



# Datenschutzordnung des Bundes Freikirchlicher Pfingstgemeinden KdÖR (BFP)

Verabschiedet von der Bundeskonferenz des BFP am 22.09.2015.

Umfangreiche Änderungen beschlossen vom Präsidium des BFP in Erzhausen am 07.02.2018.

Änderungen beschlossen vom Präsidium des BFP in Erzhausen am 06.09.2018.

## Übersicht

Präambel .....	2
<b>Kapitel 1 Allgemeine Bestimmung.....</b>	<b>2</b>
§ 1 Geltungsbereich .....	2
§ 2 Aufgabe des Datenschutzes .....	3
§ 3 Verantwortlichkeit für die Durchführung des Datenschutzes .....	3
§ 4 Begriffsbestimmungen .....	4
<b>Kapitel 2 Verarbeitung personenbezogener Daten .....</b>	<b>5</b>
§ 5 Rechtmäßigkeit der Verarbeitung und Zweckänderung.....	5
§ 6 Einwilligung .....	6
§ 7 Verarbeitung besonderer Kategorien personenbezogener Daten .....	6
§ 8 Offenlegung an freikirchliche, kirchliche und öffentliche Stellen.....	7
§ 9 Datenübermittlung an und in Drittländer oder an internationale Organisationen.....	7
<b>Kapitel 3 Rechte der betroffenen Person.....</b>	<b>8</b>
§ 10 Recht auf Transparenz und Auskunft der betroffenen Person.....	8
§ 11 Recht auf Berichtigung, Löschung und Einschränkung der Verarbeitung .....	9
§ 12 Recht auf Datenübertragbarkeit.....	10
§ 13 Widerspruchsrecht .....	10
§ 14 Recht auf Beschwerde .....	11
<b>Kapitel 4 Pflichten der verantwortlichen Stellen.....</b>	<b>11</b>
§ 15 Durchführung des Datenschutzes .....	11
§ 16 Datenverarbeitung im Auftrag .....	12
§ 17 Verzeichnis von Verarbeitungstätigkeiten.....	12
§ 18 Informationspflicht bei der Datenerhebung .....	12
§ 19 Informationspflicht bei Berichtigung, Löschung oder Einschränkung der Verarbeitung .	13
§ 20 Meldung von Verletzungen des Schutzes personenbezogener Daten an die aufsichtsführende Stelle .....	13
§ 21 Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person.....	14
§ 22 Datenschutz-Folgenabschätzung.....	14

<b>Kapitel 5</b>	<b>Örtlich Beauftragte für den Datenschutz</b>	<b>15</b>
§ 23	Bestellung von örtlich Beauftragten	15
§ 24	Aufgaben der örtlich Beauftragten	16
§ 25	Beanstandungsrecht der örtlich Beauftragten	16
<b>Kapitel 6</b>	<b>Datenschutzaufsicht</b>	<b>17</b>
§ 26	Bestellung des Beauftragten des Bundes	17
§ 27	Aufsichtsführende Stelle des Bundes für den Datenschutz	17
§ 28	Aufgaben und Befugnisse der aufsichtsführende Stelle	18
§ 29	Geldbußen	18
§ 30	Schadensersatz durch verantwortliche Stellen	19
<b>Kapitel 7</b>	<b>Vorschriften für besondere Verarbeitungssituationen</b>	<b>20</b>
§ 31	Verarbeitung personenbezogener Daten bei Dienst- und Arbeitsverhältnissen	20
§ 32	Aufzeichnungen oder Übertragungen von Veranstaltungen	20
§ 33	Videoüberwachung öffentlich zugänglicher Räume	20
<b>Kapitel 8</b>	<b>Schlussbestimmungen</b>	<b>21</b>
§ 34	Änderungen	21
§ 35	Inkrafttreten	21

## Präambel

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

## Kapitel 1 Allgemeine Bestimmung

### § 1 Geltungsbereich

- (1) Diese Datenschutzordnung gilt für die im Bund Freikirchlicher Pfingstgemeinden KdöR (im Folgenden: Bund) zusammengeschlossenen Gemeinden und deren Regionen sowie für die Bundeswerke, Arbeitszweige und Einrichtungen des Bundes und deren Verwaltung.
- (2) Stellen des Bundes im Sinne dieser Datenschutzordnung sind alle in Absatz 1 aufgeführt. Der Begriff „freikirchlich“ bezieht sich jeweils auf den Bund.

- (3) Für rechtlich selbstständige Gemeinden und Einrichtungen im Bund gilt diese Datenschutzordnung, soweit sie nicht
  - (a) durch Erklärung gegenüber dem Präsidium des Bundes die Geltung ablehnen und
  - (b) den Datenschutz für ihren Tätigkeitsbereich in einer dieser Datenschutzordnung vergleichbaren Form regeln sowie deren Durchführung sicherstellen.
- (4) Diese Ordnung findet Anwendung auf die Verarbeitung personenbezogener Daten im Rahmen der Tätigkeit einer Stelle oder in deren Auftrag, unabhängig vom Ort der Verarbeitung.
- (5) Diese Ordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten.

## §2 Aufgabe des Datenschutzes

- (1) Zweck der Datenschutzordnung ist es, den Einzelnen<sup>1</sup> davor zu schützen, dass er durch die Verarbeitung seiner personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.
- (2) Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl von Datenverarbeitungssystemen sind an dem Ziel auszurichten, nur die personenbezogenen Daten zu erheben, zu verarbeiten oder zu nutzen, die für den Zweck angemessen und sachlich relevant sind (Datenminimierung). Soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zum Schutzzweck unverhältnismäßigen Aufwand erfordert, sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren.
- (3) Den mit dem Umgang von Daten haupt-, neben- oder ehrenamtlich betrauten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Diese Personen sind bei der Aufnahme ihrer Tätigkeit auf die Wahrung der Vertraulichkeit und zur Beachtung des Datenschutzes zu verpflichten (Datengeheimnis). Diese Verpflichtung besteht auch nach Beendigung ihrer Tätigkeit fort.
- (4) Die allgemein gültigen Bestimmungen über den Schutz des Beicht- und des Seelsorgegeheimnisses sowie über die Amtsverschwiegenheit der Pastoren und der freikirchlichen Mitarbeiter gehen den Vorschriften dieser Datenschutzordnung vor.
- (5) Unberührt bleibt das Recht der Pastoren und der freikirchlichen Mitarbeiter, in Wahrnehmung ihres Seelsorgeauftrages eigene Aufzeichnungen zu führen und zu diesen Zwecken zu verwenden.

## §3 Verantwortlichkeit für die Durchführung des Datenschutzes

- (1) Das Präsidium des Bundes stellt die Einhaltung des Datenschutzes im Sinne dieser Datenschutzordnung innerhalb der Arbeitszweige und Einrichtungen des Bundes sicher. Das Präsidium kann diese Aufgabe an den Vorstand (Geschäftsführung) delegieren.
- (2) Die jeweils satzungsgemäß berufenen Vertretungsorgane der Gemeinden stellen die Einhaltung des Datenschutzes im Sinne dieser Datenschutzordnung innerhalb der Gemeinden sowie deren Arbeitszweige und Einrichtungen unter Beachtung von §23 Absatz 1 sicher.
- (3) In rechtlich selbstständigen Gemeinden und Einrichtungen des Bundes, die von der Regelung in §1 Absatz 3 keinen Gebrauch machen, stellen die jeweils berufenen Vertretungsorgane die Einhaltung dieser Datenschutzordnung unter Beachtung von §23 Absatz 1 sicher.

---

<sup>1</sup> Die in dieser Ordnung verwendete sprachliche Form der Personenbeschreibung erlaubt keinen Rückschluss auf das Geschlecht einer Person.

## §4 Begriffsbestimmungen

- (1) Personenbezogene Daten sind Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlicher Person (betroffene Person). Bestimmbar ist eine natürliche Person, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Onlinekennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.
- (2) Besondere Kategorien personenbezogener Daten sind personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Die Zugehörigkeit zu einer Kirche oder Religionsgemeinschaft ist keine besondere Kategorie personenbezogener Daten.
- (3) Verarbeitung ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.
- (4) Einschränkung der Verarbeitung ist die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken.
- (5) Profiling ist jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.
- (6) Dateisystem ist 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) Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbarer Person zugeordnet werden können.
- (8) Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung der betroffenen Person auszuschließen oder wesentlich zu erschweren.
- (9) Verantwortliche Stelle ist die natürliche oder juristische Person, freikirchliche Stelle im Sinne von § 1 oder sonstige Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Personen oder Stellen, die weder eine speichernde Stelle noch eine von ihr mit der Datenverarbeitung beauftragte Person oder Stelle noch der Betroffene selbst sind, sind Dritte.
- (10) Einwilligung ist jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung der betroffenen Person in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

- (11) Verletzung des Schutzes personenbezogener Daten ist eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von oder zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.
- (12) Drittland ist ein Land, in dem die europäischen Datenschutz-Grundverordnung keine Anwendung findet.

## **Kapitel 2 Verarbeitung personenbezogener Daten**

### **§5 Rechtmäßigkeit der Verarbeitung und Zweckänderung**

- (1) Die Verarbeitung personenbezogener Daten ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:
  - (a) eine Rechtsvorschrift erlaubt die Verarbeitung der personenbezogenen Daten oder ordnet sie an;
  - (b) die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
  - (c) die Verarbeitung ist zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich;
  - (d) die Verarbeitung ist für die Wahrnehmung einer sonstigen Aufgabe erforderlich, die im freikirchlichen Interesse liegt;
  - (e) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgt;
  - (f) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der die freikirchliche Stelle unterliegt;
  - (g) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
  - (h) 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.
- (2) Die Verarbeitung für einen anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, ist nur rechtmäßig, wenn
  - (a) eine innerkirchliche Rechtsvorschrift dies vorsieht oder zwingend voraussetzt;
  - (b) eine staatliche Rechtsvorschrift dies vorsieht und innerkirchliche Interessen dem nicht entgegenstehen;
  - (c) offensichtlich ist, dass sie im Interesse der betroffenen Person liegt, und kein Grund zu der Annahme besteht, dass diese in Kenntnis des anderen Zweckes ihre Einwilligung verweigern würde;
  - (d) 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;
  - (e) Grund zu der Annahme besteht, dass andernfalls die Wahrnehmung des freikirchlichen Auftrages gefährdet würde;
  - (f) es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist;

- (g) 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;
- (h) sie für statistische Zwecke zur Erfüllung des freikirchlichen Auftrages erforderlich ist.

## **§6 Einwilligung**

- (1) Beruht die Verarbeitung auf einer Einwilligung, muss die verantwortliche Stelle nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.
- (2) Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erfolgen, sodass es von anderen Sachverhalten klar zu unterscheiden ist.
- (3) Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.
- (4) Minderjährige, denen elektronische Angebote von freikirchlichen Stellen gemacht werden, können in die Verarbeitung ihrer Daten wirksam einwilligen, wenn sie religionsmündig sind. Sind die Minderjährigen noch nicht religionsmündig, ist die Verarbeitung nur rechtmäßig, wenn die Sorgeberechtigten die Einwilligung erteilt oder der Einwilligung zugestimmt haben. Die Einwilligung der Sorgeberechtigten ist nicht erforderlich, wenn freikirchliche Präventions- oder Beratungsdienste einem Kind unmittelbar angeboten werden.

## **§7 Verarbeitung besonderer Kategorien personenbezogener Daten**

- (1) Besondere Kategorien personenbezogener Daten dürfen nicht verarbeitet werden.
- (2) Abweichend von Absatz 1 dürfen besondere Kategorien personenbezogener Daten verarbeitet werden, wenn
  - (a) die betroffene Person in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt hat;
  - (b) die Verarbeitung ist erforderlich, damit die verantwortliche Stelle oder die betroffene Person die ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach freikirchlichem oder staatlichen Recht, die geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsehen, zulässig ist;
  - (c) die Verarbeitung zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person aus körperlichen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben;
  - (d) die Verarbeitung sich auf personenbezogene Daten bezieht, die die betroffene Person öffentlich gemacht hat;
  - (e) die Verarbeitung für im freikirchlichen Interesse liegende Zwecke des Archivs, der wissenschaftlichen oder historischen Forschung oder der Statistik erfolgt und die Interessen der betroffenen Person durch angemessene Maßnahmen gewahrt sind.

## **§8 Offenlegung an freikirchliche, kirchliche und öffentliche Stellen**

- (1) Die Offenlegung von personenbezogenen Daten an Stellen des Bundes ist zulässig, wenn
  - (a) sie zur Erfüllung der in der Zuständigkeit der offenlegenden oder der empfangenden Stelle liegenden Aufgaben erforderlich ist und
  - (b) die Voraussetzung der Rechtmäßigkeit des §5 vorliegen.
- (2) Die Verantwortung für die Zulässigkeit der Offenlegung trägt die offenlegende Stelle. Erfolgt die Offenlegung auf Ersuchen der empfangenden Stelle, trägt auch diese die Verantwortung. In diesem Fall prüft die offenlegende Stelle nur, ob das Ersuchen im Rahmen der Aufgaben der empfangenden Stelle liegt, es sei denn, dass besonderer Anlass zur Prüfung der Rechtmäßigkeit der Offenlegung besteht.
- (3) Die empfangende Stelle darf die offengelegten Daten für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihr übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nur unter den Voraussetzungen des §5 zulässig.
- (4) Sind mit personenbezogenen Daten, die nach Absatz 1 übermittelt werden dürfen, weitere personenbezogene Daten der betroffenen oder einer anderen Person so verbunden, dass eine Trennung nicht oder nur mit unververtretbarem Aufwand möglich ist, so ist die Übermittlung auch dieser Daten zulässig, soweit nicht berechnete 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 freikirchlichen Stelle weitergegeben werden.
- (6) Personenbezogene Daten dürfen an Stellen anderer öffentlich-rechtlicher Religionsgesellschaften offengelegt werden, wenn das zur Erfüllung der freikirchlichen 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 berechnete Interessen der betroffenen Person entgegenstehen.
- (7) Personenbezogene Daten dürfen an staatliche und kommunale Stellen offengelegt werden, wenn dies eine Rechtsvorschrift zulässt oder dies zur Erfüllung der freikirchlichen Aufgaben erforderlich ist, die der übermittelnden Stelle obliegen, und nicht offensichtlich berechnete Interessen der betroffenen Person entgegenstehen.

## **§9 Datenübermittlung an und in Drittländer oder an internationale Organisationen**

- (1) Jede Übermittlung personenbezogener Daten, die bereits verarbeitet wurden oder nach ihrer Übermittlung an ein Drittland oder an eine internationale Organisation verarbeitet werden sollen, ist nur zulässig, wenn die verantwortliche Stelle und der Auftragsverarbeiter die in dieser Ordnung niedergelegten Bedingungen einhalten (vgl. §16). Dies gilt auch für die etwaige Weiterübermittlung personenbezogener Daten durch das betreffende Drittland oder die betreffende internationale Organisation.
- (2) Eine Übermittlung personenbezogener Daten an oder in ein Drittland oder an eine internationale Organisation ist zulässig, wenn ein Angemessenheitsbeschluss der Europäischen Kommission vorliegt (Datenschutzniveau).
- (3) Falls die Voraussetzung des Absatz 2 nicht vorliegen, ist die Übermittlung nur zulässig, wenn

- (a) die betroffene Person in die vorgeschlagene Datenübermittlung ausdrücklich eingewilligt hat, nachdem sie über die für sie bestehenden möglichen Risiken aufgeklärt worden ist;
- (b) die Übermittlung für die Erfüllung eines Vertrages oder Rechtsverhältnisses zwischen der betroffenen Person und der verantwortlichen Stelle oder zur Durchführung von vertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich ist;
- (c) die Übermittlung zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person von der verantwortlichen Stelle mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrages erforderlich ist;
- (d) die Übermittlung aus wichtigen Gründen des freikirchlichen Interesses notwendig ist;
- (e) die Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist;
- (f) die Übermittlung zum Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen erforderlich ist, sofern die betroffene Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben.

## **Kapitel 3 Rechte der betroffenen Person**

### **§ 10 Recht auf Transparenz und Auskunft der betroffenen Person**

- (1) Die verantwortliche Stelle trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen, die nach dieser Ordnung hinsichtlich der Verarbeitung zu geben sind, in präziser, transparenter, verständlicher und leicht zugänglicher Form zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Minderjährige richten.
- (2) Die verantwortliche Stelle stellt der betroffenen Person auf Antrag Informationen über die ergriffenen Maßnahmen bzgl. Berichtigung, Löschung bzw. Einschränkung der Verarbeitung innerhalb von drei Monaten nach Eingang des Antrags zur Verfügung. Diese Frist kann um zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl der Anträge erforderlich ist. Die verantwortliche Stelle unterrichtet die betroffene Person innerhalb von drei Monaten nach Eingang über eine Fristverlängerung zusammen mit den Gründen für die Verzögerung.
- (3) Der betroffenen Person ist auf Antrag Auskunft zu erteilen über die zu ihr gespeicherten personenbezogenen Daten. Die Auskunft muss folgende Informationen enthalten:
  - (a) die Verarbeitungszwecke;
  - (b) die Kategorien personenbezogener Daten;
  - (c) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten übermittelt worden sind;
  - (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 aufsichtsführenden Stelle;
  - (g) wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten.



- (4) In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Sind die personenbezogenen Daten in Akten gespeichert, wird die Auskunft nur erteilt, soweit die betroffene Person Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem geltend gemachten Informationsinteresse steht. Die verantwortliche Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen.
- (5) Auskunft darf nicht erteilt werden, soweit die Daten oder die Tatsache ihrer Speicherung aufgrund einer 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 Freikirche gefährdet wird.
- (6) Die Auskunft ist unentgeltlich.

## **§ 11 Recht auf Berichtigung, Löschung und Einschränkung der Verarbeitung**

- (1) Personenbezogene Daten sind auf Antrag der betroffenen Person zu berichtigen, wenn sie unrichtig sind. 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) Personenbezogene Daten sind zu löschen, wenn
  - (a) ihre Speicherung unzulässig war oder
  - (b) ihre Kenntnis für die speichernde Stelle zur Erfüllung der ihr obliegenden freikirchlichen Aufgaben nicht mehr erforderlich ist;
  - (c) die betroffene Person ihre Einwilligung bezüglich der Verarbeitung ihrer Daten widerruft und es an einer anderweitigen Rechtsgrundlage für die Verarbeitung fehlt;
  - (d) die betroffene Person gemäß § 13 Widerspruch gegen die Verarbeitung einlegt und keine vorrangigen berechtigten Gründe für die Verarbeitung vorliegen;
  - (e) die Löschung der personenbezogenen Daten zur Erfüllung rechtlicher Verpflichtungen der verantwortlichen Stelle notwendig ist.
- (3) An die Stelle einer Löschung tritt eine Einschränkung der Verarbeitung, wenn
  - (a) einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen;
  - (b) Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen der betroffenen Person beeinträchtigt würden;
  - (c) eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist oder
  - (d) Grund zu der Annahme besteht, dass die Nutzung zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der speichernden Stelle oder eines Dritten liegenden Gründen unerlässlich ist.
- (4) Die Verarbeitung personenbezogener Daten ist einzuschränken, wenn
  - (a) ihre Richtigkeit von der betroffenen Person bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt;
  - (b) die Verarbeitung unrechtmäßig ist, die betroffene Person aber 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;
  - (d) die betroffene Person Widerspruch gegen die Verarbeitung gemäß §13 eingelegt hat und es noch nicht feststeht, ob die berechtigten Gründe der verantwortlichen Stelle gegenüber denen der betroffenen Person überwiegen.
- (5) Wurde die Verarbeitung der Daten eingeschränkt, so dürfen sie nicht mehr verarbeitet, insbesondere übermittelt oder sonst genutzt werden, es sei denn, dass die Nutzung zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der speichernden Stelle oder eines Dritten liegenden Gründen unerlässlich ist oder die betroffene Person der Nutzung zugestimmt hat.
- (6) 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.

## **§ 12 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, sowie 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 oder auf einem Vertrag beruht und
  - (b) die Verarbeitung mithilfe automatisierter Verfahren erfolgt.
- (2) Die betroffene Person kann verlangen, dass die personenbezogenen Daten direkt von der verantwortlichen Stelle einem anderen Dritten übermittelt werden, soweit dies technisch machbar ist.
- (3) Das Recht auf Datenübertragbarkeit gilt nicht für eine Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im freikirchlichen Interesse liegt oder in Ausübung des freikirchlichen Auftrags erfolgt, die der verantwortlichen Stelle übertragen wurde.
- (4) Das Recht gemäß Absatz 2 darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

## **§ 13 Widerspruchsrecht**

- (1) Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten gemäß § 5 Widerspruch einzulegen; dies gilt auch für die Verarbeitung personenbezogener Daten im Rahmen eines Profilings.
- (2) Der Widerspruch verpflichtet die verantwortliche Stelle dazu, die Verarbeitung zu unterlassen, soweit nicht an der Verarbeitung ein zwingendes freikirchliches Interesse besteht, das Interesse einer dritten Person überwiegt oder eine Rechtsvorschrift zur Verarbeitung verpflichtet.

## **§ 14 Recht auf Beschwerde**

- (1) Wer darlegt, dass er bei der Verarbeitung seiner personenbezogenen Daten in seinen Rechten verletzt worden ist, kann sich damit an den für ihn zuständigen Beauftragten für den Datenschutz wenden, wenn die zuständige Stelle nicht alsbald abhilft. Dies schließt auch die Beschwerde bei der aufsichtsführenden Stelle mit ein.
- (2) Niemand darf wegen der Mitteilung von Tatsachen gemäßregelt oder benachteiligt werden, die geeignet sind, den Verdacht aufkommen zu lassen, diese Ordnung oder eine andere anzuwendende Rechtsvorschrift über den Datenschutz sei verletzt worden. Beschäftigte müssen für Mitteilungen an die aufsichtsführende Stelle nicht den Dienstweg einhalten.

## **Kapitel 4 Pflichten der verantwortlichen Stellen**

### **§ 15 Durchführung des Datenschutzes**

- (1) Die freikirchlichen Stellen haben bei der Datenverarbeitung die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung dieser Datenschutzbestimmungen zu gewährleisten. Hierbei ist der Stand der Technik, die Implementierungskosten, die Art, der Umfang, die Umstände und Zwecke der Verarbeitung sowie die unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen. Ziel ist, ein dem Risiko angemessenes Schutzniveau zu gewährleisten und einen Nachweis hierüber führen zu können. Diese Maßnahmen schließen unter anderem ein:
  - (a) die Pseudonymisierung, die Anonymisierung und die Verschlüsselung personenbezogener Daten;
  - (b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
  - (c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall unverzüglich wiederherzustellen;
  - (d) eine Voreinstellung der Datenverarbeitungssysteme, die eine Verarbeitung von personenbezogenen Daten für den jeweiligen bestimmten Verarbeitungszweck begrenzt. Dies gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit;
  - (e) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.
- (2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung, unbefugte Offenlegung von oder unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.
- (3) Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

## **§ 16 Datenverarbeitung im Auftrag**

- (1) Werden geschützte personenbezogene Daten im Auftrag freikirchlicher Stellen (§ 1 Absatz 2) durch andere Personen oder Stellen verarbeitet, so ist dies nur im Rahmen der Weisungen des Auftraggebers zulässig. Im Falle der Beauftragung gilt der Auftraggeber als speichernde Stelle im Sinne des § 4 Absatz 9.
- (2) Sofern die freikirchlichen Datenschutzbestimmungen auf den Auftragnehmer keine Anwendung finden, ist die verantwortliche Stelle verpflichtet sicherzustellen, dass der Auftragnehmer diese oder gleichwertige Bestimmungen beachtet. In diesem Fall sollen sich die Vereinbarungen an Art. 28 EU-Datenschutz-Grundverordnung orientieren.
- (3) Für eine Auftragsverarbeitung in Drittländern gilt § 9.

## **§ 17 Verzeichnis von Verarbeitungstätigkeiten**

- (1) Die freikirchlichen Stellen führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält folgende Angaben:
  - (a) die Namen und die Kontaktdaten der verantwortlichen Personen oder Stellen;
  - (b) die Zwecke der Verarbeitung;
  - (c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
  - (d) gegebenenfalls die Verwendung von Profiling;
  - (e) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfängern in Drittländern oder internationalen Organisationen;
  - (f) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe der dort getroffenen geeigneten Garantien;
  - (g) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
  - (h) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 15.
  - (i) Das Verzeichnis ist schriftlich oder elektronisch zu führen und wird von der verantwortlichen Stelle dem örtlich Beauftragten für den Datenschutz sowie auf Anfrage dem Datenschutzbeauftragten des Bundes zur Verfügung gestellt.
- (2) Die im Absatz 1 genannte Pflicht gilt nicht für verantwortliche Stellen, die weniger als 250 Beschäftigte haben. Freikirchliche Stellen, die weniger als 250 Beschäftigte haben, erstellen Verzeichnisse nach Absatz 1 und 2 nur hinsichtlich der Verfahren, die die Verarbeitung besonderer Kategorien personenbezogener Daten einschließen.

## **§ 18 Informationspflicht bei der Datenerhebung**

- (1) Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt die verantwortliche Stelle der betroffenen Person auf Verlangen in geeigneter und angemessener Weise Folgendes mit:
  - (a) den Namen und die Kontaktdaten der verantwortlichen Stelle;
  - (b) gegebenenfalls die Kontaktdaten der oder des örtlich Beauftragten;
  - (c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
  - (d) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten.

- (2) Zusätzlich zu den Informationen gemäß Absatz 1 stellt die verantwortliche Stelle der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten auf Verlangen folgende weitere Informationen zur Verfügung:
  - (a) falls möglich 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) das Bestehen eines Beschwerderechts bei der aufsichtsführenden Stelle;
  - (d) ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, und welche mögliche Folgen die Nichtbereitstellung hätte.
- (3) Beabsichtigt die verantwortliche Stelle, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so stellt sie der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck zur Verfügung.
- (4) Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, so teilt die verantwortliche Stelle der betroffenen Person über die in Absatz 2 und 3 aufgeführten Informationen hinaus die zu ihr gespeicherten Daten mit, auch woher diese Daten stammen.
- (5) Die Absätze 1, 2, 3 und 4 finden keine Anwendung, wenn und so weit die betroffene Person bereits über die Informationen verfügt oder die Informationspflicht einen unverhältnismäßigen Aufwand erfordern würde.
- (6) Von dieser Verpflichtung ist die verantwortliche Stelle befreit, soweit die Daten oder die Tatsache ihrer Speicherung aufgrund einer speziellen Rechtsvorschrift oder wegen überwiegender berechtigter Interessen Dritter geheim gehalten werden müssen und das Interesse der betroffenen Person an der Auskunftserteilung zurücktreten muss oder wenn durch die Auskunft die Wahrnehmung des Auftrags der Freikirche gefährdet wird.

## **§ 19 Informationspflicht bei Berichtigung, Löschung oder Einschränkung der Verarbeitung**

- (1) Die verantwortliche Stelle teilt allen Empfängern, denen personenbezogene Daten übermittelt werden, jede Berichtigung oder Löschung der personenbezogenen Daten oder eine Einschränkung der Verarbeitung nach § 13 mit, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. Die verantwortliche Stelle unterrichtet die betroffene Person über diese Empfänger, wenn die betroffene Person dies verlangt.

## **§ 20 Meldung von Verletzungen des Schutzes personenbezogener Daten an die aufsichtsführende Stelle**

- (1) Die verantwortliche Stelle meldet der aufsichtsführenden Stelle unverzüglich die Verletzung des Schutzes personenbezogener Daten, wenn diese Verletzung eine Gefahr für die Rechte und Freiheiten natürlicher Personen darstellt. Erfolgt die Meldung nicht binnen 72 Stunden, nachdem die Verletzung des Schutzes personenbezogener Daten bekannt wurde, so ist ihr eine Begründung für die Verzögerung beizufügen.
- (2) Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese unverzüglich dem Verantwortlichen.
- (3) Die Meldung gemäß Absatz 1 enthält insbesondere folgende Informationen:

- (a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
  - (b) den Namen und die Kontaktdaten des örtlichen Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
  - (c) eine Beschreibung der möglichen Folgen der Verletzung des Schutzes personenbezogener Daten;
  - (d) eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.
- (4) Wenn und so weit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, kann die verantwortliche Stelle diese Informationen unverzüglich schrittweise zur Verfügung stellen.
  - (5) Die verantwortliche Stelle hat Verletzungen des Schutzes personenbezogener Daten zu dokumentieren. Die Dokumentation hat alle mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Abhilfemaßnahmen zu umfassen. Diese Dokumentation muss der aufsichtsführenden Stelle die Überprüfung der Einhaltung der Bestimmungen der Absätze 1 bis 4 ermöglichen.

## **§21 Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person**

- (1) Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte natürlicher Personen zur Folge, so benachrichtigt die verantwortliche Stelle die betroffene Person unverzüglich von der Verletzung.
- (2) Die Benachrichtigung der betroffenen Person hat in klarer und einfacher Sprache zu erfolgen und enthält zumindest die Art der Verletzung des Schutzes personenbezogener Daten und die in §20, Absatz 3 b–d genannten Informationen und Maßnahmen.
- (3) Von der Benachrichtigung der betroffenen Person kann abgesehen werden, wenn
  - (a) die verantwortliche Stelle durch nachträgliche Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte der betroffenen Personen aller Wahrscheinlichkeit nach nicht mehr besteht, oder
  - (b) die Benachrichtigung mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall hat stattdessen eine im freikirchlichen Bereich übliche öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

## **§22 Datenschutz-Folgenabschätzung**

- (1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte natürlicher Personen zur Folge, so führt die verantwortliche Stelle vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.
- (2) Die verantwortliche Stelle holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des örtlich Beauftragten ein, sofern ein solcher benannt wurde.

- (3) Eine Datenschutz-Folgenabschätzung ist insbesondere in folgenden Fällen erforderlich:
  - (a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;
  - (b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten oder
  - (c) die systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.
- (4) Die Folgenabschätzung umfasst insbesondere:
  - (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 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.
- (5) Falls die Verarbeitung auf einer Rechtsgrundlage im freikirchlichen, 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 Ordnung eine Datenschutz-Folgenabschätzung erfolgte, gelten die Absätze 1 bis 4 nicht.
- (6) 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.
- (7) Die verantwortliche Stelle konsultiert vor der Verarbeitung die aufsichtsführende Stelle, wenn aus der Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hat.

## **Kapitel 5 Örtlich Beauftragte für den Datenschutz**

### **§23 Bestellung von örtlich Beauftragten**

- (1) Bei den verantwortlichen Stellen sind örtlich Beauftragte (Betriebs- bzw. Gemeindebeauftragte) für den Datenschutz zu bestellen, wenn:
  - (a) bei ihnen in der Regel mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten betraut sind, und, sofern es sich um eine Gemeinde handelt, diese mehr als 50 Mitglieder hat, oder
  - (b) die Kerntätigkeit der verantwortlichen Stelle in der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten besteht.
- (2) Die Bestellung kann sich auf mehrere verantwortliche Stellen erstrecken. Die Vertretung ist dabei zu regeln.
- (3) Zu örtlich Beauftragten dürfen nur Personen bestellt werden, die die zur Erfüllung ihrer Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzen. Sie sind auf die gewissenhafte Erfüllung ihres Auftrags zu verpflichten.

- (4) Die örtlich Beauftragten sind im Rahmen ihrer Aufgaben weisungsfrei. Sie dürfen wegen dieser Tätigkeit nicht benachteiligt werden. Sie können Auskünfte verlangen, Einsicht in Unterlagen nehmen und erhalten Zugang zu personenbezogenen Daten und den Verarbeitungsvorgängen.
- (5) Zu örtlich Beauftragten sollen diejenigen nicht bestellt werden, die mit der Leitung der Datenverarbeitung beauftragt sind oder denen die Leitung der freikirchlichen Stelle obliegt.
- (6) Die Bestellung von örtlich Beauftragten erfolgt schriftlich und ist der für die Aufsicht zuständigen Stelle anzuzeigen.
- (7) Die Amtszeit von örtlich Beauftragten für den Datenschutz beträgt drei Jahre. Eine Wiederbestellung ist zulässig.
- (8) Die verantwortliche Stelle unterstützt die örtlich Beauftragten bei der Erfüllung ihrer Aufgaben und stellt die notwendigen Mittel zur Verfügung. Dies gilt insbesondere für Teilnahme an Fort- und Weiterbildungsveranstaltungen zur Erlangung und zur Erhaltung der erforderlichen Fachkunde.
- (9) Soweit mehrere verantwortliche Stellen im Sinne des Absatz 2 gemeinsam einen örtlich Beauftragten für den Datenschutz beauftragen, regeln sie, soweit erforderlich, die Beschaffung und Verwaltung der erforderlichen sachlichen und personellen Mittel.
- (10) Die verantwortlichen Stellen stellen sicher, dass örtlich Beauftragte ordnungsgemäß und frühzeitig bei allen mit dem Schutz personenbezogener Daten zusammenhängenden Fragen beteiligt werden.

## **§24 Aufgaben der örtlich Beauftragten**

- (1) Die örtlich Beauftragten wirken auf die Einhaltung der Bestimmungen für den Datenschutz hin und unterstützen die verantwortlichen Stellen bei der Sicherstellung des Datenschutzes. Sie haben insbesondere
  - (a) die verantwortliche Stelle und die haupt-, neben- oder ehrenamtlich Tätigen zu beraten;
  - (b) die ordnungsmäßige Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen;
  - (c) die bei der Verarbeitung personenbezogener Daten tätigen Personen zu informieren und zu schulen;
  - (d) auf Anfrage die verantwortliche Stelle bei der Durchführung einer Datenschutz-Folgenabschätzung zu beraten und deren Durchführung zu überwachen;
  - (e) mit der aufsichtsführenden Stelle zusammenzuarbeiten.

## **§25 Beanstandungsrecht der örtlich Beauftragten**

- (1) Stellt der Beauftragte für den Datenschutz der jeweiligen Stelle Verstöße gegen die Datenschutzbestimmungen oder sonstige Mängel bei der Verarbeitung personenbezogener Daten fest, so beanstandet er dies gegenüber den speichernden Stellen und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf.
- (2) Der Beauftragte für den Datenschutz kann von einer Beanstandung absehen oder auf eine Stellungnahme verzichten, wenn es sich um unerhebliche Mängel handelt.
- (3) Mit der Beanstandung kann der Beauftragte für den Datenschutz Vorschläge zur Beseitigung der Mängel und zur sonstigen Verbesserung des Datenschutzes verbinden. Wird der Beanstandung nicht abgeholfen, so ist der örtlich Beauftragte für den Datenschutz befugt, sich an den Datenschutzbeauftragten des Bundes zu wenden. Dieser wiederum ist befugt, sich an das Präsidium des Bundes zu wenden.



- (4) Die gemäß den Vorschriften des Absatz 1 abzugebende Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Beanstandung des Beauftragten für den Datenschutz getroffen worden sind.

## **Kapitel 6 Datenschutzaufsicht**

### **§26 Bestellung des Beauftragten des Bundes**

- (1) Das Präsidium des Bundes bestellt einen Beauftragten des Bundes für den Datenschutz.
- (2) Zum Beauftragten für den Datenschutz darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Er ist auf die gewissenhafte Erfüllung seines Auftrags zu verpflichten.
- (3) Der Beauftragte des Bundes für den Datenschutz ist in Ausübung seines Auftrags an Weisungen nicht gebunden und nur dem Recht des Bundes unterworfen.
- (4) Der Beauftragte des Bundes für den Datenschutz ist verpflichtet, über die ihm in Ausübung seines Auftrags bekannt gewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für allgemeine Mitteilungen oder für Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Die Verpflichtung besteht auch nach Beendigung des Auftrags fort. Der Beauftragte des Bundes für den Datenschutz darf, auch wenn er vom Auftrag entbunden ist, über Angelegenheiten, die der Verschwiegenheit unterliegen, ohne Genehmigung des Präsidiums des Bundes weder vor Gericht noch außergerichtlich aussagen oder Erklärungen abgeben; eine gesetzlich begründete Pflicht, Straftaten anzuzeigen, bleibt unberührt.
- (5) Der Beauftragte des Bundes für den Datenschutz untersteht nur der Rechts- und Dienstaufsicht, nicht jedoch der Fachaufsicht des Präsidiums des Bundes.
- (6) Die Amtszeit des Beauftragten des Bundes für den Datenschutz beträgt fünf Jahre. Die Wiederbestellung ist zulässig.

### **§27 Aufsichtsführende Stelle des Bundes für den Datenschutz**

- (1) Der Beauftragte des Bundes für den Datenschutz nimmt die aufsichtsführende Stelle innerhalb des Bundes wahr. Er leitet diese und vertritt sie nach außen.
- (2) Zur Erfüllung seiner Aufgaben kann er weitere Personen für die Datenschutzaufsicht hinzurufen. Dabei ist bei der Auswahl Fachwissen, Zuverlässigkeit, Eignung und Erfahrung zu berücksichtigen. Die Bestellung der Mitglieder erfolgt für mindestens zwei Jahre. Die Mitwirkung bei der Datenschutzaufsicht geschieht in der Regel ehrenamtlich.
- (3) Die aufsichtsführende Stelle handelt bei der Erfüllung ihrer Aufgaben und bei der Ausübung ihrer Befugnisse unabhängig. Sie unterliegt weder direkter noch indirekter Beeinflussung von außen und nimmt keine Weisungen entgegen.
- (4) Die Mitglieder der aufsichtsführenden Stelle sind bei der Erfüllung ihrer Aufgaben an die Wahrung des Datengeheimnisses und der Vertraulichkeit gebunden. Dies gilt nicht für Mitteilungen zwischen den Mitgliedern. Ehemalige Mitglieder dürfen sich zu Angelegenheiten, die während ihrer Mitgliedschaft der Verschwiegenheit unterlagen, ohne Genehmigung der aufsichtsführenden Stelle nicht äußern.

## **§28 Aufgaben und Befugnisse der aufsichtsführende Stelle**

- (1) Die aufsichtsführende Stelle wacht über die Einhaltung der Vorschriften über den Datenschutz. Zu diesem Zwecke kann sie Empfehlungen zur Verbesserung des Datenschutzes geben und die freikirchlichen Stellen in Fragen des Datenschutzes beraten. Auf Anforderung der Leitungsorgane des Bundes hat die aufsichtsführende Stelle Gutachten zu erstellen und Berichte zu geben.
- (2) Die freikirchlichen Stellen sind verpflichtet, die Mitglieder der aufsichtsführenden Stelle bei der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen ist Auskunft auf Fragen sowie Einsicht in alle Unterlagen und Akten über die Verarbeitung personenbezogener Daten zu geben, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme. Ihnen ist Zutritt zu den Räumen zu gewähren, in denen Daten verarbeitet werden.
- (3) Die aufsichtsführende Stelle soll die örtlich Beauftragten u. a. durch die Bereitstellung von Materialien zur Erhaltung der Fachkunde in geeigneter Form in der Wahrnehmung ihrer Aufgaben unterstützen.
- (4) Auch soll sie die verantwortlichen Stellen durch u. a. einheitliche Formblätter und Listen in der Einhaltung der Bestimmungen dieser Ordnung unterstützen. Dies gilt insbesondere für die Durchführung einer Datenschutz-Folgenabschätzung.
- (5) Werden der aufsichtsführenden Stelle Verstöße gegen die Datenschutzbestimmungen oder sonstige Mängel bei der Verarbeitung personenbezogener Daten bekannt, so beanstandet sie dies gegenüber der verantwortlichen Stelle oder gegenüber dem Auftragsverarbeiter und fordert zur Stellungnahme innerhalb einer gesetzten Frist auf. Von einer Beanstandung kann abgesehen werden, wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt. Mit der Aufforderung zur Stellungnahme können Vorschläge zur Beseitigung der Mängel oder zur sonstigen Verbesserung des Datenschutzes verbunden werden. Die Stellungnahme soll eine Darstellung der Maßnahmen enthalten, die aufgrund der Mitteilung der aufsichtsführenden Stelle getroffen worden sind.
- (6) Die aufsichtsführende Stelle ist befugt, bei Bedarf anzuordnen:
  - (f) Verarbeitungsvorgänge auf bestimmte Weise in Einklang mit dieser Ordnung zu bringen;
  - (g) Verarbeitungsvorgänge vorübergehend oder dauerhaft zu beschränken oder zu unterlassen;
  - (h) personenbezogene Daten zu berichtigen, zu sperren oder zu löschen;
  - (i) die von einer Verletzung des Schutzes personenbezogener Daten betroffene Person entsprechend zu benachrichtigen.
- (7) Die aufsichtsführende Stelle soll mit anderen Datenschutzaufsichten vor allem für den Informations- und Fachaustausch zusammenarbeiten, insbesondere Aufsichtsorgane aus dem freikirchlichen Bereich.

## **§29 Geldbußen**

- (1) Verstößt eine verantwortliche Stelle oder ein Auftragsverarbeiter, der dieser Ordnung unterliegt, vorsätzlich oder fahrlässig gegen Bestimmungen dieser Ordnung, so kann die aufsichtsführende Stelle Geldbußen verhängen oder für den Wiederholungsfall androhen. Gegen verantwortliche Stellen sind Geldbußen nur zu verhängen, soweit sie als Unternehmen im Sinne des § 4 Absatz 9 am Wettbewerb teilnehmen.
- (2) Die aufsichtsführende Stelle stellt sicher, dass die Verhängung von Geldbußen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

- (3) Geldbußen werden je nach den Umständen des Einzelfalls verhängt. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Höhe ist insbesondere Folgendes zu berücksichtigen:
- (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 der betroffenen Person entstandenen Schadens;
  - (d) etwaige einschlägige frühere Verstöße der verantwortlichen Stelle oder des Auftragsverarbeiters;
  - (e) die Bereitschaft zur Zusammenarbeit mit der aufsichtsführenden Stelle, um dem Verstoß abzuwehren und seine möglichen nachteiligen Auswirkungen zu mindern;
  - (f) die Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind;
  - (g) die Art und Weise, wie der Verstoß der aufsichtsführenden Stelle bekannt wurde;
  - (h) jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte wirtschaftliche Vorteile oder vermiedene Nachteile;
  - (i) die wirtschaftlichen Verhältnisse der verantwortlichen Stelle bzw. des Auftragsverarbeiters.
- (4) Bei Verstößen können im Einklang mit Absatz 3 Geldbußen von bis zu 100.000 EUR verhängt. Je nach den Umständen des Einzelfalls können diese zusätzlich oder anstelle von Maßnahmen nach § 28 Absatz 6 verhängt werden.

### **§ 30 Schadensersatz durch verantwortliche Stellen**

- (1) Jede Person, der wegen einer Verletzung der Regelungen dieser Ordnung ein Schaden entstanden ist, hat einen Anspruch auf Schadensersatz gegen die verantwortliche Stelle. Wegen eines Schadens, der kein Vermögensschaden ist, kann die betroffene Person eine angemessene Entschädigung in Geld verlangen.
- (2) Ein Verantwortlicher wird von der Haftung gemäß Absatz 1 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.
- (3) Auf das Mitverschulden der betroffenen Person ist § 254 des Bürgerlichen Gesetzbuches und auf die Verjährung sind die Verjährungsfristen für unerlaubte Handlungen des Bürgerlichen Gesetzbuches entsprechend anzuwenden.
- (4) Mehrere Ersatzpflichtige haften als Gesamtschuldner im Sinne des Bürgerlichen Gesetzbuches.
- (5) Vorschriften, nach denen Ersatzpflichtige in weiterem Umfang als nach dieser Vorschrift haften oder nach denen andere für den Schaden verantwortlich sind, bleiben unberührt.
- (6) Beansprucht eine betroffene Person Schadensersatz, so soll zunächst eine Anhörung des Betroffenen im vom Vorstand des Bundes einzuberufenden Vermittlungsausschuss, bestehend aus dem Datenschutzbeauftragten des Bundes, einem Vertreter der verantwortlichen Stelle, dem Verantwortlichen für Datenschutz für die verantwortliche Stelle und zwei Mitgliedern des Vorstandes des Bundes, mit dem Ziel einer Einigung stattfinden.

## **Kapitel 7 Vorschriften für besondere Verarbeitungssituationen**

### **§ 31 Verarbeitung personenbezogener Daten bei Dienst- und Arbeitsverhältnissen**

- (1) Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist.
- (2) Im Zusammenhang mit dem Verdacht auf Straftaten und Amtspflichtverletzungen, die durch Beschäftigte begangen worden sein sollen, insbesondere zum Schutz möglicher betroffener Personen, 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) Eine Offenlegung der Daten von Beschäftigten an Strafverfolgungsbehörden ist zulässig, wenn sie zur Aufdeckung einer Straftat oder Amtspflichtverletzung oder zum Schutz möglicher betroffener Personen erforderlich erscheint.

### **§ 32 Aufzeichnungen oder Übertragungen von Veranstaltungen**

- (1) Die Aufzeichnung oder Übertragung von Gottesdiensten oder anderen öffentlichen Veranstaltungen von Gemeinden des Bundes mittels audiovisueller Medien und die Veröffentlichung der Daten ist zulässig, wenn die Teilnehmenden durch geeignete Maßnahmen vorab über Art und Umfang der Aufzeichnung oder Übertragung informiert werden.

### **§ 33 Videoüberwachung öffentlich zugänglicher Räume**

- (1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie
  - (a) zur Aufgabenerfüllung oder zur Wahrnehmung des Hausrechts oder
  - (b) zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zweckeerforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Person überwiegen.
- (2) Der Umstand der Beobachtung und der Verantwortlich sind durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen.
- (3) Die Speicherung oder Verwendung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zweckes erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Person überwiegen.
- (4) Die gespeicherten Daten dürfen von der verantwortlichen Stelle an eine Strafverfolgungsbehörde übermittelt werden, falls diese die Daten anfordert.
- (5) Die Daten sind spätestens nach einem Monat oder unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

## **Kapitel 8 Schlussbestimmungen**

### **§34 Änderungen**

Zukünftige Änderungen an dieser Ordnung werden dem Präsidium vorgelegt und von diesem bestätigt.

### **§35 Inkrafttreten**

Diese Datenschutzordnung wurde vom Präsidium des Bundes Freikirchlicher Pfingstgemeinden KdÖR am 03.09.2015 beschlossen und von der Bundeskonferenz am 22.09.2015 verabschiedet und tritt am 22.09.2015 in Kraft.

Umfangreiche Änderungen an dieser Datenschutzordnung wurden vom Präsidium des Bundes Freikirchlicher Pfingstgemeinden KdÖR am 07.02.2018 beschlossen. Sie treten am 25.05.2018 in Kraft. Gleichzeitig treten die bisherigen Regelungen außer Kraft.

Weitere Änderungen an dieser Datenschutzordnung wurden vom Präsidium des Bundes Freikirchlicher Pfingstgemeinden KdÖR am 06.09.2018 beschlossen. Sie treten mit diesem Datum in Kraft.