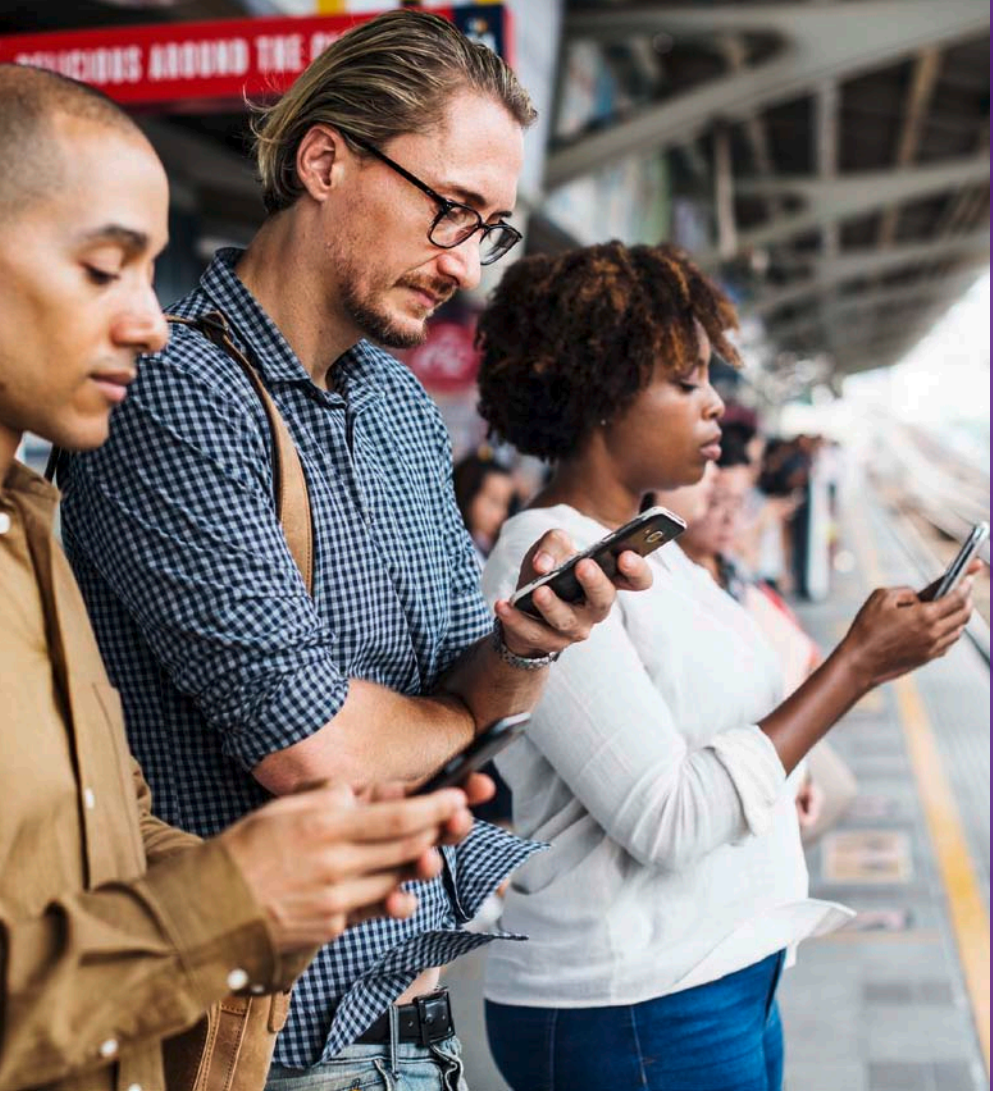


# Datenschutz

für kirchliche Öffentlichkeitsarbeit in der
Evangelisch-lutherischen Landeskirche Hannovers

EVANGELISCH-LUTHERISCHE
LANDESKIRCHE HANNOVERS

Version 1.1
Stand: 24.01.2019

Große Textteile dieser Broschüre wurde uns freundlicherweise von der Evangelischen Kirche in Hessen und Nassau zur Verfügung gestellt. Autoren der Textteile: Brigit Arndt, Hans Genthe, Matthias Hartmann, Christian Zappe, Sabine Langmaack, Sebastian Heydendahl.

Fassung für die Landeskirche Hannovers
Redaktion: Kay Oppermann, Evangelische Medienarbeit, Digitale Agentur
Juristische Beratung: OKRin Annegret von Collande, Referat 77, Landeskirchenamt
Satz: EMA, Sybille Felchow
Fotos: Pixabay.com; rawpixel, Foundry, kconcha, fancycrave1, LoboStudioHamburg

Die Informationen auf den folgenden Seiten sollen vor allem in der Evangelisch-lutherischen Landeskirche Hannovers mit Öffentlichkeits- und Pressearbeit beschäftigten haupt- und ehrenamtlichen Mitarbeitenden helfen, die Datenschutzvorgaben bei ihrer Arbeit einzuhalten.

Diese Information gibt einen ersten Überblick, welche Aufgaben und Pflichten in der Öffentlichkeits- und Pressearbeit zum Schutz der personenbezogenen Daten im Rahmen des neuen Datenschutzgesetzes umgesetzt werden müssen.

## Vorwort

**Liebe Leserinnen und Leser,**

viele von Ihnen haben sich sicher in den letzten Jahren mit dem Thema Datenschutz nur am Rande beschäftigt. Allgemein bekannt ist: Wichtige Dokumente lässt niemand offen herum liegen, wichtige Protokolle gehören nicht auf WhatsApp und Newletter dürfen nicht ungefragt versendet werden. Vieles, was darüber hinaus jedoch bereits längst gesetzlich geregelt ist, hat die kirchliche Öffentlichkeitsarbeit viel weniger beschäftigt, als Fragen des Urheberrechts, des Impressums oder der Bildnachweise. Nun schwebt seit einigen Wochen die schöne Abkürzung DSGVO wie ein Damoklesschwert über allen engagierten, beruflich wie ehrenamtlich, in der Kirche Mitarbeitenden, die analog oder digital mit Daten zu tun haben. Die wichtigste Nachricht dazu: Die Datenschutzgrundverordnung (DSGVO) hat für die Evangelische Kirche keine Gültigkeit. Das Datenschutzgesetz der EKD (vgl. Anhang) stimmt in Bezug auf die relevanten Punkte mit staatlichen Regelungen zwar überein. Jedoch verhängen im schlimmsten Fall nicht staatliche Behörden in der Kirche Bußgelder, sondern der Datenschutzbeauftragte der EKD. Alle Informationen über die ungaublich hohen Strafzahlungen bis zu 20 Mio Euro betreffen den kirchlichen Rahmen nicht. Viel wichtiger jedoch: Die kirchliche Datenschutzbehörde hat kein Interesse daran, systematisch kirchliche Stellen abzumahnen.

Ein weiteres falsches Gerücht: Fotos im öffentlichen Kontext seien kaum noch möglich. Ein schriftliches Einverständnis eines jeden Fotografierten müsse eingeholt werden. Hier urteilt das Bundesministerium des Inneren: „Das Anfertigen von Fotografien wird sich auch zukünftig auf eine – wie bislang schon – jederzeit widerrufbare Einwilligung oder alternative Erlaubnistatbestände wie die Ausübung berechtigter Interessen (Art. 6 Abs. 1 lit. f) DS-GVO) stützen können. Diese Erlaubnistatbestände (nach geltender Rechtslage Art. 7 der geltenden EU-Datenschutz-Richtlinie 95/46/EG i.V.m. den nationalen Umsetzungsgesetzen) decken seit vielen Jahren datenschutzrechtlich die Tätigkeit von Fotografen ab und werden in Art. 6 DS-GVO fortgeführt. Die Annahme, dass die DS-GVO dem Anfertigen von Fotografien entgegenstehe, ist daher unzutreffend."

Wir freuen uns, wenn Sie sich aufgrund dieses Heftes, dessen Text uns in großen Teilen von der Evangelischen Kirche in Hessen und Nassau überlassen wurde, ein Bild von der aktuellen Situation im Datenschutz machen.

*Herzliche Grüße aus der Evangelischen Medienarbeit sendet Ihnen*

*Kay Oppermann*
*Leiter Digitale Agentur*

**https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2018/04/faqs-datenschutz-grundverordnung.html**

## Hintergrund und allgemeine Informationen zum Datenschutz

Im Bereich der Evangelisch-lutherischen Landeskirche Hannovers ist das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) die geltende rechtliche Grundlage. Aufgrund der ab dem 25. Mai 2018 geltenden neuen EU Datenschutzverordnung (EU-DSGVO) wurde auch das EKD Datenschutzrecht aktualisiert und an EU-Standards angepasst. Die Aufsicht über die Einhaltung der Vorschriften zum Datenschutz obliegt im kirchlichen Bereich dem Beauftragten für den Datenschutz der EKD. Für die Evangelisch-lutherische Landeskirche Hannovers ist die Außenstelle Nord zuständig:
Regionalverantwortliche für die
Datenschutzregion Nord.
Sandra Coors
+49 (0)511 169335-0
Fax +49 (0)511 169335-20
E-Mail: nord@datenschutz.ekd.de

Die neue Fassung des DSG-EKD trat am 24. Mai 2018 in Kraft und ist auf der Webseite der EKD verfügbar.[1]

1 https://www.kirchenrecht-ekd.de/document/39740

# Inhaltsverzeichnis


Vorwort . . . 3
Hintergrund und allgemeine Informationen zum Datenschutz . . . 4
Inhaltsverzeichnis . . . 5

**1 Regelungen aus der kirchlichen Verwaltung übernehmen . . . 6**
1.1 Warum kirchlicher Datenschutz? . . . 6
1.2 Was sind personenbezogene Daten? . . . 6
1.3 Was sind besondere Kategorien von personenbezogenen Daten? . . . 7
1.4 Was hat sich am 24. Mai 2018 geändert? . . . 7
1.5 Wann dürfen Daten verarbeitet werden? . . . 9
1.6 Welche Auskunfts- und Informationsrechte haben Betroffene? . . . 10

**2 Datenschutz im Gemeindebrief . . . 11**
2.1 Veröffentlichung im gedruckten Gemeindebrief . . . 11
2.2 Veröffentlichung des Gemeindebriefes im Internet . . . 11
2.3 Kontaktdaten . . . 12
2.4 Fotos und Videos . . . 13

**3 Urheberrecht . . . 13**
3.1. Einwilligung . . . 14

**4 Mailings – speziell Fundraisingmailings . . . 14**
4.1 Vertrag mit Dienstleistern – Datenverarbeitung im Auftrag . . . 15
4.2 Speicherung, Verschlüsselung, Löschung personenbezogener Daten für Mailings . . . 15

**5 Webseiten / Internet . . . 16**
5.1 Pflicht zu Impressum und Datenschutzerklärung . . . 16
5.2 Cookie Richtlinie . . . 16
5.3 Webtracking-Tools . . . 16
5.4 Social Media Plugins . . . 16
5.5 Kontaktformulare – verschlüsseln? . . . 17

**6 Newsletter und Mailings . . . 18**
6.1 Newsletter als Auftragsverarbeitung . . . 18
6.2 Arbeiten mit altem Empfängerbestand ohne Opt In . . . 18
6.3 Neue Empfänger rechtssicher anlegen . . . 19
6.4 Schutz der Daten beim Versand . . . 29

**7 Social Media . . . 20**
7.1 Personale Kommunikation des Evangeliums . . . 20
7.2 Die Rolle der digitalen Dienstleister sozialer Medien . . . 21
7.3 Privatsphäre-Einstellungen . . . 21
7.4 Fotos, Videos, Musik . . . 21
7.5 Facebook . . . 21
7.6 WhatsApp . . . 22
7.7 YouTube . . . 23
7.8 Doodle . . . 23

**8 Cloud-Computing . . . 24**

**9 Streaming von Andachten oder Gottesdiensten . . . 24**

**10 Link-Tipps . . . 25**

**Anlagen . . . 26**
A1 EKD Datenschutzgesetz
A2 Musterdatenschutzerklärung für die Webseite
A3 Muster für ein Impressum
A4 Mustertext Einwilligungserklärung für Fotos
A5 Mustervertrag Auftragsdatenvereinbarung EKD
A6 Muster Einwilligung zur Veröffentlichung von Daten auf der Webseite

## 1 Regelungen aus der kirchlichen Verwaltung übernehmen

Im neuen EKD-Datenschutzgesetz nimmt unmittelbar auf die Medien nur Paragraf 51 Bezug („Verarbeitung personenbezogener Daten durch die Medien"), der keine Veränderung gegenüber dem bisherigen Recht darstellt. Um für die Öffentlichkeitsarbeit Insellösungen zu vermeiden, müssen Verfahren aus der Verwaltung der Gemeinden oder des Kirchenkreises soweit wie möglich übernommen werden. Dies gilt beispielsweise für Regelungen, wie nicht mehr benötigte personenbezogene Daten gelöscht werden, wie man Informationspflichten nachkommen kann und bei der Umsetzung für IT-Sicherheit. Also: am besten setzen sich die Verantwortlichen für Öffentlichkeitsarbeit mit ihrer Verwaltung zusammen, um zu vereinbaren, wie solche Regelungen übernommen werden können.

### 1.1 Warum kirchlicher Datenschutz

Die EKD Webseite[2] zum Thema Datenschutz beschreibt es so: Die allem kirchlichen und staatlichen Handeln zu Grunde liegende Menschenwürde wirkt sich auf alle Lebensbereiche aus. Eine Konsequenz ist das Grundrecht auf informationelle Selbstbestimmung aus Artikel 1 Abs. 1 und Artikel 2 Abs. 1. Das bedeutet, dass jeder Mensch grundsätzlich selbst darüber bestimmen kann, welche Daten über ihn erhoben werden. Somit muss beim Umgang mit personenbezogenen Daten auf deren Schutz geachtet werden. Für die evangelische Kirche hat der Schutz der Daten von Gemeindegliedern und Mitarbeitenden und der Daten von Menschen, die kirchliche Einrichtungen in Anspruch nehmen, vor dem Hintergrund des kirchlichen Auftrags und des christlichen Menschenbildnisses von jeher eine besondere Bedeutung.

### 1.2 Was sind personenbezogene Daten

Personenbezogene Daten sind ein Kernbegriff des Datenschutzes. Hierunter sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zu verstehen. Nur dann, wenn Daten einen Bezug zu einem Menschen aufweisen, sich auf eine identifizierbare persönliche Person beziehen, kommt das Datenschutzrecht zur Anwendung. Das können Mitarbeiter-, Nutzer- oder Kundendaten sein – egal ob sie digital oder in Papierform erfasst werden.

Beispiele für personenbezogene Daten sind Name, Geburtstag, Adresse, Telefon- und Faxnummern, Kfz-Kennzeichen, Kontonummer, Versicherungs- oder Personalnummern, Berufsangaben oder Einkommensdaten.

**Beispiele für personenbezogene Daten:**

- Name und Identifikationsmerkmale (z.B. Geburtsdatum, Namenszusätze, Ausweisnummer)
- Kontaktdaten (z.B. Postanschrift, E-Mail-Adresse, Telefonnummer)
- Körperliche Merkmale (z.B. Größe, Gewicht, Haarfarbe, genetischer
- Fingerabdruck, Krankheiten, Drogenkonsum

2 https://datenschutz.ekd.de

- Bewerber- und Mitarbeiterdaten (beruflicher Werdegang, Zeugnisse, Fotos, Bankdaten etc.)
- Geistige Zustände (z.B. Wünsche, Einstellungen, Überzeugungen, Geschäftsfähigkeit)
- Verbindungen und Beziehungen (z.B. Verwandtschafts- und Freundschaftsbeziehungen, Arbeitgeber)
- Weitere Daten (z.B. Standortdaten, Nutzungsdaten, Handlungen, Äußerungen, Werturteile etc.)

Auch IP-Adressen – also die Adresse eines Computers oder Servers – und natürlich Login-Daten zählen zu personenbezogenen Daten. Denn sie ermöglichen es, eine Verbindung zwischen IP-Adresse und Nutzernamen herzustellen. Damit ist auch jeder Seitenanbieter von den Datenschutz-Verpflichtungen betroffen.

Liegen anonymisierte Daten vor, handelt es sich nicht um personenbezogene Daten, weil die Bezugsperson weder identifiziert noch identifizierbar ist. Bei pseudonymisierten Daten ist das anders: Mit dem entsprechenden Zusatzwissen ist es möglich, die Bezugsperson zu bestimmen und es gilt das Datenschutzgesetz.

### 1.3 Was sind besondere Kategorien von personenbezogenen Daten

Beim Umgang mit besonderen Kategorien von personenbezogenen Daten gibt es nochmals gesteigerte Auflagen im Bereich des Datenschutzes. Dazu gehören personenbezogenen Daten, aus denen rassische und ethnische Herkunft, politische Meinungen, Gewerkschaftszugehörigkeit, sowie Informationen über die Verarbeitung von genetischen Daten, biometrischen Daten, Gesundheitsdaten oder Daten zum Sexualleben einer Person. Also letztlich Daten, die als besonders sensibel gelten und mit denen andere Menschen leicht diskriminiert werden könnten.

Werden solche Daten verarbeitet, muss grundsätzlich immer eine Risikoanalyse durchgeführt werden, die Folgen der vorgesehenen Datenverarbeitung für den Schutz der personenbezogenen Daten hat, sowie ein Verfahrensverzeichnis gepflegt werden.

### 1.4 Was hat sich am 24. Mai 2018 geändert?

Für den Wirkungsraum der Evangelischen Kirchen tritt das der EU-DSVGO angepasste EKD Datenschutzgesetz am 24. Mai 2018 in Kraft. Ab 25. Mai 2018 gilt in allen Mitgliedsstaaten der Europäischen Union unmittelbar die Datenschutzgrundverordnung (DSGVO) der Europäischen Union (EU). Durch das neue EU-Recht wird in Deutschland das bisherige Bundesdatenschutzgesetz (BDSG) abgelöst. Ziel dieser neuen Gesetzgebung ist es, ein einheitliches Datenschutzrecht innerhalb der EU herzustellen.

Mit dem neuen DSG-EKD, das konform ist mit der DSGVO, werden vor allem die Rechte und Kontrollmöglichkeiten derjenigen gestärkt, deren personenbezogene Daten verarbeitet werden (Betroffene). Wesentliche Elemente des bisherigen Datenschutzes[3] bleiben erhalten. Viele datenschutzrelevante Sachverhalte sind seit langem durch kirchliche Rechtsvorschriften geregelt. Kirchliche Einrichtungen müssen sich mit der Reform beschäftigen und den Datenschutz überprü-

3 https://www.wbs-law.de/it-recht/datenschutzrecht/was-ist-datenschutz/

fen, denn die neuen Regelungen gehen über die alten datenschutzrechtlichen Regeln hinaus.

Die geltenden Grundsätze für die datenschutzkonforme Datenverarbeitung bleiben weiterhin gültig: Rechtmäßigkeit, Zweckbindung, Datenminimierung (Datensparsamkeit), Richtigkeit, zeitliche Beschränkung (Speicherbegrenzung), Integrität und Vertraulichkeit sowie eine Rechenschaftspflicht der Verantwortlichen für die Einhaltung dieser Grundsätze.

Die Rechte der Nutzerinnen und Nutzer werden durch neue Transparenz- und Informationspflichten der datenverarbeitenden Stellen gestärkt. Betroffene sollen leichter Zugang zu ihren Daten und der Information über deren Nutzung haben. Außerdem wird das bislang nur gerichtlich konstruierte „Recht auf Vergessenwerden", also der Anspruch auf Löschung personenbezogener Daten, im Gesetz geregelt.

**Wichtige Änderungen sind u.a.:**

- Es werden sowohl die Rechte der Betroffenen als auch der Aufsichtsbehörden gestärkt (Recht auf Auskunft, auf Berichtigung, auf Löschung, auf Einschränkung der Verarbeitung, auf Datenübertragbarkeit und Widerspruch – § 19-25 DSG-EKD)[4]
- Verantwortliche Stellen müssen künftig in der Lage sein, die Einhaltung des Datenschutzes nachzuweisen (Rechenschaftspflicht § 5 Abs. 2 DSG-EKD)[5]
- Einführung des Rechts auf Datenübertragbarkeit (§ 24 DSG-EKD)[6]
- Einführung eines Verzeichnisses von Verarbeitungstätigkeiten (§31 DSG-EKD)[7] – zu führen von jeder verantwortlichen Stelle, die mehr als 250 Beschäftigte hat. Organisationen, die weniger als 250 Beschäftigte haben, müssen nur Verzeichnisse hinsichtlich der Verfahren führen, die die Verarbeitung von besonderen Kategorien personenbezogener Daten beinhalten.
- Einführung der Datenschutz-Folgenabschätzung statt der Vorabkontrolle (§ 34 DSG-EKD)[8]
- Einführung von Melde- und Benachrichtigungspflichten in Fällen von Datenpannen an die Datenschutzaufsicht (§ 32 DSG-EKD) und betroffene Personen (§ 33 DSG-EKD)[9]

Neben bereits bekannten Pflichten stellt der neue Datenschutz auch weitergehende Anforderungen: Neu ist beispielsweise die Pflicht, elektronische Geräte und Anwendungen datenschutzfreundlich voreinzustellen. Ebenfalls neu eingeführt wird die Pflicht zur Datenschutz-Folgenabschätzung bei besonderen Risiken für die erhobenen Daten, beispielsweise durch neue Technologien. Anders als im staatlichen Bereich verhängt die kirchliche Datenschutzaufsichtsbehörde, der Beauftragte für den Datenschutz der EKD,

4 https://www.kirchenrecht-ekd.de/document/39740#s47000083

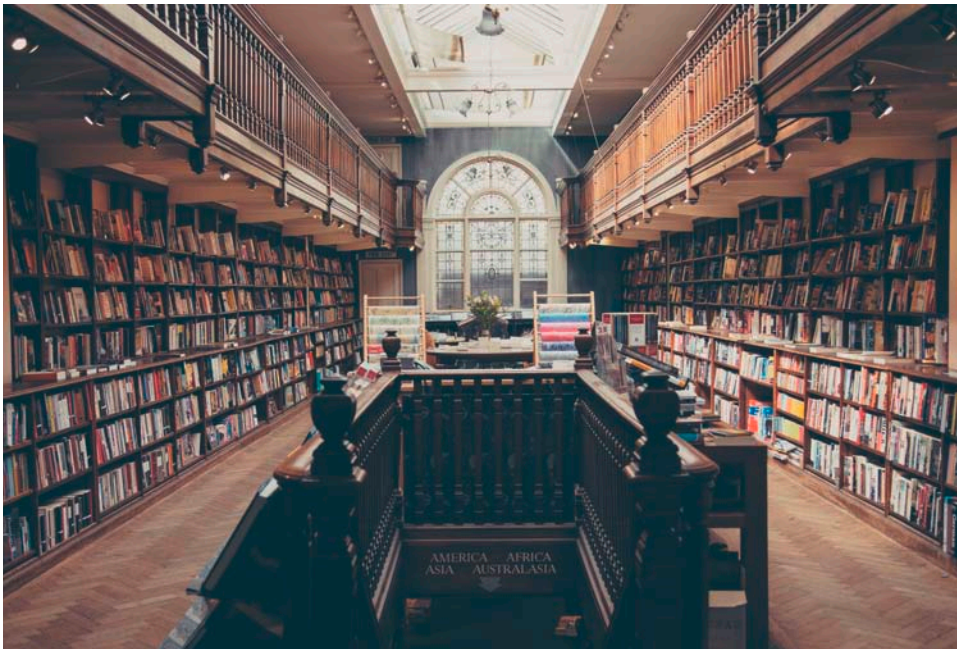
5 https://www.kirchenrecht-ekd.de/document/39740#s47000066

6 https://www.kirchenrecht-ekd.de/document/39740#s47000088

7 https://www.kirchenrecht-ekd.de/document/39740#s47000098

8 https://www.kirchenrecht-ekd.de/document/39740#s47000101

9 https://www.kirchenrecht-ekd.de/document/39740#s47000099




Geldbußen nur dann, wenn eine kirchliche Stelle als Unternehmen am Wettbewerb teilnimmt.

### 1.5 Wann dürfen Daten verarbeitet werden?

Schon vorher war es so, dass kirchliche Einrichtungen auf Verlangen der betroffenen Person bei den Datenerhebungsvorgängen informieren mussten. Laut der neuen DSGVO müssen die betroffenen Personen bereits bei Datenerhebungsvorgängen informiert werden. Das kirchliche Recht sieht eine entsprechende Informationspflicht erst dann vor, wenn die betroffene Person es verlangt. In vielen Fällen dürfte es sich aber anbieten, automatisch bereits bei der Datenerhebung über die Datenverarbeitungsvorgänge gemäß § 17 DSG-EKD zu informieren. Neu ist auch, dass nicht nur der Zweck, sondern auch die Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten angegeben werden muss. Generell gilt der Grundsatz „Verbot mit Erlaubnisvorbehalt“, das bedeutet: Die Verarbeitung personenbezogener Daten ist grundsätzlich verboten und nur in den folgenden Fällen erlaubt.

**Die Erlaubnis gilt:**

- Wenn eine Rechtsvorschrift die Verarbeitung erlaubt,
- wenn eine Einwilligung des Betroffenen vorliegt,
- wenn die Verarbeitung für die Erfüllung eines Vertrags oder zur Durchführung vorvertraglicher Maßnahmen z. B. Bewerbung erforderlich ist,
- wenn ein berechtigtes Interesse vorliegt (z.B. Kirche informiert ihre Mitglieder

über Gottesdienste und Veranstaltungen mit einem Gemeindebrief),
- oder die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist.

Darüber hinaus gibt es eine Regelung, nach der Daten später auch zu Zwecken verarbeitet werden dürfen, die nicht dem ursprünglichen Zweck der Erhebung entsprechen. Dies ist nur unter engen Voraussetzungen möglich, etwa wenn Rechtsvorschriften dies vorsehen oder der Betroffene eingewilligt hat.

### 1.6 Welche Auskunfts- und Informationsrechte haben Betroffene?

Im Wesentlichen müssen grundsätzlich folgende Informationen mitgeteilt werden – z.B. auf der Webseite der kirchlichen Einrichtung:

- Name und Kontaktdaten des Verantwortlichen,
- ggf. Kontaktdaten des Datenschutzbeauftragten (DSB), sofern vorhanden,
- Zwecke und Rechtsgrundlage der Datenverarbeitung,
- Darstellung der berechtigten Interessen zur Datenspeicherung,
- ggf. Empfänger oder Kategorien von Empfängern der Daten,
- ggf. Informationen zur Datenübermittlung in Drittländer,
- Dauer der Datenspeicherung,
- Belehrung über Betroffenenrechte (Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruchsrecht, Datenportabilität und Beschwerderecht zur Aufsichtsbehörde),
- Grundlage der Bereitstellung der Daten auf gesetzlicher oder vertraglicher Basis und Folgen der Nichtbereitstellung,
- Bestehen einer automatisierten Einzelfallentscheidung einschließlich Profiling (z.B. das Erstellen eines umfassenden Nutzerprofils oder die Bildung von sog. Scorewerten durch Verknüpfen, Speichern, Auswerten und Zusammenlegen von verschiedenen Daten zu einer Person).

Bei der Erhebung der Daten beim Betroffenen z.B. bei der Bereitstellung eines Newsletters, müssen die Nutzer entsprechend informiert werden. Dies ist in elektronischer Form möglich. Dabei ist auf eine präzise, transparente, verständliche und leicht zugängliche Form sowie eine klare und einfache Sprache zu achten. Zusätzlich müssen die Einwilligungen transparent aufzeigen, zu was der Betroffene einwilligt. Eine vage Formulierung der Einwilligung ist unzulässig. Lassen Sie die Betroffenen in Form von Kästchen selbst und frei ankreuzen, zu was Sie Ihr Einverständnis geben (Newsletter UND Schulungsangebote oder keines von beiden).

Die Betroffenen haben – wie bisher – ein umfassendes Auskunftsrecht. Neu ist allerdings, dass Betroffene auch die Auskunft und die Übermittlung der Daten in elektronischer (gängiger) Form und auch eine Kopie der Daten verlangen können. Dazu gehören: woher stammen die Daten und an wen werden sie übermittelt? Zu welchen Zwecken werden die Daten verarbeitet? Wird daraus etwa ein Profiling erstellt? Und wie lange werden die Daten gespeichert?

Darüber hinaus erhalten Betroffene erstmals per Gesetz ein „Recht auf Vergessenwerden“, also ein Recht auf Löschung der eigenen Daten, wenn:

- die Speicherung der Daten nicht mehr notwendig ist,

- der Betroffene seine Einwilligung zur Datenverarbeitung widerrufen hat,
- die Daten unrechtmäßig verarbeitet wurden,
- eine Rechtspflicht zum Löschen nach EU- oder nationalem Recht besteht.

Das Recht auf Vergessenwerden findet allerdings **keine Anwendung**, wenn:

- die freie Meinungsäußerung bzw. die Informationsfreiheit überwiegen,
- die Datenspeicherung der Erfüllung einer rechtlichen Verpflichtung dient,
- das öffentliche Interesse im Bereich der öffentlichen Gesundheit überwiegt,
- Archivzwecke, wissenschaftliche und historische Forschungszwecke dem entgegenstehen,
- die Speicherung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.

## 2 Datenschutz im Gemeindebrief

Früher dienten Gemeindebriefe vor allem der Information von Gemeindemitgliedern über das gemeindliche Leben. Heute werden in den meisten Fällen Gemeindebriefe nicht nur den Mitgliedern persönlich zugestellt, sondern auch öffentlich etwa in Geschäften, bei Ärzten oder Ämtern ausgelegt, allen Einwohnern einer Kommunalgemeinde in den Briefkasten gesteckt oder auf der Internetseite der Gemeinde veröffentlicht. Damit strahlen Gemeinden in guter Weise in die Welt aus!

Doch ergeben sich daraus hohe Anforderungen des Datenschutzrechts, weil in den Gemeindebriefen personenbezogene Daten veröffentlicht werden. Durch die Verbreitung, insbesondere im Internet, ist eine größere Missbrauchsmöglichkeit schützenswerter Daten von Personen gegeben.

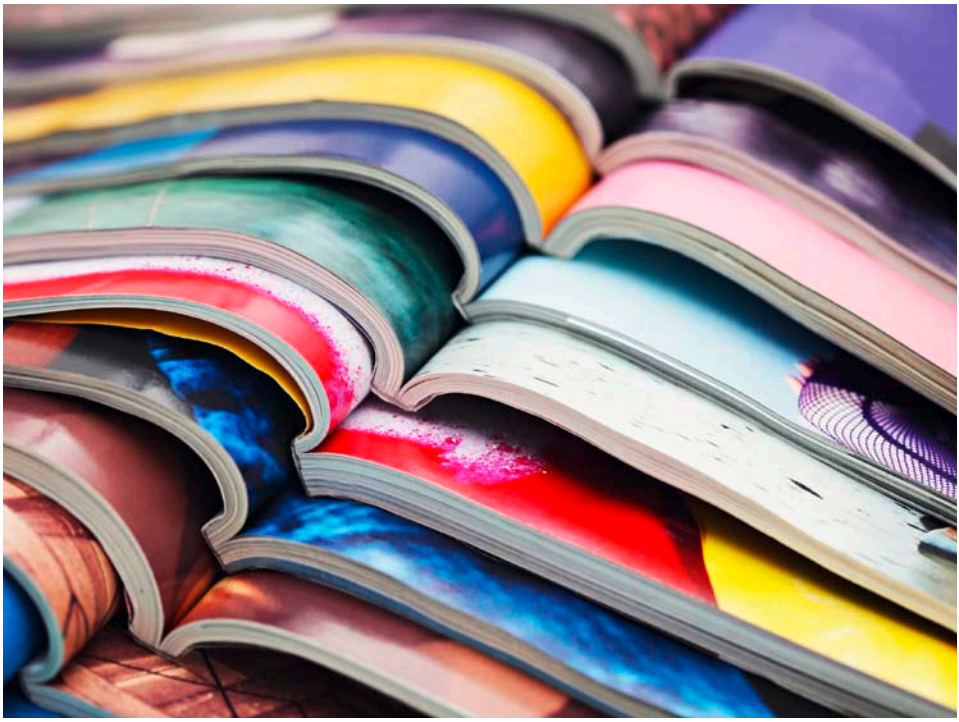
**Die folgenden Erläuterungen gelten für „öffentliche" Gemeindebriefe, die nicht ausschließlich Mitgliedern zugestellt werden.**

### 2.1 Veröffentlichung im gedruckten Gemeindebrief

Die Veröffentlichung von Amtshandlungsdaten (Taufe, Konfirmation, Trauung, Bestattung) und Geburtstags- oder Ehejubiläen ist im gedruckten Gemeindebrief zulässig, es sei denn, der Betroffene hat ausdrücklich widersprochen. Auf die Widerspruchsmöglichkeit sollte im Gemeindebrief regelmäßig hingewiesen werden. Zwar ist es derzeit rechtlich zulässig, im gedruckten Gemeindebrief die entsprechenden Adressen abzudrucken. Es wird jedoch dringend empfohlen, davon künftig abzusehen. Eine entsprechende Gesetzesänderung wird voraussichtlich noch dieses Jahr in Kraft treten.

### 2.2 Veröffentlichung des Gemeindebriefes im Internet

Bei einer Veröffentlichung des Gemeindebriefes im Internet bedarf es generell der vorherigen schriftlichen Einwilligung der Betroffenen in die Bekanntgabe ihrer Daten. Dabei muss auch der konkrete Umfang



der veröffentlichten Daten genau festgelegt werden. Ein Widerruf dieser Einwilligung ist jederzeit möglich und ist strikt zu beachten. Generell wird empfohlen, von der Veröffentlichung von Daten über Amtshandlungen oder Geburtstags- und Ehejubiläen abzusehen. Sofern Sie den kompletten Gemeindebrief auf Ihrer Homepage veröffentlichen, müssten die entsprechenden Seiten mit diesen Angaben geschwärzt bzw. gelöscht werden.

### 2.3 Kontaktdaten

Werden Mitglieder des Kirchenvorstands, Leiter von Gemeindegruppen oder andere Ansprechpartner für bestimmte Arbeitsbereiche mit ihren Kontaktdaten im Gemeindebrief bzw. auf der Webseite veröffentlicht, müssen sie ihre Einwilligung bezogen auf das jeweilige Format und auf die jeweils verwendeten Angaben erteilen. Besonders zurückhaltend sollte man bei der Angabe von privaten Kontaktdaten sein, um Missbrauch insbesondere durch die Abrufbarkeit im Internet zu verhindern. Grundsätzlich gilt auch hier, dass ein Widerruf dieser Einwilligung jederzeit möglich und strikt zu beachten ist.

**Angestellte**

Dienstliche Kontaktdaten von Mitarbeitenden, die in ihrer Tätigkeit Außenkontakt zu Gemeindegliedern oder Dritten haben, müssen mit der dienstlichen E-Mail-Adresse veröffentlicht werden. Es sollte erwogen werden, lediglich die Funktion des/der Mit-

arbeitenden anstatt des Namens zu veröffentlichen und eine funktionsbezogene E-Mail-Adresse zu verwenden.

Wenn Sie Ihren gedruckten Gemeindebrief wirklich n u r durch Hauswurf oder per Post an Gemeindemitglieder verteilen oder den Gemeindebrief nur in der Kirche oder im Gemeindehaus auslegen und damit auf eine größere Reichweite verzichten, können Sie Ausnahmen von den oben beschriebenen Regeln machen.

Die gemeindeinterne Veröffentlichung personenbezogener Daten anlässlich von Amtshandlungen (Name, Datum) ist zulässig, soweit sie der Erfüllung des kirchlichen Auftrages dient und kein Sperrvermerk der betroffenen Person oder von Amts wegen vorliegt. Die gemeindeinterne Veröffentlichung von persönlichen Jubiläen ist zulässig, so lange die betroffene Person nicht ausdrücklich widersprochen hat.

**Muster-Einwilligung zur Veröffentlichung von Daten auf der Webseite siehe Anhang** A4

### 2.4 Fotos und Videos

Auch Fotos oder Videoaufnahmen enthalten personenbezogene Daten, weil die abgebildeten Personen heutzutage mit weit verbreiteter Gesichtserkennungs-Software im Internet identifiziert werden können.

Die Veröffentlichung von Fotos und Videos sowohl im Gemeindebrief als auch auf der Internet- oder Facebookseite der Gemeinde berührt nicht allein das Datenschutzgesetz sondern auch das Kunsturhebergesetz. In diesem Gesetz ist das Recht am eigenen Bild geregelt. Es besagt, dass jeder Mensch grundsätzlich selbst darüber bestimmen darf, ob und in welchem Zusammenhang Bilder von ihm veröffentlicht werden.

Weitere Informationen zu Datenschutz im Gemeindebrief finden Sie in dieser EKD-Broschüre:

**https://datenschutz.ekd.de/wp-content/uploads/2016/08/Datenschutz-im-Gemeindebrief.pdf**

## 3 Urheberrecht

Es gilt der Grundsatz aus § 22 Kunsturhebergesetz (KunstUrhG):

- Bildnisse dürfen nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden.

Danach muss vor der Verbreitung die Einwilligung der Angehörigen der abgebildeten Person/en vorliegen. Sie muss nicht zwingend schriftlich eingeholt werden. Wegen der besseren Nachweisbarkeit bei späteren Streitfällen ist dies aber zu empfehlen. Auch bei verstorbenen Personen ist die Einwilligung bis zehn Jahre nach dem Tod bei Angehörigen notwendig.

Es gibt Ausnahmen.

Nach §23 KunstUrhG bedarf es keiner Einwilligung für

- Bildnisse aus dem Bereich der Zeitgeschichte, also etwa die Abbildung eines Bürgermeisters, solange er dieses Amt bekleidet;

- Bilder, auf denen die Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen;
- Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben

Gottesdienste, Gemeindefeste und Konzerte gelten als öffentliche Veranstaltungen. Es ist bei den Aufnahmen darauf zu achten, dass keine Einzelperson abgebildet wird, etwa durch das gezielte Hineinzoomen. Die Aufzeichnung oder Übertragung von Gottesdiensten oder kirchlichen Veranstaltungen ist zulässig, wenn die Teilnehmenden durch geeignete Maßnahmen über Art und Umfang der Aufzeichnung oder Übertragung informiert werden. Dies kann durch ein Plakat am Eingang oder Hinweiszettel auf den Sitzplätzen geschehen.

Bei Kindern und Jugendlichen gilt die Besonderheit, dass die Einwilligung durch die Eltern erklärt werden muss. Wenn Jugendliche die notwendige Einsichtsfähigkeit besitzen (etwa im Konfirmandenalter), müssen sowohl die Jugendlichen als auch die Eltern bzw. Sorgeberechtigten die Einwilligung erklären.

Bei einer Veröffentlichung im Internet hat eine unüberschaubare Vielzahl an Personen weltweit die Möglichkeit, ein Bild zu sehen, es herunterzuladen und Veränderungen durchzuführen. Deshalb ist, auch wenn eine Ausnahme gemäß § 23 KunstUrhG vorliegt, bei der Veröffentlichung im Internet im Zweifel die abgebildete Person um ihre Einwilligung zu bitten.

### 3.1 Einwilligung

Die Einwilligung muss schriftlich erklärt werden. Es ist jeweils anzugeben, zu welchem Zweck sie erteilt wird. Es ist zu bezeichnen, in welchem Medium und in welcher Verbreitung die Veröffentlichung geplant ist. Die Einwilligungserklärung muss auch den Hinweis enthalten, dass die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen werden kann. Hierdurch kommt die Freiwilligkeit zum Ausdruck.

**Muster-Einwilligung siehe Anhang** A6

## 4 Mailings – speziell Fundraising-Mailings

Viele Gemeinden und Einrichtungen nutzen Mailings zur Kommunikation mit ihren Mitgliedern und zu Fundraising-Zwecken. Fundraising ist eine kirchliche Aufgabe. Sie verbindet Beziehungspflege mit dem Werben um persönlichen und finanziellen Einsatz für Kirche und diakonische Zwecke. Diese Mitgliederdaten dürfen für Fundraising genutzt werden, es sei denn es liegt eine Meldesperre oder ein Widerspruch vor. Folgende Daten dürfen genutzt und automatisiert verarbeitet werden:

- Name und Anschrift von Spendern, zugehörige Kirchengemeinde
- Art, Betrag, Zweck und Zeitpunkt der geleisteten Spenden
- Erteilung von Zuwendungsbestätigungen

- Daten des Kontakts
- Daten der erforderlichen Buchhaltung
- Daten zur statistischen analytischen Auswertung

Entsprechendes gilt für Personen, die mit der kirchlichen und diakonischen Arbeit in Beziehung getreten sind (schon gespendet haben, oder aktiv sind, ohne Kirchenmitglied zu sein).

Damit die personenbezogenen Daten der Mitglieder oder Spender entsprechend der aktuellen Gesetzeslage geschützt sind, hier ein paar wichtige Hinweise:

### 4.1 Vertrag mit Dienstleistern – Datenverarbeitung im Auftrag

Wer z.B. für den Versand eines Mailings mit einem Dienstleister wie mit einem Lettershop arbeitet und diesem die Adressdaten übermittelt oder schon die Druckerei das Mailing individualisieren lässt, benötigt für die Zusammenarbeit mit diesen Dienstleistern eine vertragliche Vereinbarung, die den Datenschutz regelt: die sogenannte Auftragsverarbeitung = Auftragsverarbeitungsverträge (AV-Verträge). Von der EKD gibt es eine Mustervorlage, die Sie für Ihre Bedürfnisse anpassen können – Sie finden Sie in den Anlagen bzw. hier[10]:

**Hinweis:** Altverträge nach § 11 DSG-EKD bleiben wirksam, sind jedoch bis 31.12.2019 an das neue DSG-EKD anzupassen.

### 4.2 Speicherung, Verschlüsselung, Löschung personenbezogener Daten für Mailings

- Achten Sie bei der Speicherung von Adressdaten von Mitgliedern oder gar noch weiterführenden Spenderdaten darauf, dass diese bei Ihnen sicher gespeichert sind und nur zugriffsberechtigte Personen Zugriff haben
- dass diese nur verschlüsselt an verarbeitende Dienstleister verschickt werden
- dass diese nicht an Dritte weiter gegeben werden (vertraglicher Ausschluss) und nur für die Fundraising-Maßnahmen genutzt werden
- dass Personen, die den Erhalt von Spendenaufrufen ausdrücklich nicht wünschen (Robinsonliste) aus der Mailing-Liste entfernt werden
- dass diese nicht über USB Sticks oder über Cloud – oder Fileshare-Systeme wie Drop Box verschickt werden, deren Server in den USA stehen und die nicht dem EU Datenschutz unterliegen
- dass die Daten für das Mailing gemäß Nutzungsbestimmungen wieder gelöscht werden – bei Ihnen auf der Festplatte bzw. dem Server ebenso wie beim beauftragten Dienstleister (siehe 4.1. Auftragsdatenverarbeitung), sofern sie nicht aufgrund einer Rechtsvorschrift oder durch vorgeschriebene Aufbewahrungsfristen weiter aufbewahrt werden müssen.

10 https://datenschutz.ekd.de/infothek-items/av-vertrag

### 5.1 Pflicht zu Impressum und Datenschutzerklärung

Jeder Webseitenbetreiber benötigt ein aktuelles Impressum und eine Datenschutzerklärung auf der eigenen Webseite. Die Pflichtangaben für ein rechtskonformes Impressum ergeben sich aus § 5 Telemediengesetz (TMG) sowie § 55 Abs. 2 Rundfunkstaatsvertrag (RSTV). Das Impressum und die Datenschutzerklärung müssen sowohl von der Startseite als auch von allen Unterseiten aus direkt erreichbar sein. Die Datenschutzerklärung muss neben einigen allgemeinen Informationspflichten auch eine individuelle Ausgestaltung aufweisen und sollte auf die eigene Webseite zugeschnitten sein.

In dieser Handreichung finden Sie sowohl für das Impressum als auch die Datenschutzerklärung ein Muster, das Ihnen zeigt, welche Informationen auf jeden Fall im Impressum und in der Datenschutzerklärung enthalten sein müssen. So müssen integrierte Dienste wie z.B. Cookie-Verwendung oder der Einsatz von Tracking Tools beschrieben sein.

### 5.2 Cookie Richtlinie

Betreiber einer Webseite müssen sich von ihren Besuchern das Einverständnis einholen, dass diese einer Speicherung von Informationen zustimmen. Dieser Cookie-Hinweis muss beim ersten Aufruf einer Seite angezeigt werden und durch einen Klick bestätigt werden. Ein besonders gutes Umsetzungs-Beispiel finden Sie auf dieser Webseite.[11]

### 5.3 Webtracking-Tools

Die Evangelische Medienarbeit verwendet für das Tracking in den Systemen max-e und wir-e Google Analytics. Das Tracking geschieht jedoch nicht automatisch, sondern in Absprache mit dem jeweiligen Webseitenersteller.

In der Datenschutzerklärung der Systeme max-e und wir-e wird prophylaktisch immer auf die Nutzung von Google Analytics hingewiesen, so dass eine rechtskonforme Nutzung bereits geregelt ist.

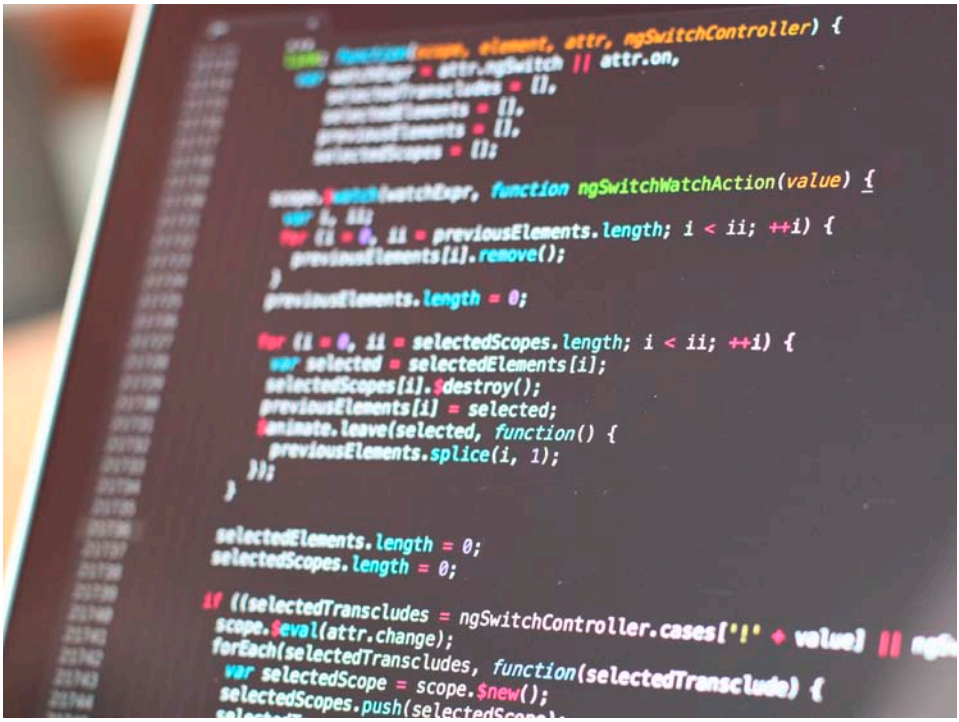
### 5.4 Social Media Plugins

Der Einsatz von Plugins zum Teilen von Beiträgen über Social-Media-Kanäle wie Facebook, Google Plus oder Twitter ist grundsätzlich auf Webseiten erlaubt, sofern der Besucher der Nutzung zugestimmt hat.

Die vom Heise Verlag entwickelte Zwei-Klick-Lösung (auch Shariff-Button genannt) stellt eine aus Datenschutzsicht geeignete Lösung dar. Das Programm stellt die Verbindung zwischen Webseitenbesucher und sozialem Netzwerk erst dann her, wenn dieser den Button gezielt anklickt. Es werden also nicht schon beim Laden der Seite im Hintergrund Daten abgerufen.

Eine weitere datenschutzkonforme und zudem einfach zu implementierende Alter-

11 http://www.schleswig-holstein.de/DE/Home/home_node.html



native zur Social Media Integration ist die reine Verlinkung der eigenen Profile bei Facebook, Google Plus oder Twitter. Auch in diesem Fall werden keine Daten übertragen und der Besucher der eigenen Webseite kann selbst entscheiden, ob er dem jeweiligen Link folgen möchte.

### 5.5 Kontaktformulare – verschlüsseln?

In Kontaktformularen dürfen nach dem Grundsatz der Datensparsamkeit nur die

Informationen abgefragt werden, die zum Zweck der weiteren Verarbeitung zwingend erforderlich sind. Pflichtfelder müssen entsprechend als solche gekennzeichnet werden. Darüber hinaus muss eine verschlüsselte Übertragung der über ein Kontaktformular versendeten Informationen sichergestellt werden. Vor der Nutzung des Formulars (bzw. vor dem Absenden) muss der Nutzer darüber belehrt werden, was mit den über ein Kontaktformular versendeten Daten geschieht. Einen Mustertext finden Sie in der Anlage.

# 6 Newsletter und Mailings

Der Versand von Newslettern und E-Mailings ist ein wichtiges Kommunikationsinstrument in der Landeskirche Hannovers. Zahlreiche Kirchenkreise, Einrichtungen, aber auch Gemeinden versenden regelmäßig Newsletter, um über ihre Angebote, Veranstaltungen und Neuigkeiten zu informieren. Bei den meisten handelt es sich dabei um rein redaktionelle Informationsmails und keine Werbemails.

Aber schon bei Hinweisen auf kostenpflichtige Seminare oder Artikel für kostenpflichtige Konzerte kann ein werblicher Charakter vermutet werden. Daher sollten auch redaktionelle Newsletter auf Nummer sicher gehen.

Sowohl das Gesetz gegen den unlauteren Wettbewerb (UWG), als auch das Telemediengesetz (TMG) und die EU Datenschutz-Grundverordnung und natürlich der EKD Datenschutz erfordern vor Kontaktaufnahme via E-Mail eine Einwilligung dazu im Vorfeld. Ohne vorherige Einwilligung (z.B. zur Eintragung in einen Newsletter) ist eine rechtssichere Kommunikation nicht möglich und unzulässig. Kirchengemeinden benötigen für die elektronische Kommunikation mit ihren Mitgliedern deren Einwilligung. Liegt diese nicht vor, darf jederzeit schriftlich, telefonisch oder persönlich der Kontakt aufgenommen werden. Das von der Evangelischen Medienarbeit bereitgestellte Newslettersystem news-e bietet mit dem Double-Opt-In Verfahren eine rechtssichere Einwilligung für den Versand.

## 6.1 Newsletter als Auftragsverarbeitung

Zum Newsletterversand werden in der Regel externe Dienstleister genutzt, die den Versand in Auftragsverarbeitung durchführen. Bestehende Verträge sind daher auf die neue Rechtslage umzustellen. Neu ist nun die explizite Regelung (§ 12 DSG-EKD)[12], dass bei elektronischen Angeboten nur religionsmündige Jugendliche die Einwilligung erteilen können, also: kein Newsletterversand an Jugendliche unter 14 Jahren ohne Zustimmung der Sorgeberechtigten. E-Mail ist als Kommunikationsmittel bei dieser Altersgruppe allerdings sowieso zu vernachlässigen. Möchte eine Gemeinde z. B. Messengerdienste anbieten, wird auch hier eine Einwilligung der Erziehungsberechtigten benötigt. (siehe auch weiter untern 7.6)

## 6.2 Arbeiten mit alten Empfängerbestand ohne Opt-In

Wenn Sie Ihren Verteiler schon lange bedienen, ohne dass die Newsletter-Empfänger seinerzeit aktiv eingewilligt haben, dürfen Sie diese Adressen auch zukünftig verwenden. Denn durch den bisherigen Bezug kann das Einverständnis vorausgesetzt werden.

Allerdings müssen Sie verständlich darüber informieren, wie sich die Mails abbestellen lassen und an wen sich der Empfänger mit seinen Fragen wenden kann. Sowohl jeder Newsletter auch Ihre Webseite muss eine Möglichkeit zum Opt-Out beinhalten.

12 https://www.kirchenrecht-ekd.de/document/39740

Sollte der Empfänger die an ihn adressierten Werbemails oder Newsletter per Opt-Out abbestellen, ist seine E-Mail-Adresse aus dem Verteiler zu nehmen. Dokumentieren Sie die Abmeldung mit Datum und wie es Sie erreicht hat. Bei dem von der Evangelischen Medienarbeit angebotenen System news-e übernimmt dieses den Eintrag für Sie. Wenn Sie Ihre Adressliste manuell pflegen, sind neue Anmeldungen (Opt-In) oder Abmeldungen (Opt-Out) manuell zu dokumentieren.

### 6.3 Neue Empfänger rechtssicher anlegen

Bei der klassischen Neu-Einwilligung (Opt-In) genügt es, die E-Mail-Adresse in ein Feld einzutragen und abzusenden. Allerdings könnte dies auch ohne Wissen und Einwilligung des potentiellen Empfängers z.B. als Streich passieren. Beim Double Opt- In kann die eigentliche Aufnahme in den Newsletter / das Mailsystem erst erfolgen, nachdem der Empfänger auf eine ihm gesendete E-Mail reagiert. Diese enthält einen Aktivierungslink, den er zunächst anklicken muss. Erst nach erfolgtem Klick durch den Verbraucher auf den Aktivierungslink findet der eigentliche Opt-In und somit die Aufnahme der E-Mail-Adresse in den Newsletter-Verteiler statt. Dieses System wirkt nicht nur als Spam-Schutz, sondern sichert außerdem den Newsletter-Betreiber ab. Mit dem Klick gibt der Empfänger die ausdrückliche Einwilligung ab, in den Newsletter aufgenommen zu werden. Daher ist das Double Opt-In Verfahren zu empfehlen, auch wenn es nicht die zwingende rechtliche Voraussetzung ist, um rechtssicher Newsletter zu betreiben. Schlussendlich kann der Empfänger seine ausdrückliche Zustimmung zum Erhalt künftiger Mails auch auf anderem Wege erteilen. Aber dieses Verfahren (das z.B. auch das Newslettermodul news-e als Bestandteil von max-e nutzt) bietet neben der rechtsicheren Datenspeicherung auch den Komfort der automatisierten Verarbeitung und vermeidet das mühsame Dokumentieren manueller Listen.

**Darüber hinaus gilt:**

- Erläutern Sie auf Ihrer Webseite vor dem Anmeldebutton, was mit den Daten des Anmelders geschieht
- Auch eine Verlinkung der Anmeldeseite mit der Datenschutzerklärung ist ratsam Bei einer Registrierung in einem Shop (sofern auf Ihrer Webseite vorhanden) darf die Einwilligung zum Empfang von Newslettern nicht standardmäßig aktiviert sein
- Bei der Newsletter-Bestellung ist der Hinweis und Verlinkung auf die Datenschutzerklärung, sowie der Hinweis auf den jederzeitigen Widerruf der Einwilligung direkt beim Newsletter-Formular darzustellen.

### 6.4 Schutz der Daten beim Versand

Schutz der Daten: E-Mails sind so zu versenden, dass für keinen der Empfänger ersichtlich ist, wie die E-Mail-Adressen oder Namen anderer Empfänger lauten. Diese und weitere personenbezogene Daten dürfen vom Unternehmen auf keinen Fall sichtbar gemacht werden.

### 7.1 Personale Kommunikation des Evangeliums

Soziale Netzwerke sind heute ein unverzichtbares Kommunikationsmittel. Die Landeskirche Hannovers nutzt die wichtigsten Sozialen Netzwerke, um einen guten Kontakt mit ihren Mitgliedern, aber auch Außenstehenden zu haben. Persönliche Kommunikation wird dem Anspruch des Evangeliums in besonderer Weise gerecht, da das Zeugnis des Glaubens immer auch ein persönliches Zeugnis sein muss.

### 7.2 Die Rolle der digitalen Dienstleister sozialer Medien

Im Unterschied zu persönlichen Gesprächen hinter verschlossenen Türen braucht es für andere Kommunikationsformen immer einen Dienstanbieter, der die Informationen weiterleitet. Das ist bei der Briefpost nicht anders als beim Telefon, wo selbstverständlich statistische Erhebungen angestellt werden, aber Briefe nicht geöffnet und Telefone nicht ohne weiteres abgehört werden dürfen. Postmitarbeiter können Postkarten lesen, müssen aber darüber schweigen.

Die digitalen Dienste-Anbieter kennen nicht nur Absender und Empfänger, sondern in jedem Fall auch alle Inhalte, ganz gleich ob es der eigene E-Mail-Provider ist oder WhatsApp, egal ob Facebook oder der eigene IT-Service im Haus. Ebenso wie Google zeichnen all diese Dienste statistische Nutzerdaten auf. Wenn der Kunde es wünscht, werden Inhalte veröffentlicht, wie Facebook-Nachrichten oder Tweets die ja nach außen dringen sollen.

Aus den unterschiedlichen Datenformaten erstellen einige digitale Dienste Nutzerprofile, um den Kunden angemessen bedienen zu können oder Gleichgesinnte zu finden, aber auch, um ihnen die passende Werbung zu schicken. Damit bezahlt der Kunde, wenn der digitale Dienst kostenfrei ist. Große Datenmengen ergeben durch ihre Verknüpfung wiederrum neue Informationen, also eine neue Qualität, und werden dadurch noch wertvoller.

Wenn Daten den Bereich des Dienste-Anbieters verlassen, dann sind sie entweder verkauft worden oder wurden gestohlen. Wichtig ist zu unterschieden zwischen anonymisierten Daten, wie Zugriffszeiten, und persönlichen Informationen, angefangen bei Adressen. So wurden große E-Mail-Anbieter schon gehackt. Social-Media-Dienste verkaufen Daten oder tauschen Daten aus. Sicherheitslücken wurden zugegeben.

### 7.3 Privatsphäre-Einstellungen

Weil es im Wesen der sozialen Medien liegt, Menschen zusammenzubringen, versuchen diese Medien immer auch personenbezogene Daten zu verknüpfen. Dazu müssen die Dienstleister die Daten ordnen und auswerten. Auch wenn die Daten nicht an Dritte weitergegeben werden, ist jeder nicht nur für seine eigenen Daten verantwortlich, sondern auch für die seiner Freunde oder Follower. Die Privatsphäre-Einstellungen sind das A und O, um den Datenschutz bei

sozialen Netzwerken so gut wie möglich zu gewährleisten.

### 7.4 Fotos, Videos, Musik

Bilder, Filme und Töne, auch Sprache, haben immer einen Urheber, der vor der Veröffentlichung gefragt werden muss und als Quelle angegeben werden muss.

Grundsätzlich sollte diese Quellenangabe im Medium selbst erfolgen, damit im Fall des Teilens diese Information nie verloren geht. Die Angabe muss nicht groß sein, aber lesbar am Rand. Auch Quellen freier Medien sollte man angeben, da diese Medien anderswo manchmal kostenpflichtig sind. Abmahnanwälte können nicht alles prüfen, aber eine fehlende Quellenangabe macht einen verdächtig. So gesehen ist es eine gute Idee, bei eigenen Produkten den eigenen Namen anzugeben.

Je besser die technische Qualität ist, umso stärker ist der Anreiz für den Dienste-Anbieter, die Medien für eigene Zwecke zu nutzen, z.B. für vergleichende Gesichtsprofile zusammenzustellen. Andererseits hat es auch keinen Zweck „briefmarkengroße" Bildchen zu posten, die keiner anschauen will. Abgesehen von Titelbildern ist niemand gezwungen, den empfohlenen Maßen zu folgen. Gerade bei Profilbildern ist weniger mehr. Ein Facebook-Post mit 1.200 Px (wie empfohlen) füllt immerhin 2/3 eines modernen HD-Bildschirms aus. Bei WhatsApp und Twitter reicht die Hälfte. Für die Vertonung von Videos auf YouTube gibt es im Internet GEMA-freie Musik.[13] Hier ist aber auch die Hinweispflicht zu beachten.

### 7.5 Facebook

Jeder Nutzer entscheidet über seine Daten selbst. Aber schon die Kommunikation mit anderen oder das Markieren anderer Personen gibt Facebook Informationen über andere, nämlich über die Beziehungen untereinander. Grundsätzlich sind die Privatsphäre-Einstellungen das A und O, um den Datenschutz bei Facebook zu verbessern.

Bei sozialen Medien wie Facebook entscheiden die Nutzer, ob sie öffentlich posten oder geschützt im Chat kommunizieren. Jeder sollte sich darüber im Klaren sein, dass Chats nicht öffentlich angezeigt werden, aber von Facebook zur Verbesserung des Nutzerprofils und zu Werbezwecken genutzt werden. Nach der Regel der Datensparsamkeit ist es zu empfehlen, nicht jedem alles zu zeigen. Sehr effektiv ist es, mehrere Freundeslisten zu führen, z.B. enge Freunde, Kollegen oder Bekannte.

Man kann dann an eine Freundesliste posten oder auch „öffentlich"[14].

Es lohnt sich, die Privatsphäre-Einstellungen genau durchzugehen. Wer so gut wie keine Informationen über sich selbst zeigt, wird weniger Kontakte mit anderen finden. Wer nie etwas „öffentlich" postet, zeigt nach außen eine leere Seite. Informationen, die sowieso jeder weiß, sind zwar für sich genommen harmlos, werden aber durch Datenverbindung wertvoller. Informationen, die zumindest Spam verursachen können, wie Handynummer und E-Mail-Adresse kann man bei Facebook getrost weglassen.

Für Facebook gilt das Mindestalter von 13 Jahren. Wer unter 16 ist, bekommt eine ein-

13 https://www.gemafreie-musik-online.de

14 https://irights.info/schlagwort/whatsapp


geschränkte Version oder muss einen Elternteil oder einen anderen Berechtigten angeben, der die Erlaubnis für die volle Nutzung von Facebook gibt.

### 7.6 WhatsApp

Der Messenger WhatsApp zeigt dem Nutzer an, wen er oder sie über diesen Dienst erreichen kann. Möglich ist das, weil WhatsApp alle Daten aus dem Adressbuch sammelt. Das macht die Kommunikation sehr einfach und den Messenger äußerst beliebt. Damit gibt der Nutzer nicht nur die eigenen Daten weiter, was jeder ab 18 für sich frei entscheiden darf, sondern auch die Daten aller anderen Menschen im Adressbuch des Smartphones, ohne diese fragen zu können, bzw. deren Einwilligung zu haben.

Schaltet man das Telefonbuch ab, werden nur noch Nummern ohne Namen angezeigt. Für professionelle Anwendungen gibt es die Praxis, für WhatsApp ein Handy zu verwenden, in dem keine Adressen gespeichert sind. Abschalten kann man den Standort und den Kalender. Wer auf die Telefonfunktion verzichten will, sollte auch das Mikrofon ausschalten.

WhatsApp hebt die Nachrichten nur bis zu ihrem Empfang auf. Auch Bilder werden nur kurzzeitig gespeichert. Inzwischen gehört WhatsApp zu Facebook. Angeblich werden keine Daten übertragen, aber Beobachtungen zeigen, dass die beiden Dienste wechselseitig fehlende Daten z.B. Telefonnummern, ergänzen. 30 Tage nach der Installation des Messengers lässt sich das Teilen

von Account-Informationen mit Facebook ausschalten. Danach kann man WhatsApp deinstallieren, neu installieren und dann die Teilen-Funktion abschalten.

Im Zuge der neuen DSGVO müssen Mitglieder bei WhatsApp künftig ein Mindestalter von 16 Jahren haben. Jugendliche dürfen den Dienst ab 16 nutzen. Kinder dürfen WhatsAPP nutzen, wenn die Eltern zustimmen.

**JUST CONNECT statt WhatsApp**
WhatsApp ist in der kirchlichen Nutzung verboten!

**Die Gründe:**
- Hochladen der Adressbücher auf Server [in Drittländern]
- Speicherung und Verwendung umfassender Protokolldaten
- Zum Teil unsichere oder lückenhafte Ende-zu-Ende-Verschlüsselung

Die Landeskirche Hannovers bietet mit der JUST CONNECT App als Bestandteil von intern-e eine adäquate Alternative an. Die App steht ab sofort (Juni 2018) im Google Play Store unter dem Namen JUST CONNECT zur Verfügung. Sie setzt einen gültigen Zugang zu intern-e voraus. Eine Version für iOS ist für den Herbst 2018 geplant.

### 7.7 YouTube

YouTube wird zu den sozialen Medien gezählt, da es auf Kommentare und Bewertungen Wert legt und Nutzer verbindet. Die Einstellungen sind im allgemeinen Google-Konto untergebracht, denn YouTube gehört zu Google. In den„Aktivitätseinstellungen" finden sich nicht nur Optionen zum Web- und Standortverlauf, sondern auch spezielle Funktionen zum Datenschutz bei YouTube.

Hier können die Nutzer den Video-Suchverlauf pausieren, sodass ihre Suchanfragen nicht mehr gespeichert werden. Zum anderen können sie auch den Video-Wiedergabeverlauf ausschalten, sodass auch nicht alle angesehenen Videos gespeichert werden. Beide Optionen sorgen bei YouTube für mehr Datenschutz, schränken aber auch den gewohnten Komfort durch maßgeschneiderte Empfehlungen ein. Jeder Nutzer muss hier seine Prioritäten abwägen.

Wer selbst Videos hochlädt, kann selbst festlegen, wer Zugriff auf die eigenen Videos erhält. So kann man einzelne Videos auf „privat" statt auf „öffentlich" stellen.

### 7.8 Doodle

Doodle ist ein Terminabstimmungs-Tool, das Daten sammelt und verbindet. Unter Datenschutzgesichtspunkten ungünstig ist, dass bei der Nutzung von Doodle kein wirksamer Zugriffsschutz gewährleistet ist. Der Zugriff auf die Umfrage erfolgt durch Weitergabe des dazugehörigen Links und deshalb ist nicht genau steuerbar, wer Einsicht oder Zugriff auf die Informationen nehmen kann. Bei lokalen PCs lässt sich z.B. auch über den Browserverlauf die einst aufgerufene Umfrage öffnen.

Ein weiterer kritischer Aspekt ist grundsätzlich darin zu sehen, dass Doodle den Webanalyse-Dienst Google Analytics einsetzt, wodurch im Rahmen der Umfrage hinterlegte Informationen der Nutzer in die USA übermittelt werden. Hier hat Doodle jedoch immerhin Schutzmaßnahmen zugunsten der Nutzer ergriffen, indem es die von Google angebotene IP-Anonymisierung aktiviert hat.

Als echte datenschutzkonforme Lösung arbeitet die Landeskirche Hannovers an einer eigenen Lösung als Teil von intern-e und als eigene Smartphone APP. Unter dem Titel meeting-e soll das Tool mobil und für Desktop ab Herbst 2018 verfügbar sein.

## 8 Cloud-Computing

Cloud Computing ist nicht nur ein Hype, auch wenn es eigentlich nichts gänzlich Neues darstellt, sondern bereits häufig Realität. Auch immer mehr kirchliche Einrichtungen nutzen Cloud-Dienste, für die es in der EKD besondere Datenschutz-Anforderungen gibt. Diese Anforderungen sind in der Entschließung zum Thema Cloud Computing vom 1. Juli 2015 festgelegt worden und finden sich hier.[15]

Bevor Sie sich für eine Nutzung entscheiden, sollten Sie folgende Fragen für sich beantworten:

- Ist sichergestellt, dass der Server, auf dem die Cloud-Dienste betrieben werden, innerhalb der EU steht und damit EU Datenschutzrecht gilt? Denn die Sicherheit personenbezogener Daten außerhalb der EU ist gesetzlich nicht gewährleistet
- Wie transparent und wie offensiv geht der Anbieter mit dem Thema Datenschutz um?
- Ist der Datenschutz Vertragsbestandteil beim Abschluss des Nutzungsvertrags?

15 https://datenschutz.ekd.de/infothek-items/entschliessung-cloud-computing/

## 9 Streaming von Andachten oder Gottesdiensten

Erfreulich ist, dass nun in Bezug auf Übertragung und Aufzeichnung von Gottesdiensten und anderen kirchlichen Veranstaltungen eine rechtliche Klarstellung erfolgt (§ 53 DSG-EKD)[16]: Diese sind zulässig, „wenn die Teilnehmenden durch geeignete Maßnahmen über Art und Umfang der Aufzeichnung oder Übertragung informiert werden."

16 https://www.kirchenrecht-ekd.de/document/39740

## 10 Link-Tipps

- https://irights.info
- https://www.datenschutzbeauftragter-info.de
- https://www.gdd.de/gdd-arbeitshilfen/praxishilfen-ds-gvo/praxishilfen-ds-gvo
- https://www.datenschutz-nord-gruppe.de/kirchlicher-datenschutz.html
- https://www.christian-zappe.de/medientipps/gemeindemenschen/
- https://datenschutz.ekd.de/portfolio_category/muster/

# Anlagen


A1 EKD Datenschutzgesetz

A2 Musterdatenschutzerklärung für die Webseite

A3 Muster für ein Impressum

A4 Mustertext Einwilligungs-erklärung für Fotos

A5 Mustervertrag Auftragsdatenvereinbarung EKD

A6 Muster Einwilligung zur Veröffentlichung von Daten auf der Webseite

A1

# Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland

**(EKD-Datenschutzgesetz – DSG-EKD)**
**Vom 15. November 2017**

(ABl. EKD S. 353)

| Lfd. Nr. | Änderndes Recht | Datum | Fundstelle | Paragrafen | Art der Änderung |
|---|---|---|---|---|---|
| | | | | | |

## Inhaltsverzeichnis

Präambel

**Kapitel 1 Allgemeine Bestimmungen**
§ 1 Schutzzweck
§ 2 Anwendungsbereich
§ 3 Seelsorgegeheimnis und Amtsverschwiegenheit
§ 4 Begriffsbestimmungen

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

**Kapitel 3 Rechte der betroffenen Person**
§ 16 Transparente Information, Kommunikation
§ 17 Informationspflicht bei unmittelbarer Datenerhebung
§ 18 Informationspflicht bei mittelbarer Datenerhebung
§ 19 Auskunftsrecht der betroffenen Person
§ 20 Recht auf Berichtigung
§ 21 Recht auf Löschung
§ 22 Recht auf Einschränkung der Verarbeitung
§ 23 Informationspflicht bei Berichtigung, Löschung oder Einschränkung der Verarbeitung
§ 24 Recht auf Datenübertragbarkeit
§ 25 Widerspruchsrecht

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

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

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

**Kapitel 7 Rechtsbehelfe und Schadensersatz**
§ 46 Recht auf Beschwerde
§ 47 Rechtsweg
§ 48 Schadensersatz durch verantwortliche Stellen

**Kapitel 8 Vorschriften für besondere Verarbeitungssituationen**
§ 49 Verarbeitung personenbezogener Daten bei Dienst- und Arbeitsverhältnissen
§ 50 Verarbeitung personenbezogener Daten für wissenschaftliche und statistische Zwecke
§ 51 Verarbeitung personenbezogener Daten durch die Medien
§ 52 Videoüberwachung öffentlich zugänglicher Räume
§ 53 Gottesdienste und kirchliche Veranstaltungen

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

## Präambel

[1]Dieses Kirchengesetz wird erlassen in Ausübung des verfassungsrechtlich garantierten Rechts der evangelischen Kirche, ihre Angelegenheiten selbstständig innerhalb der Schranken des für alle geltenden Gesetzes zu ordnen und zu verwalten. [2]Dieses Recht ist europarechtlich geachtet und festgeschrieben in Artikel 91 und Erwägungsgrund 165 Ver-

ordnung EU 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) sowie Artikel 17 Vertrag über die Arbeitsweise der Europäischen Union (AEUV). [3]In Wahrnehmung dieses Rechts stellt dieses Kirchengesetz den Einklang mit der Datenschutz-Grundverordnung her und regelt die Datenverarbeitung im kirchlichen und diakonischen Bereich. [4]Die Datenverarbeitung dient der Erfüllung des kirchlichen Auftrags.

## Kapitel 1
## Allgemeine Bestimmungen

### § 1
### Schutzzweck

Zweck dieses Kirchengesetzes ist es, die einzelne Person davor zu schützen, dass sie durch den Umgang mit ihren personenbezogenen Daten in ihrem Persönlichkeitsrecht beeinträchtigt wird.

### § 2
### Anwendungsbereich

(1) [1]Dieses Kirchengesetz gilt für die Verarbeitung personenbezogener Daten durch die Evangelische Kirche in Deutschland, die Gliedkirchen und die gliedkirchlichen Zusammenschlüsse, alle weiteren kirchlichen juristischen Personen des öffentlichen Rechts sowie die ihnen zugeordneten kirchlichen und diakonischen Dienste, Einrichtungen und Werke ohne Rücksicht auf deren Rechtsform (kirchliche Stelle). [2]Die Evangelische Kirche in Deutschland, die Gliedkirchen und die gliedkirchlichen Zusammenschlüsse stellen sicher, dass auch in den ihnen zugeordneten Diensten, Einrichtungen und Werken dieses Kirchengesetz sowie die zu seiner Ausführung und Durchführung erlassenen weiteren Bestimmungen Anwendung finden. [3]Die Evangelische Kirche in Deutschland und die Gliedkirchen führen jeweils für ihren Bereich eine Übersicht über die kirchlichen Werke und Einrichtungen mit eigener Rechtspersönlichkeit, für die dieses Kirchengesetz gilt. [4]In die Übersicht sind Name, Anschrift, Rechtsform und Tätigkeitsbereich der kirchlichen Werke und Einrichtungen aufzunehmen.

(2) Dieses Kirchengesetz gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

(3) Dieses Kirchengesetz findet Anwendung auf die Verarbeitung personenbezogener Daten im Rahmen der Tätigkeit einer kirchlichen Stelle oder in deren Auftrag, unabhängig vom Ort der Verarbeitung.

(4) Dieses Kirchengesetz findet keine Anwendung auf die Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten.

(5) [1]Die Vorschriften dieses Kirchengesetzes gehen denen des Verwaltungsverfahrens- und -zustellungsgesetzes der Evangelischen Kirche in Deutschland vor, soweit bei der Ermittlung des Sachverhaltes personenbezogene Daten verarbeitet werden.

(6) [1]Soweit andere Rechtsvorschriften, die kirchliche Stellen anzuwenden haben, die Verarbeitung personenbezogener Daten regeln, gehen sie diesem Kirchengesetz vor.

## § 3
## Seelsorgegeheimnis und Amtsverschwiegenheit

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

## § 4
## Begriffsbestimmungen

Im Sinne dieses Kirchengesetzes bezeichnet der Ausdruck:

1. "personenbezogene Daten" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden "betroffene Person") beziehen; identifizierbar ist eine natürliche Person, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;
2. "besondere Kategorien personenbezogener Daten“
   a) alle Informationen, aus denen religiöse oder weltanschauliche Überzeugungen einer natürlichen Person hervorgehen, ausgenommen Angaben über die Zugehörigkeit zu einer Kirche oder einer Religions- oder Weltanschauungsgemeinschaft,

b) alle Informationen, aus denen die 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.

3. "Verarbeitung" jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

4. "Einschränkung der Verarbeitung" die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;

5. "Profiling" jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;

6. "Pseudonymisierung" die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;

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

8. "Dateisystem" jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird;

9. "verantwortliche Stelle" die natürliche oder juristische Person, kirchliche Stelle im Sinne von § 2 Absatz 1 Satz 1 oder sonstige Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;
10. "Auftragsverarbeiter" eine natürliche oder juristische Person, kirchliche oder sonstige Stelle, die personenbezogene Daten im Auftrag der verantwortlichen Stelle verarbeitet;
11. "Empfänger" eine natürliche oder juristische Person, kirchliche oder sonstige Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht;
12. "Dritter" eine natürliche oder juristische Person, kirchliche oder sonstige Stelle, außer der betroffenen Person, der verantwortlichen Stelle, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung der kirchlichen Stelle oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;
13. "Einwilligung" jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung der betroffenen Person in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;
14. "Verletzung des Schutzes personenbezogener Daten" eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von oder zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;
15. "genetische Daten" personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden;
16. "biometrische Daten" mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten;
17. "Gesundheitsdaten" personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen;

18. "Drittland“ einen Staat, in dem die Datenschutz-Grundverordnung keine Anwendung findet.
19. "Unternehmen“ eine natürliche oder juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personen-, Kapitalgesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen;
20. "Beschäftigte“
    a) die in einem Pfarrdienst- oder in einem kirchlichen Beamtenverhältnis oder in einem sonstigen kirchlichen öffentlich-rechtlichen Dienstverhältnis stehenden Personen,
    b) Arbeitnehmerinnen und Arbeitnehmer, einschließlich der Leiharbeitnehmerinnen und Leiharbeitnehmer im Verhältnis zum Entleiher,
    c) zu ihrer Berufsausbildung Beschäftigte,
    d) Teilnehmende an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobungen (Rehabilitationen),
    e) Beschäftigte in anerkannten Werkstätten für Menschen mit Behinderungen,
    f) nach dem Bundesfreiwilligen- oder dem Jugendfreiwilligendienstgesetz oder in vergleichbaren Diensten Beschäftigte,
    g) Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,
    h) Bewerbende für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist;
21. "IT-Sicherheit“ den Schutz der mit Informationstechnik verarbeiteten Daten insbesondere vor unberechtigtem Zugriff, vor unerlaubten Änderungen und vor der Gefahr des Verlustes, um deren Vertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten.

## Kapitel 2
## Verarbeitung personenbezogener Daten

### § 5
### Grundsätze

(1) Personenbezogene Daten sind nach folgenden Grundsätzen zu verarbeiten:

1. Rechtmäßigkeit, Verhältnismäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz;

2. Zweckbindung: Personenbezogene Daten werden für festgelegte, eindeutige und legitime Zwecke erhoben. Sie dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Eine Weiterverarbeitung für im kirchlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszecke oder für statistische Zwecke gilt als vereinbar mit den ursprünglichen Zwecken;
3. Datenminimierung: Die Verarbeitung personenbezogener Daten wird auf das dem Zweck angemessene und notwendige Maß beschränkt; personenbezogene Daten sind zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert;
4. Richtigkeit: Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden;
5. Speicherbegrenzung: Personenbezogene Daten werden in einer Form gespeichert, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Personenbezogene Daten dürfen länger gespeichert werden, soweit sie für die Zwecke des Archivs, der wissenschaftlichen und historischen Forschung sowie der Statistik verarbeitet werden;
6. Integrität und Vertraulichkeit: Personenbezogene Daten werden in einer Weise verarbeitet, die eine angemessene Sicherheit gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Zerstörung oder unbeabsichtigter Schädigung.

(2) Die verantwortliche Stelle muss die Einhaltung der Grundsätze nachweisen können (Rechenschaftspflicht).

## § 6
## Rechtmäßigkeit der Verarbeitung

Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

1. eine Rechtsvorschrift erlaubt die Verarbeitung der personenbezogenen Daten oder ordnet sie an;
2. die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
3. die Verarbeitung ist zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich, einschließlich der Ausübung kirchlicher Aufsicht,
4. die Verarbeitung ist für die Wahrnehmung einer sonstigen Aufgabe erforderlich, die im kirchlichen Interesse liegt,

5. die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgt;
6. die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der die kirchliche Stelle unterliegt;
7. die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
8. die Verarbeitung ist zur Wahrung der berechtigten Interessen eines Dritten erforderlich, sofern nicht die schutzwürdigen Interessen der betroffenen Person überwiegen, insbesondere dann, wenn diese minderjährig ist.

## § 7
## Rechtmäßigkeit der Zweckänderung

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

1. eine kirchliche Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,
2. eine staatliche Rechtsvorschrift dies vorsieht und kirchliche Interessen nicht entgegenstehen;
3. die betroffene Person eingewilligt hat;
4. offensichtlich ist, dass sie im Interesse der betroffenen Person liegt, und kein Grund zu der Annahme besteht, dass diese in Kenntnis des anderen Zweckes ihre Einwilligung verweigern würde;
5. Angaben der betroffenen Person überprüft werden müssen, weil Anhaltspunkte für deren Unrichtigkeit bestehen;
6. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen darf, es sei denn, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Zweckänderung offensichtlich überwiegt;
7. Grund zu der Annahme besteht, dass andernfalls die Wahrnehmung des kirchlichen Auftrages gefährdet würde;
8. es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist;
9. 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 oder

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

(2) [1]In anderen Fällen muss die kirchliche Stelle feststellen, ob die Zweckänderung mit dem Zweck, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist. [2]Dabei berücksichtigt sie unter anderem

1. jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung;
2. den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und der kirchlichen Stelle;
3. die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß § 14 verarbeitet werden;
4. die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen;
5. das Vorhandensein geeigneter Garantien, zu denen die Verschlüsselung, die Pseudonymisierung oder die Anonymisierung gehören kann.

(3) [1]Eine Verarbeitung für andere Zwecke liegt nicht vor, wenn sie der Wahrnehmung von Visitations-, Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung, der Revision oder der Durchführung von Organisationsuntersuchungen für die verantwortliche Stelle dient. [2]Das gilt auch für die Verarbeitung zu Ausbildungs- und Prüfungszwecken durch die verantwortliche Stelle, soweit nicht überwiegende schutzwürdige Interessen der betroffenen Person entgegenstehen.

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

(5) Die Verarbeitung von besonderen Kategorien personenbezogener Daten für andere Zwecke ist nur rechtmäßig, wenn die Voraussetzungen vorliegen, die eine Verarbeitung nach § 13 Absatz 2 zulassen.

## § 8
## Offenlegung an kirchliche oder öffentliche Stellen

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

1. sie zur Erfüllung der in der Zuständigkeit der offenlegenden oder der empfangenden kirchlichen Stelle liegenden Aufgaben erforderlich ist und
2. die Zulässigkeitsvoraussetzungen des § 6 vorliegen.

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

(3) [1]Die datenempfangende kirchliche Stelle darf die offengelegten Daten für den Zweck verarbeiten, zu dessen Erfüllung sie ihr offengelegt werden. [2]Eine Verarbeitung für andere Zwecke ist nur unter den Voraussetzungen des § 7 zulässig.

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

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

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

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

(8) [1]Die datenempfangenden Stellen nach Absatz 6 und 7 dürfen die offengelegten Daten nur für den Zweck verarbeiten, zu dessen Erfüllung sie ihnen offengelegt werden. [2]Die offenlegende Stelle hat sie darauf hinzuweisen.

## § 9
## Offenlegung an sonstige Stellen

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

1. sie zur Erfüllung der in der Zuständigkeit der offenlegenden kirchlichen Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Verarbeitung nach § 8 zulassen, oder
2. eine Rechtsvorschrift dies zulässt oder
3. die datenempfangenden Stellen oder Personen ein berechtigtes Interesse an der Kenntnis der offenzulegenden Daten glaubhaft darlegen und die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Offenlegung hat, es sei denn, dass Grund zu der Annahme besteht, dass durch die Offenlegung die Wahrnehmung des Auftrags der Kirche gefährdet würde.

(2) Das Offenlegen von besonderen Kategorien personenbezogener Daten ist abweichend von Absatz 1 Nummer 3 nur zulässig, soweit dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist.

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

(4) [1]In den Fällen der Offenlegung nach Absatz 1 Nummer 3 unterrichtet die offenlegende kirchliche Stelle die betroffene Person von der Offenlegung ihrer Daten. [2]Dies gilt nicht, wenn damit zu rechnen ist, dass sie davon auf andere Weise Kenntnis erlangt oder die Wahrnehmung des Auftrages der Kirche gefährdet würde.

(5) [1]Die datenempfangenden Stellen und Personen dürfen die offengelegten Daten nur für den Zweck verarbeiten, zu dessen Erfüllung sie ihnen offengelegt werden. [2]Die offenlegende Stelle hat sie darauf hinzuweisen.

## § 10
## Datenübermittlung an und in Drittländer oder an internationale Organisationen

(1) Jede Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen, die bereits verarbeitet werden oder nach ihrer Übermittlung verarbeitet werden sollen, ist über die weiteren Voraussetzungen der Datenverarbeitung hinaus nur zulässig, wenn

1. die EU-Kommission ein angemessenes Datenschutzniveau entsprechend den Bestimmungen des Artikel 45 Absatz 2 Datenschutz-Grundverordnung festgestellt hat,

2. als geeignete Garantien Standarddatenschutzklauseln verwendet werden, die von der Kommission gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 Datenschutz-Grundverordnung erlassen oder genehmigt worden sind.

(2) Falls die Voraussetzungen des Absatz 1 nicht vorliegen, ist die Übermittlung zulässig, wenn

1. die betroffene Person in die vorgeschlagene Datenübermittlung ausdrücklich eingewilligt hat, nachdem sie über die für sie bestehenden möglichen Risiken aufgeklärt worden ist;
2. die Übermittlung für die Erfüllung eines Vertrages oder Rechtsverhältnisses zwischen der betroffenen Person und der verantwortlichen Stelle oder zur Durchführung von vertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich ist;
3. die Übermittlung zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person von der verantwortlichen Stelle mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrages erforderlich ist;
4. die Übermittlung aus wichtigen Gründen des kirchlichen Interesses notwendig ist;
5. die Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist oder
6. die Übermittlung zum Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen erforderlich ist, sofern die betroffene Person aus physischen oder rechtlichen Gründen außer Stande ist, ihre Einwilligung zu geben.

## § 11
## Einwilligung

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

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

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

(4) Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Maß Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind.

## § 12
## Einwilligung Minderjähriger in Bezug auf elektronische Angebote

[1]Minderjährige, denen elektronische Angebote von kirchlichen Stellen gemacht werden, können in die Verarbeitung ihrer Daten wirksam einwilligen, wenn sie religionsmündig sind. [2]Sind die Minderjährigen noch nicht religionsmündig, ist die Verarbeitung nur rechtmäßig, wenn die Sorgeberechtigen die Einwilligung erteilt oder der Einwilligung zugestimmt haben. [3]Die Einwilligung der Sorgeberechtigten ist nicht erforderlich, wenn kirchliche Präventions- oder Beratungsdienste einem Kind unmittelbar angeboten werden.

## § 13
## Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Besondere Kategorien personenbezogener Daten dürfen nicht verarbeitet werden.

(2) Abweichend von Absatz 1 dürfen besondere Kategorien personenbezogener Daten verarbeitet werden, wenn

1. die betroffene Person in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt hat;
2. die Verarbeitung erforderlich ist, damit die verantwortliche Stelle oder die betroffene Person die ihr aus dem Arbeits- und Dienstrecht sowie dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach kirchlichem oder staatlichem Recht oder nach einer Dienstvereinbarung nach den kirchlichen Mitarbeitervertretungsgesetzen, die geeignete Garantien für die Rechte und die Interessen der betroffenen Person vorsehen, rechtmäßig ist;
3. die Verarbeitung zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person aus körperlichen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben;
4. die Verarbeitung durch eine verantwortliche Stelle im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung erfolgt, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der verantwortlichen Stelle oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden;

5. die Verarbeitung sich auf personenbezogene Daten bezieht, die die betroffene Person öffentlich gemacht hat;
6. die Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Kirchengerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich ist;
7. die Verarbeitung auf der Grundlage kirchlichen Rechts, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen kirchlichen Interesses erforderlich ist;
8. die Verarbeitung für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage kirchlichen oder staatlichen Rechts oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Absatz 3 genannten Bedingungen und Garantien erforderlich ist;
9. die Verarbeitung aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten, auf der Grundlage des kirchlichen oder staatlichen Rechts, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses vorsieht, erforderlich ist, oder
10. die Verarbeitung für im kirchlichen 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) Besondere Kategorien personenbezogener Daten dürfen für die in Absatz 2 Nummer 8 genannten Zwecke verarbeitet werden, wenn diese Daten von Fachpersonal oder unter dessen Verantwortung verarbeitet werden und dieses Fachpersonal nach kirchlichem oder staatlichem Recht der Berufsgeheimnispflicht unterliegt, oder wenn die Verarbeitung durch eine andere Person erfolgt, die ebenfalls nach kirchlichem oder staatlichem Recht einer Geheimhaltungspflicht unterliegt.

## § 14
## Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten

Die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln ist unter den Voraussetzungen

des § 6 zulässig, wenn dies das kirchliche oder staatliche Recht, das geeignete Garantien für die Rechte der betroffenen Personen vorsieht, zulässt.

### § 15
### Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist

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

(2) [1]Kann die verantwortliche Stelle in Fällen gemäß Absatz 1 nachweisen, dass sie nicht in der Lage ist, die betroffene Person zu identifizieren, so unterrichtet sie die betroffene Person hierüber, sofern dies möglich ist. [2]In diesen Fällen finden die §§ 17 bis 24 keine Anwendung, es sei denn, die betroffene Person stellt zur Ausübung ihrer in diesen Vorschriften niedergelegten Rechte zusätzliche Informationen bereit, die ihre Identifizierung ermöglichen.

## Kapitel 3
## Rechte der betroffenen Person

### § 16
### Transparente Information, Kommunikation

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

(2) Die verantwortliche Stelle erleichtert der betroffenen Person die Ausübung ihrer Rechte gemäß den §§ 19 bis 25.

(3) [1]Die verantwortliche Stelle stellt der betroffenen Person Informationen über die ergriffenen Maßnahmen gemäß den §§ 20 bis 25 innerhalb von drei Monaten nach Eingang des Antrags zur Verfügung. [2]Diese Frist kann um zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl der Anträge erforderlich ist. [3]Die verantwortliche Stelle unterrichtet die betroffene Person innerhalb von drei Monaten nach Eingang über eine Fristverlängerung zusammen mit den Gründen für die Verzögerung.

(4) Wird die verantwortliche Stelle auf den Antrag der betroffenen Person hin nicht tätig, so unterrichtet sie die betroffene Person ohne Verzögerung, spätestens aber innerhalb von

drei Monaten nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, bei der Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen.

(5) [1]Informationen werden unentgeltlich zur Verfügung gestellt. [2]Bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person kann die verantwortliche Stelle sich weigern, aufgrund des Antrags tätig zu werden, oder ein angemessenes Entgelt verlangen.

## § 17
## Informationspflicht bei unmittelbarer Datenerhebung

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

1. den Namen und die Kontaktdaten der verantwortlichen Stelle;
2. gegebenenfalls die Kontaktdaten der oder des örtlich Beauftragten;
3. die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
4. gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten.

(2) Zusätzlich zu den Informationen gemäß Absatz 1 stellt die verantwortliche Stelle der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten auf Verlangen folgende weitere Informationen zur Verfügung:

1. falls möglich die Dauer, für die die personenbezogenen Daten gespeichert werden, oder falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
2. das Bestehen eines Rechts auf Auskunft, auf Berichtigung, auf Löschung, auf Einschränkung der Verarbeitung, auf Datenübertragbarkeit sowie eines Widerspruchsrechts gegen die Verarbeitung;
3. das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde;
4. ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, und welche mögliche Folgen die Nichtbereitstellung hätte.

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

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

## § 18
## Informationspflicht bei mittelbarer Datenerhebung

(1) [1]Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, so teilt die verantwortliche Stelle der betroffenen Person über die in § 17 Absatz 1 und 2 aufgeführten Informationen hinaus die zu ihr gespeicherten Daten mit, auch soweit sie sich auf Herkunft oder empfangende Stellen beziehen. [2]§ 17 Absatz 4 gilt entsprechend.

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

## § 19
## Auskunftsrecht der betroffenen Person

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

1. die Verarbeitungszwecke;
2. die Kategorien personenbezogener Daten;
3. die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind;
4. falls möglich, die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
5. das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch die verantwortliche Stelle oder eines Widerspruchsrechts gegen diese Verarbeitung;
6. das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde;
7. wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten.

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

(3) Die Auskunft ist unentgeltlich.

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

## § 20
## Recht auf Berichtigung

(1) [1]Unrichtige personenbezogene Daten sind auf Antrag der betroffenen Person unverzüglich zu berichtigen. [2]Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person das Recht, die Vervollständigung unvollständiger personenbezogener Daten – auch mittels einer ergänzenden Erklärung – zu verlangen.

(2) [1]Das Recht auf Berichtigung besteht nicht, wenn die personenbezogenen Daten zu Archivzwecken im kirchlichen Interesse verarbeitet werden. [2]Bestreitet die betroffene Person die Richtigkeit der personenbezogenen Daten, ist ihr die Möglichkeit einer Gegendarstellung einzuräumen. [3]Das zuständige Archiv ist verpflichtet, die Gegendarstellung den Unterlagen hinzuzufügen.

## § 21
## Recht auf Löschung

(1) Personenbezogene Daten sind zu löschen, wenn

1. ihre Speicherung unzulässig ist oder
2. ihre Kenntnis für die verantwortliche Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist;
3. die betroffene Person ihre Einwilligung bezüglich der Verarbeitung ihrer Daten widerruft und es an einer anderweitigen Rechtsgrundlage für die Verarbeitung fehlt;
4. die betroffene Person gemäß § 25 Widerspruch gegen die Verarbeitung einlegt und keine vorrangigen berechtigten Gründe für die Verarbeitung vorliegen;
5. die Löschung der personenbezogenen Daten zur Erfüllung rechtlicher Verpflichtungen der verantwortlichen Stelle notwendig ist;
6. die Löschung personenbezogener Daten verlangt wird, die bei elektronischen Angeboten, die Minderjährigen direkt gemacht worden sind, erhoben wurden.

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

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

1. zur Ausübung des Rechts auf freie Meinungsäußerung und Information;
2. zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach kirchlichem oder staatlichem Recht, dem die verantwortliche Stelle unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im kirchlichen Interesse liegt oder in Ausübung hoheitlicher Gewalt erfolgt, die der verantwortlichen Stelle übertragen wurde;
3. aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß § 13 Absatz 2 Nummer 8 bis 9;
4. für im kirchlichem Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke, soweit das in Absatz 1 genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, oder
5. zur Geltendmachung von Rechtsansprüchen sowie zur Ausübung oder Verteidigung von Rechten.

(4) Ist eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich, tritt an die Stelle des Rechts auf Löschung das Recht auf Einschränkung der Verarbeitung gemäß § 22.

(5) Vorschriften über das Archiv- und Kirchenbuchwesen bleiben unberührt.

## § 22
## Recht auf Einschränkung der Verarbeitung

(1) Die betroffene Person hat das Recht gegenüber der verantwortlichen Stelle auf Einschränkung der Verarbeitung, wenn eine der folgenden Voraussetzungen gegeben ist:

1. die Richtigkeit der personenbezogenen Daten wird von der betroffenen Person bestritten, und zwar für eine Dauer, die es der verantwortlichen Stelle ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen;
2. die Verarbeitung ist unrechtmäßig, die betroffene Person lehnt die Löschung der personenbezogenen Daten ab und verlangt stattdessen die Einschränkung der Nutzung der personenbezogenen Daten;
3. die verantwortliche Stelle benötigt die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger, die betroffene Person benötigt sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen, oder
4. die betroffene Person hat Widerspruch gegen die Verarbeitung gemäß § 25 eingelegt und es steht noch nicht fest, ob die berechtigten Gründe der verantwortlichen Stelle gegenüber denen der betroffenen Person überwiegen.

(2) Wurde die Verarbeitung gemäß Absatz 1 eingeschränkt, so dürfen diese personenbezogenen Daten – von ihrer Speicherung abgesehen – nur mit Einwilligung der betroffenen

Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen kirchlichen Interesses verarbeitet werden.

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

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

(5) Vorschriften über das Archiv- und Kirchenbuchwesen bleiben unberührt.

## § 23
## Informationspflicht bei Berichtigung, Löschung oder Einschränkung der Verarbeitung

[1]Die verantwortliche Stelle teilt allen Empfängern, denen personenbezogene Daten offengelegt werden, jede Berichtigung oder Löschung der personenbezogenen Daten oder eine Einschränkung der Verarbeitung nach den §§ 20 bis 22 mit, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. [2]Die verantwortliche Stelle unterrichtet die betroffene Person über diese Empfänger, wenn die betroffene Person dies verlangt.

## § 24
## Recht auf Datenübertragbarkeit

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

1. die Verarbeitung auf einer Einwilligung oder auf einem Vertrag beruht und
2. die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

[2]Die betroffene Person kann verlangen, dass die personenbezogenen Daten direkt von der verantwortlichen Stelle einem anderen Dritten übermittelt werden, soweit dies technisch machbar ist.

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

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

## § 25
## 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 § 6 Nummer 1, 3, 4 oder 8 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 kirchliches Interesse besteht, das Interesse einer dritten Person überwiegt oder eine Rechtsvorschrift zur Verarbeitung verpflichtet.

# Kapitel 4
# Pflichten der verantwortlichen Stellen und Auftragsverarbeiter

## § 26
## Datengeheimnis

[1]Den bei der Datenverarbeitung tätigen Personen ist untersagt, personenbezogene Daten unbefugt zu verarbeiten (Datengeheimnis). [2]Diese Personen sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis schriftlich zu verpflichten, soweit sie nicht aufgrund anderer kirchlicher Bestimmungen zur Verschwiegenheit verpflichtet wurden. [3]Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

## § 27
## Technische und organisatorische Maßnahmen, IT-Sicherheit

(1) [1]Die verantwortliche Stelle und der kirchliche Auftragsverarbeiter haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten und einen Nachweis hierüber führen zu können. [2]Diese Maßnahmen schließen unter anderem ein:

1. die Pseudonymisierung, die Anonymisierung und die Verschlüsselung personenbezogener Daten;
2. die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

3. die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall unverzüglich wiederherzustellen;
4. ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung, unbefugte Offenlegung von oder unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

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

(4) Die Einhaltung eines nach dem EU-Recht zertifizierten Verfahrens kann als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten der verantwortlichen Stelle gemäß Absatz 1 nachzuweisen.

(5) Die verantwortliche Stelle und der kirchliche Auftragsverarbeiter stellen sicher, dass natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf ihre Weisung verarbeiten.

(6) [1]Verantwortliche Stellen und Auftragsverarbeiter sind verpflichtet, IT-Sicherheit zu gewährleisten. [2]Das Nähere regelt der Rat der Evangelischen Kirche in Deutschland durch Rechtsverordnung mit Zustimmung der Kirchenkonferenz.

## § 28
## Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte natürlicher Personen trifft die verantwortliche Stelle sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung technische und organisatorische Maßnahmen, die geeignet sind, die Datenschutzgrundsätze wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieses Kirchengesetzes zu genügen und die Rechte der betroffenen Personen zu schützen.

(2) [1]Die verantwortliche Stelle trifft technische und organisatorische Maßnahmen, die geeignet sind, durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, zu verarbeiten. [2]Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten,

den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. [3]Solche Maßnahmen müssen insbesondere geeignet sein, dass personenbezogene Daten nicht ohne Eingreifen der verantwortlichen Stelle durch Voreinstellungen einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

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

## § 29
## Gemeinsam verantwortliche Stellen

(1) [1]Legen zwei oder mehr verantwortliche Stellen gemeinsam die Zwecke und die Mittel zur Verarbeitung fest, so sind sie gemeinsam verantwortliche Stellen. [2]Sie legen in einer Vereinbarung in transparenter Form fest, wer welche Verpflichtung gemäß diesem Kirchengesetz erfüllt, soweit die jeweiligen Aufgaben der verantwortlichen Stellen nicht durch Rechtsvorschriften festgelegt sind.

(2) [1]In der Vereinbarung kann eine Anlaufstelle für die betroffenen Personen angegeben werden. [2]Das Wesentliche der Vereinbarung wird der betroffenen Person auf Verlangen zur Verfügung gestellt.

(3) Ungeachtet der Einzelheiten der Vereinbarung kann die betroffene Person ihre Rechte im Rahmen dieses Kirchengesetzes bei und gegenüber jeder einzelnen verantwortlichen Stelle geltend machen.

## § 30
## Verarbeitung von personenbezogenen Daten im Auftrag

(1) [1]Werden personenbezogene Daten im Auftrag durch andere Stellen oder Personen verarbeitet, ist die auftraggebende kirchliche Stelle für die Einhaltung der Vorschriften dieses Kirchengesetzes und anderer Vorschriften über den Datenschutz verantwortlich. [2]Die in Kapitel 3 genannten Rechte sind ihr gegenüber geltend zu machen. [3]Zuständig für die Aufsicht ist die Aufsichtsbehörde der beauftragenden kirchlichen Stelle.

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

(3) [1]Der Auftragsverarbeiter ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. [2]Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind:

1. der Gegenstand und die Dauer des Auftrags;
2. der Umfang, die Art und der Zweck der vorgesehenen Verarbeitung, die Art der Daten und der Kreis der Betroffenen;

3. die nach § 27 zu treffenden technischen und organisatorischen Maßnahmen sowie ihre Kontrolle durch den Auftragsverarbeiter;
4. die Berichtigung, Löschung und Sperrung von Daten;
5. die Verpflichtung der Beschäftigten des Auftragsverarbeiters auf das Datengeheimnis;
6. gegebenenfalls die Berechtigung zur Begründung sowie die Bedingungen von Unterauftragsverhältnissen;
7. die Kontrollrechte der beauftragenden kirchlichen Stelle und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragsverarbeiters;
8. mitzuteilende Verstöße des Auftragsverarbeiters oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen;
9. der Umfang der Weisungsbefugnis, die sich die beauftragende kirchliche Stelle gegenüber dem Auftragsverarbeiter vorbehält;
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragsverarbeiter gespeicherter Daten nach Beendigung des Auftrags.

[3]Die beauftragende kirchliche Stelle hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. [4]Das Ergebnis ist zu dokumentieren.

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

(5) [1]Sofern die kirchlichen Datenschutzbestimmungen auf den Auftragsverarbeiter keine Anwendung finden, ist die kirchliche Stelle verpflichtet sicherzustellen, dass der Auftragsverarbeiter diese oder gleichwertige Bestimmungen beachtet. [2]In diesem Fall dürfen sich abweichend von Absatz 3 die Vertragsinhalte an Artikel 28 EU-Datenschutz-Grundverordnung orientieren. [3]Der Auftragsverarbeiter unterwirft sich der kirchlichen Datenschutzaufsicht.

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

(7) [1]Das Recht der Evangelischen Kirche in Deutschland, der Gliedkirchen und der gliedkirchlichen Zusammenschlüsse kann bestimmen, dass vor der Beauftragung die Genehmigung einer kirchlichen Stelle einzuholen ist oder Mustervereinbarungen zu verwenden

sind. [2]Bei der Beauftragung anderer kirchlicher Stellen kann in den Rechtsvorschriften von Absatz 3 Satz 2 Nummer 3, 5, 7 und 9 und Satz 4 abgesehen werden.

(8) Die Einhaltung von genehmigten Verhaltensregeln und die Verwendung zertifizierter und kirchlich geprüfter Informationstechnik können herangezogen werden, um die Erfüllung der datenschutzrechtlichen Anforderungen durch den Auftragsverarbeiter nachzuweisen.

## § 31
## Verzeichnis von Verarbeitungstätigkeiten

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

1. den Namen und die Kontaktdaten der verantwortlichen Stelle und gegebenenfalls der gemeinsam mit ihr verantwortlichen Stelle sowie gegebenenfalls der oder des örtlich Beauftragten;
2. die Zwecke der Verarbeitung;
3. eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
4. gegebenenfalls die Verwendung von Profiling;
5. die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfängern in Drittländern oder internationalen Organisationen;
6. gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe der dort getroffenen geeigneten Garantien;
7. wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
8. wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 27.

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

1. den Namen und die Kontaktdaten der Auftragsverarbeiter und jeder verantwortlichen Stelle, in deren Auftrag der Auftragsverarbeiter tätig ist, sowie der örtlich Beauftragten;
2. die Kategorien von Verarbeitungen, die im Auftrag jeder verantwortlichen Stelle durchgeführt werden;

3. gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe der dort getroffenen geeigneten Garantien;
4. wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 27.

(3) Das in den Absätzen 1 und 2 genannte Verzeichnis ist schriftlich oder elektronisch zu führen.

(4) Verantwortliche Stellen und Auftragsverarbeiter stellen der Aufsichtsbehörde die Verzeichnisse auf Anfrage zur Verfügung.

(5) [1]Die in den Absätzen 1 und 2 genannten Pflichten gelten nicht für verantwortliche Stellen, die weniger als 250 Beschäftigte haben. [2]Kirchliche Stellen, die weniger als 250 Beschäftigte haben, erstellen Verzeichnisse nach Absatz 1 und 2 nur hinsichtlich der Verfahren, die die Verarbeitung besonderer Kategorien personenbezogener Daten einschließen.

(6) Das Recht der Evangelischen Kirche in Deutschland, der Gliedkirchen und der gliedkirchlichen Zusammenschlüsse kann vorsehen, dass für einheitliche Verfahren das Verzeichnis zentral geführt wird.

## § 32
## Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

(1) Im Falle einer Verletzung des Schutzes personenbezogener Daten, die voraussichtlich zu einem nicht unerheblichen Risiko für die Rechte natürlicher Personen führt, meldet die verantwortliche Stelle dies unverzüglich der Aufsichtsbehörde.

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

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

1. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
2. den Namen und die Kontaktdaten der oder des örtlich Beauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
3. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
4. eine Beschreibung der von der verantwortlichen Stelle ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener

Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

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

(5) [1]Die verantwortliche Stelle hat Verletzungen des Schutzes personenbezogener Daten zu dokumentieren. [2]Die Dokumentation hat alle mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Abhilfemaßnahmen zu umfassen. [3]Diese Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Paragraphen ermöglichen.

## § 33
## Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

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

(2) Die Benachrichtigung der betroffenen Person hat in klarer und einfacher Sprache zu erfolgen und enthält zumindest die Art der Verletzung des Schutzes personenbezogener Daten und die in § 32 Absatz 3 Nummer 2, 3 und 4 genannten Informationen und Maßnahmen.

(3) Von der Benachrichtigung der betroffenen Person kann abgesehen werden, wenn

1. die verantwortliche Stelle durch nachträgliche Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte der betroffenen Personen gemäß Absatz 1 aller Wahrscheinlichkeit nach nicht mehr besteht, oder
2. die Benachrichtigung mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall hat stattdessen eine im kirchlichen Bereich übliche öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

## § 34
## Datenschutz-Folgenabschätzung

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

ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

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

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

1. systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;
2. umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß § 14 oder
3. systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

(4) Die Folgenabschätzung umfasst insbesondere:

1. eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von der verantwortlichen Stelle verfolgten berechtigten Interessen;
2. eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
3. eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen und
4. die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass die datenschutzrechtlichen Regelungen eingehalten werden.

(5) Die Aufsichtsbehörden sollen sowohl Listen zu Verarbeitungsvorgängen, für die gemäß Absatz 1 eine Datenschutz-Folgenabschätzung durchzuführen ist, als auch Listen zu Verarbeitungsvorgängen, für die keine Datenschutz-Folgenabschätzung erforderlich ist, erstellen und diese veröffentlichen.

(6) Die Aufsichtsbehörden sind gehalten, den Austausch mit staatlichen Aufsichtsbehörden und dem Europäischen Datenschutzausschuss zu suchen, um durch die Aufstellung aufeinander abgestimmter Listen die Zusammenarbeit zwischen kirchlichen und nichtkirchlichen Stellen zu erleichtern.

(7) Falls die Verarbeitung auf einer Rechtsgrundlage im kirchlichen, staatlichen oder europäischen Recht, dem die verantwortliche Stelle unterliegt, beruht und falls diese Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbei-

tungsvorgänge regeln und bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte, gelten die Absätze 1 bis 5 nicht.

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

(9) Die verantwortliche Stelle konsultiert vor der Verarbeitung die Aufsichtsbehörde, wenn aus der Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hat.

### § 35
### Audit und Zertifizierung

[1]Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch geeignete Stellen prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. [2]Näheres kann der Rat der Evangelischen Kirche in Deutschland durch Rechtsverordnung regeln.

## Kapitel 5
## Örtlich Beauftragte für den Datenschutz

### § 36
### Bestellung von örtlich Beauftragten für den Datenschutz

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

1. bei ihnen in der Regel mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten betraut sind, oder
2. die Kerntätigkeit der verantwortlichen Stelle in der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten besteht.
   Die Vertretung ist zu regeln.

(2) [1]Die Bestellung kann sich auf mehrere verantwortliche Stellen erstrecken. [2]Das Recht der Evangelischen Kirche in Deutschland, der Gliedkirchen und der gliedkirchlichen Zusammenschlüsse kann bestimmen, dass mehrere verantwortliche Stellen zur gemeinsamen Bestellung eines örtlich Beauftragten verpflichtet werden.

(3) [1]Zu örtlich Beauftragten dürfen nur Personen bestellt werden, die die zur Erfüllung ihrer Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzen. [2]Die Bestellung kann befristet für mindestens drei Jahre erfolgen.

(4) Zu örtlich Beauftragten sollen diejenigen nicht bestellt werden, die mit der Leitung der Datenverarbeitung beauftragt sind oder denen die Leitung der kirchlichen Stelle obliegt.

(5) [1]Die Bestellung von örtlich Beauftragten erfolgt schriftlich und ist der Aufsichtsbehörde und der nach dem jeweiligen Recht für die allgemeine Aufsicht zuständigen Stelle anzuzeigen; die Kontaktdaten sind zu veröffentlichen. [2]Ist der örtlich Beauftragte nicht Beschäftigter einer verantwortlichen Stelle, sind seine Leistungen vertraglich zu regeln.

(6) Soweit bei verantwortlichen Stellen keine Rechtsverpflichtung für die Bestellung von Personen als örtlich Beauftragte besteht, hat die Leitung die Erfüllung der Aufgabe in anderer Weise sicherzustellen.

## § 37
## Stellung

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

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

(3) [1]Zur Erlangung und zur Erhaltung der erforderlichen Fachkunde hat die verantwortliche Stelle den örtlich Beauftragten die Teilnahme an Fort- und Weiterbildungsveranstaltungen zu ermöglichen und die Kosten zu tragen. [2]Die dazu notwendige Freistellung hat ohne Minderung der Bezüge oder des Erholungsurlaubes zu erfolgen. [3]Im Konfliktfall kann die Aufsichtsbehörde angerufen werden.

(4) Betroffene Personen und Mitarbeitende können sich unmittelbar an die örtlich Beauftragten wenden.

(5) Staatliche Vorschriften über Zeugnisverweigerungsrechte für Datenschutzbeauftragte finden für örtlich Beauftragte entsprechende Anwendung.

(6) Die verantwortlichen Stellen stellen sicher, dass örtlich Beauftragte ordnungsgemäß und frühzeitig bei allen mit dem Schutz personenbezogener Daten zusammenhängenden Fragen beteiligt werden.

### § 38
### Aufgaben

[1]Die örtlich Beauftragten wirken auf die Einhaltung der Bestimmungen für den Datenschutz hin und unterstützen die verantwortlichen Stellen bei der Sicherstellung des Datenschutzes. [2]Sie haben insbesondere

1. die verantwortliche Stelle und die Beschäftigten zu beraten;
2. die ordnungsmäßige Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen;
3. die bei der Verarbeitung personenbezogener Daten tätigen Personen zu informieren und zu schulen;
4. mit der Aufsichtsbehörde zusammenzuarbeiten;
5. die verantwortliche Stelle bei der Datenschutz-Folgenabschätzung zu beraten und deren Durchführung zu überwachen.

## Kapitel 6
## Unabhängige Aufsichtsbehörden

### § 39
### Errichtung der Aufsichtsbehörden und Bestellung der Beauftragten für den Datenschutz

(1) [1]Über die Einhaltung dieses Kirchengesetzes in der Evangelischen Kirche in Deutschland, den Gliedkirchen und den gliedkirchlichen Zusammenschlüssen wachen unabhängige kirchliche Aufsichtsbehörden für den Datenschutz (Aufsichtsbehörden). [2]Jede Aufsichtsbehörde wird von einem oder einer Beauftragten für den Datenschutz geleitet und nach außen vertreten.

(2) Der Rat der Evangelischen Kirche in Deutschland errichtet die Aufsichtsbehörde für den Bereich der Evangelischen Kirche in Deutschland und ihres Evangelischen Werkes für Diakonie und Entwicklung sowie für die gesamtkirchlichen Werke und Einrichtungen und bestellt den Beauftragten oder die Beauftragte für den Datenschutz der Evangelischen Kirche in Deutschland.

(3) [1]Die Gliedkirchen und die gliedkirchlichen Zusammenschlüsse errichten die Aufsichtsbehörde für ihren Bereich einzeln oder gemeinschaftlich, soweit sie die Aufgaben nicht der Aufsichtsbehörde der Evangelischen Kirche in Deutschland übertragen. [2]Die

Gliedkirchen können für die ihnen zugeordneten diakonischen Dienste, Einrichtungen und Werke eigene Aufsichtsbehörden errichten.

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

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

## § 40
## Unabhängigkeit

(1) [1]Die Aufsichtsbehörden handeln bei der Erfüllung ihrer Aufgaben und bei der Ausübung ihrer Befugnisse völlig unabhängig. [2]Sie unterliegen weder direkter noch indirekter Beeinflussung von außen und ersuchen weder um Weisung noch nehmen sie Weisungen entgegen.

(2) Die Aufsichtsbehörden unterliegen der Rechnungsprüfung, soweit hierdurch die Unabhängigkeit nicht beeinträchtigt wird.

## § 41
## Tätigkeitsbericht

[1]Die Aufsichtsbehörden erstellen mindestens alle zwei Jahre einen Tätigkeitsbericht, der eine Liste der Arten der gemeldeten Verstöße und der Arten der getroffenen Maßnahmen enthalten kann. [2]Sie übermitteln den Bericht den jeweiligen kirchenleitenden Organen oder den jeweiligen Leitungsorganen der Diakonischen Werke und veröffentlichen ihn. [3]Auf dieser Grundlage können sie den leitenden Organen berichten.

## § 42
## Rechtsstellung

(1) [1]Den Aufsichtsbehörden werden die Finanzmittel zur Verfügung gestellt, die sie benötigen, um ihre Aufgaben und Befugnisse effektiv wahrnehmen zu können. [2]Die Finanzmittel sind in einem eigenen Haushaltsplan oder als Teil eines Gesamthaushaltes gesondert auszuweisen und zu verwalten.

(2) Die Aufsichtsbehörden wählen ihr Personal aus und besetzen die Personalstellen.

(3) Die Beauftragten für den Datenschutz sind die Vorgesetzten der Mitarbeitenden in den Aufsichtsbehörden.

(4) [1]Die Beauftragten für den Datenschutz bestellen aus dem Kreis ihrer Mitarbeitenden in den Aufsichtsbehörden einen Vertreter oder eine Vertreterin. [2]Vertreter oder Vertreterin können auch Beauftragte für den Datenschutz anderer Gliedkirchen oder der oder die Beauftragte für den Datenschutz der Evangelischen Kirche in Deutschland sein.

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

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

(7) [1]Beauftragte für den Datenschutz und ihre Mitarbeitenden dürfen, auch wenn sie nicht mehr im Amt sind, über Angelegenheiten, die der Verschwiegenheit unterliegen, ohne Genehmigung weder vor Gericht noch außergerichtlich aussagen oder Erklärungen abgeben. [2]Die Entscheidung über Aussagegenehmigungen treffen die Beauftragten für den Datenschutz für sich und ihre Mitarbeitenden in eigener Verantwortung. [3]Die Beauftragten für den Datenschutz gelten als oberste Aufsichtsbehörde im Sinne des § 99 Verwaltungsgerichtsordnung.

(8) [1]Eine Kündigung von Beauftragten für den Datenschutz im Arbeitsverhältnis ist während der Amtszeit nur zulässig, soweit Tatsachen vorliegen, die zu einer Kündigung aus wichtigem Grund berechtigen. [2]Dies gilt für den Zeitraum von einem Jahr nach Beendigung des Amtes entsprechend.

(9) Beauftragte für den Datenschutz im Kirchenbeamtenverhältnis scheiden während der Amtszeit aus dem Dienst aus, wenn nach den Bestimmungen der §§ 76, 77, 79 oder 80 des Kirchenbeamtengesetzes der EKD die Voraussetzungen einer Entlassung oder Gründe nach § 24 des Deutschen Richtergesetzes vorliegen, die bei einem Richter auf Lebenszeit dessen Entlassung aus dem Dienst rechtfertigen, oder wenn ein Disziplinargericht auf Entfernung aus dem Dienst erkennt.

## § 43
## Aufgaben

(1) Die Aufsichtsbehörden haben insbesondere die einheitliche Anwendung und Durchsetzung des kirchlichen Datenschutzrechtes in ihrem Zuständigkeitsbereich zu überwachen und sicherzustellen.

(2) [1]Sie sensibilisieren, informieren und beraten die kirchliche Öffentlichkeit sowie die verantwortlichen Stellen und kirchlichen Auftragsverarbeiter über Fragen und maßgebliche Entwicklungen des Datenschutzes sowie über die Vermeidung von Risiken. [2]Sie unterrichten betroffene Personen auf Anfrage über deren persönliche Rechte aus diesem Kirchengesetz, wobei spezifische Maßnahmen für Minderjährige besondere Beachtung finden.

(3) Sie schulen die örtlich Beauftragten und bilden sie fort.

(4) Werden personenbezogene Daten in Drittländern verarbeitet, prüfen die Aufsichtsbehörden die Einhaltung der datenschutzrechtlichen Vorgaben und beraten über Möglichkeiten einer gesetzeskonformen Verarbeitung.

(5) Die Aufsichtsbehörden können auf Anregung der kirchenleitenden Organe oder von Amts wegen Gutachten und Stellungnahmen zu Rechtssetzungsvorhaben, die sich auf den Schutz von personenbezogenen Daten auswirken, abgeben.

(6) Die Aufsichtsbehörden können auf Anregung der kirchenleitenden Organe oder von Amts wegen Musterverträge und Standards zur Verarbeitung personenbezogener Daten erstellen, deren Einsatz und Umsetzung überprüfen und die Ergebnisse veröffentlichen; sie sollen Listen gemäß § 34 Absatz 5 bereitstellen.

(7) Kirchliche Gerichte unterliegen der Prüfung durch die Aufsichtsbehörden nur, soweit sie in eigenen Angelegenheiten als Verwaltung tätig werden.

(8) [1]Der Prüfung durch die Aufsichtsbehörden unterliegen nicht:

1. Aufzeichnungen gemäß § 3 Satz 1;
2. personenbezogene Daten, die dem Post- und Fernmeldegeheimnis oder dem Arztgeheimnis unterliegen, sowie personenbezogene Daten in Personalakten, wenn die betroffene Person der Prüfung der auf sie bezogenen Daten im Einzelfall zulässigerweise gegenüber den Beauftragten für den Datenschutz widerspricht.

[2]Die Aufsichtsbehörden teilen die Ergebnisse ihrer Prüfungen den verantwortlichen Stellen mit. [3]Damit können Vorschläge zur Verbesserung des Datenschutzes, insbesondere zur Beseitigung von festgestellten Mängeln bei der Verarbeitung personenbezogener Daten, verbunden sein.

(9) [1]Die Beauftragten für den Datenschutz arbeiten zusammen und bilden eine Datenschutzkonferenz, auf der gemeinsame Stellungnahmen und Handreichungen zu Datenschutz- und Kohärenzfragen beschlossen werden können. [2]Sie tauschen mit den staatlichen Aufsichtsbehörden für den Datenschutz Erfahrungen und zweckdienliche Informationen aus und geben im Bedarfsfall Stellungnahmen ab.

## § 44
## Befugnisse

(1) [1]Die Aufsichtsbehörden können verlangen, dass die verantwortlichen Stellen sie bei der Erfüllung ihrer Aufgaben unterstützen. [2]Auf Verlangen ist ihnen Auskunft sowie Einsicht in alle Unterlagen und Akten über die Verarbeitung personenbezogener Daten zu geben, alle diesbezüglichen Informationen bereitzustellen, insbesondere über die gespeicherten Daten und über die eingesetzten Datenverarbeitungsprogramme. [3]Ihnen ist jederzeit Zutritt zu allen Diensträumen, einschließlich aller Verarbeitungsanlagen und -geräte zu gewähren, um Untersuchungen und Überprüfungen vorzunehmen. [4]Stellen Aufsichtsbehörden fest, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen dieses Kirchengesetz verstoßen, können sie Hinweise geben.

(2) [1]Stellen die Aufsichtsbehörden Verstöße gegen die Datenschutzbestimmungen oder sonstige Mängel bei der Verarbeitung personenbezogener Daten fest, so beanstanden sie dies gegenüber der verantwortlichen Stelle oder gegenüber dem Auftragsverarbeiter und fordern zur Stellungnahme innerhalb einer gesetzten Frist auf. [2]Von einer Beanstandung kann abgesehen werden, wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt. [3]Mit der Aufforderung zur Stellungnahme können Vorschläge zur Beseitigung der Mängel oder zur sonstigen Verbesserung des Datenschutzes verbunden werden. [4]Die Stellungnahme soll eine Darstellung der Maßnahmen enthalten, die aufgrund der Mitteilung der Aufsichtsbehörde getroffen worden sind.

(3) Um einen rechtmäßigen Zustand wiederherzustellen oder eine drohende Verletzung des Schutzes personenbezogener Daten abzuwenden, sind die Aufsichtsbehörden befugt, anzuordnen:

1. Verarbeitungsvorgänge auf bestimmte Weise und in einem bestimmten Zeitraum mit diesem Kirchengesetz in Einklang zu bringen;
2. Verarbeitungsvorgänge vorübergehend oder dauerhaft zu beschränken oder zu unterlassen;
3. die Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation auszusetzen;
4. personenbezogene Daten zu berichtigen, zu sperren oder zu löschen;
5. die von einer Verletzung des Schutzes personenbezogener Daten betroffene Person entsprechend zu benachrichtigen;
6. dem Antrag der betroffenen Person zu entsprechen.

(4) [1]Halten die Aufsichtsbehörden einen Angemessenheitsbeschluss der Europäischen Kommission nach § 10 Absatz 1 Nummer 1 oder eine von der Europäischen Kommission erlassene oder genehmigte Standarddatenschutzklausel nach § 10 Absatz 1 Nummer 2, auf deren Gültigkeit es bei der Entscheidung der Aufsichtsbehörden ankommt, für rechtswid-

rig, so können sie ihr Verfahren aussetzen und einen Antrag auf gerichtliche Entscheidung stellen. 2Soweit nicht Besonderheiten der kirchlichen Verwaltungsgerichtsordnung entgegenstehen, finden die Regelungen des § 21 des Bundesdatenschutzgesetzes entsprechende Anwendung.

## § 45
## Geldbußen

(1) Verstößt eine verantwortliche Stelle oder ein kirchlicher Auftragsverarbeiter vorsätzlich oder fahrlässig gegen Bestimmungen dieses Kirchengesetzes, so können die Aufsichtsbehörden Geldbußen verhängen oder für den Wiederholungsfall androhen. Gegen verantwortliche Stellen sind Geldbußen nur zu verhängen, soweit sie als Unternehmen im Sinne des § 4 Nummer 9 am Wettbewerb teilnehmen.

(2) Die Aufsichtsbehörden stellen 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 Betrag wird in jedem Einzelfall Folgendes gebührend berücksichtigt:

1. Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;
2. Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;
3. jegliche von der verantwortlichen Stelle oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;
4. der Grad der Verantwortung der verantwortlichen Stelle oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß § 27 getroffenen technischen und organisatorischen Maßnahmen;
5. etwaige einschlägige frühere Verstöße der verantwortlichen Stelle oder des Auftragsverarbeiters;
6. die Bereitschaft zur Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern;
7. die Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind;
8. die Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang die verantwortliche Stelle oder der Auftragsverarbeiter den Verstoß mitgeteilt hat;
9. die Einhaltung der früher gegen die verantwortliche Stelle oder den Auftragsverarbeiter in Bezug auf denselben Gegenstand angeordneten Maßnahmen, sofern solche Maßnahmen angeordnet wurden;

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

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

(5) Bei Verstößen werden im Einklang mit Absatz 3 Geldbußen von bis zu 500.000 Euro verhängt.

(6) Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich oder anstelle von Maßnahmen nach § 44 Absatz 3 verhängt.

## Kapitel 7
## Rechtsbehelfe und Schadensersatz

### § 46
### Recht auf Beschwerde

(1) Jede Person kann sich unbeschadet anderweitiger Rechtsbehelfe mit einer Beschwerde an die Aufsichtsbehörde wenden, wenn sie der Ansicht ist, bei der Verarbeitung ihrer personenbezogenen Daten in ihren Rechten verletzt worden zu sein.

(2) Die Aufsichtsbehörde unterrichtet die betroffene Person über den Stand und das Ergebnis der Beschwerde und weist auf die Möglichkeit gerichtlichen Rechtsschutzes gemäß § 47 hin.

(3) [1]Niemand darf wegen der Mitteilung von Tatsachen, die geeignet sind, den Verdacht aufkommen zu lassen, dieses Kirchengesetz oder eine andere Rechtsvorschrift über den Datenschutz sei verletzt worden, gemaßregelt oder benachteiligt werden. [2]Mitarbeitende müssen für Mitteilungen an die Aufsichtsbehörde nicht den Dienstweg einhalten.

### § 47
### Rechtsweg

(1) Der Rechtsweg zu den kirchlichen Verwaltungsgerichten ist eröffnet

1. für Klagen gegen Verwaltungsakte und andere Entscheidungen der Aufsichtsbehörden,
2. für Klagen in Fällen, in denen sich die Aufsichtsbehörde nicht mit einer Beschwerde gemäß § 46 befasst oder die betroffene Person nicht innerhalb von drei Monaten über den Stand oder das Ergebnis der erhobenen Beschwerde in Kenntnis gesetzt hat,

3. für Klagen betroffener Personen gegen kirchliche Stellen und Auftragsverarbeiter wegen einer Verletzung ihrer Rechte aus diesem Kirchengesetz,
4. für Klagen der Aufsichtsbehörden gegen kirchliche Stellen und Auftragsverarbeiter, soweit dies zur Durchsetzung ihrer Befugnisse erforderlich ist.

(2) Vor Erhebung einer Klage nach Absatz 1 Nummer 1 oder 3 ist nach Maßgabe des jeweils anwendbaren Rechts ein Vorverfahren durchzuführen.

### § 48
### Schadensersatz durch verantwortliche Stellen

(1) [1]Jede Person, der wegen einer Verletzung der Regelungen über den kirchlichen Datenschutz ein Schaden entstanden ist, hat nach diesem Kirchengesetz Anspruch auf Schadensersatz gegen die verantwortliche Stelle. [2]Wegen eines Schadens, der nicht Vermögensschaden ist, kann die betroffene Person eine angemessene Entschädigung in Geld verlangen.

(2) Eine verantwortliche Stelle wird von der Haftung gemäß Absatz 1 befreit, wenn sie nachweist, dass sie für den eingetretenen Schaden nicht 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.

## Kapitel 8
## Vorschriften für besondere Verarbeitungssituationen

### § 49
### Verarbeitung personenbezogener Daten bei Dienst- und Arbeitsverhältnissen

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

(2) Im Zusammenhang mit dem Verdacht auf Straftaten und Amtspflichtverletzungen, die durch Beschäftigte begangen wurden, insbesondere zum Schutz möglicher Betroffener,

dürfen unter Beachtung des Verhältnismäßigkeitsgrundsatzes personenbezogene Daten von Beschäftigten verarbeitet werden, solange der Verdacht nicht ausgeräumt ist und die Interessen von möglichen Betroffenen dies erfordern.

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

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

1. die empfangende Person oder Stelle ein überwiegendes rechtliches Interesse darlegt;
2. Art oder Zielsetzung der dem oder der Beschäftigten übertragenen Aufgaben die Offenlegung erfordert;
3. offensichtlich ist, dass die Offenlegung im Interesse der betroffenen Person liegt und keine Anhaltspunkte vorliegen, dass sie in Kenntnis des Zwecks der Offenlegung ihre Einwilligung nicht erteilen würde oder
4. sie zur Aufdeckung einer Straftat oder Amtspflichtverletzung oder zum Schutz möglicher Betroffener erforderlich erscheint.

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

(6) [1]Verlangt die verantwortliche Stelle zur Begründung oder im Rahmen eines Beschäftigungsverhältnisses medizinische oder psychologische Untersuchungen und Tests, hat sie Anlass und Zweck der Begutachtung möglichst tätigkeitsbezogen zu bezeichnen. [2]Ergeben sich keine medizinischen oder psychologischen Bedenken, darf die verantwortliche Stelle lediglich die Offenlegung des Ergebnisses der Begutachtung verlangen; ergeben sich Bedenken, darf auch die Offenlegung der festgestellten möglichst tätigkeitsbezogenen Risikofaktoren verlangt werden. [3]Im Übrigen ist eine Weiterverarbeitung der bei den Untersuchungen oder Tests erhobenen Daten ohne schriftliche Einwilligung der betroffenen Person nur für den Zweck zulässig, für den sie erhoben worden sind.

(7) [1]Personenbezogene Daten, die vor Begründung eines Beschäftigungsverhältnisses erhoben wurden, sind unverzüglich zu löschen, sobald feststeht, dass ein solches nicht zustande kommt. [2]Dies gilt nicht, soweit überwiegende berechtigte Interessen der verantwortlichen Stelle der Löschung entgegenstehen oder die betroffene Person in die weitere Speicherung einwilligt. [3]Nach Beendigung eines Beschäftigungsverhältnisses sind personenbezogene Daten zu löschen, soweit diese Daten nicht mehr benötigt werden.

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

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

## § 50
## Verarbeitung personenbezogener Daten für wissenschaftliche und statistische Zwecke

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

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

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

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

1. die betroffene Person eingewilligt hat oder
2. dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist,

es sei denn, dass Grund zu der Annahme besteht, dass durch die Veröffentlichung der Auftrag der Kirche gefährdet würde.

## § 51
## Verarbeitung personenbezogener Daten durch die Medien

(1) Soweit personenbezogene Daten von verantwortlichen Stellen ausschließlich für eigene journalistisch-redaktionelle oder literarische Zwecke verarbeitet werden, gelten von den Vorschriften dieses Kirchengesetzes nur die §§ 8, 22, 25, 26 und 48. Hierunter fällt die Herausgabe von Adressen-, Telefon- oder vergleichbaren Verzeichnissen nur, wenn mit ihr zugleich eine journalistisch-redaktionelle oder literarische Tätigkeit verbunden ist.

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

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

## § 52
## Videoüberwachung öffentlich zugänglicher Räume

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

1. in Ausübung des Hausrechts der kirchlichen Stelle oder
2. zum Schutz von Personen und Sachen

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

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

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

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

1. solange das öffentliche Interesse an der Strafverfolgung das Recht auf Benachrichtigung der betroffenen Person erheblich überwiegt oder
2. wenn die Benachrichtigung im Einzelfall einen unverhältnismäßigen Aufwand erfordert.

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

### § 53
### Gottesdienste und kirchliche Veranstaltungen

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

## Kapitel 9
## Schlussbestimmungen

### § 54
### Ergänzende Bestimmungen

(1) Der Rat der Evangelischen Kirche in Deutschland kann durch Rechtsverordnung mit Zustimmung der Kirchenkonferenz Durchführungsbestimmungen zu diesem Kirchengesetz und ergänzende Bestimmungen zum Datenschutz erlassen.

(2) Die Gliedkirchen können für ihren Bereich Durchführungsbestimmungen zu diesem Kirchengesetz und ergänzende Bestimmungen zum Datenschutz erlassen, soweit sie dem Recht der Evangelischen Kirche in Deutschland nicht widersprechen.

(3) [1]Soweit personenbezogene Daten von Sozialleistungsträgern offengelegt werden, gelten zum Schutz dieser Daten ergänzend die staatlichen Bestimmungen entsprechend. [2]Werden hierzu Bestimmungen gemäß Absatz 1 erlassen, ist vorher das Evangelische Werk für Diakonie und Entwicklung anzuhören.

(4) Dieses Kirchengesetz soll innerhalb von fünf Jahren überprüft werden.

### § 55
### Übergangsregelungen

(1) [1]Bisherige Bestellungen der Beauftragten für den Datenschutz gemäß den §§ 18 bis 18b des EKD-Datenschutzgesetzes in der Fassung der Bekanntmachung vom 1. Januar 2013 (ABl. EKD S. 2, S. 34) gelten fort. [2]Für diese Bestellungen gelten die Regelungen der §§ 39 bis 45 mit Inkrafttreten dieses Kirchengesetzes.

(2) [1]Bisherige Bestellungen der Betriebsbeauftragten und örtlichen Beauftragten für den Datenschutz gemäß § 22 des EKD-Datenschutzgesetzes in der Fassung der Bekanntmachung vom 1. Januar 2013 (ABl. EKD S. 2, S. 34) gelten fort. [2]Für diese Bestellungen gelten die Regelungen der §§ 36 bis 38 mit Inkrafttreten dieses Kirchengesetzes.

(3) Vereinbarungen nach § 11 des EKD-Datenschutzgesetzes in der Fassung der Bekanntmachung vom 1. Januar 2013 (ABl. EKD S. 2, S. 34), gelten fort und sind spätestens bis zum 31. Dezember 2019 an dieses Kirchengesetz anzupassen.

(4) [1]Verfahrensverzeichnisse betreffend die Videoüberwachung gemäß § 52 sind bis zum 24. Mai 2018 zu erstellen. [2]Die Erstellung der Verfahrensverzeichnisse nach § 31 dieses Kirchengesetzes hat bis zum 30. Juni 2019 zu erfolgen.

## § 56
## Inkrafttreten, Außerkrafttreten

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

# A2 Vorlage einer Datenschutzerklärung

## 1. Allgemeine Informationen

### 1.1 Einleitung

Wir freuen uns über Ihren Besuch auf unserer Internetseite und dem Interesse an der kirchlichen Arbeit. Gemäß § 13 Abs. 1 Telemediengesetz (TMG) in Verbindung mit dem Datenschutzgesetz der Evangelischen Kirche in Deutschland (DSG-EKD) informieren wir Sie über die Art, den Umfang und den Zweck der auf unserer Internetseite erhobenen personenbezogenen Daten. Personenbezogene Daten sind alle Angaben zu einer bestimmten oder durch diese Daten bestimmbaren natürlichen Person, wie z.B. Name, Anschrift, E-Mail, Telefonnummer.

Wir verwenden Ihre Daten ausschließlich im Rahmen des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD), das die Vorgaben der Datenschutzgrundverordnung der Europäischen Union (DSGVO) im Bereich der evangelischen Kirchen umsetzt. Zur Einhaltung dieser Vorschriften haben wir umfangreiche technische und organisatorische Maßnahmen getroffen, um die Sicherheit ihrer Daten zu gewährleisten.

### 1.2 Verantwortliche kirchliche Stelle

Verantwortliche Stelle für die Verarbeitung Ihrer personenbezogenen Daten ist:

*(Hier bitte den Anbieter der Webseite nennen. Im Fall der Webseiten im System max-e ist dies die Digitale Agentur der Evangelischen Medienarbeit.)*

### 1.3 Örtlicher Datenschutzbeauftragter

Sollten Sie zu den in unserer Datenschutzerklärung dargestellten Maßnahmen noch Fragen haben, so können Sie sich an unseren örtlichen Datenschutzbeauftragten wenden.

*(Hier bitte Name und Kontaktdaten des örtlichen Datenschutzbeauftragten nennen.)*

## 2. Verarbeitung Ihrer personenbezogenen Daten beim Besuch unserer Internetseite

Grundsätzlich können Sie unsere Seiten nutzen, ohne uns mitzuteilen, wer Sie sind. Aus technischen Gründen und aus Gründen der Datensicherheit sowie zur Optimierung unserer Online-Angebote, verarbeiten wir jedoch Ihre IP-Adresse, den Namen Ihres Internet-Providers, die Internetseite von der Sie uns besuchen, den genutzten Browsertyp, das verwendete Betriebssystem und die Seiten, die Sie bei uns auswählen, sowie das Datum und die Uhrzeit Ihres Zugriffs. Wir nutzen diese Informationen ausschließlich für systemrelevante und statistische Zwecke, die grundsätzlich in anonymisierter Form erfolgen, so dass Rückschlüsse auf Ihre Person nicht möglich sind.

Für die Nutzung einzelner Angebote (z.B. Cookies) können sich hiervon Abweichungen ergeben, die weiter untern gesondert erläutert werden.

In diesem Zusammenhang weisen wir insbesondere darauf hin, dass die Datenübertragung im Internet immer auch Sicherheitslücken aufweist, so dass ein lückenloser Schutz vor Zugriffe Dritter nicht möglich ist.

## 3. Verwendung von Cookies und Tracking

### 3.1 Cookies

Wir verwenden auf unseren Seiten sogenannte Cookies. Das sind kleine Textdateien, die auf Ihrem Endgerät gespeichert werden und uns eine Analyse der Nutzung unserer Seiten ermöglichen. Die durch die Cookies erzeugten Informationen verwenden wir, um unsere Seiten für Sie als Nutzer attraktiver zu gestalten und um bestimmte Funktionen unserer Seiten zu gewährleisten. Einige von uns verwendete Cookies werden direkt nach Ihrem Besuch unserer Seiten wieder gelöscht (sog. Session-Cookies). Andere ermöglichen es uns, Sie bei späteren Besuchen auf unseren Seiten wiederzuerkennen (sog. Persistente Cookies).

Sie können die Installation von Cookies durch eine entsprechende Einstellung im Browser verhindern, oder sich durch die Browser-Software vor dem Setzen eines Cookie informieren lassen. Bei Letzterem können Sie individuell entscheiden, ob ein Cookie gesetzt werden darf oder nicht. Wir weisen jedoch darauf hin, wenn Sie das Setzen von Cookies generell nicht akzeptieren, kann die Funktionalität unserer Seiten eingeschränkt sein.

### 3.2 Einsatz von Google-Analytics mit Anonymisierungsfunktion

Auf unseren Seiten setzen wir Google-Analytics ein. Google-Analytics ist ein Webanalysedienst der Firma Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043 USA. Google-Analytics verwendet ebenfalls Cookies, die auf Ihrem Computer gespeichert werden, um eine Analyse der Benutzung unserer Seiten durchzuführen. Die durch die Cookies erzeugten Informationen, z.B. IP-Adresse, Datum, Zeit, Ort und Häufigkeit Ihres Besuchs auf unseren Seiten, werden in der Regel an Server von Google in den USA übertragen und dort gespeichert. Erfolgt der Zugriff auf unseren Seiten innerhalb der Mitgliedsstaaten der Europäischen Union, oder anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum, so kürzt Google Ihre IP-Adresse vor einer Übertragung auf Server in den USA (Anonymisierungsfunktion). Nur in Ausnahmefällen wird die volle IP-Adresse an Server von Google in den USA übertragen und dort gekürzt.

Google verwendet die über Cookies gewonnenen Informationen, um die Nutzung unserer Seiten auszuwerten, um Berichte über Aktivitäten auf unseren Seiten für uns zusammenzustellen und um weitere mit der Nutzung unserer Seiten verbundene Dienstleistungen für uns zu erbringen. Google wird die gewonnenen Informationen evtl. an Dritte übertragen, soweit dies gesetzlich vorgeschrieben ist, oder Dritte die Daten im Auftrag von Google verarbeiten. Die durch Google Analytics ermittelte IP-Adresse wird

nach Angaben von Google nicht mit anderen Daten von Google zusammengeführt.

Sie können die Installation von Google-Cookies durch entsprechende Einstellungen im Browser verhindern, oder sich durch die Browser-Software vor dem Setzen eines Cookie informieren lassen. Bei Letzterem können Sie individuell entscheiden, ob ein Cookie gesetzt werden darf oder nicht. Wir weisen jedoch darauf hin, wenn Sie das Setzen von Cookies generell nicht akzeptieren, kann die Funktionalität unserer Seiten eingeschränkt sein. Darüber hinaus haben Sie die Möglichkeit die Erfassung Ihrer Seiten-Nutzung (inkl. Ihrer IP-Adresse) durch Google, sowie die Verarbeitung dieser Daten durch Google, zu verhindern, indem sie das unter dem folgenden Link verfügbare Browser-Plugin herunterladen und installieren:

**https://tools.google.com/dlpage/gaoptout?hl=de**

Die Nutzung dieser Deaktivierungsfunktion verhindert aber nicht, dass Informationen an uns oder an andere von uns gegebenenfalls eingesetzte Analyse-Software übermittelt wird.

### 3.3 Einsatz von Google-Maps

Auf unseren Seiten verwenden wir Google-Maps, um geographische Informationen direkt auf unseren Seiten visuell darzustellen. Google-Maps ist ein Dienst der Firma Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043 USA. Wenn Sie Google-Maps auf unseren Seiten aufrufen, wird von Google ein Cookie auf Ihrem Endgerät gesetzt, um die Nutzung der Maps-Funktionen auf unseren Seiten auszuwerten.

Wenn Sie die Verarbeitung Ihrer Daten durch Google-Maps nicht möchten, so haben Sie die Möglichkeit die Installation dieser Cookies durch entsprechende Einstellungen im Browser zu verhindern, oder sich durch die Browser-Software vor dem Setzen eines Cookie informieren zu lassen. Bei Letzterem können Sie individuell entscheiden, ob ein Cookie gesetzt werden darf oder nicht. Wir weisen jedoch darauf hin, wenn Sie das Setzen von Cookies generell nicht akzeptieren, kann die Funktionalität unserer Seiten eingeschränkt sein.

Die Nutzung von Google-Maps erfolgt entsprechend den Google-Nutzungsbedingungen, die Sie über folgenden Link einsehen können:

**http://www.google.de/intl/de/policies/terms/regional.html**

Die zusätzlichen Nutzungsbedingungen für Google-Maps erreichen Sie über folgendem Link:

**https://www.google.com/intl/de_de/help/terms_maps.html**

### 3.4 Einsatz von reCAPTCHA

Auf unseren Seiten verwenden wir reCAPTCHA. ReCAPTCHA ist ein Dienst der Firma Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043 USA. Mit reCAPTCHA schützen wir unsere Dateneingabeformulare, indem wir mit diesem Dienst feststellen können, ob die Dateneingabe menschlichen Ursprungs ist, oder missbräuchlich durch automatisierte maschinelle Verarbeitung erfolgt.

Unseres Wissens werden bei der Überprüfung durch reCAPTCHA neben Ihrer IP-Adresse, Informationen über das Betriebssystem, den Browsertyp, die Verweildauer, das Eingabeverhalten des Nutzers inkl. aller Mausbewegungen an Google übertragen. Google verwendet diese Informationen zur

Optimierung seiner Produkte. Nach Angaben von Google wird die durch reCAPTCHA übermittelte IP-Adresse nicht generell mit anderen Daten von Google zusammengeführt. Das geschieht aber, wenn Sie sind zu diesem Zeitpunkt bei Ihrem Google-Konto angemeldet haben.

Wenn Sie diese Datenübermittlung an Google nicht möchten, müssen Sie sich bei Ihrem Google-Konto abmelden, bevor Sie unsere Seite besuchen. Weitere Informationen zu den Datenschutzrichtlinien von Google finden Sie unter:

**http://www.google.de/intl/de/privacy**

oder

**https://www.google.com/intl/de/policies/privacy**

### 3.5 Einsatz von Facebook-Komponenten

Auf unseren Seiten setzen wir Social Media Plugins von Facebook ein, um unsere Seiten persönlicher zu gestalten. Diese Plugins sind Komponenten der Firma Facebook Inc., 1601 S. California Ave, Palo Alto, CA 94304, USA.

Wenn Sie unsere Seiten aufrufen, die ein Facebook-Plugin enthalten, wird eine direkte Verbindung zwischen Ihrem Browser und Servern von Facebook hergestellt. Durch diesen Verbindungsaufbau erfährt Facebook davon, welche Seite bzw. Unterseite durch Ihren Browser gerade bei uns aufgerufen wird, auch wenn Sie kein Facebook-Konto besitzen. Wenn Sie während des Aufrufs unserer Seiten bei Ihrem Facebook-Konto angemeldet sind, ordnet Facebook diese Informationen Ihrem persönlichen Konto bei Facebook zu. Das gilt insbesondere auch dafür, wenn Sie z.B. den Gefällt-mir-Button anklicken und einen Kommentar dazu schreiben. Diese Informationen werden an Facebook übertagen und zu Ihrem persönlichen Benutzerkonto bei Facebook gespeichert. Sie werden zudem auf Facebook veröffentlicht und Ihren Facebook-Freunden angezeigt.

Facebook verwendet diese Informationen zu Werbezwecken, Marktforschung und bedarfsgerechte Gestaltung der Facebook-Seiten. Hierzu erstellt Facebook Nutzungs-, Interessen- und Beziehungsprofile, um z.B. die Nutzung unserer Seiten bezüglich eingeblendeter Werbeanzeigen auszuwerten, anderen Facebook-Nutzern über Ihre Aktivitäten zu informieren und um weitere mit der Nutzung von Facebook verbundene Dienstleistungen zu erbringen. Wenn Sie diese Datenübermittlung an Facebook nicht möchten, müssen Sie sich bei Facebook abmelden, bevor Sie unsere Seiten aufrufen.

Weitere Datenschutzhinweise von Facebook finden Sie unter folgendem Link:

**https://de-de.facebook.com/about/privacy**

und Informationen zu Facebook-Plugins finden Sie unter:

**https://developers.facebook.com/docs/plugins**

### 3.6 Einsatz von Twitter

Auf unseren Seiten verwenden wir Social Media Plugins des Kurznachrichtendienstes Twitter. Twitter ist ein Dienst der Twitter Inc., 795 Folsom St., Suite 600, San Francisco, CA 94107, USA.

Wenn Sie unsere Seiten aufrufen, die ein solches Plugin von Twitter enthalten, wird eine direkte Verbindung zwischen Ihrem Browser und Twitter-Servern hergestellt. Durch diese Verbindungsaufnahme zu Twitter, wird Twitter darüber informiert, dass Sie mit Ihrer IP-Adresse unsere Seiten aufgerufen haben. Wenn Sie den Tweet-Button von Twitter auf unseren Seiten anklicken,

während Sie bei Ihrem Twitter-Konto angemeldet sind, können Sie die Inhalte unserer Seiten auf Ihrem Twitter-Profil verlinken. Dadurch ordnet Twitter den Besuch auf unseren Seiten Ihrem Konto bei Twitter zu. Wir weisen darauf hin, dass wir weder Einfluss noch Kenntnis davon haben, welche Daten an Twitter übermittelt werden und wie deren Nutzung durch Twitter erfolgt.

Weitere Informationen finden Sie in der Datenschutzerklärung von Twitter unter:
**http://twitter.com/privacy**
Ihre Datenschutzeinstellungen können Sie in den Konto-Einstellungen unter:
**http://twitter.com/account/settings**
ändern.

### 3.7 Einsatz von YouTube-Komponenten

Auf unseren Seiten setzen wir Video-Komponenten der Firma YouTube, LLC 901 Cherry Ave., 94066 San Bruno, CA, USA ein. YouTube ist ein Unternehmen der Google LLC, Amphitheatre Parkway, Mountain View, CA 94043, USA.

Wir nutzen YouTube mit der Option -erweiterter Datenschutzmodus-. Wenn Sie unsere Seiten aufrufen, die ein eingebettetes YouTobe-Video enthalten, wird eine Verbindung zu YouTube-Servern hergestellt und der Inhalt des Videos in Ihrem Browser auf unseren Seiten dargestellt. Das YouTube-Plugin übermittelt im -erweiterten Datenschutzmodus- nur die Bezeichnung der Seite an YouTube Server die Sie besuchen, wenn Sie das Video anschauen. Haben Sie sich an Ihrem YouTube-Konto angemeldet, werden diese Informationen Ihrem Konto bei YouTube zugeordnet. Wenn Sie das nicht möchten, müssen Sie sich vor dem Besuch unserer Seiten von Ihrem YouTube-Konto abmelden.

Weitere Informationen zum Datenschutz von YouTube finden Sie unter folgendem Link:
**https://www.google.de/intl/de/policies/privacy/**

### 3.8 Einsatz von Vimeo-Komponenten

Auf unseren Seiten kommen Video-Komponenten der Firma Vimeo zum Einsatz. Vimeo ist ein Dienst der Vimeo LLC, 555 West 18th Street, New York, New York 10011, USA.

Wenn Sie unsere Seiten aufrufen, die ein eingebettetes Vimeo-Video enthalten, wird eine Verbindung zu Vimeo-Servern hergestellt und der Inhalt des Videos in Ihrem Browser auf unseren Seiten dargestellt. Das Vimeo-Plugin übermittelt dabei an Vimeo-Server die Bezeichnung der Seite die Sie besuchen, wenn Sie das Video anschauen. Haben Sie sich an Ihrem Vimeo-Konto angemeldet, werden diese Informationen Ihrem Konto bei Vimeo zugeordnet. Wenn Sie das nicht möchten, müssen Sie sich vor dem Besuch unserer Seite von Ihrem Vimeo-Konto abmelden.

Weitere Informationen zum Datenschutz von Vimeo finden Sie unter folgendem Link, insbesondere zur Erhebung und Nutzung der Daten durch Vimeo:
**https://vimeo.com/privacy**

### 3.9 Einsatz von Social Media Schaltflächen mit Shariff

Auf unseren Seiten verwenden wir Shariff-Schaltflächen. Shariff wurde von Spezialisten der Computerzeitschrift c't entwickelt, um mehr Privatsphäre im Internet zu ermöglichen. Die Shariff-Schaltflächen ersetzen dabei die üblichen Share-Buttons der sozialen Netzwerke und schützen dadurch die Nutzer.

Wenn Sie unsere Seiten aufrufen, die Shariff-Schaltflächen enthalten, findet nicht sofort eine Verbindungsaufnahme zu Servern der sozialen Netzwerke statt. Erst durch einen Klick auf die entsprechende Schaltfläche des sozialen Netzwerks wird eine Verbindung zum jeweiligen sozialen Netzwerk hergestellt und erst dann werden Ihre Daten an das soziale Netzwerk übertragen. Auf unseren Seiten binden die sozialen Netzwerke Facebook und Twitter mit Shariff ein.

Weitere Informationen über das das c't-Projekt „Shariff" finden Sie unter

**http://www.heise.de/ct/artikel/Shariff-Social-Media-Buttons-mit-Datenschutz-2467514.html**

### 3.10 Einsatz von Instagram

Auf unseren Seiten verwenden wir Instagram. Instagram ist ein Dienst der Instagram LLC., 1601 Willow Road, Menlo Park, CA 94025, USA.

Wenn Sie Seiten unseres Webauftritts aufrufen, die ein solches Plugin enthalten (z.B. Instagram-Kamera Logo), stellt Ihr Browser eine direkte Verbindung zu den Servern von Instagram her. Durch das eingebundene Instagram-Plugin erfährt Instagram, dass Sie unsere Seiten aufgerufen haben. Sind Sie bei Ihrem Instagram-Konto angemeldet, ordnet Instagram den Besuch auf unseren Seiten Ihrem Instagram-Konto zu und speichert diese Daten auf Instagram-Servern in den USA ab. Wenn Sie nicht möchten, dass Instagram den Besuch auf unseren Seiten Ihrem Instagram-Konto zuordnet, müssen Sie sich vor dem Besuch unserer Seiten bei Instagram abmelden.

Weitere Informationen hierzu finden Sie in der Datenschutzerklärung von Instagram unter dem Link:

**https://help.instagram.com/155833707900388**

## 4. Freiwillige Bereitstellung personenbezogener Daten

### 4.1 Kontaktmöglichkeiten

Unsere Seiten bieten Ihnen die Möglichkeit direkt per E-Mail und / oder über ein Kontaktformular mit uns in Verbindung zu treten. Stellen Sie uns Ihre personenbezogenen Daten zum Zweck der Kontaktaufnahme zur Verfügung, verarbeiten wir Ihre Daten ausschließlich für die Korrespondenz mit Ihnen. Eine Weitergabe an Dritte erfolgt nicht.

### 4.2 Newsletter

Auf unseren Seiten können Sie einen von uns bereitgestellten Newsletter abonnieren. Mit dem Newsletter erhalten Sie regelmäßig Informationen über aktuelle christliche und gesellschaftliche Themen und besondere Hinweise auf kirchliche Seminare und Veranstaltungen. Wenn Sie das möchten, füllen Sie das zugehörige Anmeldeformular aus und klicken auf Newsletter jetzt abonnieren. Sie erhalten dann eine E-Mail von uns an die von Ihnen angegebene E-Mail-Adresse. Um die Registrierung für den Newsletter abzuschließen, klicken Sie in der E-Mail auf den Link Anmeldung bestätigen. Mit der dadurch erfolgten Registrierung speichern wir Ihre personenbezogenen Daten (Anrede, Name, E-Mail, IP-Adresse, sowie das Datum und die Uhrzeit Ihrer Anmeldung) und senden Ihnen bis zu einer Abmeldung unseren Newsletter zu.

Die im Rahmen der Newsletter-Anmeldung verarbeiteten Daten verwenden wir ausschließlich um Ihnen unseren Newsletter zuzusenden. Eine Weitergabe Ihrer Daten an Dritte erfolgt nicht. Unseren Newsletter können Sie jederzeit kündigen. Dazu schreiben

Sie uns einfach eine E-Mail, oder beachten die Abmeldehinweise am Ende eines jeden Newsletters. Kontaktdaten, an die Sie sich wenden können, finden Sie im Impressum.

### 4.3 Bewerbungen auf Stellenanzeigen

Soweit wir offene Stellen haben, veröffentlichen wir auf unseren Seiten Stellenanzeigen. Auf die Stellenanzeigen können Sie sich mit den sonst auch üblichen Unterlagen bewerben. Bewerben Sie sich bei uns, speichern wir Ihre personenbezogenen Daten in unserer Interessenten-Datenbank.

Erfolgt auf Ihre Bewerbung hin eine Anstellung, übernehmen wir Ihre im Rahmen der Bewerbung angegebenen personenbezogenen Daten in die Personalakte. Die Weiterverarbeitung Ihrer Bewerberdaten erfolgt dann, im sonst auch üblichen Rahmen rechtlicher Vorschriften bei einem Anstellungsverhältnis.

Erfolgt keine Anstellung bei uns, so löschen wir Ihre Bewerbungsdaten unter Berücksichtigung des Allgemeinen Gleichbehandlungsgesetzes spätestens sechs Monate nach Mitteilung einer Ablehnung aus unserer Interessenten-Datenbank. Es sei denn, Sie haben uns ausdrücklich Ihre Einwilligung für eine längere Speicherung gegeben (z.B. für evtl. andere freiwerdende Stellen).

## 5. Auskunft/Widerruf/ Berichtigung/Löschung

Sie können sich aufgrund des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) bei Fragen zur Erhebung, Verarbeitung oder Nutzung Ihrer personenbezogenen Daten und deren Berichtigung, Sperrung, Löschung oder einem Widerruf einer erteilten Einwilligung unentgeltlich an uns wenden. Wir weisen ebenfalls darauf hin, dass Ihnen ein Recht auf Berichtigung falscher Daten oder Löschung personenbezogener Daten zusteht, sollte diesem Anspruch keine gesetzliche Aufbewahrungspflicht entgegenstehen.

Zur Ausübung Ihrer Rechte wenden Sie sich bitte an die im Impressum unter „Redaktionelle Verantwortung" angegebenen E-Mail oder postalische Adresse.

### 6. Beschwerderecht

Wenn Sie der Ansicht sind, dass die Verarbeitung Ihrer personenbezogenen Daten rechtswidrig erfolgt, können Sie sich jederzeit an die für uns zuständige Aufsichtsbehörde unter folgenden Kontaktdaten wenden:

Der Beauftragte für den Datenschutz der Evangelischen Kirche in Deutschland
Dienststelle BfD EKD, Böttcherstraße 7, 30419 Hannover, Tel.: 0049(0)511-169 335-0

# A3 Muster für ein Impressum

Die Pflichtangaben für ein rechtskonformes Impressum für Kirchengemeinden ergeben sich aus § 5 Telemediengesetz (TMG)[1] sowie § 55 Abs. 2 Rundfunkstaatsvertrag (RStV). Gem. § 5 TMG8 sind notwendige Angaben:

- Name des Dienstanbieters
- Rechtsform
- Adresse (= ladungsfähige Anschrift, kein Postfach)
- Vorname, Name des Vertretungsberechtigten
- Kontaktdaten („Angaben, die eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation mit ihnen ermöglichen, einschließlich der Adresse der elektronischen Post“
- E-Mail-Adresse (zwingend!)
- Telefonnummer (nicht zwingend, aber anzuraten)
- Faxnummer (wenn vorhanden, anzuraten)
- Sofern vorhanden (z.B. bei einer gGmbH): Umsatzsteuer-Identifikationsnummer oder Wirtschafts-Identifikationsnummer
- Diese Angaben müssen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar sein. Gem. § 55 Abs. 2 RStV[2] sind für journalistisch-redaktionell gestaltete Angebote zusätzlich folgende Angaben notwendig:
- Verantwortlicher für redaktionelle Inhalte (Name, Anschrift)

Bitte die weiteren gesetzlichen Voraussetzungen wie z. B. Aufenthalt des für die redaktionellen Inhalte Verantwortlichen im Inland beachten

Weitere Einzelheiten zum Impressum können Sie – wenn gewünscht – einem Leitfaden des Bundesministeriums der Justiz[3] oder der Webseite http://www.anbieterkennung.de entnehmen.

Die einzelnen Kirchengemeinden der Landeskirche Hannovers ordnen und verwalten ihre Angelegenheiten selbständig. Daher ergibt sich folgendes Musterimpressum:

Die (Name der Kirchengemeinde) ist eine Körperschaft des öffentlichen Rechts mit Sitz in (Ort) und wird durch den Kirchenvorstand vertreten.

- Inhaltlich verantwortlich gemäß § 55 Abs. 2 RStV:
- Verantwortlicher (Vor- und Nachname)
- Telefon
- Telefax
- E-Mail

1 Vgl. www.gesetze-im-internet.de/tmg/__5.html

2 Vgl. www.urheberrecht.org/law/normen/rstv/RStV13/text/2010_06. php3

3 Vgl. http://tinyurl.com/d6vb79w

# A4 Muster-Einwilligung zur Veröffentlichung von Daten auf der Webseite

Gemeinde: _____

Anschrift: _____

_____

Einwilligungserklärung für die Veröffentlichung von Daten auf der Webseite der Kirchengemeinde

Name/Vorname: _____

Anschrift: _____

_____

Ich stimme der Veröffentlichung meiner Daten auf der Webseite der Kirchengemeinde zu:

(Zutreffendes bitte ankreuzen)

- ☐ Name
- ☐ Vorname
- ☐ Adresse
- ☐ Funktion
- ☐ Telefonnummer
- ☐ Handynummer
- ☐ E-mail Adresse
- ☐ Beruf
- ☐ _____

Die erfassten Daten werden ausschließlich für kirchengemeindliche Zwecke verwendet. Eine Nutzung für andere Zwecke bedarf der erneuten Zustimmung.

Mir ist bekannt, dass Daten aus dem Internet kopiert, woanders verwendet oder auch verändert werden können, ohne dass die Kirchengemeinde darauf Einfluss hat.

Eine erteilte Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden. Die Einwilligung kann unter Bedingungen oder mit Auflagen erteilt werden.

Bei minderjährigen Kindern/Jugendlichen hat die Unterzeichnung in der Regel durch alle sorgeberechtigten Personen zu erfolgen. Unterschreibt ein Personensorgeberechtigter allein, so versichert er mit seiner Unterschrift, dazu von allen Personensorgeberechtigten ermächtigt worden zu sein. Bei Jugendlichen (14–17 Jahre) kann ihre/seine Unterschrift erforderlich sein.

_____ _____

Datum Unterschrift

# A5 Zusatzvereinbarung zur Verarbeitung personenbezogener Daten im Auftrag

| | |
|---|---|
| Aktenzeichen: | 0005.8-2018-1 |
| Version: | 1.0 |
| Stand: | 17. April 2018 |
| Status: | Freigegeben |
| Ansprechpartner juristisch: | Der Beauftragte für den Datenschutz der EKD<br>0511 768 128-0<br>info@datenschutz.ekd.de |
| Ansprechpartner technisch: | keiner |

**Erläuterung**

Wenn eine kirchliche Stelle einen Vertrag zur Durchführung einer Auftragsverarbeitung (kurz: AV) mit einer anderen Stelle, die nicht den kirchlichen Datenschutzbestimmungen unterliegt, abschließt, so muss gemäß § 30 Absatz 5 Satz 1 EKD-Datenschutzgesetz dennoch sichergestellt sein, dass der Auftragsverarbeiter die Vorgaben des § 30 EKD-Datenschutzgesetz oder gleichwertige Bestimmungen beachtet. Unter gleichwertigen Bestimmungen sind die des Artikel 28 EU-Datenschutz-Grundverordnung (kurz: DSGVO) zu verstehen.

Während zwischen zwei kirchlichen Stellen ein AV-Vertrag (AVV) in jedem Fall auf Grundlage des EKD-Datenschutzgesetz abzuschließen ist, darf der Vertragsinhalt bei Beauftragung eines nicht kirchlichen Auftragsverarbeiters folglich auch anhand der Vorgaben der DSGVO gestaltet werden, was in der Praxis Vertragsabschlüsse erleichtern kann.

Zulässig ist dies jedoch gemäß § 30 Absatz 5 Satz 3 EKD-Datenschutzgesetz nur, wenn sich der Auftragsverarbeiter durch den AVV bzw. einer in diesen Vertrag einbezogenen Zusatzvereinbarung der kirchlichen Datenschutzaufsicht unterwirft. Das folgende Muster soll auftraggebende kirchliche Stellen bei der wirksamen Umsetzung dieses Vorgehens unterstützen.

Evangelische Kirche in Deutschland

DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

# Zusatzvereinbarung zum Vertrag nach Artikel 28 EU-Datenschutz-Grundverordnung zur Verarbeitung von personenbezogenen Daten im Auftrag

zwischen

*Bezeichnung der verantwortlichen Stelle*
*Straße Hausnummer*
*Postleitzahl Ort*

und

*Bezeichnung des Auftragsverarbeiters*
*Straße Hausnummer*
*Postleitzahl Ort*

In Ergänzung des zwischen den Parteien am Datum des Vertragsschlusses geschlossenen Vertrages zur Auftragsverarbeitung gemäß Artikel 28 EU-Datenschutz-Grundverordnung unterwirft sich der Auftragsverarbeiter gemäß § 30 Absatz 5 Satz 3 Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz; veröffentlicht in ABl. EKD 2017, S. 353) der kirchlichen Datenschutzaufsicht. Die Unterwerfung erstreckt sich auf die Aufgaben und Befugnisse der kirchlichen Datenschutzaufsicht nach §§ 43, 44 EKD-Datenschutzgesetz.

| Bezeichnung der verantwortlichen Stelle | Bezeichnung des Auftragsverarbeiters |
|---|---|
| (Ort, Datum) | (Ort, Datum) |
| (Unterschriften mit Amts- / Funktionsbezeichnungen) | (Unterschriften mit Amts- / Funktionsbezeichnungen) |

# A6 Einwilligung Veröffentlichung von Fotos

Gemeinde _____

Anschrift: _____

_____

Einverständniserklärung der abgebildeten Person

Name/Vorname: _____

Anschrift: _____

_____

Ich erkläre mein Einverständnis zur Veröffentlichung von Fotos, die bei
*<Fest oder Ereignis eintragen bei welchem das Foto gemacht wird>*
entstehen, auf denen auch ich zu sehen bin,

☐ im Gemeindebrief oder einem anderen gedruckten Produkt (z.B. Flyer)
☐ auf der Internetseite der Gemeinde
☐ auf einem Social Media Profil der Gemeinde (Facebook, Twitter, Instagram, Snapchat) –
unzutreffendes bitte durchstreichen.

Die Veröffentlichung darf ohne weitere Nachfrage erfolgen. Ich bin damit einverstanden, dass die notwendigen Daten maschinell gespeichert und verarbeitet werden. Die erfassten Daten werden ausschließlich für kirchengemeindliche Zwecke verwendet. Mir ist bekannt, dass digitale Bilder aus dem Internet kopiert, woanders verwendet oder auch verändert werden können, ohne dass die Kirchengemeinde darauf Einfluss hätte.

Ich behalte mir das Recht vor, der zukünftigen Veröffentlichung meiner Bilder im Internet jederzeit zu widersprechen. Die Kirchengemeinde wird im Falle eines Widerspruchs das Bild zeitnah aus dem von ihr verantworteten Bereich im Internet (in der Regel die Internetseite der Kirchengemeinde) entfernen.

_____ _____

Datum Unterschrift

EVANGELISCH-LUTHERISCHE
LANDESKIRCHE HANNOVERS