Datenschutz für kirchliche Öffentlichkeitsarbeit in der Evangelischen Kirche in Hessen und Nassau (EKHN)

Bild: Istock / gintas77

Version	**1.0**
Stand:	18.5.2018
Autoren:	Birgit Arndt und Hans Genthe, Medienhaus der EKHN, Matthias Hartmann, Öffentlichkeitsbeauftragter im Evangelischen Dekanat Gießen und Christian Zappe, Diplom Jurist, Medien- und Social Media Recht
Rechtliche Prüfung:	OKR Sabine Langmaack, Rechtsabteilung der EKHN, Sebastian Heydendahl, stell. Örtlich Beauftragter für den Datenschutz in der Kirchenverwaltung der EKHN

Vorwort

Liebe Leserin, lieber Leser, liebe Medienschaffende in der EKHN,

dieser Broschüre können Sie alles Wichtige zum Datenschutz im Bereich Öffentlichkeitsarbeit entnehmen. Der Anlass dafür ist die europäische Datenschutzgrundverordnung (DSGVO), die am 25. Mai 2018 in Kraft tritt und den Umgang mit Daten erstmals einheitlich für die gesamte Europäische Union regelt. Diese bevölkerungsreiche Region verfügt und über genügend politischen Einfluss, um den Schutz persönlicher Daten gegenüber den Interessen der großen Daten-Unternehmen, die fast alle in den USA sitzen, durchzusetzen. Die Grundidee lautet: Daten über Personen gehören diesen Personen und dürfen nicht gegen ihren Willen gesammelt und verwendet werden.

Eine Kränkung für die Kirchen

Für uns, die wir in der evangelischen Kirche arbeiten, bedeutet diese neue EU-Verordnung eigentlich nicht viel neues, denn das Datenschutzgesetz der Evangelischen Kirche in Deutschland und ihrer Gliedkirchen enthält auch bisher schon weitgehend ähnliche Regelungen. Das Problem ist nur: Es blieb bislang vielfach Theorie. Viele Engagierte in den Kirchen stehen im Dilemma zwischen Datenschutz und Alltagspraxis, denn die Angebote der gängigen sozialen Medien und Online-Plattformen sind einfach zu verlockend. „Ohne WhatsApp kann ich keine Konfirmandenarbeit mehr machen“, sagen viele Pfarrerinnen und Pfarrer. Verständlich, ist es doch ihre Aufgabe „nahe bei den Menschen zu sein“, wie das im Kirchen-Jargon heißt. Da bleibt eben außen vor, dass WhatsApp die kompletten Adressbücher ihrer Nutzerinnen und Nutzer auf Server in Drittländer transferiert sowie umfassende Protokolldaten erstellt und auswerten kann.

Ja, die Grundidee des Datenschutzes ist für uns Engagierte in den Kirchen eine Zumutung und sogar eine Kränkung. „Wir sind doch die Guten, die nichts Böses im Schulde führen! Wir wollen doch nur die Menschen erreichen und sie miteinander vernetzen, um mit ihnen gegen die geistliche Leere und die soziale Kälte an zu leben!“

Der Datenschutz tickt anders. Er legt den Fokus auf Diskretion und die Integrität des Einzelnen. Ein Grundwiderspruch, zumindest scheinbar. Aus Sicht des Datenschutzes ist es undenkbar, etwas so persönliches wie einen runden Geburtstag oder eine Taufe einfach zu veröffentlichen. Doch viele Kirchengemeinden tun in ihrem Gemeindebrief genau das, damit Nachbarn Bescheid wissen, mal vorbeikommen und gratulieren können. Das Ziel ist schöne, soziale Wärme – sonst nichts. Viele mögen das, andere aber nicht. Die Bevölkerung sitzt derzeit in zwei Zügen, die in ganz unterschiedliche Richtung fahren: Die einen sind Daten-sensibel und pochen auf ihre geschützte Privatsphäre, die anderen sind Daten-freizügig und wollen die Welt an ihrem Leben teilhaben lassen. Beide sind zu achten. In der Kirche müssen wir respektvoll mit den Menschen und ihren individuellen Einstellungen umgehen. Das ist eigentlich eine ur-evangelische Haltung. Konkret bedeutet sie in diesem Fall: Wir fragen die Menschen, wie sie es mit ihren Daten halten. Das ist auch die Grundidee der Europäischen Datenschutzgrundverordnung: Frage die Leute und handele danach. Eigentlich sinnvoll, allerdings macht das Arbeit. Denn alle müssen gefragt werden bzw. dürfen widersprechen: Möchtest Du im Gemeindebrief erwähnt werden? Möchtest Du, dass wir ein Foto mit dir auf unsere Website stellen?

Umdenken

Wie jede andere Institution muss sich die Kirche das Vertrauen der Menschen und die Integrität einer seriösen Organisation verdienen. Dafür müssen wir umdenken und lernen, den Datenschutz in unsere Arbeit zu integrieren. Das ist ein längerer Lernprozess. Und er darf nicht nur in unseren Köpfen stattfinden, sondern muss auch in eine praxis-taugliche Ausrüstung münden. Wir brauchen Soziale Medien und Online-Plattformen, die mit dem Datenschutz übereinstimmen und uns zugleich Wege zu den Menschen eröffnen. Das zu entwickeln ist die Aufgabe der nächsten Monate und Jahre. Einstweilen finden Sie auf den folgenden Seiten Informationen, Anregungen und praktische Hilfen für den Alltag. Schauen Sie ab und zu mal vorbei, denn es kann sein, dass wir die Empfehlungen dieser Broschüre zur DSGVO aufgrund der aktuellen Diskussion in den nächsten Wochen noch ergänzen. Bei praktischen Fragen, die über sie hinausgehen, wenden Sie sich bitte an uns oder die Öffentlichkeitsbeauftragten in Ihrem Dekanat oder Einrichtung.

Stephan Krebs, Leiter Öffentlichkeitsarbeit EKHN
Birgit Arndt, Geschäftsführerin Medienhaus

Hintergrund und allgemeine Informationen zum Datenschutz

Im Bereich der Evangelischen Kirche von Hessen und Nassau (EKHN) 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 EKHN ist zuständig die Außenstelle Dortmund für die Datenschutzregion Mitte-West:

Friedhof 4, 44135 Dortmund

Tel: +49 (0)231 533827-0

Fax: +49 (0)231 533827-20

E-Mail: mitte-west@datenschutz.ekd.de

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

Die Informationen auf den folgenden Seiten sollen vor allem in der EKHN 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.

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

Inhaltsverzeichnis

Vorwort ... **2**

Hintergrund und allgemeine Informationen zum Datenschutz ... **4**

Inhaltsverzeichnis ... **5**

1 Regelungen aus der kirchlichen Verwaltung übernehmen ... **7**

1.1 Warum kirchlicher Datenschutz? ... 7

1.2 Was sind personenbezogene Daten? ... 7

1.3 Was sind besondere Kategorien von personenbezogenen Daten? ... 8

1.4 Was ändert sich am 24. Mai 2018? ... 9

1.5 Wann dürfen Daten verarbeitet werden? ... 10

1.6 Welche Auskunfts- und Informationsrechte haben Betroffene? ... 10

2 Datenschutz im Gemeindebrief ... **13**

2.1 Amtshandlungsdaten ... 14

2.2 Geburtstage, Jubiläen und Konfirmationsjubiläen ... 14

2.3 Kontaktdaten ... 14

2.4 Muster-Einwilligung Veröffentlichung von Daten im Gemeindebrief ... 15

2.5 Fotos und Videos ... 16

3 Urheberrecht ... **16**

3.1. Einwilligung ... 17

3.2 Muster-Einwilligung ... 18

4 Mailings – speziell Fundraisingmailings ... **19**

4.1 Vertrag mit Dienstleistern – Datenverarbeitung im Auftrag ... 19

4.2 Speicherung, Verschlüsselung, Löschung personenbezogener Daten für Mailings ... 20

4.3 Ihr Fundraising-Experte vor Ort ist für Sie da ... 21

5 Webseiten / Internet ... **21**

5.1 Pflicht zu Impressum und Datenschutzerklärung ... 21

5.2 Cookie Richtlinie ... 21

5.3 Webtracking-Tools ... 22

5.4 Social Media Plugins ... 22

5.5 Kontaktformulare - verschlüsseln? ... 22

5.6 Gemeindebrief im Netz ... 23

6 Newsletter und Mailings ... **23**

6.1 Newsletter als Auftragsdatenverarbeitung ... 24

6.2 Arbeiten mit alten Empfängerbestand ohne Opt In ... 24

6.3 Neue Empfänger rechtssicher anlegen ... 25

6.4 Schutz der Daten beim Versand ... 26

7 Social Media 26
7.1 Personale Kommunikation des Evangeliums 26
7.2 Die Rolle der digitalen Dienstleister sozialer Medien 26
7.3 Privatsphäre-Einstellungen 27
7.4 Foto, Videos, Musik 27
7.5 Facebook 28
7.6 WhatsApp 29
7.7 YouTube 30
7.8 Doodle 31
8 Cloud-Computing 31
9 Streaming von Andachten oder Gottesdiensten 32
10 Link-Tipps 32
Anlagen 33

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 Dekanats 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.

[2] https://datenschutz.ekd.de

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
- 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, sowie ein Verfahrensverzeichnis gepflegt werden.

1.4 Was ändert sich am 24. Mai 2018?

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 Datenschutzgrund-verordnung (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 überprüfen, denn die neuen Regelungen gehen über die alten datenschutzrechtlichen Regeln hinaus.

Die geltenden Grundsätze für die datenschutzkonforme Datenverarbeitung bleiben weiterhin gültig: Rechtmäßigkeit, Zweckbindung, Datenminimierung (Daten-sparsamkeit), 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 Unternehmen gestärkt. Betroffene sollen leichter Zugang zu ihren Daten und der Information über deren Nutzung haben. Außerdem wird das bislang nur gerichtlich konstruierte „Recht auf

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

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

[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

1.5 Wann dürfen Daten verarbeitet werden?

Schon vorher war es so, dass kirchliche Einrichtungen über Datenverarbeitungsvorgänge informieren mussten. Neu ist nun, dass nicht nur der Zweck, sondern auch die Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten angegeben werden muss. Es gilt der Grundsatz „Verbot mit Erlaubnisvorbehalt“, das bedeutet: Die Verarbeitung personenbezogener Daten ist grundsätzlich verboten und nur in Ausnahmefällen erlaubt.

Die Erlaubnis gilt:

- wenn eine Einwilligung des Betroffenen vorliegt,
- wenn die Verarbeitung für die Erfüllung eines Vertrags oder zur Durchführung vorvertraglicher Maßnahmen 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 dann zulässig, wenn die Verarbeitung mit dem ursprünglichen Erhebungszweck kompatibel ist. Hierzu zählt ausdrücklich die Nutzung zu statistischen Zwecken. Allerdings müssen die Betroffenen darüber vorab informiert werden.

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 möglichst 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

Copyright: S. Hofschläger / pixelio.de

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 Amtshandlungsdaten

Die Veröffentlichung von Amtshandlungsdaten (Taufe, Konfirmation, Trauung, Bestattung) ist nur unter engen Voraussetzungen möglich. Sie dürfen nur nach einer vorherigen schriftlichen Einwilligung (bei Konfirmanden auch die ausdrückliche Einwilligung zur Veröffentlichung der Adresse) veröffentlicht werden. Ein Widerruf dieser Einwilligung ist jederzeit möglich. Im Gemeindebrief sollte auf die jederzeitige Möglichkeit des Widerrufs der Einwilligung hingewiesen werden.

2.2 Geburtstage, Jubiläen und Konfirmationsjubiläen

Bei der Veröffentlichung von Geburtstagen, Jubiläen und Konfirmationsjubiläen gilt, dass vor einer Veröffentlichung des Gemeindebriefes die schriftliche Einwilligung einzuholen ist. Ein Widerruf dieser Einwilligung ist jederzeit möglich. Die Veröffentlichung von Adressen und genauen Geburtstagen ist nicht zulässig.

Der EKD-Datenschutzbeauftragte empfiehlt folgende reduzierte Form der Veröffentlichung:

Geburtstage im Januar
Eva Musterfrau 85 Jahre
Max Mustermann 80 Jahre

2.3 Kontaktdaten

Ehrenamtliche

Werden die Mitglieder des Kirchenvorstands im Gemeindebrief mit ihren Kontaktdaten veröffentlicht, müssen ihre EKHN-E-Mail-Adressen verwendet werden.

Die Nennung anderer Ansprechpartner/innen für bestimmte Arbeitsbereiche kann sinnvoll sein und die Kommunikation beschleunigen. Die EKD empfiehlt, private Kontaktdaten nicht im Gemeindebrief zu veröffentlichen, um Missbrauch insbesondere durch die Abrufbarkeit im Internet zu verhindern. Grundsätzlich gilt auch hier, dass Daten (Name, Vorname, Kontaktmöglichkeiten usw.) nur nach einer vorherigen schriftlichen Einwilligung veröffentlicht werden dürfen. Ein Widerruf dieser Einwilligung ist jederzeit möglich.

Angestellte

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

2.4 Muster-Einwilligung Veröffentlichung von Daten im Gemeindebrief

Gemeinde/ Anschrift

Einverständniserklärung für die Veröffentlichung von Daten im Gemeindebrief

Name / Vorname / Anschrift

Im Fall von Minderjährigen auch die der Erziehungsberechtigten

Name / Vorname / Anschrift

Ich bin damit einverstanden, dass meine folgenden Daten bzw. die meines Kindes im auch im Internet verfügbaren Gemeindebrief, veröffentlicht werden dürfen:

( ) Geburtstag ( ) Ehejubiläum

( ) Amtshandlungsdaten ( ) zur Konfirmation auch die Adresse

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.

Datum Unterschrift

2.5 Fotos und Videos

Auch Fotos oder Videoaufnahmen enthalten personenbezogene Daten, weil die abgebildeten Personen von heute 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.

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 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 Einsichts-fähigkeit 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

3.2 Muster-Einwilligung

Gemeinde / Anschrift ….

Einverständniserklärung der abgebildeten Person

Vor- und Nachname

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

( ) auf der Internetseite der Gemeinde

( ) der Facebook-Seite.

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

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. Verantwortliche Stelle für die personenbezogenen Daten sind die jeweilige Gemeinde und die EKHN. Diese Mitgliederdaten dürfen für Fundraising genutzt werden, es sei denn es liegt eine Meldesperre oder ein Widerspruch vor. Folgende Daten dürfen genutzt 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 Auftragsdatenverarbeitung = 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]:

[10] https://datenschutz.ekd.de/infothek-items/adv-vertrag

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 verabredungsgemäß 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.

Eine kirchliche Stelle, die nicht über die Mitgliederdaten verfügt, kann sich an die zuständige Stelle (z.B. Kirchengemeinde) wenden. Die zuständige Stelle kann dann zustimmen und folgende Daten übermitteln:

- Name, aktuelle Anschrift, Geburtsdatum, Geschlecht, Familienstand, Zahl und Alter der minderjährigen Kinder, Gemeindezugehörigkeit
- Für Mailings im Raum der EKHN bietet sich die in KiRa bereits vordefinierte „Impulspost-Auswertung“ an, die diese Daten integriert, Sperrvermerke und Widersprüche berücksichtigt und auch für den Versand bereits optimal vorbereitet hat.

Auch hier sind alle notwendigen Sicherungsmaßnahmen der Daten zu beachten!

4.3 Ihr Fundraising-Experte vor Ort ist für Sie da

Sie sind unsicher oder haben Fragen? Hier finden Sie Ansprechpartner für Ihr Fundraising-Projekt bzw. Ihre Datenschutz-Frage zum Fundraising.[11]

5 Webseiten / Internet

5.1 Pflicht zu Impressum und Datenschutzerklärung

Jeder Webseitenbetreiber benötigt ein aktuelles Impressum und eine Datenschutzerklärung auf der eigenen Webseite. 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.[12]

[11] http://fundraising.facettnet.ekhn.de/beratung.html
[12] http://www.schleswig-holstein.de/DE/Home/home_node.html

5.3 Webtracking-Tools

Die Verwendung von Webtracking Tools wie Google Analytics und Matomo (ehemals PIWIK) ist zulässig, sofern diese Bedingungen erfüllt sind:

- In der Datenschutzerklärung wird auf die Nutzung hingewiesen (gilt für beide)
- Nur für Google Analytics:
    - Die in Google Analytics erfassten IP-Adressen werden mit Hilfe der Funktion „anonymizelp“ anonymisiert bei Google gespeichert und
    - Es gibt einen AV-Vertrag zwischen Webseitenbetreiber und Google

Bei Matomo (wird im FacettNet genutzt): hier liegen die Statistikdaten auf einem eigenen Webserver der EKHN – außerdem unterstützt Matomo die Anonymisierung von IP-Daten und ist daher für kirchliche Einrichtungen (sofern nicht eh im FacettNet) eine sehr empfehlenswerte Lösung.

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 Alternative 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.

5.6 Gemeindebrief im Netz

Im Absatz 2 haben wir ausführlich über die Einwilligung zur Veröffentlichung von persönlichen Daten wie Geburtstagen oder Jubiläen gesprochen. Wenn diese Einwilligungen nicht vorliegen, achten Sie unbedingt darauf, dass entsprechende Gemeindebriefseiten NICHT auf Ihrer Webseite veröffentlicht werden – und entfernen Sie diese z.B. mit dem Programm Adobe Acrobat aus einer PDF Datei.

6 Newsletter und Mailings

Copyright: S. Hofschläger / pixelio.de

Der Versand von Newslettern und E-Mailings ist ein wichtiges Kommunikationsinstrument in der EKHN. Zahlreiche Dekanate, 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.

6.1 Newsletter als Auftragsdatenverarbeitung

Zum Newsletterversand werden in der Regel externe Dienstleister genutzt, die den Versand in Auftragsdatenverarbeitung durchführen. Bestehende Verträge sind daher auf die neue Rechtslage umzustellen. Neu ist nun die explizite Regelung (§ 12 DSG-EKD)[13], 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, aber will eine Gemeinde beispielsweise Messengerdienste anbieten, greift diese Regelung in der Praxis.

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.

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 den Webseiten im FacettNet übernimmt Typo 3 diese Aufgabe für Sie. Wenn Sie Ihre

[13] https://www.kirchenrecht-ekd.de/document/39740

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 von FacettNet Seiten 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 Social Media

Foto: iStock / alexsl

7.1 Personale Kommunikation des Evangeliums

Soziale Netzwerke sind heute ein unverzichtbares Kommunikationsmittel. Die EKHN nutzt die wichtigsten Sozialen Netzwerke, um in einem 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 anstellt 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 digitalen 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 verkauft Daten oder tauschen Daten aus. Sicherheitslücken wurden zugegeben.

7.3 Privatsphäre-Einstellungen

Weil es im Wesen der sozialen Medien liegt, Menschen zusammen zu bringen, 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 Foto, 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.[14] 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] https://www.gemafreie-musik-online.de

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 eingeschränkte 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.

Hinweis

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

Stattdessen wird Jugendreferenten empfohlen, datenschutzkonformere Messenger-Dienste, wie z.B. Threema oder Signal zu verwenden. Zusätzlich ist ein EKHN-eignes Portal in Arbeit, welches eine Kommunikation mit den Mitgliedern auf gutem Wege ermöglichen wird. Es wird der Zugriff auf das EKHN-eigene Mailsystem zur Verfügung stehen, es wird eine Chat-Funktion geben, der sichere und datenschutzfreundliche Austausch von Dokumenten über die kirchliche Infrastruktur, sowie eine Kooperation von Menschen in unterschiedlichen Gruppen ermöglichen .[15]

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.

[15] https://irights.info/schlagwort/whatsapp

Wer selbst Videos hoch lädt, 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 wird von kirchlicher Seite Dudle – ein Softwaretool der Evangelischen Kirche Württemberg mit ähnlichen Funktionen empfohlen. Es ist über diesen Link kostenlos nutzbar: dudle.elk-wue.de

8 Cloud-Computing

Foto: iStock / Rick_Jo

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 01. Juli 2015 festgelegt worden und finden sich hier.[16]

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 nicht gesetzlich gewährleistet
- Wie transparent und wie offensiv geht der Anbieter mit dem Thema Datenschutz um?
- Ist der Datenschutz Vertragsbestandteil beim Abschluss des Nutzungsvertrags?

Es gibt Anbieter, die speziell für kirchliche Einrichtungen sichere und kostengünstige Lösungen anbieten wie z.B. die ECKD Kigst[17] oder Owncloud.[18]

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)[19]: Diese sind zulässig, *„wenn die Teilnehmenden durch geeignete Maßnahmen über Art und Umfang der Aufzeichnung oder Übertragung informiert werden*."

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/

[16] https://datenschutz.ekd.de/infothek-items/entschliessung-cloud-computing/
[17] https://www.eckd-kigst.de/portfolio/it-services/anwendungen-und-it-dienste/sicherer-datenaustausch/
[18] https://owncloud.com/de/kirchencloud-owncloud-als-basis-fuer-sicheren-datenaustausch-kirchlichen-organisationen/
[19] https://www.kirchenrecht-ekd.de/document/39740

Anlagen

- EKD Datenschutzgesetz
- Muster für Datenschutzerklärung im Web
- Muster für Impressum
- Mustertext Einwilligungserklärung für Fotos
- Mustertext Datennutzung im Kontaktformular
- Mustervertrag Auftragsdatenvereinbarung EKD
- Muster Einwilligung Veröffentlichung von Daten im Gemeindebrief