Kirchenordnung über den Datenschutz
(KO.HA.DS)

Die Heilsarmee in Deutschland
Körperschaft des öffentlichen Rechts

Inhalt

Präambel 5

Kapitel 1 – Allgemeine Bestimmungen 6
§ 1 Gegenstand und Ziel 6
§ 2 Sachlicher Anwendungsbereich 6
§ 3 Räumlicher Anwendungsbereich 6
§ 4 Begriffsbestimmungen 7

Kapitel 2 – Grundsätze 11
§ 5 Grundsätze für die Verarbeitung personenbezogener Daten 11
§ 6 Rechtmäßigkeit der Verarbeitung 12
§ 7 Bedingungen für die Einwilligung 14
§ 8 Bedingungen für die Einwilligung Minderjähriger in Bezug auf elektronische Angebote 15
§ 9 Verarbeitung besonderer Kategorien personenbezogener Daten 15
§ 10 Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten 17
§ 11 Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist 17

Kapitel 3 – Rechte der betroffenen Person 17

Abschnitt 1: Transparenz und Modalitäten 17
§ 12 Transparente Information, Kommunikation 17

Abschnitt 2: Informationspflicht und Recht auf Auskunft zu personenbezogenen Daten 18
§ 13 Informationspflicht bei unmittelbarer Datenerhebung 18
§ 14 Informationspflicht bei mittelbarer Datenerhebung 19
§ 15 Auskunftsrecht der betroffenen Person 20

Abschnitt 3: Berichtigung und Löschung 21
§ 16 Recht auf Berichtigung 21
§ 17 Recht auf Löschung („Recht auf Vergessenwerden“) 21
§ 18 Recht auf Einschränkung der Verarbeitung 22
§ 19 Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung 23
§ 20 Recht auf Datenübertragbarkeit 23

Abschnitt 4: Widerspruchsrecht und automatisierte Entscheidungsfindung im Einzelfall 23
§ 21 Widerspruchsrecht 23
§ 22 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling 24
§ 23 – entfällt – 25

Kapitel 4 – Verantwortlicher und Auftragsverarbeiter 25

Abschnitt 1: Allgemeine Pflichten 25
§ 24 Verantwortung der für die Verarbeitung verantwortlichen Stelle 25
§ 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen 25
§ 26 Gemeinsam für die Verarbeitung verantwortliche Stellen 26
§ 27 – entfällt – 26
§ 28 Auftragsverarbeiter 26
§ 29 Verarbeitung unter der Aufsicht der verantwortlichen Stelle oder des Auftragsverarbeiters 28
§ 30 Verzeichnis von Verarbeitungstätigkeiten 28
§ 31 Zusammenarbeit mit der Aufsichtsbehörde 30

Abschnitt 2: Sicherheit personenbezogener Daten 30
§ 32 Sicherheit der Verarbeitung 30
§ 33 Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde 31
§ 34 Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person 31

Abschnitt 3: Datenschutz-Folgenabschätzung und vorherige Konsultation 32
§ 35 Datenschutz-Folgenabschätzung 32
§ 36 Vorherige Konsultation 33

Abschnitt 4: Datenschutzbeauftragter 34

§ 37 – abweichend – ... 34
§ 37 a Benennung eines Datenschutzbeauftragten ... 34
§ 37 b Örtlicher Datenschutzassistent/Datenschutzkoordinator ... 35
§ 38 Stellung des Datenschutzbeauftragten ... 36
§ 39 Aufgaben des Datenschutzbeauftragten ... 37

Abschnitt 5: – entfällt – ... 37
§ 40 – entfällt – ... 37
§ 41 – entfällt – ... 37
§ 42 – entfällt – ... 37
§ 43 – entfällt – ... 37

Kapitel 5 – Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen ... 37
§ 44 Allgemeine Grundsätze der Datenübermittlung ... 37
§ 45 Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses ... 38
§ 46 Datenübermittlung vorbehaltlich geeigneter Garantien ... 38
§ 47 – entfällt – ... 38
§ 48 – entfällt – ... 38
§ 49 Ausnahmen für bestimmte Fälle ... 38
§ 50 – entfällt – ... 39

Kapitel 6 – Unabhängige Aufsichtsbehörden ... 39

Abschnitt 1: Unabhängigkeit ... 39
§ 51 Aufsichtsbehörde ... 39
§ 52 Unabhängigkeit ... 40
§ 53 Allgemeine Bedingungen für die Mitglieder der Aufsichtsbehörde ... 40
§ 54 Errichtung der Aufsichtsbehörde ... 40

Abschnitt 2: Zuständigkeit, Aufgaben und Befugnisse ... 41
§ 55 Zuständigkeit ... 41
§ 56 – entfällt – ... 42
§ 57 Aufgaben ... 42
§ 58 Befugnisse ... 43
§ 59 Tätigkeitsbericht ... 45

Kapitel 7 – entfällt – ... 46
§ 60 – entfällt – ... 46
§ 61 – entfällt – ... 46
§ 62 – entfällt – ... 46
§ 63 – entfällt – ... 46
§ 64 – entfällt – ... 46
§ 65 – entfällt – ... 46
§ 66 – entfällt – ... 46
§ 67 – entfällt – ... 46
§ 68 – entfällt – ... 46
§ 69 – entfällt – ... 46
§ 70 – entfällt – ... 46
§ 71 – entfällt – ... 46
§ 72 – entfällt – ... 46
§ 73 – entfällt – ... 46
§ 74 – entfällt – ... 46
§ 75 – entfällt – ... 46
§ 76 – entfällt – ... 46

Kapitel 8 – Rechtsbehelfe, Haftung und Sanktionen ... 46
§ 77 Recht auf Beschwerde bei einer Aufsichtsbehörde ... 46
§ 78 – abweichend – ... 46
§ 78 a Rechtsweg ... 47
§ 79 – entfällt – ... 47
§ 80 – entfällt – ... 47
§ 81 – entfällt – ... 47
§ 82 Haftung und Recht auf Schadenersatz ... 47

§ 83 Allgemeine Bedingungen für die Verhängung von Geldbußen ... 48
§ 84 – entfällt – ... 49

Kapitel 9 – Vorschriften für besondere Verarbeitungssituationen ... 49
§ 85 – abweichend – ... 49
§ 85 a Verarbeitung personenbezogener Daten durch die Medien ... 49
§ 86 – abweichend – ... 50
§ 86 a Offenlegung an kirchliche oder öffentliche Stellen ... 50
§ 86 b Offenlegung an sonstige Stellen ... 51
§ 87 – entfällt – ... 51
§ 88 – abweichend – ... 51
§ 88 a Verarbeitung personenbezogener Daten bei Dienst- und Arbeitsverhältnissen ... 51
§ 89 – abweichend – ... 53
§ 89 a Verarbeitung personenbezogener Daten für wissenschaftliche und statistische Zwecke ... 53
§ 90 – entfällt – ... 53
§ 91 – abweichend – ... 53
§ 91 a Seelsorgegeheimnis und Amtsverschwiegenheit ... 54
§ 91 b Gottesdienste und kirchliche Veranstaltungen ... 54
§ 91 c Videoüberwachung öffentlich zugänglicher Räume ... 54

Kapitel 10 – entfällt – ... 55
§ 92 – entfällt – ... 55
§ 93 – entfällt – ... 55

Kapitel 11 – Schlussbestimmungen ... 55
§ 94 – entfällt – ... 55
§ 95 – entfällt – ... 55
§ 96 – entfällt – ... 55
§ 97 – entfällt – ... 55
§ 98 – abweichend – ... 55
§ 98 a Ergänzende Bestimmungen ... 55
§ 98 b Übergangsregeln ... 55
§ 99 Inkrafttreten, Außerkrafttreten ... 56

Die in dieser Rechtsverordnung verwendete sprachliche Form der Personenbeschreibung erlaubt keinen Rückschluss auf das Geschlecht einer Person.

Der Aufbau dieser Kirchenordnung orientiert sich an der DSGVO Stand 2018.

Präambel

[1]Die Heilsarmee in Deutschland (Religionsgemeinschaft und Körperschaft des öffentlichen Rechts) hat mit ihrer Vision 2030,

„Zu Jesus rufen –
in Jesus wachsen –
wie Jesus handeln“.

zugleich die Orientierung für die Ausrichtung ihres Wirkens gegeben.

[2]Zeitgleich wurde auch in kompakter Form zum Ausdruck gebracht, wie dieses Wirken gestaltet werden soll:

zeitgemäß – stark – effektiv.

[3]Diese Kirchenordnung wird erlassen in Ausübung des verfassungsrechtlich garantierten Rechtes der Bundesrepublik Deutschland für die Kirche, Die Heilsarmee in Deutschland, K. d. ö. R, ihre Angelegenheiten selbstständig innerhalb der Schranken des für alle geltenden Gesetzes zu ordnen und zu verwalten (Art. 140 GG, i. V. m. Art. 137 WRV). [4]Dieses Recht ist europarechtlich geachtet und festgeschrieben in Artikel 91 und Erwägungsgrund 165 EU 2016/679 des Europäischen Parlamentes und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46 EG (Datenschutz-Grundverordnung) sowie Artikel 17 Vertrag über die Arbeitsweise der Europäischen Union (AEUV). [5]In Wahrnehmung dieses Rechts hält diese Kirchenordnung den Einklang mit der Datenschutz-Grundverordnung aufrecht und regelt die Datenverarbeitung im Bereich der Die Heilsarmee in Deutschland, Körperschaft des öffentlichen Rechts, und aller ihrer Organisationseinheiten sowie zuzuordnenden Gliedwerke. [6]Die Datenverarbeitung dient der Erfüllung des kirchlichen Auftrags.

Kapitel 1 – Allgemeine Bestimmungen

§ 1 | Gegenstand und Ziel

(1) [1]Diese Kirchenordnung über den Datenschutz enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten. [2]Nachfolgend wird diese Kirchenordnung als Datenschutzordnung bezeichnet.

(2) Zweck dieser Datenschutzordnung ist es, die einzelnen Personen davor zu schützen, dass sie durch den Umgang mit ihren personenbezogenen Daten in ihrer Persönlichkeit beeinträchtigt werden.

(3) – entfällt –

§ 2 | Sachlicher Anwendungsbereich

(1) [1]Diese Datenschutzordnung findet Anwendung auf die Verarbeitung personenbezogener Daten im Rahmen der Tätigkeit der freikirchlichen Stelle oder auf die Verarbeitung personenbezogener Daten in deren Auftrag. [2]Sie gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Datensystem gespeichert sind oder gespeichert werden sollen.

(2) Diese Datenschutzordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten.

(3) Die Vorschriften dieser Datenschutzordnung gehen Verwaltungsvorschriften der freikirchlichen Stellen vor, soweit bei der Ermittlung des Sachverhaltes personenbezogene Daten verarbeitet werden.

(4) Soweit andere Rechtsvorschriften, die freikirchliche Stellen anzuwenden haben, die Verarbeitung personenbezogener Daten regeln, gehen sie dieser Verordnung vor.

§ 3 | Räumlicher Anwendungsbereich

(1) [1]Diese Datenschutzordnung gilt für die Verarbeitung personenbezogener Daten durch die Kirche Die Heilsarmee in Deutschland, für

a. das Territoriale Hauptquartier,
b. die regionalen Verwaltungen und weiteren Verwaltungseinheiten,
c. die kirchlichen Stiftungen,
d. die Korps und Sozialeinrichtungen, wie auch deren Arbeitszweige, Programme und Dienste,
e. sonstige Arbeitsbereiche,
f. die kirchlichen Körperschaften, Stiftungen, Werke, Einrichtungen und die sonstigen kirchlichen Rechtsträger ohne Rücksicht auf deren Rechtsform.

[2]Die Heilsarmee in Deutschland, ihre Gliedstrukturen und Gliedwerke stellen sicher, dass auch in den ihnen zugeordneten Diensten, Vereinen, Einrichtungen und Werken diese Datenschutzordnung sowie die zu ihrer Ausführung und Durchführung erlassenen weiteren

Bestimmungen Anwendung finden.

(2) Die Heilsarmee in Deutschland führt ein Verzeichnis aller ihr zugeordneten Stellen sowie der Werke und Einrichtungen mit eigener Rechtspersönlichkeit.

(3) Der Begriff „(frei)kirchlich“ oder „(frei)kirchliche Stelle(n)“ bezieht sich auf alle Stellen gemäß der Absätze 1 und 2.

(4) Diese Datenschutzordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer freikirchlichen Stelle nach Absatz 3 oder durch einen Auftragsverarbeiter innerhalb des Geltungsbereiches dieser Ordnung erfolgt, unabhängig vom Ort der Verarbeitung.

§ 4 | Begriffsbestimmungen

Im Sinne dieser Datenschutzordnung 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 identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;

2. „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;

3. „Einschränkung der Verarbeitung“
   die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;

4. „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;

5. „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;

6. „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;

7. „Verantwortliche Stelle“/„örtliche verantwortliche Stelle“
   die natürliche oder juristische Person, freikirchliche Stelle im Sinne von § 3 Absatz 3 oder sonstige Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;

8. „Auftragsverarbeiter“
   eine natürliche oder juristische Person, freikirchliche Stelle oder sonstige Stelle, die personenbezogene Daten im Auftrag für die verantwortliche Stelle verarbeitet;

9. „Empfänger“
   eine natürliche oder juristische Person, freikirchliche oder sonstige Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht.

10. „Dritter“
    eine natürliche oder juristische Person, freikirchliche oder sonstige Stelle, außer der betroffenen Person, die verantwortliche Stelle, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung der freikirchlichen Stelle, der Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;

11. „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;

12. „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;

13. „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;

14. „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;

15. „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;

16. „Hauptniederlassung“
    im Falle einer verantwortlichen Stelle mit Niederlassungen außerhalb der Bundesrepublik Deutschland, in einem Mitgliedstaat der Union, ist das Territoriale Hauptquartier die Hauptniederlassung, es sei denn, die Entscheidungen hinsichtlich der Zwecke und Mittel der Verarbeitung personenbezogener Daten werden in einer anderen Niederlassung der verantwortlichen Stelle in der Union getroffen und diese Niederlassung ist befugt, diese Entscheidungen umsetzen zu lassen; in diesem Fall gilt die Niederlassung, die derartige Entscheidungen trifft, als Hauptniederlassung;

17. „Vertreter“
    eine in der Union niedergelassene natürliche oder juristische Person, die von der verantwortlichen Stelle oder dem Auftragsverarbeiter schriftlich gemäß Artikel 27 der DSGVO bestellt wurde und die verantwortliche Stelle oder den Auftragsverarbeiter in Bezug auf die ihnen jeweils nach dieser Verordnung obliegenden Pflichten vertritt;

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

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

20. „verbindliche interne Datenschutzvorschriften“
    Maßnahmen zum Schutz personenbezogener Daten, zu deren Einhaltung sich eine verantwortliche Stelle verpflichtet im Hinblick auf Datenübermittlungen oder eine Kategorie von Datenübermittlungen personenbezogener Daten an eine verantwortliche Stelle oder einen Auftragsverarbeiter der internationalen Heilsarmee in einem oder mehreren Drittländern;

21. „Aufsichtsbehörde“
    von der Die Heilsarmee in Deutschland gemäß § 51, ggf. gemeinsam mit anderen Kirchen, eingerichtete oder beauftragte unabhängige Stelle;

22. „betroffene Aufsichtsbehörde“
    eine Aufsichtsbehörde, die von der Verarbeitung personenbezogener Daten betroffen ist, weil
    a) die verantwortliche Stelle oder der Auftragsverarbeiter im Zuständigkeitsbereich dieser Aufsichtsbehörde niedergelassen ist,

    b) diese Verarbeitung erhebliche Auswirkungen auf betroffene Personen mit Wohnsitz im Zuständigkeitsbereich dieser Aufsichtsbehörde hat oder haben kann oder

    c) eine Beschwerde bei dieser Aufsichtsbehörde eingereicht wurde;

23. „grenzüberschreitende Verarbeitung“
    entweder
    a) eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten von Niederlassungen einer verantwortlichen Stelle, eines Auftragsverarbeiters oder

der internationalen Heilsarmee in der Union in mehr als einem Mitgliedstaat erfolgt, wenn die verantwortliche Stelle oder der Auftragsverarbeiter in mehr als einem Mitgliedstaat niedergelassen ist, oder

b) eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten einer einzelnen Niederlassung einer verantwortlichen Stelle, eines Auftragsverarbeiters oder der internationalen Heilsarmee in der Union erfolgt, die jedoch erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat oder haben kann;

24. – entfällt –

25. – entfällt –

26. „Internationale Organisation“
eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Ländern geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde.

27. „Besondere Kategorien personenbezogener Daten“
beinhalten alle Informationen zu natürlichen Personen,

a) aus denen religiöse oder weltanschauliche Überzeugungen hervorgehen, ausgenommen Angaben über die Zugehörigkeit zu einer Kirche oder Religions- oder Weltanschauungsgemeinschaft,

b) aus denen die rassische und ethnische Herkunft hervorgehen,

c) aus denen politische Meinungen oder die Gewerkschaftszugehörigkeit hervorgehen,

d) über deren genetische Daten,

e) und deren biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,

f) und deren Gesundheitsdaten,

g) und deren Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person;

28. „Beschäftigte“
a) die im Offiziersdienst oder diesem gleichgestellten Dienstverhältnis stehenden Personen,

b) die in einem Angestelltenverhältnis stehenden Personen,

c) Arbeitnehmer einschließlich der Leiharbeitnehmer im Verhältnis zum Entleiher,

d) zu ihrer Berufsausbildung Beschäftigte,

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

f) Beschäftigte in anerkannten Werkstätten für Menschen mit Behinderungen,

g) nach dem Bundesfreiwilligen- oder dem Jugendfreiwilligendienstgesetz oder in vergleichbaren Diensten Beschäftigte,

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) Bewerbende für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist;

29. „Anonymisierung“
die Verarbeitung personenbezogener Daten in einer Weise, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig hohen Aufwand an Zeit, Kosten und Arbeitskraft einer betroffenen Person zugeordnet werden können.

30. „DSGVO“ bzw. „EU-DSGVO“
steht für die Datenschutz-Grundverordnung der Europäischen Union mit der offiziellen Bezeichnung:
1. 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.

Kapitel 2 – Grundsätze

§ 5 | Grundsätze für die Verarbeitung personenbezogener Daten

(1) Für die Verarbeitung personenbezogener Daten im Geltungsbereich dieser Datenschutzordnung gelten folgende Grundsätze:

a) „Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“
Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.

b) „Zweckbindung“
Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden;
eine Weiterverarbeitung für im freikirchlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt als vereinbar mit den ursprünglichen Zwecken.

c) „Datenminimierung“
Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

d) „Richtigkeit“
Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig

sind, unverzüglich gelöscht oder berichtigt werden.

e) „Speicherbegrenzung“
[1]Personenbezogene Daten müssen 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. [2]Personenbezogene Daten dürfen länger gespeichert werden, soweit sie für die Zwecke des Archivs, der wissenschaftlichen und historischen Forschung sowie der Statistik verarbeitet werden. [3]Sie sind zu anonymisieren oder pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

f) „Integrität und Vertraulichkeit“
Personenbezogene Daten müssen 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;

(2) „Rechenschaftspflicht“
Die verantwortliche Stelle ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können.

§ 6 | Rechtmäßigkeit der Verarbeitung

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

a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

b) 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;

c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der die verantwortliche Stelle unterliegt;

d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;

e) – entfällt –

f) die Verarbeitung ist zur Wahrung der berechtigten Interessen der verantwortlichen Stelle oder eines Dritten erforderlich, sofern nicht die schutzwürdigen Interessen der betroffenen Person überwiegen, insbesondere dann, wenn diese minderjährig ist;

g) eine Rechtsvorschrift erlaubt die Verarbeitung der personenbezogenen Daten oder ordnet sie an;

h) die Verarbeitung ist zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich, einschließlich der Ausübung kirchlicher Aufsicht;

i) die Verarbeitung ist für die Wahrnehmung einer sonstigen Aufgabe erforderlich, die im kirchlichen Interesse liegt.

(2) – entfällt –

(3) Die Rechtsgrundlage für die Verarbeitungen gemäß Absatz 1 Buchstaben c und g wird festgelegt durch

a) Unionsrecht oder

b) das staatliche Recht, dem die freikirchliche Stelle unterliegt, oder

c) kirchliches Recht der Heilsarmee in Deutschland.

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

a) eine kirchliche Rechtsvorschrift dies vorsieht oder zwingend voraussetzt;

b) eine staatliche Rechtsvorschrift dies vorsieht und kirchliche Interessen nicht entgegenstehen;

c) die betroffene Person eingewilligt hat;

d) dies im Interesse der betroffenen Person liegt und kein Grund zu der Annahme besteht, dass diese in Kenntnis des anderen Zweckes ihre Einwilligung verweigern würde;

e) Angaben der betroffenen Person überprüft werden müssen, weil Anhaltspunkte für deren Unrichtigkeit bestehen;

f) die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen darf, es sei denn, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Zweckänderung offensichtlich überwiegt;

g) es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist;

h) sie zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse der betroffenen Person an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann;

i) sie für statistische Zwecke zur Erfüllung des kirchlichen Auftrages erforderlich ist.

(5) $_1$In anderen Fällen muss die freikirchliche Stelle feststellen, ob die Zweckänderung mit dem Zweck, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist. $_2$Dabei berücksichtigt sie 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 der kirchlichen Stelle;

c) die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß § 10 dieser Datenschutzordnung 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 kann.

(6) [1]Eine Verarbeitung für andere Zwecke liegt nicht vor, wenn sie der Wahrnehmung von Visitations-, Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung, der Revision oder der Durchführung von Organisationsuntersuchungen für die verantwortliche Stelle dient. [2]Das gilt auch für die Verarbeitung zu Ausbildungs- und Prüfungszwecken durch die verantwortliche Stelle, soweit nicht überwiegende schutzwürdige Interessen der betroffenen Person entgegenstehen.

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

(8) Die Verarbeitung von besonderen Kategorien personenbezogener Daten für andere Zwecke ist nur rechtmäßig, wenn die Voraussetzungen vorliegen, die eine Verarbeitung nach § 9 Absatz 2 dieser Datenschutzordnung zulassen.

§ 7 | Bedingungen für die Einwilligung

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

(2) [1]Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. [2]Soweit die Erklärung unter Umständen abgegeben worden ist, die gegen diese Datenschutzordnung verstoßen, ist sie unwirksam.

(3) [1]Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. [2]Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. [3]Die betroffene Person wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt. [4]Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.

(4) Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Umfang 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.

§ 8 Bedingungen für die Einwilligung Minderjähriger in Bezug auf elektronische Angebote

(1) [1]Minderjährige, denen elektronische Angebote von kirchlichen Stellen gemacht werden, können in die Verarbeitung ihrer Daten wirksam einwilligen, wenn sie religionsmündig sind. [2]Sind die Minderjährigen noch nicht religionsmündig, ist die Verarbeitung nur rechtmäßig, wenn die Sorgeberechtigten die Einwilligung erteilt oder der Einwilligung zugestimmt haben.

(2) Die verantwortliche Stelle unternimmt unter Berücksichtigung der verfügbaren Technik angemessene Anstrengungen, um sich in Fällen nach Absatz 1 Satz 2 zu vergewissern, dass die Einwilligung durch den Träger der elterlichen Verantwortung für den Minderjährigen oder mit dessen Zustimmung erteilt wurde.

(3) – entfällt –

(4) Die Einwilligung der Sorgeberechtigten ist nicht erforderlich, wenn kirchliche Präventions- oder Beratungsdienste einem Kind unmittelbar angeboten werden.

§ 9 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;

b) die Verarbeitung ist erforderlich, damit die verantwortliche Stelle oder die betroffene Person die ihr aus dem Arbeits- und Dienstrecht sowie dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach kirchlichem oder staatlichem Recht oder einer Dienstvereinbarung und den Arbeits- und Finanzrichtlinien, die geeignete Garantien für die Rechte und die Interessen der betroffenen Person vorsehen müssen, rechtmäßig 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 durch eine verantwortliche Stelle im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der verantwortlichen Stelle oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden;

e) die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person öffentlich gemacht hat;

f) die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Schlichtungsausschüsse sowie Kirchengerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich,

g) die Verarbeitung ist auf der Grundlage des kirchlichen Rechts, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen kirchlichen Interesses erforderlich;

h) die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage kirchlichen oder staatlichen Rechts oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Absatz 3 genannten Bedingungen und Garantien erforderlich,

i) die Verarbeitung ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten, auf der Grundlage des kirchlichen oder staatlichen Rechts, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsieht, erforderlich, oder

j) 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 vorsieht, für im kirchlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke erforderlich.

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

(4) – entfällt –

§ 10 Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten

Die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln ist unter den Voraussetzungen des § 6 Absatz 1 dieser Datenschutzordnung zulässig, wenn dies das kirchliche oder staatliche Recht, das geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht, zulässt.

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

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

(2) $_1$Kann die verantwortliche Stelle in Fällen gemäß Absatz 1 nachweisen, dass sie nicht in der Lage ist, die betroffene Person zu identifizieren, so unterrichtet sie die betroffene Person hierüber, sofern möglich. $_2$In diesen Fällen finden die §§ 15 bis 20 keine Anwendung, es sei denn, die betroffene Person stellt zur Ausübung ihrer in diesen Vorschriften niedergelegten Rechte zusätzliche Informationen bereit, die ihre Identifizierung ermöglichen.

Kapitel 3 – Rechte der betroffenen Person

Abschnitt 1: Transparenz und Modalitäten

§ 12 Transparente Information, Kommunikation

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

(2) Die verantwortliche Stelle erleichtert der betroffenen Person die Ausübung ihrer Rechte gemäß den §§ 15 bis 22 dieser Datenschutzordnung.

(3) $_1$Die verantwortliche Stelle stellt der betroffenen Person Informationen über die auf Antrag gemäß den §§ 15 bis 22 ergriffenen Maßnahmen innerhalb von drei Monaten 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. $_3$Die verantwortliche Stelle unterrichtet die betroffene Person innerhalb von drei Monaten nach Eingang über eine Fristverlängerung zusammen mit den Gründen für die Verzögerung.

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

Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen.

(5) [1]Informationen werden unentgeltlich zur Verfügung gestellt. [2]Bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person kann die verantwortliche Stelle entweder

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]Die verantwortliche Stelle hat den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags zu erbringen.

(6) Hat die verantwortliche Stelle begründete Zweifel an der Identität der natürlichen Person, die den Antrag gemäß den §§ 15 bis 21 stellt, so kann sie unbeschadet des § 11 zusätzliche Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind.

(7) – entfällt –

(8) – entfällt –

Abschnitt 2: Informationspflicht und Recht auf Auskunft zu personenbezogenen Daten

§ 13 Informationspflicht bei unmittelbarer Datenerhebung

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

a) den Namen und die Kontaktdaten der verantwortlichen Stelle;

b) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;

c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;

d) -- entfällt --

e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und

f) gegebenenfalls die Absicht der verantwortlichen Stelle, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß § 46 oder § 49 Absatz 1 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 die verantwortliche Stelle der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten auf Verlangen 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, auf Berichtigung, auf Löschung, auf Einschränkung der Verarbeitung, auf Datenübertragbarkeit sowie eines Widerspruchsrechts gegen die Verarbeitung;

c) wenn die Verarbeitung auf § 6 Absatz 1 Buchstabe a oder § 9 Absatz 2 Buchstabe 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 Aufsichtsbehörde;

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 möglichen Folgen die Nichtbereitstellung hätte.

f) – entfällt –

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

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

§ 14 Informationspflicht bei mittelbarer Datenerhebung

(1) $_1$Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, so teilt die verantwortliche Stelle der betroffenen Person, über die in § 13 Absatz 1 und 2 aufgeführten Informationen hinaus, die zu ihr gespeicherten Daten mit, auch soweit sie sich auf Herkunft oder empfangende Stellen beziehen. $_2$§ 13 Absatz 4 gilt entsprechend.

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

§ 15 Auskunftsrecht der betroffenen Person

(1) [1]Der betroffenen Person ist auf Antrag Auskunft zu erteilen über die zu ihr gespeicherten personenbezogenen Daten. [2]Die Auskunft muss folgende Informationen enthalten:

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;

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 die verantwortliche Stelle oder eines Widerspruchsrechts gegen diese Verarbeitung;

f) das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde;

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 § 22 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) – entfällt –

(3) Die Auskunft ist unentgeltlich.

(4) – entfällt –

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

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

Abschnitt 3: Berichtigung und Löschung

§ 16 | Recht auf Berichtigung

(1) [1]Die betroffene Person hat das Recht, von der verantwortlichen Stelle 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.

§ 17 | Recht auf Löschung („Recht auf Vergessenwerden“)

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

a) Die Kenntnis der personenbezogenen Daten ist für die verantwortliche Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich.

b) Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß § 6 Absatz 1 Buchstabe a oder § 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.

c) Die betroffene Person legt gemäß § 21 Absatz 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß § 21 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 erforderlich, der die verantwortliche Stelle unterliegt.

f) Personenbezogene Daten, die bei elektronischen Angeboten, die Minderjährigen direkt gemacht worden sind, erhoben wurden, sind auf Verlangen zu löschen.

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

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

a) zur Ausübung des Rechts auf freie Meinungsäußerung und Information;

b) zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem kirchlichen oder staatlichen Recht, dem die verantwortliche Stelle unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im kirchlichen Interesse liegt oder in Ausübung hoheitlicher Gewalt erfolgt, die der verantwortlichen Stelle übertragen wurde;

c) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß § 9 Absatz 2 Buchstaben h und i sowie § 9 Absatz 3;

d) für im kirchlichen 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, Ausübung oder Verteidigung von Rechtsansprüchen.

(4) Ist eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich, tritt an die Stelle des Rechts auf Löschung das Recht auf Einschränkung der Verarbeitung gemäß § 18.

§ 18 Recht auf Einschränkung der Verarbeitung

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

a) die Richtigkeit der personenbezogenen Daten von der betroffenen Person bestritten wird, und zwar für eine Dauer, die es der verantwortlichen Stelle ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen,

b) die Verarbeitung unrechtmäßig ist und die betroffene Person die Löschung der personenbezogenen Daten ablehnt und stattdessen die Einschränkung der Nutzung der personenbezogenen Daten verlangt;

c) die verantwortliche Stelle die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger benötigt, die betroffene Person sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt, oder

d) die betroffene Person Widerspruch gegen die Verarbeitung gemäß § 21 Absatz 1 eingelegt hat, solange noch nicht feststeht, ob die berechtigten Gründe der verantwortlichen Stelle gegenüber denen der betroffenen Person überwiegen.

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

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

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

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

[1]Die verantwortliche Stelle teilt allen Empfängern, denen personenbezogene Daten offengelegt wurden, jede Berichtigung oder Löschung der personenbezogenen Daten oder eine Einschränkung der Verarbeitung nach § 16, § 17 Absatz 1 und § 18 mit, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. [2]Die verantwortliche Stelle unterrichtet die betroffene Person über diese Empfänger, wenn die betroffene Person dies verlangt.

§ 20 Recht auf Datenübertragbarkeit

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

a) die Verarbeitung auf einer Einwilligung gemäß § 6 Absatz 1 Buchstabe a oder § 9 Absatz 2 Buchstabe a oder auf einem Vertrag gemäß § 6 Absatz 1 Buchstabe b 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 der verantwortlichen Stelle einer anderen verantwortlichen Stelle übermittelt werden, soweit dies technisch machbar ist.

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

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

Abschnitt 4: Widerspruchsrecht und automatisierte Entscheidungsfindung im Einzelfall

§ 21 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 Buchstabe f erfolgt, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmungen gestütztes Profiling. [2]Die verantwortliche Stelle verarbeitet die personenbezogenen Daten nicht mehr, es sei denn, es besteht ein zwingendes kirchliches Interesse oder die verantwortliche Stelle kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person

überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

(2) Werden personenbezogene Daten verarbeitet, um Direktwerbung 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) Im Zusammenhang mit der Nutzung von Diensten der Informationsgesellschaft kann die betroffene Person ungeachtet der Richtlinie 2002/58/EG ihr Widerspruchsrecht mittels automatisierter Verfahren ausüben, bei denen technische Spezifikationen verwendet werden.

(6) 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 gemäß § 89 a Absatz 1 erfolgt, Widerspruch einzulegen, es sei denn, die Verarbeitung ist zur Erfüllung einer im kirchlichen oder öffentlichen Interesse liegenden Aufgabe erforderlich.

§ 22 | 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 Vorschriften des kirchlichen oder staatlichen Rechts, denen die verantwortliche Stelle 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 Buchstaben a und c genannten Fällen trifft die verantwortliche Stelle angemessene Maßnahmen, 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 der verantwortlichen Stelle, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört.

(4) Entscheidungen nach Absatz 2 dürfen nicht auf besonderen Kategorien personenbezogener Daten nach § 9 Absatz 1 beruhen, sofern nicht § 9 Absatz 2 Buchstabe a oder g gilt und angemessene Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person getroffen wurden.

Abschnitt 5 – entfällt –

§ 23 – entfällt –

Kapitel 4 – Verantwortlicher und Auftragsverarbeiter

Abschnitt 1: Allgemeine Pflichten

§ 24 Verantwortung der für die Verarbeitung verantwortlichen Stelle

(1) [1]Die verantwortliche Stelle setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. [2]Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

(2) Sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht, müssen die Maßnahmen gemäß Absatz 1 die Anwendung geeigneter Datenschutzvorkehrungen durch die verantwortliche Stelle umfassen.

(3) Die Einhaltung der nach EU-Recht genehmigten Verhaltensregeln oder eines nach EU-Recht genehmigten Zertifizierungsverfahrens kann als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten der verantwortlichen Stelle nachzuweisen.

(4) Den bei der Datenverarbeitung tätigen Personen ist untersagt, personenbezogene Daten unbefugt zu verarbeiten (Datengeheimnis).

(5) [1]Die Beschäftigten, gemäß § 4 Punkt 28, der freikirchlichen Stellen sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis schriftlich zu verpflichten, soweit sie nicht aufgrund anderer kirchlicher Bestimmungen zur Verschwiegenheit verpflichtet wurden. [2]Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

§ 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

(1) [1]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 trifft die verantwortliche Stelle sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen – wie z. B. Pseudonymisierung –, die geeignet sind, die Datenschutzgrundsätze, wie etwa Datenminimierung, wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Datenschutzordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

(2) [1]Die verantwortliche Stelle trifft technische und organisatorische Maßnahmen, die geeignet sind, durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den

jeweiligen bestimmten Verarbeitungszweck erforderlich ist, zu verarbeiten. 2Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. 3Solche Maßnahmen müssen insbesondere geeignet sein, dass personenbezogene Daten nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

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

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

§ 26 | Gemeinsam für die Verarbeitung verantwortliche Stellen

(1) 1Legen zwei oder mehr verantwortliche Stellen gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam verantwortliche Stellen. 2Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Datenschutzordnung erfüllt, soweit die jeweiligen Aufgaben der verantwortlichen Stellen nicht durch Rechtsvorschriften festgelegt sind. 3In der Vereinbarung kann eine Anlaufstelle für die betroffenen Personen angegeben werden.

(2) 1Die Vereinbarung gemäß Absatz 1 muss die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam verantwortlichen Stellen gegenüber betroffenen Personen gebührend widerspiegeln. 2Das Wesentliche der Vereinbarung wird der betroffenen Person auf Verlangen zur Verfügung gestellt.

(3) Ungeachtet der Einzelheiten der Vereinbarung gemäß Absatz 1 kann die betroffene Person ihre Rechte im Rahmen dieser Datenschutzordnung bei und gegenüber jeder einzelnen der verantwortlichen Stellen geltend machen.

§ 27 | – entfällt –

§ 28 | Auftragsverarbeiter

(1) Erfolgt eine Verarbeitung im Auftrag einer kirchlichen Stelle, so arbeitet diese nur mit sorgfältig ausgewählten Auftragsverarbeitern, die hinreichend gewährleisten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Datenschutzordnung und anderer Vorschriften über den Datenschutz erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

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

(3) 1Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach kirchlichem oder staatlichem Recht, der bzw. das den

Auftragsverarbeiter in Bezug auf die beauftragende kirchliche Stelle bindet und in dem

1. Gegenstand und Dauer der Verarbeitung,
2. Art und Zweck der Verarbeitung,
3. die Art der personenbezogenen Daten, die Kategorien betroffener Personen und
4. die Pflichten und Rechte der beauftragenden kirchlichen Stelle

festgelegt sind.

[2]Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter

a) die personenbezogenen Daten nur auf dokumentierte Weisung der beauftragenden kirchlichen Stelle – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeitet, sofern er nicht durch das kirchliche oder staatliche Recht, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter der beauftragenden kirchlichen Stelle diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen 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 § 32 erforderlichen Maßnahmen ergreift;

d) die in den Absätzen 2 und 4 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;

e) angesichts der Art der Verarbeitung die beauftragende kirchliche Stelle nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, ihrer Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;

f) unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen die beauftragende kirchliche Stelle bei der Einhaltung der in den §§ 32 bis 36 genannten Pflichten unterstützt;

g) nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl der beauftragenden kirchlichen Stelle entweder löscht oder zurückgibt, sofern nicht nach kirchlichem oder staatlichem Recht eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht;

h) der beauftragenden kirchlichen Stelle alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Paragraphen niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen –, die von der beauftragenden Stelle oder einem anderen von dieser beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.

Mit Blick auf Buchstabe h informiert der Auftragsverarbeiter die beauftragende kirchliche Stelle unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen diese Datenschutzordnung oder gegen andere Datenschutzbestimmungen des kirchlichen oder staatlichen Rechts verstößt.

(4) [1]Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen der beauftragenden kirchlichen Stelle auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach kirchlichem oder staatlichem Recht dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen der beauftragenden kirchlichen Stelle und dem Auftragsverarbeiter gemäß Absatz 3 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 dieser Datenschutzordnung erfolgt. [2]Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber der beauftragenden kirchlichen Stelle für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

(5) Die Einhaltung von gemäß EU-Recht genehmigten Verhaltensregeln oder eines gemäß EU-Recht genehmigten Zertifizierungsverfahrens durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um hinreichende Garantien im Sinne der Absätze 1 und 4 nachzuweisen.

(6)–(8) – entfällt –

(9) Der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

(10) Unbeschadet der §§ 82 und 83 gilt ein Auftragsverarbeiter, der unter Verstoß gegen diese Datenschutzordnung die Zwecke und Mittel der Verarbeitung bestimmt, in Bezug auf diese Verarbeitung als verantwortliche Stelle.

(11) [1]Sofern die kirchlichen Datenschutzbestimmungen auf den Auftragsverarbeiter keine Anwendung finden, ist die kirchliche Stelle verpflichtet sicherzustellen, dass der Auftragsverarbeiter diese oder gleichwertige Bestimmungen beachtet. [2]In diesem Fall dürfen sich abweichend von Absatz 3 die Vertragsinhalte an Artikel 28 DSGVO orientieren. [3]Der Auftragsverarbeiter unterwirft sich der kirchlichen Datenschutzaufsicht.

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

(13) Das Recht der Heilsarmee in Deutschland kann bestimmen, dass vor der Beauftragung die Genehmigung einer übergeordneten kirchlichen Stelle einzuholen ist oder Mustervereinbarungen zu verwenden sind.

§ 29 Verarbeitung unter der Aufsicht der verantwortlichen Stelle oder des Auftragsverarbeiters

Der Auftragsverarbeiter und jede der verantwortlichen Stelle oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich auf Weisung der verantwortlichen Stelle verarbeiten, es sei denn, dass sie nach dem kirchlichen oder staatlichen Recht zur Verarbeitung verpflichtet sind.

§ 30 Verzeichnis von Verarbeitungstätigkeiten

(1) [1]Jede verantwortliche Stelle führt ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. [2]Dieses Verzeichnis enthält sämtliche folgenden Angaben:

a) den Namen und die Kontaktdaten der verantwortlichen Stelle und gegebenenfalls der gemeinsam mit ihm verantwortlichen Stelle sowie des Datenschutzbeauftragten sowie gegebenenfalls eines örtlichen Datenschutzassistenten oder örtlichen Datenschutzkoordinators;

b) die Zwecke der Verarbeitung;

c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;

d) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;

e) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, einschließlich der Angabe der dort getroffenen geeigneten Garantien;

f) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;

g) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 32 Absatz 1;

h) gegebenenfalls die Verwendung von Profiling.

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

a) den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jeder verantwortlichen Stelle, in deren Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;

b) die Kategorien von Verarbeitungen, die im Auftrag jeder verantwortlichen Stelle durchgeführt werden;

c) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation sowie der dort getroffenen geeigneten Garantien;

d) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 32 Absatz 1.

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

(4) Die verantwortliche Stelle oder der Auftragsverarbeiter sowie gegebenenfalls der Vertreter des Auftragsverarbeiters stellen der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.

(5) [1]Die in den Absätzen 1 und 2 genannten Pflichten gelten nicht für verantwortliche Stellen, die weniger als 40 Beschäftigte haben, es sei denn, die von ihnen vorgenommene Verarbeitung birgt

ein Risiko für die Rechte und Freiheiten der betroffenen Personen, die Verarbeitung erfolgt nicht nur gelegentlich oder es erfolgt eine Verarbeitung besonderer Datenkategorien gemäß § 9 Absatz 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des § 10. $_2$Freikirchliche Stellen, die weniger als 40 Beschäftigte haben, erstellen Verzeichnisse nach Absatz 1 und 2 nur hinsichtlich der Verfahren, die die Verarbeitung besonderer Kategorien personenbezogener Daten einschließen.

§ 31 Zusammenarbeit mit der Aufsichtsbehörde

Die verantwortliche Stelle und der Auftragsverarbeiter und gegebenenfalls deren Vertreter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

Abschnitt 2: Sicherheit personenbezogener Daten

§ 32 Sicherheit der Verarbeitung

(1) 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 des Risikos für die Rechte und Freiheiten natürlicher Personen treffen die verantwortliche Stelle und der kirchliche Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung, Anonymisierung und 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 berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

(3) Die Einhaltung von nach EU-Recht genehmigten Verhaltensregeln oder eines nach EU-Recht genehmigten Zertifizierungsverfahrens kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 genannten Anforderungen nachzuweisen.

(4) Die verantwortliche Stelle und der kirchliche Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung der verantwortlichen Stelle verarbeiten, es sei denn, sie sind nach dem kirchlichen oder staatlichen Recht zur Verarbeitung verpflichtet.

§ 33 Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

(1) [1]Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet die verantwortliche Stelle unverzüglich und möglichst binnen 72 Stunden, nachdem ihr die Verletzung bekannt wurde, diese der gemäß § 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. [2]Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

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

(3) Die Meldung gemäß Absatz 1 enthält zumindest 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 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 der verantwortlichen Stelle ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

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

(5) [1]Die verantwortliche Stelle dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen. [2]Diese Dokumentation ermöglicht der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Paragraphen.

§ 34 Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

(1) Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt die verantwortliche Stelle 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 Buchstaben b, c und d genannten Informationen und Empfehlungen.

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

a) die verantwortliche Stelle geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden, 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) die verantwortliche Stelle durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 aller Wahrscheinlichkeit nach nicht mehr besteht,

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

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

Abschnitt 3: Datenschutz-Folgenabschätzung und vorherige Konsultation

§ 35 Datenschutz-Folgenabschätzung

(1) [1]Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt die verantwortliche Stelle vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. [2]Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

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

(3) 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 gemäß § 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche

Verurteilungen und Straftaten gemäß § 10 oder

c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

(4) Die Aufsichtsbehörde soll eine Liste der Verarbeitungsvorgänge führen, für die gemäß Absatz 1 eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese.

(5) Die Aufsichtsbehörde kann des Weiteren eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist.

(6) – entfällt –

(7) Die Folgenabschätzung enthält zumindest Folgendes:

a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von der verantwortlichen Stelle 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 die datenschutzrechtlichen Regelungen eingehalten werden.

(8) Die Einhaltung von nach EU-Recht genehmigten Verhaltensregeln durch die zuständige verantwortliche Stelle oder die zuständigen Auftragsverarbeiter ist bei der Beurteilung der Auswirkungen der von diesen durchgeführten Verarbeitungsvorgänge, insbesondere für die Zwecke einer Datenschutz-Folgenabschätzung, gebührend zu berücksichtigen.

(9) – entfällt –

(10) Falls die Verarbeitung gemäß § 6 Absatz 1 Buchstabe c auf einer Rechtsgrundlage im kirchlichen, staatlichen oder europäischen Recht, dem die verantwortliche Stelle unterliegt, beruht und falls diese Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge regeln und bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte, gelten die Absätze 1 bis 7 nicht.

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

§ 36 | Vorherige Konsultation

(1) Die verantwortliche Stelle konsultiert vor der Verarbeitung die Aufsichtsbehörde, wenn aus einer Datenschutz-Folgenabschätzung gemäß § 35 hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern die verantwortliche Stelle keine Maßnahmen zur Eindämmung des

Risikos trifft.

(2)–(4) – entfallen –

(5) Ungeachtet des Absatzes 1 können verantwortliche Stellen durch kirchliches oder staatliches Recht verpflichtet werden, bei der Verarbeitung zur Erfüllung einer im kirchlichen oder öffentlichen Interesse liegenden Aufgabe, einschließlich der Verarbeitung zu Zwecken der sozialen Sicherheit und der öffentlichen Gesundheit, die Aufsichtsbehörde zu konsultieren und deren vorherige Genehmigung einzuholen.

Abschnitt 4: Datenschutzbeauftragter

§ 37 – abweichend –

– abweichende Regelung, siehe § 37 a & § 37 b

§ 37 a Benennung eines Datenschutzbeauftragten

(1) Die Leitung der Heilsarmee in Deutschland ernennt einen gemeinsamen Datenschutzbeauftragten für die freikirchlichen Stellen dieser Datenschutzordnung als gemeinsamen Organisations-/Konzerndatenschutzbeauftragten.

(2) Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in § 39 genannten Aufgaben.

(3) Der Datenschutzbeauftragte kann

a) Beschäftigter der Heilsarmee in Deutschland oder einer freikirchlichen Stelle sein oder

b) Offizier der Heilsarmee in Deutschland sein oder

c) seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.

(4) Die Amtszeit des Datenschutzbeauftragten wird beendet durch

a) Erreichen der Regelaltersgrenze oder Pensionierung,

b) Widerruf der Ernennung durch das Kabinett der Heilsarmee in Deutschland,

c) Niederlegung des Amtes durch den Datenschutzbeauftragten mit einer Frist von sechs Monaten zum Halbjahresende,

d) Ablauf der bei der Ernennung vereinbarten Dauer,

e) Ablauf oder Kündigung des Dienstleistungsvertrages entsprechend der vertraglich geregelten Fristen.

(5) Der Datenschutzbeauftragte kann Mitglied des Kabinetts der Heilsarmee in Deutschland sein, jedoch darf er nicht der territorialen Leitung angehören.

(6) Die verantwortliche Stelle veröffentlicht die Kontaktdaten des Datenschutzbeauftragten und teilt diese Daten der Aufsichtsbehörde mit.

§ 37 b Örtlicher Datenschutzassistent/Datenschutzkoordinator

(1) Organisationseinheiten können einen örtlichen Datenschutzassistenten (DAS) oder Datenschutzkoordinator (DSK), nach Genehmigung durch den Direktor Personal der Heilsarmee in Deutschland, benennen.

(2) Die Benennung soll für mindestens drei Jahre erfolgen. Die erneute Benennung ist zulässig.

(3) Zum örtlichen Datenschutzassistenten/-koordinator dürfen nur Personen bestellt werden, die das zur Erfüllung ihrer Aufgaben erforderliche Fachwissen und die notwendige Zuverlässigkeit besitzen.

a) Der Datenschutzassistent
muss über ein fundiertes Basiswissen des Datenschutzes verfügen, welches es ihm ermöglicht, einfache örtliche Anfragen zu bewerten und den Datenschutzbeauftragten, vor Ort, in seiner Tätigkeit zu unterstützen.

b) Der Datenschutzkoordinator
verfügt über ein erweitertes Wissen des Datenschutzes. Dies ermöglicht ihm, auch komplexere örtliche Anfragen und Vorgänge zu bewerten. Er unterstützt, vor Ort, den Datenschutzbeauftragten in seiner Tätigkeit.

(4) Zum örtlichen Datenschutzassistenten/-koordinator sollen diejenigen nicht benannt werden, die mit der Leitung der Datenverarbeitung beauftragt sind oder denen die Leitung einer Organisationseinheit obliegt.

(5) Die Ernennung des örtlichen Datenschutzassistenten/-koordinators erfolgt schriftlich und ist dem Datenschutzbeauftragten anzuzeigen.

(6) Ist der örtliche Datenschutzassistent/-koordinator nicht Beschäftigter einer Organisationseinheit der Heilsarmee in Deutschland, sind seine Leistungen vertraglich zu regeln.

(7) Die Leitung der Organisationseinheit, als örtlich verantwortliche Stelle, stellt sicher, dass der örtliche Datenschutzassistent/-koordinator frühzeitig über Projekte für Verfahren, bei denen es zur Verarbeitung von personenbezogenen Daten kommen wird, informiert wird.

(8) Betroffene Personen und Beschäftigte können sich unmittelbar an den örtlichen Datenschutzassistenten/-koordinator wenden.

(9) Der örtliche Datenschutzassistent/-koordinator ist in seiner Tätigkeit der jeweiligen Leitung der Organisationseinheit direkt zu unterstellen.

(10) Im Rahmen seiner Aufgaben gem. Absatz 12 ist der örtliche Datenschutzassistent/ -koordinator an Vorgaben des Datenschutzbeauftragten gebunden, ansonsten ist er in Ausübung dieser Aufgaben weisungsfrei. Er darf wegen seiner Tätigkeit nicht benachteiligt werden.

(11) Zur Erlangung und zur Aufrechterhaltung des erforderlichen Fachwissens hat die örtliche verantwortliche Stelle/Leitung der Organisationseinheit die Teilnahme an entsprechenden

Fortbildungsveranstaltungen zu ermöglichen und die Kosten zu tragen.

(12) Für die Organisationseinheit, die den örtlichen Datenschutzkoordinator/-assistenten benannt hat, übernimmt der Datenschutzkoordinator/-assistent folgende Aufgaben:

a) Ansprechpartner in der Organisationseinheit bei einfachen datenschutzrelevanten Fragestellungen,

b) Umsetzung von Standardprozessen (z. B. Verpflichtung auf das Datengeheimnis, Auftragsverarbeitungsverträge, Werbewiderspruch),

c) Aufrechterhaltung eines gewissen Datenschutzniveaus in der Organisationseinheit (z. B. durch Mitarbeitersensibilisierung),

d) Unterstützung des Datenschutzbeauftragten,

e) Einholen von relevanten Informationen,

f) bei Bedarf Verwalten, Aktualisieren, Pflegen oder Vorbereiten von Datenschutzdokumenten,

g) regelmäßige Berichte an den Datenschutzbeauftragten.

§ 38 Stellung des Datenschutzbeauftragten

(1) Die verantwortliche Stelle stellt sicher, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.

(2) Die verantwortliche Stelle unterstützt den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben gemäß § 39, indem sie die für die Erfüllung dieser Aufgaben erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur Erhaltung seines Fachwissens erforderlichen Ressourcen zur Verfügung stellt.

(3) [1]Die verantwortliche Stelle stellt sicher, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält. [2]Der Datenschutzbeauftragte darf von der Leitung oder dem Kabinett der Heilsarmee in Deutschland wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. [3]Der Datenschutzbeauftragte berichtet unmittelbar der höchsten Managementebene der verantwortlichen Stelle.

(4) Betroffene Personen können den Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß dieser Verordnung im Zusammenhang stehenden Fragen zu Rate ziehen.

(5) Der Datenschutzbeauftragte ist nach dem kirchlichen und staatlichen Recht bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung oder der Vertraulichkeit gebunden.

(6) [1]Der Datenschutzbeauftragte kann andere Aufgaben und Pflichten wahrnehmen. [2]Die verantwortliche Stelle stellt sicher, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.

(7) [1]Eine Kündigung des Datenschutzbeauftragten im Arbeits- oder Dienstverhältnis ist während der Amtszeit nur zulässig, soweit Tatsachen vorliegen, die zu einer Kündigung aus wichtigem Grund

berechtigen. [2]Dies gilt für den Zeitraum von einem Jahr nach Beendigung des Amtes entsprechend.

§ 39 Aufgaben des Datenschutzbeauftragten

(1) Dem Datenschutzbeauftragten obliegen folgende Aufgaben:

a) Unterrichtung und Beratung der verantwortlichen Stelle und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Datenschutzordnung sowie nach sonstigen Datenschutzvorschriften;

b) Überwachung der Einhaltung dieser Datenschutzordnung, anderer Datenschutzvorschriften staatlichen Rechts sowie der Strategien der verantwortlichen Stelle für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;

c) Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß § 35;

d) Zusammenarbeit mit der Aufsichtsbehörde;

e) Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß § 36, und gegebenenfalls Beratung zu allen sonstigen Fragen.

(2) Der Datenschutzbeauftragte trägt bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt.

Abschnitt 5: – entfällt –

§ 40 – entfällt –
§ 41 – entfällt –
§ 42 – entfällt –
§ 43 – entfällt –

Kapitel 5 – Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen

§ 44 Allgemeine Grundsätze der Datenübermittlung

[1]Jedwede Übermittlung personenbezogener Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, ist nur zulässig, wenn die verantwortliche Stelle und der Auftragsverarbeiter die in diesem Kapitel niedergelegten Bedingungen einhalten und auch die sonstigen Bestimmungen dieser Datenschutzordnung eingehalten werden; dies gilt auch für die etwaige Weiterübermittlung personenbezogener Daten durch das betreffende Drittland oder die betreffende internationale Organisation an ein anderes Drittland oder eine andere internationale Organisation. [2]Alle

Bestimmungen dieses Kapitels sind anzuwenden, um sicherzustellen, dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird.

§ 45 Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses

(1) [1]Eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation darf vorgenommen werden, wenn die EU-Kommission beschlossen hat, dass das betreffende Drittland, ein Gebiet oder einer oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet, gem. Artikel 45 Absatz 2 und Absatz 5 DSGVO. [2]Eine solche Datenübermittlung bedarf keiner besonderen Genehmigung.

(2)–(9) – entfallen –

§ 46 Datenübermittlung vorbehaltlich geeigneter Garantien

Falls kein Beschluss nach § 45 vorliegt, darf eine verantwortliche Stelle oder ein Auftragsverarbeiter personenbezogene Daten an ein Drittland oder eine internationale Organisation nur übermitteln, sofern Standarddatenschutzklauseln als geeignete Garantien verwendet werden, die von der EU-Kommission gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 DSGVO erlassen oder genehmigt worden sind.

§ 47 – entfällt –

§ 48 – entfällt –

§ 49 Ausnahmen für bestimmte Fälle

(1) Falls weder ein Angemessenheitsbeschluss nach § 45 Absatz 1 vorliegt noch geeignete Garantien nach § 46 bestehen, ist eine Übermittlung oder eine Reihe von Übermittlungen personenbezogener Daten an ein Drittland oder eine internationale Organisation nur unter einer der folgenden Bedingungen zulässig:

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

b) die Übermittlung ist für die Erfüllung eines Vertrages oder Rechtsverhältnisses zwischen der betroffenen Person und der verantwortlichen Stelle oder zur Durchführung von vertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich;

c) die Übermittlung ist zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person von der verantwortlichen Stelle mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrages erforderlich;

d) die Übermittlung ist aus wichtigen Gründen des 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;

g) die Übermittlung erfolgt aus einem Register, das gemäß dem Recht der Union oder der Mitgliedstaaten zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, aber nur soweit die im Recht der Union oder der Mitgliedstaaten festgelegten Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind;

h) die Übermittlung ist aus wichtigen Gründen des kirchlichen Interesses notwendig.

(2) $_1$Datenübermittlungen gemäß Absatz 1 Buchstabe g dürfen nicht die Gesamtheit oder ganze Kategorien der im Register enthaltenen personenbezogenen Daten umfassen. $_2$Wenn das Register der Einsichtnahme durch Personen mit berechtigtem Interesse dient, darf die Übermittlung nur auf Anfrage dieser Personen oder nur dann erfolgen, wenn diese Personen die Adressaten der Übermittlung sind.

(3) – entfällt –

(4) Das öffentliche Interesse im Sinne des Absatzes 1 Buchstabe d ist im Unionsrecht oder im staatlichen Recht, dem die verantwortliche Stelle unterliegt, anerkannt.

(5) – entfällt –

(6) Die verantwortliche Stelle oder der Auftragsverarbeiter erfasst die von ihm vorgenommene Beurteilung sowie die angemessenen Garantien im Sinne des Absatzes 1 der vorliegenden Regelung in der Dokumentation gemäß § 30.

§ 50 | – entfällt –

Kapitel 6 – Unabhängige Aufsichtsbehörden

Abschnitt 1: Unabhängigkeit

§ 51 | Aufsichtsbehörde

(1) Über die Einhaltung dieser Datenschutzordnung im Bereich der Heilsarmee in Deutschland und den freikirchlichen Stellen, gem. § 3 Absatz 3 wacht eine unabhängige Aufsichtsbehörde für den Datenschutz (Aufsichtsbehörde).

(2) Die Heilsarmee in Deutschland errichtet die Aufsichtsbehörde für den Geltungsbereich dieser Datenschutzordnung gem. § 54.

(3) Die Aufsichtsbehörde kann gemeinschaftlich mit anderen Religionsgemeinschaften, z. B. im Rahmen der Vereinigung evangelischer Freikirchen, errichtet werden.

(4) Die Aufsichtsbehörde kann auch per Aufgabenübertragung an eine bereits bestehende, unabhängige Aufsichtsbehörde errichtet werden.

§ 52 Unabhängigkeit

(1) Die Aufsichtsbehörde handelt bei der Erfüllung ihrer Aufgaben und bei der Ausübung ihrer Befugnisse gemäß dieser Datenschutzordnung völlig unabhängig.

(2) Das Mitglied oder die Mitglieder der Aufsichtsbehörde unterliegen bei der Erfüllung ihrer Aufgaben und der Ausübung ihrer Befugnisse gemäß dieser Datenschutzordnung weder direkter noch indirekter Beeinflussung von außen und ersuchen weder um Weisung noch nehmen sie Weisungen entgegen.

(3) Das Mitglied oder die Mitglieder der Aufsichtsbehörde sehen von allen mit den Aufgaben ihres Amtes nicht zu vereinbarenden Handlungen ab und üben während ihrer Amtszeit keine andere mit ihrem Amt nicht zu vereinbarende entgeltliche oder unentgeltliche Tätigkeit aus.

(4)–(5) – entfallen –

(6) Die Aufsichtsbehörde unterliegt der Rechnungsprüfung sofern hierdurch die Unabhängigkeit nicht beeinträchtigt wird.

§ 53 Allgemeine Bedingungen für die Mitglieder der Aufsichtsbehörde

(1) Die Zusammensetzung der Aufsichtsbehörde wird mit der Ordnung zur Errichtung geregelt, gem. § 54.

(2) Jedes Mitglied muss über die für die Erfüllung seiner Aufgaben und die Ausübung seiner Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten verfügen.

(3) Das Amt eines Mitglieds endet mit Ablauf der Amtszeit, mit seinem Rücktritt oder verpflichtenden Versetzung in den Ruhestand gemäß dem kirchlichen oder staatlichen Recht.

(4) Ein Mitglied wird seines Amtes nur enthoben, wenn es eine schwere Verfehlung begangen hat oder die Voraussetzungen für die Wahrnehmung seiner Aufgaben nicht mehr erfüllt.

§ 54 Errichtung der Aufsichtsbehörde

(1) Die Heilsarmee in Deutschland bestimmt per Rechtsvorschrift die Errichtung der Aufsichtsbehörde und regelt Folgendes:

a) die Errichtung der Aufsichtsbehörde,

b) die erforderlichen Qualifikationen und sonstigen Voraussetzungen für die Ernennung zum Mitglied der Aufsichtsbehörde,

c) die Vorschriften und Verfahren für die Ernennung des Mitglieds oder der Mitglieder der Aufsichtsbehörde,

d) die Amtszeit, von mindestens vier Jahren, des Mitglieds oder der Mitglieder der Aufsichtsbehörde,

e) die Frage, ob und – wenn ja – wie oft das Mitglied oder die Mitglieder der Aufsichtsbehörde wiederernannt werden können,

f) die Bedingungen im Hinblick auf die Pflichten des Mitglieds oder der Mitglieder und der Bediensteten der Aufsichtsbehörde, die Verbote von Handlungen, beruflichen Tätigkeiten und Vergütungen während und nach der Amtszeit, die mit diesen Pflichten unvereinbar sind, und die Regeln für die Beendigung des Beschäftigungsverhältnisses.

(2) [1]Das Mitglied oder die Mitglieder und die Bediensteten jeder Aufsichtsbehörde sind gemäß dem kirchlichen und staatlichen Recht sowohl während ihrer Amts- beziehungsweise Dienstzeit als auch nach deren Beendigung verpflichtet, über alle vertraulichen Informationen, die ihnen bei der Wahrnehmung ihrer Aufgaben oder der Ausübung ihrer Befugnisse bekannt geworden sind, Verschwiegenheit zu wahren. [2]Während dieser Amts- beziehungsweise Dienstzeit gilt diese Verschwiegenheitspflicht insbesondere für die von natürlichen Personen gemeldeten Verstößen gegen diese Datenschutzordnung.

(3) [1]In den Fällen nach § 51 Absatz 3 oder § 51 Absatz 4 bedarf es außer der Rechtsvorschrift der Heilsarmee zur Errichtung der Aufsichtsbehörde eines Vertrages oder eines anderen Rechtsinstruments des kirchlichen oder staatlichen Rechts zur Regelung der Grundlagen für die Tätigkeit der Aufsichtsbehörde im Geltungsbereich dieser Datenschutzordnung. [2]In dem Vertrag oder anderen Rechtsinstrument sind insbesondere festzuhalten:

a) die Grundlagen zur Gewährleistung der Unabhängigkeit der Aufsichtsbehörde, im Sinne des § 52 dieser Datenschutzordnung;

b) bei in diesen Fällen zulässiger Abweichung von den Anforderungen des § 53 dieser Datenschutzordnung, dass die effektive Fähigkeit zur Erfüllung der aufsichtsbehördlichen Aufgaben, im Sinne des § 53, gewährleistet bleibt;

c) die Regelungen entsprechend den Anforderungen des § 54 Absatz 1 Buchstaben b–f, sofern die Rechtsvorschrift zur Errichtung der Aufsichtsbehörde die inhaltliche Regelung dieser Anforderungen auf den Vertrag oder das andere Rechtsinstrument überträgt;

d) die Gewährleistung der Einhaltung der Verschwiegenheitsverpflichtung gemäß § 54 Absatz 2.

e) Der Vertrag oder das andere Rechtsinstrument ist schriftlich abzufassen.

Abschnitt 2: Zuständigkeit, Aufgaben und Befugnisse

§ 55 | Zuständigkeit

(1) Die Aufsichtsbehörde ist für die Erfüllung der Aufgaben und die Ausübung der Befugnisse, die ihr mit dieser Datenschutzordnung oder über sonstige kirchliche Rechtsvorschriften übertragen wurden, im Geltungsbereich dieser Datenschutzordnung zuständig.

(2) – entfällt –

(3) Die Aufsichtsbehörde ist nicht zuständig für die Aufsicht über die von kirchlichen Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen.

§ 56 – entfällt –

§ 57 Aufgaben

(1) Unbeschadet anderer in dieser Datenschutzordnung dargelegter Aufgaben muss die Aufsichtsbehörde in ihrem Zuständigkeitsbereich

a) die Anwendung dieser Datenschutzordnung überwachen und durchsetzen;

b) die kirchliche 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 Kinder;

c) im Einklang mit dem kirchlichen Recht und auf Anregung der kirchenleitenden Organe oder von Amts wegen Gutachten und Stellungnahmen zu legislativen, administrativen oder Vorhaben der Rechtssetzung, die sich auf den Schutz von personenbezogenen Daten auswirken, abgeben;

d) die verantwortliche Stelle und die Auftragsverarbeiter für die ihnen aus dieser Verordnung entstehenden Pflichten sensibilisieren;

e) auf Anfrage jeder betroffenen Person Informationen über die Ausübung ihrer Rechte aufgrund dieser Datenschutzordnung zur Verfügung stellen und gegebenenfalls zu diesem Zweck mit anderen Aufsichtsbehörden zusammenarbeiten;

f) sich mit Beschwerden einer betroffenen Person oder Beschwerden einer Stelle oder einer Organisation 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, insbesondere, wenn eine weitere Untersuchung oder Koordinierung mit einer anderen Aufsichtsbehörde notwendig ist;

g) mit anderen Aufsichtsbehörden zusammenarbeiten, auch durch Informationsaustausch, und ihnen Amtshilfe leisten, um die einheitliche Anwendung und Durchsetzung dieser Datenschutzordnung zu gewährleisten;

h) Untersuchungen über die Anwendung dieser Datenschutzordnung durchführen, auch auf der Grundlage von Informationen einer anderen Aufsichtsbehörde oder kirchlichen Behörde;

i) maßgebliche Entwicklungen verfolgen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie und der Geschäftspraktiken;

j) – entfällt –

k) eine Liste der Verarbeitungsarten erstellen und führen, für die gemäß § 35 Absatz 4 eine Datenschutz-Folgenabschätzung durchzuführen ist;

l) Beratung in Bezug auf die in § 36 genannten Verarbeitungsvorgänge leisten;

m)–t) – entfallen –

u) interne Verzeichnisse über Verstöße gegen diese Verordnung und gemäß § 58 Absatz 2 ergriffene Maßnahmen führen und

v) jede sonstige Aufgabe im Zusammenhang mit dem Schutz personenbezogener Daten erfüllen.

(2) – entfällt –

(3) Die Erfüllung der Aufgaben der Aufsichtsbehörde ist für die betroffene Person und gegebenenfalls für den Datenschutzbeauftragten unentgeltlich.

(4) [1]Bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen kann die Aufsichtsbehörde eine angemessene Gebühr auf der Grundlage der Verwaltungskosten verlangen oder sich weigern, aufgrund des Antrags tätig zu werden. [2]In diesem Fall trägt die Aufsichtsbehörde die Beweislast für den offenkundig unbegründeten oder exzessiven Charakter des Antrags.

(5) [1]Die Aufsichtsbehörde kann Aufgaben der Personalverwaltung und Personalwirtschaft auf andere freikirchliche Stellen übertragen. [2]Diesen kirchlichen Stellen dürfen personenbezogene Daten der Beschäftigten offengelegt werden, soweit deren Kenntnis zur Erfüllung der übertragenen Aufgaben erforderlich ist.

(6) Die Aufgaben nach Absatz 1 Buchstaben b bis f und k können bei gemeinsamen Aufsichtsbehörden, gem. § 51 Absatz 3 oder bei Aufgabenübertragung gem. § 51 Absatz 4 abweichend festgelegt werden.

(7) Der Prüfung durch die Aufsichtsbehörde unterliegen nicht:

a) Aufzeichnungen gemäß § 91 a Satz 1;

b) personenbezogene Daten, die dem Post- und Fernmeldegeheimnis oder dem Arztgeheimnis unterliegen, sowie personenbezogene Daten in Personalakten, wenn die betroffene Person der Prüfung der auf sie bezogenen Daten im Einzelfall zulässigerweise gegenüber dem Datenschutzbeauftragten widerspricht.

§ 58 | Befugnisse

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

a) die verantwortliche Stelle, den Auftragsverarbeiter und gegebenenfalls den Vertreter der verantwortlichen Stelle oder des Auftragsverarbeiters anzuweisen, alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind,

b) Untersuchungen in Form von Datenschutzüberprüfungen durchzuführen,

c) – entfällt – ,

d) die verantwortliche Stelle oder den Auftragsverarbeiter auf einen vermeintlichen Verstoß gegen diese Datenschutzordnung hinzuweisen,

e) von der verantwortlichen Stelle und dem Auftragsverarbeiter Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind, zu erhalten,

f) jederzeit Zutritt zu allen Diensträumen, einschließlich aller Verarbeitungsanlagen und Verarbeitungsgeräte der verantwortlichen Stelle und des Auftragsverarbeiters zu erhalten, um Untersuchungen und Überprüfungen vornehmen zu können.

(2) Jede Aufsichtsbehörde verfügt über sämtliche folgenden Abhilfebefugnisse, die es ihr gestatten,

a) die verantwortliche Stelle oder einen Auftragsverarbeiter zu warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen diese Datenschutzordnung verstoßen,

b) die verantwortliche Stelle oder einen Auftragsverarbeiter zu verwarnen, wenn er mit Verarbeitungsvorgängen gegen diese Datenschutzordnung verstoßen hat,

c) die verantwortliche Stelle oder den Auftragsverarbeiter anzuweisen, den Anträgen der betroffenen Person auf Ausübung der ihr nach dieser Datenschutzordnung zustehenden Rechte zu entsprechen,

d) die verantwortliche Stelle oder den Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit dieser Datenschutzordnung zu bringen,

e) die verantwortliche Stelle anzuweisen, die von einer Verletzung des Schutzes personenbezogener Daten betroffenen Personen 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 §§ 16, 17 und 18 und die Unterrichtung der Empfänger, an die diese personenbezogenen Daten gemäß § 17 Absatz 2 und § 19 offengelegt wurden, über solche Maßnahmen anzuordnen,

h) – entfällt – ,

i) eine Geldbuße gemäß § 83 zu verhängen, zusätzlich zu oder anstelle von in diesem Absatz genannten Maßnahmen, je nach den Umständen des Einzelfalls,

j) die Aussetzung der Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation anzuordnen.

(3) Die Aufsichtsbehörde verfügt über sämtliche folgenden Genehmigungsbefugnisse und beratenden Befugnisse, die es ihr gestatten,

a) gemäß dem Verfahren der vorherigen Konsultation nach § 36 die verantwortliche Stelle zu beraten,

b) zu allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten stehen, von sich aus oder auf Anfrage Stellungnahmen an staatliche Organe, die Bundesregierung oder Landesregierungen oder im Einklang mit dem kirchlichen und staatlichen Recht an sonstige Einrichtungen und Stellen sowie an die kirchliche Öffentlichkeit zu richten,

c) die Verarbeitung gemäß § 36 Absatz 5 zu genehmigen, falls im kirchlichen oder staatlichen Recht eine derartige vorherige Genehmigung verlangt wird,

d)–j) – entfallen – .

(4)–(6) – entfallen – .

(7) [1]Hält die Aufsichtsbehörde einen Angemessenheitsbeschluss der Europäischen Kommission nach § 45 Absatz 1, einen Beschluss über die Anerkennung von Standardschutzklauseln nach § 46 oder über die Allgemeingültigkeit von genehmigten Verhaltensregeln, auf dessen Gültigkeit es für eine Entscheidung der Aufsichtsbehörde ankommt, für rechtswidrig, so kann sie ihr Verfahren aussetzen und einen Antrag auf gerichtliche Entscheidung stellen. [2]Soweit nicht kirchliche Besonderheiten entgegenstehen, finden die Regelungen des § 21 BDSG (Bundesdatenschutzgesetz vom 30.06.2017) entsprechend Anwendung.

§ 59 | Tätigkeitsbericht

[1]Die Aufsichtsbehörde erstellt mindestens alle zwei Jahre einen Tätigkeitsbericht, der eine Liste der Arten der gemeldeten Verstöße und der Arten der getroffenen Maßnahmen enthalten kann. [2]Sie übermittelt den Bericht den jeweiligen kirchenleitenden Organen oder den jeweiligen Leitungsorganen und veröffentlicht ihn. [3]Auf dieser Grundlage kann sie den leitenden Organen berichten.

Kapitel 7 – entfällt –

§ 60 – entfällt –
§ 61 – entfällt –
§ 62 – entfällt –
§ 63 – entfällt –
§ 64 – entfällt –
§ 65 – entfällt –
§ 66 – entfällt –
§ 67 – entfällt –
§ 68 – entfällt –
§ 69 – entfällt –
§ 70 – entfällt –
§ 71 – entfällt –
§ 72 – entfällt –
§ 73 – entfällt –
§ 74 – entfällt –
§ 75 – entfällt –
§ 76 – entfällt –

Kapitel 8 – Rechtsbehelfe, Haftung und Sanktionen

§ 77 Recht auf Beschwerde bei einer Aufsichtsbehörde

(1) Jede betroffene Person hat unbeschadet eines anderweitigen Rechtsbehelfs das Recht auf Beschwerde bei der Aufsichtsbehörde, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen diese Datenschutzordnung verstößt.

(2) Die Aufsichtsbehörde unterrichtet den Beschwerdeführer über den Stand und die Ergebnisse der Beschwerde einschließlich der Möglichkeit eines gerichtlichen Rechtsschutzes nach § 78 a.

(3) $_1$Niemand darf wegen der Mitteilung von Tatsachen an die Aufsichtsbehörde, die geeignet sind, den Verdacht aufkommen zu lassen, diese Datenschutzordnung oder eine andere Rechtsvorschrift über den Datenschutz sei verletzt worden, gemaßregelt oder benachteiligt werden. $_2$Beschäftigte gem. § 4 Punkt 28 müssen für Mitteilungen an die Aufsichtsbehörde nicht den Dienstweg einhalten.

§ 78 – abweichend –

– abweichende Regelung, siehe § 78 a

§ 78 a Rechtsweg

(1) Der Rechtsweg aus Streitigkeiten nach dieser Datenschutzordnung ist zu der Schlichtungsstelle für den Datenschutz der Heilsarmee in Deutschland eröffnet

a) für alle Rechtsbehelfe (Klagen) gegen Entscheidungen der Aufsichtsbehörde,

b) für Klagen in Fällen, in denen sich die Aufsichtsbehörde nicht mit einer Beschwerde gemäß § 77 dieser Datenschutzordnung befasst oder die betroffene Person nicht innerhalb von drei Monaten über den Stand oder das Ergebnis der erhobenen Beschwerde in Kenntnis gesetzt hat,

c) für Klagen betroffener Personen gegen kirchliche Stellen und Auftragsverarbeiter wegen einer Verletzung ihrer Rechte aus dieser Datenschutzordnung,

d) für Klagen der Aufsichtsbehörde gegen kirchliche Stellen und Auftragsverarbeiter, soweit dies zur Durchsetzung ihrer Befugnisse erforderlich ist.

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

§ 79 – entfällt –
§ 80 – entfällt –
§ 81 – entfällt –

§ 82 Haftung und Recht auf Schadenersatz

(1) [1]Jede Person, der wegen eines Verstoßes gegen diese Datenschutzordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen die verantwortliche Stelle oder gegen den Auftragsverarbeiter. [2]Wegen eines Schadens, der nicht Vermögensschaden ist, kann die betroffene Person eine angemessene Entschädigung in Geld verlangen.

(2) [1]Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Datenschutzordnung entsprechende Verarbeitung verursacht wurde. [2]Ein Auftragsverarbeiter haftet für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Datenschutzordnung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen der für die Datenverarbeitung verantwortlichen Stelle oder gegen diese Anweisungen gehandelt hat.

(3) Die verantwortliche Stelle wird von der Haftung gemäß Absatz 2 befreit, wenn sie nachweist, dass sie für den Umstand, durch den der Schaden eingetreten ist, nicht verantwortlich ist.

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

(5) Hat eine verantwortliche Stelle oder ein Auftragsverarbeiter gemäß Absatz 4 vollständigen Schadenersatz für den erlittenen Schaden gezahlt, so ist diese verantwortliche Stelle oder der Auftragsverarbeiter berechtigt, von den übrigen an derselben Verarbeitung beteiligten für die Datenverarbeitung verantwortlichen Stellen oder Auftragsverarbeitern den Teil des

Schadenersatzes zurückzufordern, der unter den in Absatz 2 festgelegten Bedingungen ihrem Anteil an der Verantwortung für den Schaden entspricht.

(6) – entfällt –

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

(8) Auf das Mitverschulden der betroffenen Person ist § 254 des Bürgerlichen Gesetzbuches anzuwenden.

(9) Auf die Verjährung sind die Verjährungsfristen für unerlaubte Handlungen des Bürgerlichen Gesetzbuches entsprechend anzuwenden.

§ 83 | Allgemeine Bedingungen für die Verhängung von Geldbußen

(1) [1]Die Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Paragraphen für Verstöße gegen diese Datenschutzordnung gemäß den Absätzen 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.
[2]Gegen verantwortliche Stellen sind Geldbußen nur zu verhängen, soweit sie als Unternehmen im Sinne des § 4 Nummer 18 am Wettbewerb teilnehmen.

(2) [1]Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach § 58 Absatz 2 Buchstaben a bis g und j 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 der verantwortlichen Stelle oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;

d) Grad der Verantwortung der verantwortlichen Stelle oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß den §§ 25 und 32 getroffenen technischen und organisatorischen Maßnahmen;

e) etwaige einschlägige frühere Verstöße der verantwortlichen Stelle oder des Auftragsverarbeiters;

f) die Bereitschaft zur Zusammenarbeit mit der Aufsichtsbehörde, 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 Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang die verantwortliche Stelle oder der Auftragsverarbeiter den Verstoß mitgeteilt hat;

i) Einhaltung der nach § 58 Absatz 2 früher gegen den für die betreffende verantwortliche Stelle oder den Auftragsverarbeiter in Bezug auf denselben Gegenstand angeordneten

Maßnahmen, wenn solche Maßnahmen angeordnet wurden;

j) – entfällt –

k) jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.

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

(4) Bei Verstößen werden im Einklang mit Absatz 2 Geldbußen von bis zu 500.000 EUR verhängt.

(5) – entfällt –

(6) Bei Nichtbefolgung einer Anweisung der Aufsichtsbehörde gemäß § 58 Absatz 2 werden im Einklang mit Absatz 2 Geldbußen von bis zu 500.000 EUR verhängt.

(7)–(9) – entfallen –

§ 84 – entfällt –

Kapitel 9 – Vorschriften für besondere Verarbeitungssituationen

§ 85 – abweichend –

– abweichende Regelung, siehe § 85 a

§ 85 a Verarbeitung personenbezogener Daten durch die Medien

(1) [1]Soweit personenbezogene Daten von Personen der Kirchengeschichte von verantwortlichen Stellen ausschließlich für eigene journalistisch-redaktionelle oder literarische Zwecke verarbeitet werden, gelten von den Vorschriften dieser Verordnung nur die §§ 86 a, 18, 21, 24 Absatz 4 und § 82. [2]Hierunter fällt die Herausgabe von Adressen-, Telefon- oder vergleichbaren Verzeichnissen nur, wenn mit ihr zugleich eine journalistisch-redaktionelle oder literarische Tätigkeit verbunden ist.

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

(3) [1]Wird jemand durch eine Berichterstattung in seinem Persönlichkeitsrecht beeinträchtigt, so kann er Auskunft über die der Berichterstattung zugrunde liegenden, zu seiner Person gespeicherten Daten verlangen. [2]Die Auskunft kann verweigert werden, soweit aus den Daten auf die berichtenden oder einsendenden Personen oder die Gewährsleute von Beiträgen, Unterlagen und Mitteilungen für den redaktionellen Teil geschlossen werden kann. [3]Die betroffene Person kann die Berichtigung unrichtiger Daten verlangen.

§ 86 – abweichend –

– abweichende Regelung, siehe §§ 86 a, 86 b

§ 86 a Offenlegung an kirchliche oder öffentliche Stellen

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

a) sie zur Erfüllung der in der Zuständigkeit der offenlegenden oder empfangenden kirchlichen Stelle liegenden Aufgabe erforderlich ist und

b) die Zulässigkeitsvoraussetzungen des § 6 vorliegen.

(2) [1]Die Verantwortung für die Zulässigkeit der Offenlegung trägt die offenlegende verantwortliche Stelle. [2]Erfolgt die Offenlegung auf Ersuchen der empfangenden kirchlichen Stelle, trägt diese die Verantwortung. [3]In diesem Fall prüft die offenlegende verantwortliche Stelle nur, ob das Ersuchen im Rahmen der Aufgaben der datenempfangenden kirchlichen Stelle liegt, es sei denn, dass besonderer Anlass zur Prüfung der Rechtmäßigkeit der Offenlegung besteht.

(3) [1]Die datenempfangende kirchliche Stelle darf die offengelegten Daten für den Zweck verarbeiten, zu dessen Erfüllung sie ihr offengelegt werden. [2]Eine Verarbeitung für andere Zwecke ist nur unter den Voraussetzungen des § 6 Absätze 4 bis 8 zulässig.

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

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

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

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

(8) Die datenempfangenden Stellen nach Absatz 6 und 7 dürfen die offengelegten Daten nur für den Zweck verarbeiten, zu dessen Erfüllung sie ihnen offengelegt werden. [2]Die offenlegende Stelle hat darauf hinzuweisen.

§ 86 b Offenlegung an sonstige Stellen

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

a) sie zur Erfüllung der in der Zuständigkeit der offenlegenden kirchlichen Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Verarbeitung nach § 86 a dieser Datenschutzordnung zulassen, oder

b) eine Rechtsvorschrift dies zulässt, oder

c) die datenempfangenden Stellen oder Personen ein berechtigtes Interesse an der Kenntnis der offenzulegenden Daten glaubhaft darlegen und die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Offenlegung hat, es sei denn, dass Grund zu der Annahme besteht, dass durch die Offenlegung die Wahrnehmung des Auftrags der Kirche gefährdet würde.

(2) Das Offenlegen von besonderen Kategorien personenbezogener Daten ist abweichend von Absatz 1 Buchstabe c nur zulässig, soweit dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist.

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

(4) $_1$In den Fällen der Offenlegung nach Absatz 1 Buchstabe c unterrichtet die offenlegende kirchliche Stelle die betroffene Person von der Offenlegung ihrer Daten. $_2$Dies gilt nicht, wenn damit zu rechnen ist, dass sie davon auf andere Weise Kenntnis erlangt oder die Wahrnehmung des Auftrags der Kirche gefährdet würde.

(5) $_1$Die datenempfangenden Stellen und Personen dürfen die offengelegten Daten nur für den Zweck verarbeiten, zu dessen Erfüllung sie ihnen offengelegt werden. $_2$Die offenlegende Stelle hat sie darauf hinzuweisen.

§ 87 – entfällt –

§ 88 – abweichend –

– abweichende Regelung, siehe § 88 a

§ 88 a Verarbeitung personenbezogener Daten bei Dienst- und Arbeitsverhältnissen

(1) Daten von Beschäftigten dürfen nur verarbeitet werden, soweit dies zur Begründung, Durchführung, Beendigung oder Abwicklung des Beschäftigungsverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch für Zwecke der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht.

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

(3) [1]Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. [2]Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder die verantwortliche Stelle und die beschäftigte Person gleich gelagerte Interessen verfolgen. [3]Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. [4]Die verantwortliche Stelle hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht aufzuklären.

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

a) die empfangende Person oder Stelle ein überwiegendes rechtliches Interesse darlegt;

b) Art oder Zielsetzung der dem Beschäftigten übertragenen Aufgaben die Offenlegung erfordert;

c) offensichtlich ist, dass die Offenlegung im Interesse der betroffenen Person liegt und keine Anhaltspunkte vorliegen, dass sie in Kenntnis des Zwecks der Offenlegung ihre Einwilligung nicht erteilen würde, oder

d) sie zur Aufdeckung einer Straftat oder Amtspflichtverletzung oder zum Schutz möglicher Betroffener erforderlich erscheint.

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

(6) [1]Personenbezogene Daten, die vor Begründung eines Beschäftigungsverhältnisses erhoben wurden, sind unverzüglich zu löschen, sobald feststeht, dass ein solches nicht zustande kommt. [2]Dies gilt nicht, soweit überwiegende berechtigte Interessen der verantwortlichen Stelle der Löschung entgegenstehen oder die betroffene Person in die weitere Speicherung einwilligt. [3]Nach Beendigung eines Beschäftigungsverhältnisses sind personenbezogene Daten zu löschen, soweit diese Daten nicht mehr benötigt werden.

(7) [1]Verlangt die verantwortliche Stelle zur Begründung oder im Rahmen eines Beschäftigungsverhältnisses medizinische oder psychologische Untersuchungen und Tests, hat sie Anlass und Zweck der Begutachtung möglichst tätigkeitsbezogen zu bezeichnen. [2]Ergeben sich keine medizinischen oder psychologischen Bedenken, darf die verantwortliche Stelle lediglich die Offenlegung des Ergebnisses der Begutachtung verlangen; ergeben sich Bedenken, darf auch die Offenlegung der festgestellten möglichst tätigkeitsbezogenen Risikofaktoren verlangt werden. [3]Im Übrigen ist eine Weiterverarbeitung der bei den Untersuchungen oder Tests erhobenen Daten ohne schriftliche Einwilligung der betroffenen Person nur für den Zweck zulässig, für den sie erhoben worden sind.

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

Beschäftigten dient.

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

§ 89 – abweichend –

– abweichende Regelung, siehe § 89 a

§ 89 a Verarbeitung personenbezogener Daten für wissenschaftliche und statistische Zwecke

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

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

(3) [1]Die personenbezogenen Daten sind zu anonymisieren, sobald dies möglich ist. [2]Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. [3]Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Zweck dies erfordert.

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

§ 90 – entfällt –

§ 91 – abweichend –

– abweichende Regelung, siehe §§ 91 a, 91 b, 91 c

§ 91 a Seelsorgegeheimnis und Amtsverschwiegenheit

[1]Aufzeichnungen, die in Wahrnehmung eines kirchlichen Seelsorgeauftrags erstellt werden, dürfen Dritten nicht zugänglich sein. [2]Die besonderen Bestimmungen über den Schutz des Seelsorgegeheimnisses bleiben unberührt. [3]Gleiches gilt für die sonstigen Verpflichtungen zur Wahrung gesetzlicher Geheimhaltungs- und Verschwiegenheitspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen.

§ 91 b Gottesdienste und kirchliche Veranstaltungen

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

§ 91 c Videoüberwachung öffentlich zugänglicher Räume

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

a) in Ausübung des Hausrechts der kirchlichen Stelle oder

b) zum Schutz von Personen und Sachen

erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. [2]Das Interesse an der nicht überwachten Teilnahme am Gottesdienst ist besonders schutzwürdig.

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

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

(4) [1]Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet und verarbeitet, so ist diese über die jeweilige Verarbeitung zu benachrichtigen. [2]Von der Benachrichtigung kann abgesehen werden,

a) solange das öffentliche Interesse an der Strafverfolgung das Recht auf Benachrichtigung der betroffenen Person erheblich überwiegt oder

b) wenn die Benachrichtigung im Einzelfall einen unverhältnismäßigen Aufwand erfordert.

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

Kapitel 10 – entfällt –

§ 92 – entfällt –
§ 93 – entfällt –

Kapitel 11 – Schlussbestimmungen

§ 94 – entfällt –
§ 95 – entfällt –
§ 96 – entfällt –
§ 97 – entfällt –

§ 98 – abweichend –

– abweichende Regelung, siehe §§ 98 a, 98 b

§ 98 a Ergänzende Bestimmungen

(1) Die territoriale Leitung oder ein Leitungsorgan der Heilsarmee in Deutschland kann, unter Einhaltung ihrer verfassungsmäßig bestimmten Entscheidungsverfahren, durch Rechtsverordnung

a) Durchführungsbestimmungen/Ausführungsbestimmungen zu dieser Datenschutzordnung und

b) ergänzende Bestimmungen zum Datenschutz erlassen.

(2) Soweit personenbezogene Daten von Sozialleistungsträgern offengelegt werden, gelten zum Schutz dieser Daten ergänzend die staatlichen Bestimmungen entsprechend.

(3) Diese Datenschutzordnung soll innerhalb von fünf Jahren überprüft werden.

§ 98 b Übergangsregeln

(1) Die bisherigen Bestellungen des Datenschutzbeauftragten im Geltungsbereich dieser Datenschutzordnung gelten fort. Für diese Bestellungen gelten die Regelungen der §§ 37 a, 38, 39, 51, 52, 53, 54, 57, 58, 59, 83 mit Inkrafttreten dieser Datenschutzordnung.

(2) $_1$Verzeichnisse der Verarbeitungstätigkeiten betreffend die Videoüberwachung nach § 91 c sind unverzüglich zu erstellen. $_2$Die Erstellung der Verzeichnisse der Verarbeitungstätigkeiten nach § 30 dieser Datenschutzordnung hat bis zum 30. Juni 2019 zu erfolgen.

§ 99 | Inkrafttreten, Außerkrafttreten

[1]Diese Kirchenordnung wurde von der Gesetzgebungskonferenz am 07.09.2018 beschlossen und durch den Territorialleiter bestätigt. [2]Sie tritt am Tag nach ihrer Bekanntgabe über die Datenbank „iuris“ in Kraft. [3]Gleichzeitig treten die Kirchenordnung über den Datenschutz vom 20.11.2016 und die Rechtsverordnung über den Datenschutz vom 08.05.2018 außer Kraft.

Beschluss durch die Gesetzgebungskonferenz:	07.09.2018
Bestätigung durch Territorialleiter:	17.09.2018
Bekanntgabe:	20.09.2018
in Kraft ab:	21.09.2018
außer Kraft am:	