



# Datenschutzordnung

**des Mülheimer Verbandes  
Freikirchlich-Evangelischer Gemeinden e.V. (MV)**

beschlossen vom Vorstand des MV am 3. Mai 2018

# Inhaltsverzeichnis

<b>Präambel</b> .....	<b>4</b>
<b>Kapitel 1: Allgemeine Bestimmungen</b> .....	<b>4</b>
§1 Zweck und Aufgabe des Datenschutzes.....	4
§2 Geltungsbereich dieser Datenschutzordnung .....	4
§3 Seelsorgegeheimnis und Amtsverschwiegenheit.....	4
§4 Verantwortlichkeit für die Durchführung des Datenschutzes .....	5
§5 Begriffsbestimmungen .....	5
<b>Kapitel 2: Verarbeitung personenbezogener Daten</b> .....	<b>7</b>
§6 Grundsätze .....	7
§7 Rechtmäßigkeit der Verarbeitung und Zweckänderung.....	7
§8 Einwilligung in die Verarbeitung.....	8
§9 Einwilligung Minderjähriger in Bezug auf elektronische Angebote .....	8
§10 Verarbeitung besonderer Kategorien personenbezogener Daten.....	8
§11 Offenlegung an freikirchliche, kirchliche und öffentliche Stellen .....	9
§12 Datenübermittlung an und in Drittländer oder an internationale Organisationen .....	9
<b>Kapitel 3: Rechte der betroffenen Person</b> .....	<b>10</b>
§13 Recht auf transparente Information und Auskunft der betroffenen Person.....	10
§14 Recht auf Berichtigung der personengebundenen Daten.....	10
§15 Recht auf Löschung der personengebundenen Daten .....	11
§16 Recht auf Einschränkung der Verarbeitung .....	11
§17 Recht auf Datenübertragbarkeit.....	12
§18 Recht auf Widerspruch und Beschwerde.....	12
<b>Kapitel 4: Pflichten der verantwortlichen Stellen</b> .....	<b>12</b>
§19 Wahrung des Datengeheimnisses.....	12
§20 Maßnahmen zur Durchführung des Datenschutzes und der IT-Sicherheit.....	12
§21 Verarbeitung von personenbezogenen Daten im Auftrag.....	13
§22 Verzeichnis von Verarbeitungstätigkeiten .....	13
§23 Informationspflicht bei der Datenerhebung .....	14
§24 Informationspflicht bei Berichtigung, Löschung oder Einschränkung der Verarbeitung .....	14
§25 Meldung von Verletzungen des Schutzes personenbezogener Daten.....	14
§26 Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person .....	15
§27 Datenschutz-Folgenabschätzung .....	15
<b>Kapitel 5: Verantwortliche für Datenschutz</b> .....	<b>16</b>
§28 Bestellung des Verantwortlichen für Datenschutz.....	16
§29 Pflichten der verantwortlichen Stellen gegenüber den Verantwortlichen für Datenschutz ....	17
§30 Aufgaben der Verantwortlichen für Datenschutz .....	17
§31 Beanstandungsrecht der Verantwortlichen für Datenschutz .....	17

<b>Kapitel 6: Datenschutzaufsicht</b> .....	<b>18</b>
§32 Bestellung des Datenschutzbeauftragten des MV.....	18
§33 Aufgaben des Datenschutzbeauftragten des MV.....	18
§34 Befugnisse des Datenschutzbeauftragten des MV.....	18
§35 Aufsichtsführende Stelle des MV für den Datenschutz.....	19
§36 Schadenersatz.....	19
§37 Sanktionen.....	19
<b>Kapitel 7: Schlussbestimmungen</b> .....	<b>21</b>
§38 Gleichstellung.....	21
§39 Übergangsfristen.....	21
§40 Änderungen dieser Datenschutzordnung.....	21
§41 Inkrafttreten dieser Datenschutzordnung.....	21

# Präambel

Diese Ordnung wird erlassen in Ausübung des verfassungsrechtlich garantierten Rechts des Mülheimer Verbandes Freikirchlich-Evangelischer Gemeinden e.V., als Freikirche seine Angelegenheiten selbstständig innerhalb der Schranken des für alle geltenden Gesetzes zu ordnen und zu verwalten.

Dieses Recht ist europarechtlich geachtet und festgeschrieben in Artikel 91 und Erwägungsgrund 165 Verordnung EU 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) sowie Artikel 17 (Vertrag über die Arbeitsweise der Europäischen Union – AEUV). In Wahrnehmung dieses Rechts stellt diese Ordnung den Einklang mit der Datenschutz-Grundverordnung für den Mülheimer Verband Freikirchlich-Evangelischer Gemeinden e.V. her und regelt die Datenverarbeitung des MV und der zu ihm gehörenden Mitglieder (rechtsfähige Gemeinden oder andere juristische Personen). Die Datenverarbeitung dient der Erfüllung des freikirchlichen Auftrags.

## Kapitel 1: Allgemeine Bestimmungen

### §1 Zweck und Aufgabe des Datenschutzes

- (1) Zweck der Datenschutzordnung ist es, den Einzelnen 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).

### §2 Geltungsbereich dieser Datenschutzordnung

- (1) Diese Datenschutzordnung gilt für den Mülheimer Verband Freikirchlich-Evangelischer Gemeinden e.V. mit seinen Einrichtungen, Arbeitsbereichen, für die von ihm eingesetzten Kommissionen und Beauftragungen, für die Mülheimer Verband Freikirchlich-Evangelischer Gemeinden gGmbH, an der er als Gesellschafter beteiligt ist und für die zu ihm gehörenden Mitglieder (rechtsfähige Gemeinden oder andere juristische Personen) mit deren Einrichtungen und Arbeitsbereichen, soweit letztere die Übernahme dieser Ordnung gegenüber dem MV in Textform und rechtsverbindlich angezeigt haben.
- (2) Diese Ordnung findet Anwendung auf die Verarbeitung personenbezogener Daten im Rahmen der Tätigkeit einer Stelle oder in deren Auftrag, unabhängig vom Ort der Verarbeitung.
- (3) Stellen des MV im Sinne dieser Datenschutzordnung sind alle in Absatz 1 aufgeführten.
- (4) Diese Ordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten.

### §3 Seelsorgegeheimnis und Amtsverschwiegenheit

- (1) Die Pastoren, Vikare und sonstigen pastoral arbeitenden Mitarbeiter des MV und seiner Mitglieder unterliegen dieser Datenschutzordnung.
- (2) Abweichend von Absatz (1) gehen die allgemein gültigen Bestimmungen über den Schutz des Beicht- und des Seelsorgegeheimnisses sowie über die Amtsverschwiegenheit der Pastoren, Vikare und sonstigen pastoral arbeitenden Mitarbeiter des MV und seiner Mitglieder den Vorschriften dieser Datenschutzordnung vor.
- (3) Unberührt bleibt das Recht der Pastoren, Vikare und sonstigen pastoral arbeitenden Mitarbeiter des MV, in Wahrnehmung ihres Seelsorgeauftrages eigene Aufzeichnungen zu führen und zu diesen Zwecken zu verwenden. Diese Aufzeichnungen dürfen dritten Personen nicht zugänglich sein.

#### §4 Verantwortlichkeit für die Durchführung des Datenschutzes

- (1) Für den Mülheimer Verband Freikirchlich-Evangelischer Gemeinden e.V. und für die Mülheimer Verband Freikirchlich-Evangelischer Gemeinden gGmbH gilt:
  - (a) Verantwortlich für die Umsetzung der Vorgaben dieser Datenschutzordnung sind für den Verein der geschäftsführende Vorstand des Vereins und für die gGmbH der Geschäftsführer der gGmbH.
  - (b) Verein und gGmbH gemeinsam bestellen nach eigenem Ermessen einen „Verantwortlichen für Datenschutz des MV“, der die Einhaltung des Datenschutzes im Sinne dieser Ordnung innerhalb der Stellen in Verein und gGmbH sicherstellt.
  - (c) Solange kein Verantwortlicher für Datenschutz des MV bestellt ist, stellt der Datenschutzbeauftragte des MV die Einhaltung des Datenschutzes im Sinne dieser Ordnung in Verein und gGmbH sicher.
- (2) Für zum Mülheimer Verband Freikirchlich-Evangelischer Gemeinden e.V. gehörende Mitglieder (rechtsfähige Gemeinden oder andere juristische Personen), die die Übernahme dieser Ordnung gegenüber dem MV in Textform und rechtsverbindlich angezeigt haben, gilt:
  - (a) Die Leitung des Mitglieds des MV sorgt eigenverantwortlich innerhalb ihrer jeweiligen Organisation für die Umsetzung der Vorgaben dieser Datenschutzordnung.
  - (b) Die Leitung des Mitglieds des MV bestellt, falls gefordert, einen „Verantwortlichen für Datenschutz des Mitglieds“, der die Einhaltung des Datenschutzes im Sinne dieser Ordnung innerhalb der Stellen des Mitglieds, dessen Arbeitszweigen und Einrichtungen sicherstellt. Falls kein Verantwortlicher bestellt werden muss, stellt die Leitung selbst die Einhaltung des Datenschutzes sicher.

#### §5 Begriffsbestimmungen

- (1) „*Personenbezogene Daten*“ sind Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen 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) „*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.
- (3) „*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.
- (4) „*Besondere Kategorien personenbezogener Daten*“ sind
  - (a) alle Informationen, aus denen religiöse oder weltanschauliche Überzeugungen einer natürlichen Person hervorgehen. Ausnahme: Für den Bereich der freikirchlichen Arbeit der verantwortlichen Stellen laut §2 Absatz (1) gelten die Zugehörigkeit zu einer Kirche oder Religionsgemeinschaft nicht als besondere Kategorie personenbezogener Daten;
  - (b) alle Informationen, aus denen die rassische und ethnische Herkunft, politische Meinungen oder die Gewerkschaftszugehörigkeit einer natürlichen Person hervorgehen;
  - (c) genetische Daten;
  - (d) biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person
  - (e) Gesundheitsdaten;
  - (f) Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.
- (5) „*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.

- (6) „Einschränkung der Verarbeitung“ ist die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken.
- (7) „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.
- (8) „Drittland“ ist ein Staat, in dem die europäischen Datenschutz-Grundverordnung keine Anwendung findet.
- (9) „Profiling“ bezeichnet jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.
- (10) „Pseudonymisierung“ ist 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.
- (11) „Anonymisierung“ ist die Verarbeitung personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig hohen Aufwand an Zeit, Kosten und Arbeitskraft einer betroffenen Person zugeordnet werden können.
- (12) „Genetische Daten“ sind 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.
- (13) „Biometrische Daten“ sind 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.
- (14) „Gesundheitsdaten“ sind 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.
- (15) „Dateisystem“ bezeichnet 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.
- (16) „IT-Sicherheit“ ist der Schutz der mit Informationstechnik verarbeiteten Daten insbesondere vor unberechtigtem Zugriff, vor unerlaubten Änderungen und vor der Gefahr des Verlustes, um deren Vertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten.
- (17) „Unternehmen“ ist eine natürliche oder juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personen-, Kapitalgesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen;
- (18) „Verantwortliche Stelle“ ist jede der in §1 genannten Stellen, die Daten für sich selbst speichert oder durch andere speichern lässt. Es ist möglich, zwei oder mehr verantwortliche Stellen als „Gemeinsam verantwortliche Stellen“ zusammenzufassen. 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.
- (19) „Verantwortlicher für Datenschutz“ ist der vom MV (Verein und gGmbH gemeinsam) für sich selbst oder der von einem Mitglied des MV für sich berufene Verantwortliche für Datenschutz.
- (20) „Datenschutzbeauftragter des MV“ ist der vom Vorstand des MV bestellte Beauftragte für den Datenschutz.

## Kapitel 2: Verarbeitung personenbezogener Daten

### §6 Grundsätze

- (1) Personenbezogene Daten sind im Geltungsbereich dieser Datenschutzordnung nach folgenden Grundsätzen zu verarbeiten:
  - (a) Rechtmäßigkeit, Verhältnismäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
  - (b) Zweckbindung: Personenbezogene Daten werden für festgelegte, eindeutige und legitime Zwecke erhoben. Sie dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Eine Weiterverarbeitung für im kirchlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt als vereinbar mit den ursprünglichen Zwecken.
  - (c) Datenminimierung: Die Verarbeitung personenbezogener Daten wird auf das dem Zweck angemessene und notwendige Maß beschränkt; personenbezogene Daten sind zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.
  - (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: Personenbezogene Daten werden in einer Form gespeichert, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Personenbezogene Daten dürfen länger gespeichert werden, soweit sie für die Zwecke des Archivs, der wissenschaftlichen und historischen Forschung sowie der Statistik verarbeitet werden.
  - (f) Integrität und Vertraulichkeit: Personenbezogene Daten werden in einer Weise verarbeitet, die eine angemessene Sicherheit gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Zerstörung oder unbeabsichtigter Schädigung.
- (2) Die verantwortliche Stelle muss die Einhaltung der Grundsätze nachweisen können (Rechenschaftspflicht).

### §7 Rechtmäßigkeit der Verarbeitung und Zweckänderung

- (1) Die Verarbeitung personenbezogener Daten 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, der der Verantwortliche unterliegt oder für die Wahrnehmung einer sonstigen Aufgabe erforderlich, die im rechtlichen freikirchlichen Interesse liegt.
  - (d) Die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen.
  - (e) Die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.
  - (f) Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn die betroffene Person 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) die betroffene Person eingewilligt hat;

- (d) wenn 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) 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;
- (f) Grund zu der Annahme besteht, dass andernfalls die Wahrnehmung des freikirchlichen Auftrages gefährdet würde;
- (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 freikirchlichen Auftrages erforderlich ist.

## **§8 Einwilligung in die Verarbeitung**

- (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.

## **§9 Einwilligung Minderjähriger in Bezug auf elektronische Angebote**

- (1) 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.

## **§10 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 erforderlich ist, damit die verantwortliche Stelle oder die betroffene Person die ihr aus dem Arbeits- und Dienstrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach freikirchlichem oder staatlichem 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 ist 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 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 erforderlich ist;



- (f) 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.
- (3) Die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen ist unter den Voraussetzungen von §7 dieser Datenschutzordnung zulässig, wenn dies das kirchliche oder staatliche Recht, das geeignete Garantien für die Rechte der betroffenen Personen vorsieht, zulässt.

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

- (1) Die Offenlegung von personenbezogenen Daten an Stellen des MV ist zulässig, wenn
  - (a) sie zur Erfüllung der in der Zuständigkeit der offenlegenden oder der empfangenden verantwortlichen Stelle liegenden Aufgaben erforderlich ist und
  - (b) die Voraussetzung der Rechtmäßigkeit des §7 vorliegen.
- (2) Die Verantwortung für die Zulässigkeit der Offenlegung trägt die offenlegende freikirchliche Stelle. Erfolgt die Offenlegung auf Ersuchen der empfangenden freikirchlichen Stelle, trägt auch diese die Verantwortung. In diesem Fall prüft die offenlegende verantwortliche Stelle nur, ob das Ersuchen im Rahmen der Aufgaben der empfangenden freikirchlichen Stelle liegt, es sei denn, dass besonderer Anlass zur Prüfung der Rechtmäßigkeit der Offenlegung besteht.
- (3) Die empfangende freikirchliche 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 §7 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 unverhältnismäßigem 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.

### **§12 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. §21). 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

### §13 Recht auf transparente Information 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 wurden, 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. Stellt die betroffene Person den Antrag elektronisch, so können die Informationen in einem gängigen elektronischen Format zur Verfügung gestellt werden.
- (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. Bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person kann die verantwortliche Stelle sich weigern, aufgrund des Antrags tätig zu werden oder ein angemessenes Entgelt verlangen.

### §14 Recht auf Berichtigung der personengebundenen Daten

- (1) Personenbezogene Daten sind auf Antrag der betroffenen Person zu berichtigen, wenn sie unrichtig sind.

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

## **§15 Recht auf Löschung der personengebundenen Daten**

- (1) Die betroffene Person hat das Recht, von der verantwortlichen Stelle zu verlangen, dass die betreffenden personenbezogenen Daten unverzüglich gelöscht werden. Der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern mindestens einer der folgenden Gründe zutrifft:
  - (a) Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
  - (b) Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.
  - (c) Die betroffene Person legt gemäß §18 Widerspruch gegen die Verarbeitung ein, und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor.
  - (d) Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
  - (e) Die Löschung der personenbezogenen Daten ist zur Erfüllung einer Verpflichtung nach dem Kirchenrecht des Bundes erforderlich, dem der Verantwortliche unterliegt.
- (2) Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er gemäß Absatz (1) zu deren Löschung verpflichtet, so trifft er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, um die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten anzustreben.
- (3) Die Absätze (1) und (2) gelten nicht,
  - (a) soweit die Verarbeitung erforderlich ist zur Ausübung des Rechts auf freie Meinungsäußerung und Information;
  - (b) zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach staatlichem oder kirchlichen Recht, dem der Verantwortliche unterliegt, erfordert;
  - (c) zur Wahrnehmung einer Aufgabe aufgrund eines wichtigen Interesses des MV;
  - (d) für im Interesse des MV liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke, soweit das in Absatz (1) genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt;
  - (e) oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.
- (4) 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.

## **§16 Recht auf Einschränkung der Verarbeitung**

- (1) 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 §18 eingelegt hat und noch nicht feststeht, ob die berechtigten Gründe der verantwortlichen Stelle gegenüber denen der betroffenen Person überwiegen.
- (2) Wurde die Verarbeitung der Daten gemäß Absatz (1) eingeschränkt, so dürfen sie – von ihrer Speicherung abgesehen – nicht mehr verarbeitet, insbesondere übermittelt oder sonst genutzt werden, es sei denn, dass die Nutzung zu wissenschaftlichen Zwecken, zur Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus sonstigen im überwiegenden Interesse der speichernden Stelle oder eines Dritten liegenden Gründen unerlässlich ist oder die betroffene Person der Nutzung zugestimmt hat.
- (3) 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.

### **§17 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.

### **§18 Recht auf Widerspruch und Beschwerde**

- (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 §7 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.
- (3) Wer darlegt, dass er bei der Verarbeitung seiner personenbezogenen Daten in seinen Rechten verletzt worden ist, kann sich damit an den für ihn zuständigen Verantwortlichen für Datenschutz wenden, wenn die zuständige verantwortliche Stelle nicht alsbald abhilft. Dies schließt auch die Möglichkeit einer Beschwerde bei der aufsichtsführenden Stelle ein.

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

### **§19 Wahrung des Datengeheimnisses**

- (1) Den mit dem Umgang von personenbezogenen Daten betrauten Personen ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten (Datengeheimnis). Das gilt insbesondere für das Offenlegen solcher Daten. Diese Personen sind bei der Aufnahme ihrer Tätigkeit auf die Wahrung der Vertraulichkeit und zur Beachtung des Datenschutzes durch die Abgabe einer Datenschutzerklärung zu verpflichten. Diese Verpflichtung besteht auch nach Beendigung ihrer Tätigkeit fort.

### **§20 Maßnahmen zur Durchführung des Datenschutzes und der IT-Sicherheit**

- (1) Die verantwortlichen 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 erfordern die Beachtung folgender Aspekte:

- (a) die Pseudonymisierung, die Anonymisierung und die Verschlüsselung personenbezogener Daten;
  - (b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
  - (c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
  - (d) Der Verantwortliche und gegebenenfalls der Auftragsverarbeiter treffen technische und organisatorische Maßnahmen, die geeignet sind, durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, zu verarbeiten. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere geeignet sein, dass personenbezogene Daten nicht ohne Eingreifen der verantwortlichen Stelle durch Voreinstellungen einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden;
  - (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.

## **§21 Verarbeitung von personenbezogenen Daten im Auftrag**

- (1) Werden geschützte personenbezogene Daten im Auftrag freikirchlicher Stellen gemäß §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 verantwortliche Stelle im Sinne des §4 Absatz (9).
- (2) Sofern die freikirchlichen Datenschutzbestimmungen auf den Auftragnehmer keine Anwendung finden, ist der Auftraggeber verpflichtet, sicherzustellen, dass der Auftragnehmer diese Bestimmungen beachtet und sich der Aufsicht des Datenschutzbeauftragten des MV unterwirft.
- (3) Für eine Auftragsverarbeitung in Drittländern gilt §12.

## **§22 Verzeichnis von Verarbeitungstätigkeiten**

- (1) Die verantwortlichen 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) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfängern in Drittländern oder internationalen Organisationen.
- (2) Auftragsverarbeiter, die nicht dieser Datenschutzordnung unterliegen, sind zur Einhaltung der EU Verordnung 2016/679 verpflichtet.
- (3) Das in den Absatz (1) genannte Verzeichnis ist schriftlich zu führen. Ein gängiges elektronisches Format ist zulässig.
- (4) Die verantwortliche Stelle stellt dem örtlich Verantwortlichen für den Datenschutz sowie dem Datenschutzbeauftragten des MV die Verzeichnisse auf Anfrage zur Verfügung.
- (5) Die in Absatz (1) und (2) genannten Pflichten gelten nicht für verantwortliche Stellen die weniger als 50 Mitglieder haben oder Auftragsverarbeiter, die weniger als 250 Mitarbeiter

beschäftigen. In diesen Fällen sind Verzeichnisse gemäß den Absätzen (1) und (2) nur hinsichtlich der Verfahren, die die Verarbeitung besonderer Kategorien personenbezogener Daten einschließen, zu erstellen.

### **§23 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 Verantwortlichen für Datenschutz des MV bzw. des betreffenden Mitglieds;
  - (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 soweit 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.

### **§24 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.

### **§25 Meldung von Verletzungen des Schutzes personenbezogener Daten**

- (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 soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, kann die verantwortliche Stelle diese Informationen unverzüglich schrittweise zur Verfügung stellen.
- (5) Die verantwortliche Stelle hat Verletzungen des Schutzes personenbezogener Daten zu dokumentieren. Die Dokumentation hat alle mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Abhilfemaßnahmen zu umfassen. Diese Dokumentation muss der aufsichtsführenden Stelle die Überprüfung der Einhaltung der Bestimmungen der Absätze (1) bis (4) ermöglichen.

## **§26 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.

## **§27 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) Eine Datenschutz-Folgenabschätzung ist insbesondere in folgenden Fällen erforderlich:
  - (a) bei systematischer und umfassender 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) bei umfangreicher Verarbeitung besonderer Kategorien von personenbezogenen Daten;
  - (c) bei systematischer umfangreicher Überwachung öffentlich zugänglicher Bereiche.

- (3) 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;
  - (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.
- (4) 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.
- (5) 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.
- (6) 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: Verantwortliche für Datenschutz

### §28 Bestellung des Verantwortlichen für Datenschutz

- (1) Der Mülheimer Verband Freikirchlich-Evangelischer Gemeinden e.V. und der Mülheimer Verband Freikirchlich-Evangelischer Gemeinden gGmbH bestellen gemeinsam nach eigenem Ermessen einen für sie Verantwortlichen für Datenschutz des MV.
  - (a) Solange kein Verantwortlicher bestellt ist, übernimmt der Datenschutzbeauftragte des MV die Aufgaben des Verantwortlichen.
  - (b) Die Bestellung des Verantwortlichen geschieht einvernehmlich durch den Vorstand des Vereins und durch die Geschäftsführung der gGmbH. Die Bestellung ist der aufsichtsführenden Stelle anzuzeigen.
  - (c) Der Verantwortliche darf nicht zur Geschäftsführung der gGmbH gehören.
  - (d) Der Verantwortliche darf nicht mit der Leitung der Datenverarbeitung in Verein oder gGmbH betraut sein.
  - (e) Der Verantwortliche darf ehrenamtlicher und angestellter Mitarbeiter des Vereins oder der gGmbH sein.
- (2) Mitglieder des MV (rechtsfähige Gemeinden oder andere juristische Personen), die die Übernahme dieser Ordnung gegenüber dem MV in Textform und rechtsverbindlich angezeigt haben, müssen einen Verantwortlichen für Datenschutz des Mitglieds bestellen.
  - (a) Die Pflicht zur Bestellung gilt nur dann, wenn beim Mitglied in der Regel mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten betraut sind, oder wenn das Mitglied mehr als 50 Mitglieder hat, oder wenn die Kerntätigkeit einer verantwortlichen Stelle des Mitglieds in der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten besteht.
  - (b) Die Bestellung des Verantwortlichen geschieht durch die rechtliche Leitung des Mitglieds. Die Bestellung ist der aufsichtsführenden Stelle in Textform anzuzeigen.
  - (c) Der Verantwortliche darf nicht mit der Leitung der Datenverarbeitung beim Mitglied betraut sein.
  - (d) Der Verantwortliche darf ehrenamtlicher und angestellter Mitarbeiter des Mitglieds sein. Er muss nicht zu den Mitgliedern des Mitglieds gehören.



- (e) Der Verantwortliche darf nur im Ausnahmefall und zeitlich begrenzt als Übergangsregelung ab Inkrafttreten dieser Ordnung bis längstens 31.12.2019 zur rechtlichen Leitung des Mitglieds gehören.
- (3) Als Verantwortlicher für Datenschutz darf nur eine Person bestellt werden, die die zur Erfüllung ihrer Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Sie ist auf die gewissenhafte Erfüllung ihres Auftrags zu verpflichten.
- (4) Die Bestellung kann sich auf mehrere verantwortliche Stellen erstrecken und somit für gemeinsam verantwortliche Stellen gelten.
  - (f) Legen zwei oder mehr verantwortliche Stellen gemeinsam die Zwecke und die Mittel zur Verarbeitung fest, so gelten sie als gemeinsam verantwortliche Stellen.
  - (g) Sie legen in einer formlosen Vereinbarung in transparenter Form fest, wer welche Aufgaben und Verpflichtungen gemäß dieser Datenschutzordnung erfüllt, soweit die jeweiligen Aufgaben der verantwortlichen Stellen nicht durch Rechtsvorschriften festgelegt sind.
- (5) Die Amtszeit des Verantwortlichen für Datenschutz beträgt fünf Jahre. Eine Wiederbestellung ist zulässig.
- (6) Der Verantwortliche für Datenschutz hat das Recht, seine Bestellung mit Frist von sechs Monaten zum Jahresende zu beenden.

### **§29 Pflichten der verantwortlichen Stellen gegenüber den Verantwortlichen für Datenschutz**

- (1) Die verantwortlichen Stellen unterstützen den Verantwortlichen für den Datenschutz bei der Erfüllung seiner Aufgaben und stellen die notwendigen Mittel zur Verfügung. Dies gilt insbesondere für Teilnahme an Fort- und Weiterbildungsveranstaltungen zur Erlangung und zur Erhaltung der erforderlichen Fachkunde.
- (2) Die verantwortlichen Stellen stellen sicher, dass der Verantwortliche für den Datenschutz ordnungsgemäß und frühzeitig bei allen mit dem Schutz personenbezogener Daten zusammenhängenden Fragen beteiligt wird.

### **§30 Aufgaben der Verantwortlichen für Datenschutz**

- (1) Die Verantwortlichen für Datenschutz 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.

### **§31 Beanstandungsrecht der Verantwortlichen für Datenschutz**

- (1) Stellt der Verantwortliche für Datenschutz bei der jeweiligen verantwortlichen Stelle Verstöße gegen die Datenschutzbestimmungen oder sonstige Mängel bei der Verarbeitung personenbezogener Daten fest, so beanstandet er dies gegenüber den verantwortlichen Stellen und fordert zur schriftlichen Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf.
- (2) Der Verantwortliche für Datenschutz kann von einer Beanstandung absehen oder auf eine Stellungnahme verzichten, wenn es sich um unerhebliche Mängel handelt.
- (3) Mit der Beanstandung kann der Verantwortliche für den Datenschutz Vorschläge zur Beseitigung der Mängel und zur sonstigen Verbesserung des Datenschutzes verbinden. Wird der Beanstandung nicht abgeholfen, so ist der Verantwortliche für Datenschutz befugt, sich an den Datenschutzbeauftragten des MV zu wenden. Dieser wiederum ist befugt, sich an den Vorstand des MV bzw. an die Leitung des betreffenden Mitglieds zu wenden.
- (4) Die gemäß den Vorschriften des Absatzes (1) abzugebende Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Beanstandung getroffen worden sind.

## Kapitel 6: Datenschutzaufsicht

### §32 Bestellung des Datenschutzbeauftragten des MV

- (1) Der Vorstand des MV bestellt den Datenschutzbeauftragten des MV.
- (2) Zum Datenschutzbeauftragten des MV darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Er ist auf die gewissenhafte Erfüllung seines Auftrags aufgrund einer Vereinbarung zu verpflichten.
- (3) Der Datenschutzbeauftragte des MV ist in Ausübung seines Auftrags an Weisungen nicht gebunden. Er darf nicht dem Vorstand des Vereins, der Geschäftsführung der gGmbH oder der rechtlichen Leitung eines Mitglieds angehören.
- (4) Der Datenschutzbeauftragte des MV untersteht nur der Rechts- und Dienstaufsicht, nicht jedoch der Fachaufsicht des Vorstandes des MV.
- (5) Der Datenschutzbeauftragte des MV 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 Datenschutzbeauftragte des MV darf, auch wenn er vom Auftrag entbunden ist, über Angelegenheiten, die der Verschwiegenheit unterliegen, ohne Genehmigung des Vorstands des MV weder vor Gericht noch außergerichtlich aussagen oder Erklärungen abgeben; eine gesetzlich begründete Pflicht, Straftaten anzuzeigen, bleibt unberührt.
- (6) Die Amtszeit des Datenschutzbeauftragten des MV beträgt mindestens zwei Jahre. Die Wiederbestellung ist zulässig.
- (7) Der Datenschutzbeauftragte des MV hat das Recht, seine Bestellung mit Frist von sechs Monaten zum Jahresende zu beenden.

### §33 Aufgaben des Datenschutzbeauftragten des MV

- (1) Der Datenschutzbeauftragte des MV wacht über die Einhaltung der Vorschriften über den Datenschutz. Zu diesem Zwecke kann er Empfehlungen zur Verbesserung des Datenschutzes geben und die verantwortlichen Stellen in Fragen des Datenschutzes beraten. Auf Anforderung der Leitungsorgane des MV bzw. der seiner Mitglieder hat der Datenschutzbeauftragte des MV Gutachten zu erstellen und Berichte zu geben.
- (2) Die verantwortlichen Stellen sind verpflichtet, den Datenschutzbeauftragten des MV bei der Erfüllung seiner Aufgaben zu unterstützen. Ihm 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; ihm ist Zutritt zu den Räumen zu gewähren, in denen Daten verarbeitet werden.

### §34 Befugnisse des Datenschutzbeauftragten des MV

- (1) Stellt der Datenschutzbeauftragte des MV für den Datenschutz Verstöße gegen die Datenschutzbestimmungen oder sonstige Mängel bei der Verarbeitung personenbezogener Daten fest, so beanstandet er dies gegenüber den verantwortlichen Stellen und fordert zur schriftlichen Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf.
  - (a) Der Datenschutzbeauftragte des MV kann von einer Beanstandung absehen oder auf eine Stellungnahme verzichten, wenn es sich um unerhebliche Mängel handelt.
  - (b) Mit der Beanstandung kann der Datenschutzbeauftragte des MV Vorschläge zur Beseitigung der Mängel und zur sonstigen Verbesserung des Datenschutzes verbinden. Wird der Beanstandung nicht abgeholfen, so ist er befugt, sich an den Vorstand des MV zu wenden.
  - (c) Die gemäß den Vorschriften des Absatzes (1) abzugebende Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Beanstandung des Datenschutzbeauftragten des MV getroffen worden sind.
- (2) Um einen rechtmäßigen Zustand wiederherzustellen oder eine drohende Verletzung des Schutzes personenbezogener Daten abzuwenden, ist der Datenschutzbeauftragte des MV befugt, anzuordnen:
  - (a) Verarbeitungsvorgänge auf bestimmte Weise und in einem bestimmten Zeitraum mit dieser Datenschutzordnung in Einklang zu bringen;
  - (b) Verarbeitungsvorgänge vorübergehend oder dauerhaft zu beschränken oder zu unterlassen;

- (c) die Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation auszusetzen;
- (d) personenbezogene Daten zu berichtigen, zu sperren oder zu löschen;
- (e) die von einer Verletzung des Schutzes personenbezogener Daten betroffene Person entsprechend zu benachrichtigen;
- (f) dem Antrag der betroffenen Person zu entsprechen.

### **§35 Aufsichtsführende Stelle des MV für den Datenschutz**

- (1) Der Datenschutzbeauftragte des MV nimmt die aufsichtsführende Stelle innerhalb des MV wahr.
- (2) Die Arbeitsweise der aufsichtsführenden Stelle wird in einer eigenen Geschäftsordnung geregelt. Diese wird durch die aufsichtsführende Stelle und den geschäftsführenden Vorstand des Mülheimer Verbandes Freikirchlich-Evangelischer Gemeinden e.V. einvernehmlich beschlossen.
- (3) Zu den Aufgaben der aufsichtsführenden Stelle gehören auf jeden Fall:
  - (a) Die aufsichtsführende Stelle soll die Verantwortlichen für Datenschutz u. a. durch die Bereitstellung von Materialien zur Erhaltung der Fachkunde in geeigneter Form in der Wahrnehmung ihrer Aufgaben unterstützen.
  - (b) Die aufsichtsführende Stelle soll 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.
  - (c) Die aufsichtsführende Stelle soll mit anderen Datenschutzaufsichten vor allem für den Informations- und Fachaustausch zusammenarbeiten, insbesondere mit Aufsichtsorganen aus dem freikirchlichen Bereich.
- (4) Der aufsichtsführenden Stelle werden durch den MV (Verein und gGmbH) und durch die Mitglieder des MV (rechtsfähige Gemeinden oder andere juristische Personen), die die Übernahme dieser Ordnung gegenüber dem MV in Textform und rechtsverbindlich angezeigt haben, die Finanzmittel zur Verfügung gestellt, die sie benötigt, um ihre Aufgaben und Befugnisse effektiv wahrnehmen zu können. Die Finanzmittel sind in einem eigenen Haushalt oder als Teil eines Gesamthaushaltes gesondert auszuweisen und zu verwalten. Näheres regelt die Geschäftsordnung.

### **§36 Schadenersatz**

- (1) Jede Person, der wegen einer Verletzung der Regelungen dieser Datenschutzordnung ein Schaden entstanden ist, hat einen Anspruch auf Schadenersatz gegen die verantwortliche Stelle. Wegen eines Schadens, der nicht 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 ein Betroffener Schadenersatz, so soll zunächst eine Anhörung des Betroffenen im vom Vorstand des MV einzuberufenden Vermittlungsausschuss, bestehend aus dem Datenschutzbeauftragten des MV, einem Vertreter der verantwortlichen Stelle, dem Verantwortlichen für Datenschutz für die verantwortliche Stelle und zwei Mitgliedern des Vorstandes des MV, mit dem Ziel einer Einigung stattfinden.

### **§37 Sanktionen**

- (1) Verstößt eine verantwortliche Stelle oder Auftragsverarbeiter, der Stelle des MV oder Stelle eines Mitglieds ist, vorsätzlich oder fahrlässig gegen Bestimmungen dieser Datenschutzordnung, so kann die aufsichtsführende Stelle Geldbußen verhängen oder für den Wiederholungsfall androhen. Die Verhängung einer Geldbuße darf nur in Textform inklusive einer Begründung erfolgen.

- (2) Die aufsichtsführende Stelle stellt sicher, dass die Verhängung einer Geldbuße in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.
- (3) Geldbußen werden je nach den Umständen des Einzelfalls verhängt. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall Folgendes gebührend berücksichtigt:
  - (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) der Grad der Verantwortung der verantwortlichen Stelle oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß §20 getroffenen technischen und organisatorischen Maßnahmen;
  - (e) etwaige einschlägige frühere Verstöße der verantwortlichen Stelle oder des Auftragsverarbeiters;
  - (f) die Bereitschaft zur Zusammenarbeit mit der aufsichtsführenden Stelle, um dem Verstoß abzuweichen und seine möglichen nachteiligen Auswirkungen zu mindern;
  - (g) die Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind;
  - (h) die Art und Weise, wie der Verstoß der aufsichtsführenden Stelle bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang die verantwortliche Stelle oder der Auftragsverarbeiter den Verstoß mitgeteilt hat;
  - (i) die Einhaltung der früher gegen die verantwortliche Stelle oder den Auftragsverarbeiter in Bezug auf denselben Gegenstand angeordneten Maßnahmen, sofern solche Maßnahmen angeordnet wurden;
  - (j) ob die verantwortliche Stelle eine wirtschaftliche Tätigkeit ausübt (im Sinne des §5 Nummer 17) oder ob sie ohne jegliche Gewinnerzielungsabsicht arbeitet;
  - (k) jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.
- (4) Verstößt eine verantwortliche Stelle 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.
- (5) Bei Verstößen werden unter Berücksichtigung von Absatz (3) Geldbußen von bis zu 4% des Gesamtjahresumsatzes der betreffenden Organisation bzw. des Unternehmens, höchstens aber 50.000 Euro verhängt. Bei Organisationen, die ohne jegliche Gewinnabsicht arbeiten, sind Geldbußen auf höchstens 20.000 Euro begrenzt.
- (6) Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich oder anstelle von Maßnahmen nach §34 Absatz (2) verhängt.
- (7) Die aufgrund von Geldbußen vereinnahmten Gelder fließen in den Haushalt der aufsichtsführenden Stelle.
- (8) Die verantwortlichen Stellen, die mit einer Geldbuße sanktioniert werden, haben das Recht, Beschwerde beim Vorstand des MV einzulegen. Dieser beruft für den jeweils zu klärenden Fall einen Vermittlungsausschuss ein, bestehend aus dem Datenschutzbeauftragten des MV, einem Vertreter der verantwortlichen Stelle, dem Verantwortlichen für Datenschutz für die verantwortliche Stelle und zwei Mitgliedern des Vorstands des MV. Der Vermittlungsausschuss entscheidet mit einfacher Mehrheit unter Berücksichtigung von Absatz (3) über die Bestätigung oder Veränderung der Sanktion. Gegen diesen Beschluss, der in Textform inklusive einer Begründung dargelegt werden muss, können keine Rechtsmittel eingelegt werden.

## **Kapitel 7: Schlussbestimmungen**

### **§38 Gleichstellung**

Wird in dieser Datenschutzordnung die männliche sprachliche Form der Personenbeschreibung verwendet, erlaubt dieses keinen Rückschluss auf das Geschlecht einer Person.

### **§39 Übergangsfristen**

Die Erstellung der Verfahrensverzeichnisse nach §20 dieser Datenschutzordnung hat bis zum 30. Juni 2019 zu erfolgen.

### **§40 Änderungen dieser Datenschutzordnung**

Der Vorstand des MV ist berechtigt, die MV-Datenschutzordnung zu ändern und erneut zu beschließen.

### **§41 Inkrafttreten dieser Datenschutzordnung**

Diese Datenschutzordnung wurde aufgrund der Beauftragung durch die Mitgliederversammlung des Mülheimer Verbandes Freikirchlich-Evangelischer Gemeinden e.V. (MV) vom 19. April 2018 vom Vorstand des MV am 3. Mai 2018 beschlossen und tritt somit an diesem Tag in Kraft.