Datenschutz in Kirchengemeinden

Handreichung für Kirchenvorstände und Gemeindesekretariate

in der Evangelischen Kirche von Kurhessen-Waldeck

Inhaltsverzeichnis

Datenschutz allgemein

„Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt."
(Artikel 1 Abs. 1 GG)

„Jeder hat das Recht auf freie Entfaltung seiner Persönlichkeit."
(Artikel 2 Abs. 1 Satz 1 GG)

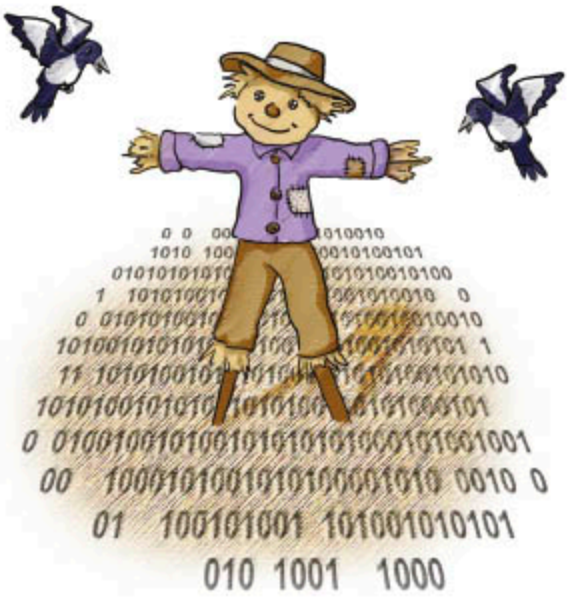
„Die Bestimmungen der Artikel 136, 137, 138, 139 und 141 der deutschen Verfassung vom 11. August 1919 sind Bestandteil dieses Grundgesetzes."
(Artikel 140 GG)

„Jede Religionsgemeinschaft ordnet und verwaltet ihre Angelegenheiten selbständig innerhalb der Schranken des für alle geltenden Gesetzes ..."
(Artikel 137 Abs. 3 der deutschen Verfassung vom 11. August 1919)

Die beiden ersten Artikel des Grundgesetzes der Bundesrepublik Deutschland geben allem staatlichen Handeln die Achtung der Werte „Menschenwürde" und „allgemeines Persönlichkeitsrecht" vor. Diese gesetzliche Vorgabe hat viele Ausprägungen und Konsequenzen. Eine davon ist das Recht auf informationelle Selbstbestimmung. Das heißt konkret, dass jeder Mensch grundsätzlich selbst darüber entscheidet, welche seiner persönlichen Daten von wem, wann, wie und wozu verwendet werden dürfen.

Im so genannten „Volkszählungsurteil" des Bundesverfassungsgerichtes vom 15.12.1983 wird in einem der Leitsätze zunächst jegliche Erhebung, Verarbeitung und Nutzung personenbezogener Daten verboten. Das Urteil sieht in der weiteren Erläuterung nur zwei Tatbestände vor, die überhaupt einen Umgang mit personenbezogenen Daten erlauben (Verbot mit Erlaubnisvorbehalt). Dies ist zum einen die vorherige, informierte und schriftliche Einwilligung der betroffenen Person, die auf freier Entscheidung beruhen muss, oder eine gesetzliche Regelung zur Verarbeitung personenbezogener Daten.

Das staatliche Datenschutzrecht gilt aufgrund des Artikels 140 GG in Verbindung mit Artikel 137 Abs. 3 der deutschen Verfassung vom 11. August 1919 nicht direkt. Die Evangelische Kirche in Deutschland (EKD) und ihre Gliedkirchen sind verpflichtet, ein dem staatlichen Niveau vergleichbares Datenschutzrecht zu schaffen. Sie tragen dem Datenschutz und allen daraus abzuleitenden Rechten und Pflichten durch ein eigenes Datenschutzgesetz Rechnung, welches in wesentlichen Teilen an das Bundesdatenschutzgesetz (BDSG) angelehnt ist und kirchliche Besonderheiten durch eigenständige Regelungen ergänzt. Das EKD-Datenschutzgesetz (DSG-EKD) ist ein „Auffanggesetz", das dann zum Tragen kommt, wenn andere kirchliche oder staatliche Rechtsvorschriften, die die näheren Umstände der Erhebung, Verarbeitung und Nutzung personenbezogener Daten beschreiben, fehlen.



Da es sich beim Datenschutz zunächst um ein Bürger- und Freiheitsrecht handelt, aus welchem sich eine staatliche Verpflichtung ableitet, werden hier auch explizite und unabdingbare Rechte für die einzelne Person benannt. Große Bedeutung kommt dem Recht auf Auskunft zu, welche persönlichen Daten gespeichert sind und zu welchen Zwecken sie genutzt oder an Dritte übermittelt werden. Daneben bestehen noch Ansprüche unter anderem auf Berichtigung falscher Daten, auf Sperrung oder auf Löschung nicht mehr benötigter oder unzulässig gespeicherter Daten.

Für die Evangelische Kirche in Deutschland (EKD) und ihrer Gliedkirchen hat der Schutz der Daten der Gemeindeglieder, der Menschen, die kirchliche oder diakonische Angebote (z. B. Kindertagesstätten, Diakoniestationen) wahrnehmen, und der Mitarbeitenden besondere Bedeutung. Datenschutzgerechtes Handeln wird in Zukunft nicht nur eine gesetzliche Verpflichtung, sondern in Anbetracht der „Datenskandale" der jüngsten Vergangenheit auch immer mehr ein Qualitäts- und Gütemerkmal kirchlichen Handelns sein.

Das kirchliche Datenschutzrecht sieht deshalb unter anderem die Verpflichtung jeder einzelnen Gliedkirche zur Bestellung einer/eines Datenschutzbeauftragten als Aufsichtsbehörde vor. Es ist ein grundsätzliches Anliegen aller Datenschutzbeauftragten der evangelischen Landeskirchen in Deutschland, über dieses elementare Recht des Datenschutzes zu informieren und über dessen Einhaltung zu wachen.

Verantwortlich für die Einhaltung der Vorschriften über den Datenschutz ist der Kirchenvorstand. Mitarbeitende im Haupt-, Neben- oder Ehrenamt sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten (§ 6 DSG-EKD).

Der zentrale Ort der Verwaltung ist in der Regel das Gemeindebüro. Hier laufen meist „alle Fäden" zusammen, hier ist der „Umschlagplatz" für personenbezogene Daten von Gemeindegliedern, Mitarbeitenden oder Menschen, die angebotene Dienste der Kirchengemeinde in Anspruch nehmen. Das meiste bleibt in den Kirchengemeinden, anderes kann oder muss sogar an Dritte weitergegeben werden.

Bei allem Handeln muss aber darauf geachtet werden, dass nicht alles, was wünschenswert oder technisch möglich ist, auch erlaubt ist. Manche pragmatische Lösung entpuppt sich im Nachhinein als datenschutzrechtlich bedenklich oder gar unzulässig. Die vielen Anfragen im Laufe der letzten Jahre aus Kirchengemeinden, aber auch Beschwerden von Betroffenen haben mir gezeigt, dass sich einerseits eine hohe Sensibilität entwickelt hat und andererseits ein gewisses Maß an Unsicherheit vorhanden ist, wie mit personenbezogenen Daten in Kirchengemeinden umzugehen ist.

Die meisten Anregungen habe ich bei vielen durchgeführten Schulungen zum Thema Datenschutz im Rahmen von Fortbildungsveranstaltungen für Gemeindesekretärinnen erhalten. Nicht alles, was nachgefragt wurde, kann hier wiedergegeben werden. Bei der Erstellung der Handreichung habe ich mich bemüht, Antworten zu den häufigsten Fragen auf der Grundlage der aktuell geltenden Rechtsvorschriften zu geben. Die Handreichung soll Sie bei der Erfüllung Ihrer Aufgaben dahingehend unterstützen, mit den Ihnen anvertrauten personenbezogenen Daten von Gemeindegliedern, Mitarbeitenden und Menschen, die kirchliche oder diakonische Angebote wahrnehmen, verantwortungsbewusst im Rahmen der datenschutzrechtlichen Bestimmungen umzugehen.

Michael Horst
Beauftragter für Datenschutz
Mai 2015

Gemeindebüro-PC

In der Regel ist in jeder Kirchengemeinde ein dienstlicher Rechner vorhanden. Meist müssen mehrere Personen auf gemeinsame Dateien und Dokumente sowie auf Programme zugreifen können. Heutige Betriebssysteme erlauben es, auf einem Gerät mehrere Nutzer mit eigener Nutzerkennung anzulegen. Davon sollte unbedingt Gebrauch gemacht werden. In der Regel besteht die Nutzerkennung aus dem Benutzernamen und einem persönlichen und geheimen Passwort, das in der Komplexität der Passwortrichtlinie entsprechen sollte. Ein Passwort darf nie (!) Dritten bekannt gegeben werden, auch nicht Vorgesetzten, die darum bitten oder es anordnen. Die Nutzerkennung dient unter anderem dazu, nachprüfen zu können, wer, wann, was und wie geändert hat (Anlage zu § 9 DSG-EKD, Eingabekontrolle). Das schützt die zugangsberechtigten Nutzer davor, im einem Problemfall in Beweisnot zu geraten, weil mehrere Personen mit der gleichen Nutzerkennung gearbeitet haben und nicht mehr feststellbar ist, wer Daten eingegeben, verändert oder gelöscht hat.

Die private Nutzung eines personalisierten E-Mail-Postfachs auf dem dienstlichen PC ist nicht ausdrücklich verboten. Dennoch ist dringend davon abzuraten, diese zu gestatten oder durch betriebliche Übung zuzulassen. Diese Postfächer dürfen wegen des möglichen privaten Inhalts von E-Mails aufgrund des § 88 Telekommunikationsgesetz (TKG) nicht mehr eingesehen werden, und zwar auch dann nicht, wenn

man nur die Inhalte dienstlicher E-Mails zur Kenntnis nehmen will, z. B. bei Urlaub oder sonstiger längerer Abwesenheit von Mitarbeitenden (siehe „Private Nutzung dienstlicher Telekommunikationstechnik").

Die private Nutzung des Internets z. B. zum Erreichen eines privaten E-Mail-Postfaches kann durch das vertretungsberechtigte Organ der jeweiligen kirchlichen Körperschaft zugelassen werden (§ 5 Abs. 4 IuK-Gesetz). Es empfiehlt sich der Abschluss einer Dienstvereinbarung mit der zuständigen Mitarbeitervertretung.

Kirchenvorstandsprotokolle

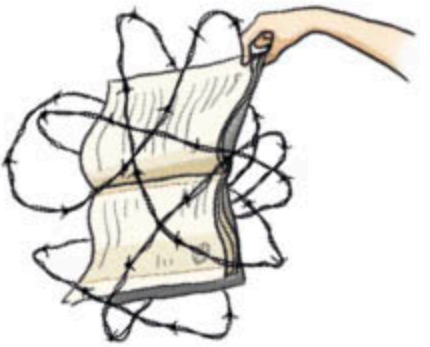
„Über die Ergebnisse der Verhandlungen des Kirchenvorstandes wird eine Niederschrift in das Verhandlungsbuch eingetragen, ..." (Artikel 31 Abs. 1 Grundordnung-GO). Dieses enthält unter anderem regelmäßig personenbezogene Daten, z. B. bei Beschlüssen zu Einstellungen von Mitarbeitenden oder Änderungen im Beschäftigungsverhältnis bis hin zu dokumentierten Problemfällen.

Gemäß § 2 Abs. 1 der Richtlinien zur Führung der Niederschriften über Kirchenvorstandssitzungen ist das Verhandlungsbuch in gebundener Form oder als Lose-Blatt-Buch, dessen Blätter auf alterungsbeständigem Papier und mit dokumentenechter Farbe ausgedruckt werden, mit fortlaufenden Blattzahlen zu führen. Der Kirchenvorstand kann beschließen, dass seine stimmberechtigten Mitglieder eine Abschrift der Niederschrift erhalten.

Die Niederschriften für das Lose-Blatt-Buch können elektronisch (z. B. als Word-Dokument oder Pdf-Datei) erzeugt und gespeichert werden. Das weckt vielfach den Wunsch, die neuen Möglichkeiten der Kommunikationstechnik zu nutzen und die Protokolle als Datei (meist unverschlüsselt!) per E-Mail über öffentliche Netze an die Kirchenvorstandsmitglieder zu versenden. Auf der Grundlage der aktuellen datenschutzrechtlichen Regelungen ist dieses nicht erlaubt.

Nach § 6 Abs. 2 IuK-Gesetz ist die Speicherung von Kirchenvorstandsprotokollen auf privaten Endgeräten nicht zulässig (siehe „Dienstliche Nutzung privater Endgeräte"). Die Verschlüsselung der Dateien, die nach § 7 Abs. 2 Satz 2 der Richtlinie vorzusehen ist, böte zwar mehr Sicherheit, ist aber mit der Regelung des IuK-Gesetzes nicht vereinbar. Abschriften der Protokolle sollten deshalb nur als Kopien verteilt oder per Post verschickt werden. Auch diese sind von den Kirchenvorstandsmitgliedern im häuslichen Umfeld für Dritte unzugänglich aufzubewahren und beim Ausscheiden aus dem Kirchenvorstand zu vernichten.

Alternativen, z. B. ein geschützter Bereich für Kirchenvorstandsmitglieder auf einer Internetplattform, können nur dann in Betracht gezogen werden, wenn die datenschutzrechtlichen Bestimmungen eingehalten werden. Das heißt unter anderem, dass die Vertraulichkeit des Inhalts von Kirchenvorstandsprotokollen gewahrt bleiben und die Speicherung auf privaten Geräten ausgeschlossen sein muss (nur lesender Zugriff).



Kirchenbücher

„Die Führung der Kirchenbücher gehört zu den Verwaltungsaufgaben des Pfarrers oder der Pfarrerin" (§ 1 Abs. 1 Satz 2 Kirchenbuchordnung). Mehrere Kirchengemeinden können die Führung von Kirchenbüchern einer gemeinsamen Stelle (z. B. Kirchenbuchamt) übertragen. Die kirchenbuchführenden Stellen sind verpflichtet, die sich aus den Kirchenbüchern ergebenden Daten dem Kirchenkreisamt bzw. dem Gemeindeamt zur Weitergabe an die zuständigen Stellen mitzuteilen. Darüber hinaus dürfen Auskünfte aus den Kirchenbüchern nur Berechtigten mündlich oder schriftlich in beglaubigter Form erteilt werden. Die Erteilung von Auskünften be-

schränkt sich auf die Beantwortung konkreter Einzelfragen. Berechtigte sind in der Regel nähere Verwandte der betroffenen Person bzw. Behörden im Rahmen ihrer Zuständigkeit.

Kirchenbücher dürfen an Dritte nicht ausgeliehen und es dürfen auch keine fotomechanischen Kopien erstellt werden. Für die Einsichtnahme in Kirchenbücher gelten die Vorschriften des kirchlichen Archivrechts und der dazu erlassenen Benutzerordnung. Danach hat jede Person, die ein berechtigtes Interesse glaubhaft macht, das Recht, Archivgut nach Maßgabe dieser Vorschriften zu nutzen. Archivgut, das sich wie in den Kirchenbüchern auf natürliche Personen bezieht, darf frühestens 10 Jahre nach dem Tod der betroffenen Person genutzt werden. Ist der Todestag nicht festzustellen, endet die Schutzfrist 100 Jahre nach der Geburt. Besondere Bestimmungen können längere Schutzfristen vorsehen. Etwaige gesonderte Sperrvermerke sind zu berücksichtigen. Für weitergehende Auskünfte wenden Sie sich am besten an das Landeskirchliche Archiv der EKKW.

Gemeindegliederverzeichnis

Nach dem Kirchenmitgliedschaftsgesetz der EKD (§ 14 Abs. 2 KMG) wird durch gliedkirchliches Recht bestimmt, welche kirchliche Stelle zur Führung des Gemeindegliederverzeichnisses verpflichtet ist. Aus § 2 Abs. 1 Kirchenbuchordnung lässt sich ableiten, dass das Führen des Gemeindemitgliederverzeichnisses ebenfalls zu den Verwaltungsaufgaben des Pfarrers oder der Pfarrerin gehört.

Das Gemeindegliederverzeichnis setzt sich zusammen aus den kommunalen Meldedaten und den kirchlichen Daten des Kirchenmitglieds und dessen Familienangehörigen, die nicht derselben oder keiner öffentlich-rechtlichen Religionsgemeinschaft angehören. Zur Verwaltung wird in der EKKW das Programm KirA eingesetzt, das einerseits vielfältige Möglichkeiten bietet, andererseits häufig Fragen aufwirft, welche Nutzung erlaubt oder nicht zulässig ist.

Grundsätzlich darf eine Kirchengemeinde nach § 19 Melderechtsrahmengesetz (MRRG), den Landesmeldegesetzen und gliedkirchlicher Rechtsvorschriften die von der Meldebehörde übermittelten Daten der Gemeindemitglieder unter Berücksichti-

gung kommunaler und kirchlicher Sperren zur Erfüllung ihrer Aufgaben verarbeiten und nutzen. Die kommunalen Daten von oben beschriebenen Familienangehörigen werden zur Feststellung des Kirchensteuersatzes übermittelt und sind an diesen konkreten Zweck gebunden. Für die Nutzung dieser Daten zu einem anderen Zweck bedarf es zwingend einer Rechtsvorschrift, die das zulässt.

Die personenbezogenen Daten aus dem Gemeindegliederverzeichnis sind ein hohes, sensibles und zu schützendes Gut. Der Schutzbedarf ist wegen der kommunalen Sperren AKSP 1, 3 und 6 in „sehr hoch" einzustufen. Das verpflichtet zu einem sorgsamen Umgang mit den Meldewesendaten. Bei allen Auswertungen aus KirA, bei denen kommunale oder kirchliche Sperren aufgehoben werden sollen, muss geprüft werden, ob dies mit dem Zweck der Sperren vereinbar ist.

Da Daten aus dem Gemeindegliederverzeichnis nie unverschlüsselt außerhalb des geschützten Intranets oder des gesamtkirchlichen E-Mail-Systems (...@ekkw.de) an andere E-Mail-Adressen verschickt werden dürfen, werden diese systemseitig zwangsverschlüsselt.

Gemeindebrief

Häufig wird die Frage gestellt, ob die Veröffentlichung von Amtshandlungen und persönlichen Jubiläen im Gemeindebrief zulässig ist. Auch wenn es in der EKKW keine konkrete Rechtsvorschrift gibt, die das ausdrücklich erlaubt, kann nach allgemeiner Auffassung davon ausgegangen werden, dass eine gemeindeinterne Veröffentlichung anlässlich von Amtshandlungen mit Name und Datum zulässig ist, soweit

sie zur Erfüllung des kirchlichen Auftrags dient und kein Sperrvermerk der betroffenen Person oder von Amts wegen vorliegt. Auch die Veröffentlichung von persönlichen Jubiläen kann zulässig sein, soweit die betroffene Person nicht ausdrücklich widersprochen hat. Ein Hinweis auf die Widerspruchsmöglichkeit im Gemeindebrief kann hilfreich sein. Auf die Veröffentlichung von Adressen sollte wegen des Fehlens einer Rechtsvorschrift verzichtet werden.

Als gemeindeintern gilt eine Veröffentlichung, wenn sie im Rahmen gottesdienstlicher Veranstaltungen oder in Publikationsorganen der Kirchengemeinde erfolgt, die nur Gemeindegliedern zugestellt werden oder nur in kirchlichen Räumen ausliegen. Eine Verteilung, die darüber hinausgeht, etwa an alle Haushalte eines Kirchengemeindegebietes, in Geschäften, Arztpraxen oder kommunalen Dienststellen, ist unzulässig.

Fotos, auf denen Personen erkennbar abgebildet oder namentlich genannt sind, dürfen nur mit deren Einverständnis im Gemeindebrief veröffentlicht werden. Das gilt auch für gemeindliche Veranstaltungen. Die weit verbreitete Meinung, dass das Einverständnis ab einer bestimmten Anzahl von Personen nicht erforderlich sei, ist nicht haltbar. Vielmehr kommt es darauf an, dass z. B. die Veranstaltung selbst das Objekt des Fotos ist und nicht deren Teilnehmer (§ 23 Abs. 1 Kunsturhebergesetz-KunstUrhG).

Bei der Erstellung der Verteilerlisten aus KirA sind gegebenenfalls kommunale Sperren, insbesondere AKSP 1, 2, 3 und 6 und kirchliche Sperren zu berücksichtigen. Die Listen sollten nach der Verteilung wieder im Gemeindebüro abgegeben und nicht anderweitig (z. B. Altpapiertonne) entsorgt werden.

Soll der Gemeindebrief auch auf der Homepage der Kirchengemeinde verfügbar sein, sind die Amtshandlungs- und Jubiläumsdaten vorher zu entfernen, wenn keine schriftliche Einverständniserklärung der betroffenen Person ausdrücklich für diese Form der Veröffentlichung vorliegt. Dies gilt gleichermaßen, wenn beabsichtigt wird, die Fotos im Gemeindebrief auch im Internet zu veröffentlichen (Muster einer Einverständniserklärung siehe Anhang).

Führen von Personalakten

Nach der Personalaktenordnung der EKKW wird die Personalakte bei der für die Ernennung oder Einstellung von Mitarbeitenden zuständigen Körperschaft oder der für sie zuständigen Verwaltungsstelle geführt (personalaktenführende Stelle). Die Personalakte kann in eine Hauptakte und eine oder mehrere Beiakten gegliedert sein. Außerhalb der Personalakte dürfen keine ausschließlich das Dienst-, Arbeits- oder Ausbildungsverhältnis eines Mitarbeiters oder einer Mitarbeiterin betreffenden Vorgänge geführt werden.

Entsprechend dieser Regelung sind die Haupt- und Beiakten der Mitarbeitenden bei der Kirchengemeinde oder dem zuständigen Kirchenkreisamt zu führen. Darüber hinaus können auch Personal-Nebenakten geführt werden, in die aber nur Kopien von solchen Vorgängen aufgenommen werden dürfen, die auch in der Haupt- oder Beiakte enthalten sind. Nebenakten entstehen z. B. in Kirchengemeinden, wenn das zuständige Kirchenkreisamt personalaktenführende Stelle ist oder umgekehrt.

In der Praxis bedeutet das, dass sämtliche personalaktenfähigen Dokumente im Original (z. B. auch Krankmeldungen) in der Haupt- bzw. Beiakte bei der personalaktenführenden Stelle abgeheftet werden. Die Kirchengemeinde bzw. im umgekehrten Fall das Kirchenkreisamt erhält nur Kopien der Vorgänge, die zu ihrer Aufgabenerfüllung erforderlich sind.

Für das Führen von elektronischen Personalakten oder auch nur Teilen davon fehlt es zurzeit an den rechtlichen und technisch-organisatorischen Rahmenbedingungen. Gleichwohl dürfen Personalaktendaten in automatisierten Verfahren verarbeitet werden, wenn das z. B. für die Gehalts- oder Besoldungsberechnung erforderlich ist. Zu beachten ist, dass diese in der Regel der Zustimmung der Mitarbeitervertretung und einer Dienstvereinbarung bedürfen.

Daten von Beschäftigten dürfen ohne Einverständnis der betroffenen Person an Stellen außerhalb des kirchlichen Bereichs nur übermittelt werden, wenn ein überwiegendes rechtliches Interesse der datenempfangenden Stelle dargelegt wird und kirchliche Interessen nicht entgegenstehen. Die Übermittlung an künftige Dienstherren oder Arbeitgeber ist nur mit der Einwilligung der betroffenen Person zulässig. Das heißt, dass z. B. bei einem geplanten Stellenwechsel in eine andere Gemeinde dem zukünftigen Arbeitgeber auch auf Anfrage keine Auskunft über die sich bewerbende Person erteilt werden darf.

Übermittlung an Stellen außerhalb der Kirchengemeinde

Neben der Nutzung personenbezogener Daten, z. B. aus dem Gemeindegliederverzeichnis, spielt die Übermittlung an Dritte häufig eine Rolle. Dritte sind Personen und Stellen außerhalb der verantwortlichen Stelle (Kirchengemeinde). Übermittlung ist das Bekanntgeben von personenbezogenen Daten an Dritte durch Weitergabe oder Einsichtnahme. Fehlt es an speziellen Rechtsvorschriften, die eine Übermittlung ausdrücklich zulassen, ist der Rückgriff auf das DSG-EKD erforderlich.

An kirchliche Stellen dürfen Daten übermittelt werden, wenn es zur Erfüllung von Aufgaben der übermittelnden oder empfangenden Stelle erforderlich ist (§ 12 Abs. 1 DSG-EKD). Damit kann eine Zweckänderung verbunden sein, die zulässig sein muss, denn die Daten sind stets an den Zweck gebunden, für den sie erhoben worden sind.

Die Übermittlung an öffentliche Stellen des Bundes, der Länder und der Gemeinden ist nur zulässig, wenn es zur Erfüllung der kirchlichen Aufgabe der übermittelnden

Stelle erforderlich ist (§ 12 Abs. 7 DSG-EKD). Diese Regelung existiert nur im DSG-EKD und schränkt die Zulässigkeit der Übermittlung an öffentliche Stellen erheblich ein. Für alle anderen Fälle gilt § 13 DSG-EKD, bei dessen Anwendung häufig zwischen einem berechtigten Interesse des Empfängers und dem schutzwürdigen Interesse der betroffenen Person abgewogen werden muss. Im Zweifel empfiehlt es sich, letzteres anzunehmen oder beim Beauftragten für Datenschutz nachzufragen.

In der Praxis kommt es nicht selten vor, dass personenbezogene Daten unverschlüsselt über öffentliche Kommunikationsnetze gesendet werden. Leider wird dieser Wunsch auch von öffentlichen Stellen an Kirchengemeinden herangetragen, z. B. bei der Übermittlung von Excel-Dateien mit Daten angemeldeter Kinder in Kindertagesstätten. Über dieses Medium ist die Vertraulichkeit nicht gewährleistet, da E-Mails über öffentliche Kommunikationsnetze einer Postkarte gleichen.

Es ist darauf zu achten, dass für vertrauliche Daten ein sicherer Transportweg gewählt wird, wenn sie das Intranet verlassen sollen. Die Verschlüsselung einer E-Mail oder einer angehängten Datei stellt eine relativ sichere Methode dar. Diese muss aber auf dem gesamten Transportweg ununterbrochen vorhanden sein. Das Versenden eines Briefes oder eines Faxes ist ebenfalls eine sichere Alternative. Andere Datenträger zum Transport (USB-Sticks, CDs oder DVDs) sollten passwortgeschützt und verschlüsselt sein.

Manchmal kann es notwendig sein, Dienste von Dritten in Anspruch zu nehmen, z. B. Wartung und Entsorgung von EDV-Systemen, Akten- oder Datenträgervernichtung oder ähnliches. Immer dann, wenn personenbezogene Daten betroffen sind, ist ein Vertrag mit dem Dienstanbieter zu schließen, der den Anforderungen des § 11 DSG-EKD entsprechen muss.

In den letzten Jahren werden zunehmend auch Internetdienste angeboten, die für Kirchengemeinden interessant erscheinen, weil sie bequem und ohne großen Aufwand, oft kostenfrei oder für relativ niedrige Gebühren in Anspruch genommen werden können. Das sind beispielsweise „Doodle" für Terminabsprachen, „mozy.de" zur Datensicherung oder Cloud-Dienste wie „Drop-Box" zum Speichern von Daten oder Bildern, die mehreren Nutzern zugänglich gemacht werden sollen.

Bei vielen dieser Anbieter werden die Daten nicht in Deutschland oder einem EU-Mitgliedsstaat verarbeitet. Mit diesen Dienstleistern dürfen keine Verträge abgeschlossen werden, da dies nach den Vorschriften des DSG-EKD unzulässig ist. Die Firmen erfüllen oft nicht annähernd die Datenschutzstandards, die nach dem DSG-EKD anzulegen sind, und notwendige Verträge mit den Anforderungen an deren Inhalt gemäß § 11 DSG-EKD können nicht abgeschlossen werden oder werden es nicht.

Keine Auftragsdatenverarbeitung ist z. B. das Binden von Lose-Blatt-Büchern (Sitzungsniederschriften von Kirchenvorstandssitzungen oder Kirchenbüchern). Die Firmen sollten aber sorgfältig ausgewählt und mit diesen eine Verpflichtung zur Verschwiegenheit vereinbart werden.

Für Terminabsprachen kann das Angebot der Evangelischen Landeskirche in Württemberg genutzt werden:

https://www.service.elk-wue.de/services/terminabsprache-dudleelk-wuede.html

Homepage und Social Media

Viele Kirchengemeinden nutzen inzwischen die Möglichkeit, sich im Internet mit einer eigenen Homepage oder auf einer Social-Media-Plattform wie Facebook mit einer sogenannten „Fanpage" zu präsentieren. Hierbei sind einige rechtliche Rahmenbedingungen zu beachten. Nach dem Telemediengesetz (TMG) besteht für den eigenen Internetauftritt eine Impressumspflicht, die die Mindestanforderungen gemäß § 5 TMG erfüllen muss. Diese Pflicht besteht auch für eine „Fanpage" bei Facebook. Die Verantwortlichen für die Homepage sind darüber hinaus verpflichtet, die Nutzer des Internetauftritts in Form einer Datenschutzerklärung in allgemein verständlicher Form über Art, Umfang und Zweck der Erhebung und Verwendung personenbezogener Daten zu unterrichten (§ 13 TMG). Beides, Impressum und Datenschutzerklärung, muss leicht und jederzeit für den Nutzer abrufbar sein.

Personenbezogene Daten dürfen im Internet nur dann veröffentlicht werden, wenn dazu das Einverständnis der betroffenen Person vorliegt. Im Einzelfall ist stets zu prüfen, ob diese Voraussetzung erfüllt ist (siehe auch „Gemeindebrief").

Gerne werden auch Bilder „ins Netz" gestellt. Hier ist große Sorgfalt geboten, insbesondere wenn es sich um Fotos von Kindern z. B. der Kindertagesstätte oder aus der Jugendarbeit handelt. Grundsätzlich dürfen Bilder nur verwendet werden, wenn zu jedem einzelnen Bild das Einverständnis der abgebildeten Person(en) bzw. bei Kin-

dern und Jugendlichen das der Personensorgeberechtigten (Eltern) in Schriftform vorliegt. Bei Jugendlichen ab einem Alter von etwa 13-14 Jahren (z. B. Konfirmandinnen oder Konfirmanden) ist neben dem Einverständnis der Eltern auch das der bzw. des Jugendlichen erforderlich.

In Einzelfällen kann das Einverständnis auch konkludent angenommen werden, wenn z. B. von einem neu gewählten Kirchenvorstand ein Gruppenfoto zum Zweck der Veröffentlichung auf der Homepage erstellt werden soll und die Mitglieder darüber vorher informiert worden sind. Es bleibt dann der oder dem Einzelnen überlassen, ob er oder sie sich für ein solches Foto zur Verfügung stellt oder nicht. Tut er oder sie es, kann von einem konkludenten Einverständnis ausgegangen werden.

Die Nutzung sozialer Netzwerke wie Facebook, Twitter und Co. durch kirchliche Stellen bleibt unter dem Aspekt des Datenschutzes weiter fragwürdig. Durch den Umstand, dass die Server der Anbieter oft nicht in Deutschland, sondern in anderen Staaten innerhalb oder außerhalb der Europäischen Union betrieben werden, ist weder deutsches noch kirchliches Datenschutzrecht anwendbar. Es entsteht ein quasi „rechtsfreier" Raum. Das Anbieten einer „Fanpage" bei Facebook ist wegen der unzureichenden Datenschutzstandards sehr zweifelhaft, kann aber aufgrund der aktuellen Rechtslage nicht beanstandet werden.

Anders verhält es sich bei sogenannten „Apps", für die Facebook ebenfalls eine Plattform bietet. „Apps" sind Anwendungen, die sich meist auf eigenen Servern des „App"-Anbieters befinden, aber auf der Plattform von Facebook eingebunden werden, um die vorhandenen Wirkungen zu nutzen (z. B. Auslesen des Adressverzeichnisses von Nutzern und automatisches Posten von Mitteilungen an deren „Freunde" = Schneeballeffekt). Bei solchen „Apps" handelt es sich um eine unzulässige Datenerhebung durch kirchliche Stellen, die ohne Wissen und Zustimmung der „Freunde" der Nutzer erfolgt und deshalb nicht verwendet werden dürfen.

Gerne werden auf Homepages sogenannte „social plug-ins" wie z. B. der „like it"-Button von Facebook integriert. Entgegen einer weitverbreiteten Meinung werden allein durch das Vorhandensein eines „social plug-in" auf einer Homepage bei Aufruf der Seite Daten von Nutzern individualisiert (bei gleichzeitiger Anmeldung

bei Facebook personalisiert) an Facebook übermittelt. Deshalb sollten diese „social plug-ins“ grundsätzlich nur mit der Zwei-Klick-Variante oder der verbesserten Ein-Klick-Variante auf der Homepage implementiert werden.

http://www.heise.de/ct/artikel/2-Klicks-fuer-mehr-Datenschutz-1333879.html

http://www.heise.de/newsticker/meldung/c-t-entwickelt-datenschutzfreundliche-Social-Media-Buttons-weiter-2466687.html

Private Nutzung dienstlicher Telekommunikationstechnik

Das gesamtkirchliche E-Mail-System (...@ekkw.de) ist laut § 5 Abs. 3 des am 1. Januar 2015 in Kraft getretenen IuK-Gesetzes zur dienstlichen und innerkirchlichen Kommunikation zu nutzen. Das impliziert, dass die private Nutzung nicht zulässig ist, auch wenn ein ausdrückliches Verbot nicht normiert ist. Für kirchliche Stellen, die nicht daran angeschlossen sind oder andere Anbieter nutzen, gilt diese Regelung jedoch nicht. Damit ergibt sich für die Mitarbeitenden die Möglichkeit, ihr personalisiertes dienstliches Postfach auch für private Zwecke nutzen zu können.

Wird dies erlaubt oder nur stillschweigend geduldet, wird die Dienststelle im Sinne des Telekommunikationsgesetzes (TKG) zum Telekommunikationsanbieter. Für diesen Fall gilt § 88 TKG „Telekommunikationsgeheimnis“. Danach ist es dem Anbieter von Telekommunikation untersagt, sich oder anderen Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen (Verletzung des Telekommunikationsgeheimnisses).

In der Praxis bedeutet das, dass sich die Postfächer der personalisierten dienstlichen E-Mail-Adressen von Mitarbeitenden, bezogen auf den Inhalt als auch die näheren Umstände der Kommunikation, der Einsichtnahme durch Dienstvorgesetzte oder Kolleginnen und Kollegen vollständig entziehen. Davon betroffen sind auch offensichtlich dienstliche E-Mails. Wegen des nicht auszuschließenden Verlustes privater

E-Mails dürfen sogenannte Spam-Filter nicht eingesetzt werden. Es wird empfohlen, die private Nutzung dienstlicher E-Mail-Adressen grundsätzlich zu untersagen und das Verbot stichprobenartig zu überprüfen.

Das gilt gleichermaßen auch für vorhandene Telefonanlagen. Werden private Gespräche zugelassen, dürfen weder Inhalt noch die näheren Umstände der Kommunikation, z. B. in Form von Einzelverbindungsnachweisen bekannt werden. Bei inzwischen allgemein üblichen Flatrates ist eine Kostenkontrolle für Telefonate nicht mehr notwendig. Für kostenpflichtige Anrufe (z. B. Service-Nummern, Auslandsgespräche oder in Mobilfunknetze) sollten Regelungen getroffen werden.

Die private Nutzung des Internets kann vom vertretungsberechtigten Organ der jeweiligen Körperschaft zugelassen werden (§ 5 Abs. 4 Satz 2 IuK-Gesetz). Damit besteht für die Mitarbeitenden die Möglichkeit, auf ein privates E-Mail-Konto zuzugreifen. Dafür sollte eine Dienstvereinbarung abgeschlossen werden, die stichprobenartige Kontrollen, zunächst möglichst anonymisiert, konkret regelt. Andernfalls sind Kontrollen über das „Surf"-Verhalten von Mitarbeitenden, wie bei der privaten E-Mail-Nutzung, unzulässig.

Dienstliche Nutzung privater Endgeräte

Es wird häufig mit unterschiedlichen Motivationen, „zuhause habe ich einen PC", „ein Gerät statt zwei", „ich arbeite lieber mit meinem Gerät" (meist Apple-Nutzer), der Wunsch geäußert, private stationäre oder mobile Endgeräte auch für dienstliche Zwecke nutzen zu dürfen.

Neben rechtlichen Schwierigkeiten stehen der Einbindung privater Endgeräte in die IT-Infrastruktur auch erhebliche datenschutzrelevante Sicherheitsbedenken entgegen.

Die Kirchengemeinde ist auch für den datenschutzkonformen Umgang mit von ihr erhobenen, verarbeiteten und genutzten personenbezogenen Daten auf privaten Endgeräten verantwortlich. Gleichzeitig entziehen sich diese Geräte ohne Ein-

willigung des Besitzers vollständig der Kontrolle durch die Dienststelle und auch durch den Datenschutzbeauftragten. Ob das Betriebssystem sicher und auf dem aktuellsten Stand ist, ebenso die Anwendungen, die Firewall oder der Antivirenscanner, bleibt dem Eigentümer überlassen. Können, und wenn ja, werden dienstliche und private Daten auf einem Endgerät so getrennt, dass Dritte keinen Zugriff auf dienstliche Inhalte haben (z. B. Familien-E-Mailpostfach)? Entstehen Ansprüche auf Nutzungsentgelte gemäß §§ 670 und 675 Bürgerliches Gesetzbuch (BGB)?

Auf mobilen Endgeräten (Smartphone oder Tablet) können zurzeit private und dienstliche Daten nicht getrennt werden. Im Falle eines Verlustes ist eine Fernlöschung (remote wipe) der dienstlichen Daten zwingend erforderlich. Dieser Befehl löscht auch alle privaten Daten, was gegen § 303 a Strafgesetzbuch (StGB) verstößt. Smartphones und Tablets können leicht durch schadhafte Apps oder die Nutzung offener WLAN-Netze kompromittiert werden und stellen bei Einbindung in die IT-Infrastruktur eine Gefährdung des Intranets dar.

Deshalb ist in § 6 Abs. 2 IuK-Gesetz geregelt, dass private Geräte zur dienstlichen Nutzung nur zugelassen werden können, wenn die IT-Sicherheit nicht gefährdet oder beeinträchtigt wird. Der Zugriff auf dienstliche Daten ist nur zulässig, wenn er ausschließlich über die zentral zur Verfügung gestellten Intranetzugänge der Landeskirche erfolgt. Diese Regelung schließt die dienstliche Nutzung privater Geräte und auch den Versand von Kirchenvorstandsprotokollen per E-Mail und deren Speicherung auf privaten Geräten aus.

- EKD-Datenschutzgesetz (DSG-EKD, Nr. 978*)
- Verwaltungsverordnung zur Durchführung des DSG-EKD (Datenschutzverordnung-DSVO, Nr. 979*)
- Kirchengesetz über den Einsatz von Informations- und Kommunikationstechnik in der EKKW (IuK-Gesetz, Nr. 720*)
- Intranetrichtlinie (Nr. 723*)
- Kirchengesetz über die Kirchenmitgliedschaft, das kirchliche Meldewesen und den Schutz der Daten der Kirchenmitglieder (KMG, Nr.123a*)
- Ordnung über die Führung der Kirchenbücher (Kirchenbuchordnung, Nr. 645*)
- Richtlinien zur Führung der Niederschriften über Kirchenvorstandssitzungen (Nr. 75*)
- Archivgesetz (Nr. 630*)
- Kassationsordnung (Nr. 635*)
- Personalaktenordnung (Nr. 370*)

* Nummer in der Rechtssammlung der Evangelischen Kirche von Kurhessen- Waldeck (http://www.kirchenrecht-ekhn.de/)

Einverständnis-Erklärung

Ich bin damit bis auf Widerruf einverstanden, dass folgendes Foto [genaue Bezeichnung z.B. Nr.] von mir / meiner Tochter / meines Sohnes [Name, Vorname] durch [Name der Einrichtung] veröffentlicht wird.

Art der Veröffentlichung:

- ◯ Internet
- ◯ Regionale Tageszeitung
- ◯ Überregionale Tageszeitung
- ◯ Gemeindebrief
- ◯ Sonstiges.....

Zweck der Veröffentlichung:

- ◯ Öffentlichkeitsarbeit
- ◯ Werbung
- ◯ Sonstiges.....

Ich bin darüber hinaus auch mit der Nennung meines Namens einverstanden ◯ ja ◯ nein

Datenschutzrechtlicher Hinweis:
Durch die beabsichtigte Verwendung im Internet können die Personenabbildungen und/oder Namen sowie sonstige veröffentlichte personenbezogene Informationen der Personen weltweit abgerufen und gespeichert werden. Entsprechende Daten können damit etwa auch über so genannte „Suchmaschinen" aufgefunden werden. Dabei kann nicht ausgeschlossen werden, dass andere Personen oder Unternehmen diese Daten mit weiteren im Internet verfügbaren Daten der Personen verknüpfen und damit ein Persönlichkeitsprofil erstellen, die Daten verändern oder zu anderen Zwecken nutzen. Dies kann insbesondere dazu führen, dass andere Personen versuchen Kontakt aufzunehmen. Über die Archivfunktion von Suchmaschinen sind die Daten zudem häufig auch dann noch abrufbar, wenn die Angaben aus den oben genannten Internet-Angeboten bereits entfernt oder geändert wurden.

Die Einwilligung ist freiwillig; aus der Verweigerung der Einwilligung oder ihrem Widerruf entstehen keine Nachteile.

Es handelt sich hierbei nicht um eine generelle Einwilligung, sondern nur um eine Einwilligung für das oben spezifizierte Foto und für den angegebenen Zweck.

[Ort, Datum]

....

[Unterschrift] [Unterschriften der Sorgeberechtigten]

Gemeinsame Erklärung

Zu der Frage, ob Fotos von Kindergartenkindern im Internet veröffentlicht werden dürfen, auf denen Kindergartenkinder zu erkennen sind:

1 **Geplante Veröffentlichung als Datenübermittlung:** Das Veröffentlichen von Bildern im Internet ist eine Datenübermittlung an einen unbekannten Personenkreis. Der Datenschutz ist hiervon betroffen, wenn

I. Die abgebildeten Personen klar erkennbar sind und/oder

II. Die Namen der abgebildeten Personen mitgeteilt werden.

2 **Kunsturhebergesetz keine Rechtsgrundlage:** § 23 Abs. 1 Kunsturhebergesetz ist keine ausreichende Rechtsgrundlage für eine solche Veröffentlichung im Internet. Selbst dann, wenn einer der Ausnahmetatbestände (z.B. Teilnahme an öffentlichen Veranstaltungen) zutrifft, verletzt gerade die Publikation im Word Wide Web die berechtigten Interessen des Betroffenen im Sinne von § 23 II Kunsturhebergesetz. Hierbei ist zu berücksichtigen, dass

I. Fotos beliebig auf die eigene Festplatte heruntergeladen werden können,

II. Digitale Bilder mit Bildbearbeitungsprogrammen nachbearbeitet, verändert und in einemn völlig anderen Kontext gestellt werden können,

III. Die Veröffentlichung von Kinderbildern dem Jugendschutz zuwider läuft.

3 **Einwilligung erforderlich:**
Die kirchliche Datenschutzanordnung und das Datenschutzgesetz der EKD kennen keine Norm, (Rechtsgrundlage), die die Bildveröffentlichung im Internet zulassen würde. Es ist daher vor der Einstellung von Fotos in die Website der Pfarrgemeinde oder des Kindergartens in jedem Fall die Zustimmung der Sorgeberechtigten erforderlich. Liegt sie nicht vor, ist die Veröffentlichung rechtswidrig. Ein Verstoß hiergegen kann nach dem Kunsturhebergesetz mit Freiheitsstrafe bis zu einem Jahr bestraft werden.

4 **Schriftlichkeit der Einwilligung:**
Die Einwilligung aller abgebildeten Personen muss schriftlich vorliegen und auf den konkreten Einzelfall bezogen sein. Die Sorgeberechtigten müssen die Möglichkeit haben, die Bilder vor Abgabe der Einwilligungserklärung zu sehen. Formularmäßig erklärte Einwilligungen, etwa im Aufnahmevertrag, reichen nicht aus.

18.03.2008
Konferenz der Datenschutzbeauftragten im Bereich der Katholischen Kirche Deutschlands

05.02.2008
Konferenz der Datenschutzbeauftragten der Evangelischen Landeskirhe

Merkblatt über den Datenschutz in der Evangelischen Kirche von Kurhessen-Waldeck

Für den Datenschutz in der Evangelischen Kirche von Kurhessen-Waldeck sind neben bereichsspezifischen Regelungen folgende Rechtsvorschriften zu beachten:

- Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz - DSG-EKD) vom 12. November 1993 (ABl. EKD S. 505), geändert durch Kirchengesetz vom 7. November 2002 (ABl. EKD S. 381) und durch Kirchengesetz vom 7. November 2012 (ABl. EKD S. 452)
- Verordnung zur Durchführung des Kirchengesetzes über den Datenschutz (Datenschutzverordnung) vom 28. Januar 1987 (KABl. S. 41) geändert durch Verordnung vom 14. Februar 1994 (KABl. S. 87/88)

Daneben gelten

- für die Amtsverschwiegenheit der kirchlichen Mitarbeiter (§ 31 Pfarrdienstgesetz der EKD, § 24 Kirchenbeamtengesetz der EKD, § 3 Abs. 2 TV-L) und
- sonstige Geheimhaltungs- und Verschwiegenheitspflichten (z.B. Seelsorge-, Steuer-, Arztgeheimnis).

In gleicher Weise sind künftige Rechts- und Verwaltungsvorschriften der Evangelischen Kirche von Kurhessen-Waldeck zum Datenschutz zu beachten.

Grundsätze des Datenschutzes

Zweck des kirchlichen Datenschutzes ist, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

Personenbezogene Daten sind Einzelangaben über

- persönliche Verhältnisse (z.B. Name, Geburtsdatum, Familienstand, Gesundheitszustand) oder
- sachliche Verhältnisse (z.B. Eigentumsverhältnisse, Rechtsbeziehungen zu Dritten)

einer bestimmten oder bestimmbaren natürlichen Person (z.B. Gemeindemitglieder, kirchliche Mitarbeiter) und dürfen nur für die rechtmäßige Erfüllung kirchlicher Aufgaben erhoben, verarbeitet und genutzt werden. Maßgebend sind die durch das kirchliche Recht bestimmten oder herkömmlichen Aufgaben auf dem Gebiet der Verkündigung, Seelsorge, Diakonie und Unterweisung sowie der kirchengemeindlichen und pfarramtlichen Verwaltung.

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind grundsätzlich nur zulässig, wenn das Datenschutzgesetz der EKD oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit die betroffene Person eingewilligt hat.

Im Einzelnen

1. Alle Informationen, die Mitarbeitende auf Grund ihrer Arbeit erhalten, sind von ihnen vertraulich zu behandeln. Die Pflicht besteht auch nach Beendigung des Dienst- oder Arbeitsverhältnisses fort.

2. Den Mitarbeitenden ist untersagt, ihre zum Zugriff auf bestimmte Arbeitsprogramme und Daten berechtigenden Passwörter zu offenbaren oder sich Passwörter anderer Mitarbeiter zu beschaffen.

3. Daten und Datenträger sind stets sicher und verschlossen zu verwahren und vor jeder Einsicht oder sonstigen Nutzung durch Unbefugte zu schützen. Datenträger sind alle Medien, auf denen Daten verzeichnet sind, so z.B. in- und externe Sicherungsmedien -CD-Rom, Stick etc.-, Belege, Erfassungsbögen, EDV-Listen, Adressaufkleber.

4. Auskünfte sowie Abschriften und Kopien aus Datensammlungen dürfen nur unter Beachtung bestehender Datenschutzbestimmungen und anderer Rechtsvorschriften erteilt oder angefertigt werden. Eine Weitergabe derartiger Mitteilungen zur geschäftlichen oder gewerblichen Datenverwendung ist untersagt.

5. Personenbezogene Datenbestände, die durch neue ersetzt und nicht aus besonderen zulässigen Gründen weiterhin benötigt werden, müssen in einer Weise vernichtet oder gelöscht werden, die jeden Missbrauch der Daten ausschließt.

6. Daten und Datenträger dürfen
   - kirchlich Mitarbeitenden, die Aufgrund ihrer dienstlichen Aufgaben zum Empfang der Daten ermächtigt und ausdrücklich zur Wahrung des Datenschutzes verpflichtet worden sind
   - oder im Rahmen der Auftragsdatenverarbeitung zugänglich gemacht werden.

7. Mängel beim Datenschutz, der Datensicherung und der ordnungsgemäßen Verarbeitung sind dem/der jeweiligen Vorgesetzten oder dem Datenschutzbeaufragten unverzüglich anzuzeigen.

8. Verstöße gegen den Datenschutz sind Verletzungen der Dienstpflicht im Sinne des Disziplinarrechts, der arbeitsrechtlichen Vorschriften oder der Amtspflichten ehrenamtlich Tätiger. Sie können Schadensersatzansprüche des Dienstherrn bzw. Arbeitgebers oder Dritter begründen.

9. Bestimmte Handlungen, die einen Verstoß gegen das Datengeheimnis beinhalten, werden durch das Strafgesetzbuch mit Strafe bedroht.
   Auf die Straftatbestände
   - § 202a (Ausspähen von Daten),
   - § 263a (Computerbetrug)
   - § 303a (Datenveränderung) und
   - § 303b (Computersabotage)

   wird besonders verwiesen. Danach kann bestraft werden, wer rechtswidrig Daten verändert oder beseitigt, wer den Ablauf der Datenverarbeitung einer Behörde oder eines Wirtschaftsunternehmens stört, wer sich oder einem Dritten unbefugt besonders gesicherte Daten aus fremden Datenbanksystemen verschafft und wer fremdes Vermögen durch unbefugtes Einwirken auf einen Datenverarbeitungsvorgang schädigt.

Der Beauftragte für Datenschutz der
Evangelischen Kirche in Hessen und Nassau und der
Evangelischen Kirche von Kurhessen-Waldeck
Michael Horst
Paulusplatz 1
64285 Darmstadt
Tel.: 06151-405129
Fax: 06151-405555129
E-Mail: Datenschutz@ekhn-kv.de

Illustration und Layout:
Valentina Ansel, Armadillodesign