand anhand der entstehenden Auswirkungen eines Verlustes der Daten festgelegt werden.

(3) Unabhängig von der Einteilung in Datenschutzklassen sind geeignete technische Abwehrmaßnahmen gegen Angriffe und den Befall von Schadsoftware z.B. durch den Einsatz aktueller Sicherheitstechnik wie Virenscanner, Firewall-Technologien und eines regelmäßigen Patch-Managements (geplante Systemaktualisierungen) vorzunehmen.

§ 17
Maßnahmen des oder der Mitarbeitenden

[1]Unbeschadet der Aufgaben des Verantwortlichen im Sinne des § 4 Ziffer 9. KDG trägt jeder und jede Mitarbeitende die Verantwortung für die datenschutzkonforme Ausübung seiner Tätigkeit. [2]Es ist ihm oder ihr untersagt, personenbezogene Daten zu einem anderen als dem in der jeweils rechtmäßigen Aufgabenerfüllung liegenden Zweck zu verarbeiten.

Kapitel 5
Besondere Gefahrenlagen

§ 18
Nutzung von Cloud-Diensten

Für die Verarbeitung personenbezogener Daten mit einem Cloud-Dienst gilt ergänzend zu den Vorschriften der §§ 5 ff.:

(1) Es sind primär bereits geprüfte und freigegebene Cloud-Dienste zu nutzen.

(2) [1]Vor der Nutzung anderer Cloud-Dienste ist anhand nachfolgender Aspekte zu prüfen, ob die erforderlichen Sicherheitsanforderungen erfüllt werden. [2]Folgende Aspekte können ein erhöhtes Risiko darstellen:

a) ungeplante vorzeitige Vertragsbeendigung durch den Diensteanbieter,
b) unzureichend gesicherte administrative Zugänge,
c) mangelnde Portabilität von personenbezogenen Daten und IT-Systemen,
d) generelle Abhängigkeit vom Cloud-Diensteanbieter mangels Wechselmöglichkeit,
e) Gefährdung der Integrität von Informationen aufgrund herstellerspezifischer Datenformate,
f) gemeinsame Nutzung der Cloud-Infrastruktur durch mehrere Kunden,
g) Unkenntnis über den Speicherort der Informationen,
h) hohe Mobilität der Informationen sowie
i) unbefugter Zugriff auf Informationen beispielsweise durch Administrationspersonal des Cloud-Diensteanbieters oder Dritte.

(3) Vor der Nutzung des Cloud-Dienstes ist in Abhängigkeit von der Risikoanalyse eine Exit-Strategie zu definieren (z. B. Datenlöschung, Datenübertragung).

§ 19
Autorisierte Programme

Auf dienstlichen IT-Systemen dürfen ausschließlich vom Verantwortlichen autorisierte Programme und Kommunikationstechnologien verwendet werden.

§ 20
Nutzung dienstlicher IT-Systeme zu auch privaten Zwecken

[1]Die Nutzung dienstlicher IT-Systeme zu auch privaten Zwecken ist grundsätzlich unzulässig. [2]Ausnahmen regelt der Verantwortliche unter Beachtung der jeweils geltenden gesetzlichen Regelungen.

§ 21
Nutzung privater IT-Systeme zu dienstlichen Zwecken

(1) [1]Die Verarbeitung personenbezogener Daten auf privaten IT-Systemen zu dienstlichen Zwecken ist grundsätzlich unzulässig. [2]Sie kann als Ausnahme von dem Verantwortlichen unter Beachtung der jeweils geltenden gesetzlichen Regelungen zugelassen werden.

(2) [1]Die Zulassung erfolgt schriftlich und beinhaltet mindestens

a) die Angabe der Gründe, aus denen die Nutzung des privaten IT-Systems erforderlich ist,
b) eine Regelung über den Einsatz einer zentralisierten Verwaltung von Mobilgeräten (z.B. Mobile Device Management) auf dem privaten IT-System des oder der Mitarbeitenden,
c) das Recht des Verantwortlichen zur Löschung durch Fernzugriff aus wichtigem und unabweisbarem Grund; ein wichtiger und unabweisbarer Grund liegt insbesondere vor, wenn der Schutz personenbezogener Daten Dritter nicht auf andere Weise sichergestellt werden kann,
d) eine jederzeitige Überprüfungsmöglichkeit des Verantwortlichen,
e) die Dauer der Nutzung des privaten IT-Systems für dienstliche Zwecke,
f) das Recht des Verantwortlichen festzulegen, welche Programme verwendet oder nicht verwendet werden dürfen sowie
g) die Verpflichtung zum Nachweis einer Löschung der zu dienstlichen Zwecken verarbeiteten personenbezogenen Daten, wenn die Freigabe der Nutzung des privaten IT-Systems endet, das IT-System weitergegeben oder verschrottet wird.

[2]Ergänzend ist dem oder der betreffenden Mitarbeitenden eine spezifische Handlungsanweisung auszuhändigen, die Regelungen zur Nutzung des privaten IT-Systems enthält.

(3) Der Zugang von privaten IT-Systemen über sogenannte webbasierte Lösungen kann mit den Mitarbeitenden vereinbart werden, soweit alle datenschutzrechtlichen Voraussetzungen für eine sichere Nutzung gegeben sind.

(4) [1]Die Weiterleitung dienstlicher personenbezogener Daten auf private E-Mail-Konten ist unzulässig. [2]Dies gilt auch für personalisierte E-Mail-Adressen. 3Ausnahmeregelungen können von dem Verantwortlichen getroffen werden, soweit das datenschutzrechtliche Schutzniveau, insbesondere nach dem KDG oder dieser Durchführungsverordnung, nicht unterschritten wird.

(5) Der oder die Mitarbeitende hat sicherzustellen, dass unberechtigte Dritte, insbesondere Familienmitglieder, keinen Zugriff auf dienstliche personenbezogene Daten haben.

§ 22
Externe Zugriffe, Auftragsverarbeitung

(1) [1]Der Zugriff aus und von anderen IT-Systemen durch Externe (z.B. externe Dienstleister, externe Dienststellen) schafft besondere Gefahren hinsichtlich der Ausspähung von Daten. [2]Derartige Zugriffe dürfen nur aufgrund vertraglicher Vereinbarung erfolgen. [3]Insbesondere mit Auftragsverarbeitern, die nicht den Regelungen des KDG unterfallen, ist grundsätzlich neben der Anwendung der EU-Datenschutzgrundverordnung die Anwendung des KDG zu vereinbaren.

(2) Bei Zugriffen durch Externe ist mit besonderer Sorgfalt darauf zu achten und nicht nur vertraglich, sondern nach Möglichkeit auch technisch sicherzustellen, dass keine Kopien der personenbezogenen Datenbestände gefertigt werden können.

(3) [1]Muss dem Externen bei Vornahme der Arbeiten ein Systemzugang eröffnet werden, ist dieser Zugang entweder zu befristen oder unverzüglich nach Beendigung der Arbeiten zu deaktivieren. [2]Im Zuge dieser Arbeiten vergebene Passwörter sind nach Beendigung der Arbeiten unverzüglich zu ändern.

(4) Bei der dauerhaften Inanspruchnahme von externen IT-Dienstleistern sind geeignete vergleichbare Regelungen zu treffen.

(5) [1]Eine Fernwartung von IT-Systemen darf darüber hinaus nur erfolgen, wenn der Beginn aktiv seitens des Auftraggebers eingeleitet wurde, über sichere Verbindungen erfolgt und die Fernwartung systemseitig protokolliert wird. [2]Im Falle der Einbeziehung externer Dienstleister sind auch die datenschutzrechtlichen Anforderungen und Verantwortlichkeiten sowie technische Schutzmaßnahmen vertraglich zu regeln.

(6) Die Verbringung von IT-Systemen mit Daten der Datenschutzklasse III zur Durchführung von Wartungsarbeiten in den Räumen eines Externen darf nur erfolgen, wenn die Durchführung der Wartungsarbeiten in eigenen Räumen nicht möglich ist und sie unter den Bedingungen einer Auftragsverarbeitung erfolgt.

§ 23
Verschrottung und Vernichtung von IT-Systemen, Abgabe von IT-Systemen zur weiteren Nutzung

(1) [1]Bei der Verschrottung bzw. der Vernichtung von IT-Systemen im Sinne des § 4 Abs. 2 Nr. 1 dieser Verordnung, insbesondere Datenträgern, Faxgeräten und Druckern, sind den jeweiligen DIN-Normen entsprechende Maßnahmen zu ergreifen, die die Lesbarkeit oder Wiederherstellbarkeit der Daten zuverlässig ausschließen. 2Dies gilt auch für den Fall der Abgabe von IT-Systemen, insbesondere Datenträgern, zur weiteren Nutzung.

(2) Absatz 1 gilt auch für die Verschrottung, Vernichtung oder Abgabe von privaten IT-Systemen, die gemäß § 20 zu dienstlichen Zwecken genutzt werden.

§ 24
Passwortlisten der Systemverwaltung

Alle nicht zurücksetzbaren Passwörter (z.B. BIOS- und Administrationspasswörter) sind besonders gesichert aufzubewahren.

§ 25
Übermittlung personenbezogener Daten per Fax

[1]Die Übermittlung personenbezogener Daten per Fax ist grundsätzlich unzulässig. [2]In spezifischen Bestimmungen können Ausnahmen, insbesondere Übergangsbestimmungen, vorgesehen werden; dabei sind die Vorschriften der §§ 5 ff. und die jeweils aktuellen Sicherheitsstandards zu beachten.

§ 26
Sonstige Formen der Übermittlung personenbezogener Daten

(1) [1]E-Mails, die personenbezogene Daten der Datenschutzklasse II oder III enthalten, dürfen ausschließlich im Rahmen eines geschlossenen und gesicherten Netzwerks oder in verschlüsselter Form mit geeignetem Verschlüsselungsverfahren übermittelt werden. [2]Das Verschlüsselungsverfahren ist dem aktuellen Stand der Technik und dem jeweiligen Sicherheitsbedarf entsprechend angemessen auszuwählen.

(2) Eine Übermittlung personenbezogener Daten per E-Mail an Postfächer, auf die mehr als eine Person Zugriff haben (sog. Funktionspostfächer), ist in Fällen personenbezogener Daten der Datenschutzklassen II und III grundsätzlich nur zulässig, wenn durch vorherige Abstimmung mit dem Empfänger sichergestellt ist, dass ausschließlich autorisierte Personen Zugriff auf dieses Postfach haben.

(3) Für die Übermittlung von Video- und Sprachdaten insbesondere im Zusammenhang mit Video- und Telefonkonferenzen gilt Absatz 1 unter Berücksichtigung des aktuellen Standes der Technik entsprechend.

§ 27
Kopier- / Scangeräte

Bei Kopier-/Scangeräten mit eigener Speichereinheit ist sicherzustellen, dass ein Zugriff auf personenbezogene Daten durch unberechtigte Mitarbeitende oder sonstige Dritte nicht möglich ist.

Kapitel 6
Übergangs- und Schlussbestimmungen

§ 28
Inkrafttreten

Diese Durchführungsverordnung tritt zum 01.03.2019 in Kraft.



Katholisches
Datenschutzzentrum