Jochim Selzer

Datenschutz in Kirchengemeinden

digitalcourage

KURZ&MÜNDIG

KOSTENFREI

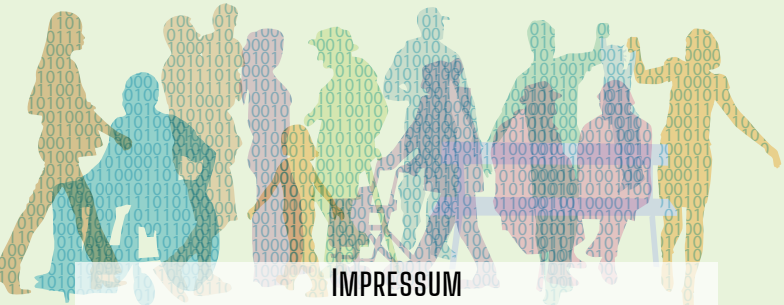
Art d'Ameublement

Band 20

Im Zentrum kirchlicher Arbeit steht die Begegnung mit Menschen, jung und alt – sei es in der Gemeinde oder in kirchlichen Kitas, Jugendzentren oder Sozialberatungen.

Auch hier werden Computer und Smartphones gebraucht:

- für Adressen- und Telefonlisten,
- Einladungen per E-Mail,
- Gemeindebriefe per Newsletter,
- Ehrenamtliche koordinieren sich per Messenger-App,
- Freizeiten werden per Videocall vorbereitet,
- digitale Fotos sollen auf die Homepage gestellt werden.



Impressum

1. Auflage 06-23, Art d'Ameublement, cc-by 4.0, ISBN 978-3934636-51-4

Autor: Jochim Selzer

Redaktion: Claudia Fischer, verstandenwerden.de

Layout: Isabel Wienold, iwi-design.de

Bildlizenzen: S. 30 Jochim Selzer cc-by 4.0;
Alle weiteren Bilder: iwi-design.de, Isabel Wienold cc-by 4.0

Die beiden großen Amtskirchen haben sich der Europäischen Datenschutzgrundverordnung DSGVO folgend ein eigenes Datenschutzrecht gegeben: Das evangelische DSG-EKD und das katholische KDG, das von den deutschen Bistümern anerkannt worden ist.

Das kirchliche Datenschutzrecht ähnelt dem staatlichen zwar sehr, weicht aber in Details ab, z. B. bei Antwortfristen. Es gilt nicht nur für die Gemeinden selbst, sondern auch für kirchliche Einrichtungen wie Schulen, Sozialkaufhäuser oder Chöre.

Datenschutz ist eine Grundhaltung. Fassen Sie Datenschutz nicht nur als eine rechtliche Verpflichtung auf. Vielmehr geht es hier um eine Grundhaltung Ihren Mitmenschen gegenüber.

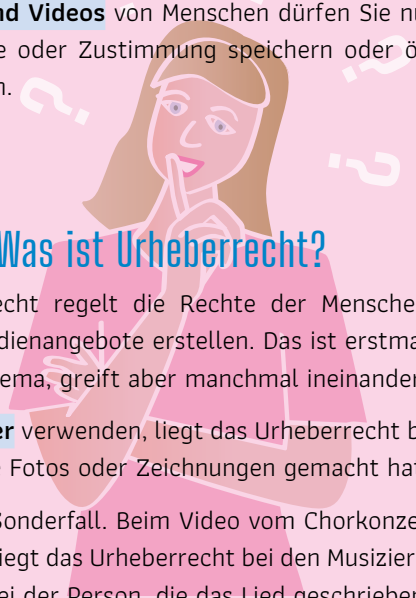
Wenn Sie Ihren Gemeindemitgliedern das Recht zugestehen, selbst zu entscheiden, was sie anderen von sich erzählen, ergibt sich vieles von selbst.

Denken Sie Datenschutz in der korrekten Richtung. Es geht nicht darum, sich eine Datenschutzerklärung unterschreiben zu lassen. Ihre Aufgabe ist, sich um Ihren Datenschutz Gedanken zu machen, datensparsam zu arbeiten und sinnvolle Entscheidungen zu treffen. Unterschriften kommen danach.

Was ist Datenschutz?

Datenschutz bezieht sich auf **personenbezogene oder personenbeziehbare Daten**, beispielsweise Namen, Geburtsdaten und Telefonnummern der Kindergruppe. Was dürfen Sie erheben und verarbeiten? Wie dürfen Sie es speichern? Wer darf wie darauf zugreifen?

Auch **Fotos und Videos** von Menschen dürfen Sie nur mit deren Freigabe oder Zustimmung speichern oder öffentlich verwenden.



Was ist Urheberrecht?

Das Urheberrecht regelt die Rechte der Menschen, die Texte oder Medienangebote erstellen. Das ist erstmal kein Datenschutzthema, greift aber manchmal ineinander.

Wenn Sie **Bilder** verwenden, liegt das Urheberrecht bei der Person, die die Fotos oder Zeichnungen gemacht hat.

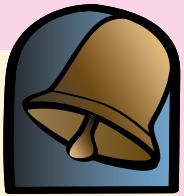
Musik ist ein Sonderfall. Beim Video vom Chorkonzert auf Ihrer Website liegt das Urheberrecht bei den Musizierenden genauso wie bei der Person, die das Lied geschrieben oder die Noten verfasst hat. Zuständig ist die GEMA. Wer auf dem Video zu sehen sein darf, ist eine Datenschutzfrage (siehe oben).

Was ist Datensicherheit?

Bei Datensicherheit geht es darum, dass **Daten nicht verloren gehen**, z. B. wenn ein Computer kaputtgeht (vgl § 7.1 f KDG, § 4(21) DSG-EKD). Außerdem heißt Datensicherheit, dass Sie Ihre Daten vor Zugriff von außen schützen, z. B. wenn jemand in Ihr Computersystem eindringt.

Sie sollten regelmäßige **Datensicherungen** anfertigen und Ihre Geräte mit Firewall, Passwörtern und Verschlüsselung schützen. Aktivieren Sie Bildschirmschoner und schließen Sie Bürotüren ab, wenn Sie kurz weggehen.

Auch wenn Sie z. B. Rechnungen **digital archivieren**, müssen Sie sicherstellen, dass sie innerhalb der buchhalterischen Aufbewahrungsfristen zuverlässig zur Verfügung stehen.



Merke: Datenschutz und Datensicherheit sollten nicht von der gleichen Person beaufsichtigt werden,

und

erheben Sie grundsätzlich nur die Daten, die Sie wirklich brauchen (Datensparsamkeit, § 7.1 f KDG und §5(1)3 DSG-EKD) und seien Sie kulant, wenn jemand seine Rechte einfordert oder Daten löschen lassen möchte.

Was sind Betroffenenrechte?

Auskunft

Institutionen, auch Kirchen, müssen auf Anfrage Auskunft erteilen, was sie über den/die Fragesteller.in gespeichert haben. Wenn jemand danach fragt, schauen Sie ins kirchliche Datenschutzrecht, oder fragen Sie bei Ihrer Datenschutzaufsicht nach – z. B. können Antwortfristen dort anders sein als allgemeine gesetzliche Regeln.

Nehmen Sie solche Anfragen ernst. Wenn Sie voreilig behaupten, nichts gespeichert zu haben, und Ihnen das Gegenteil nachgewiesen wird, kann dies rechtliche Konsequenzen haben. Eine häufige Falle ist z. B., das Newsletter-Abonnement oder Foto-Verzeichnisse zu übersehen.

Das Beantworten von Selbstauskunftsanfragen kann sehr umfangreich werden. Im Prinzip ist jede Mail, in der auch nur der Name der Fragestellerin steht, betroffen. Wenn die Chorleiterin irgendwo auf Papier eine Geburtstagsliste der Mitglieder führt, ist auch das ein Datensatz, den die Gemeinde offenlegen muss.

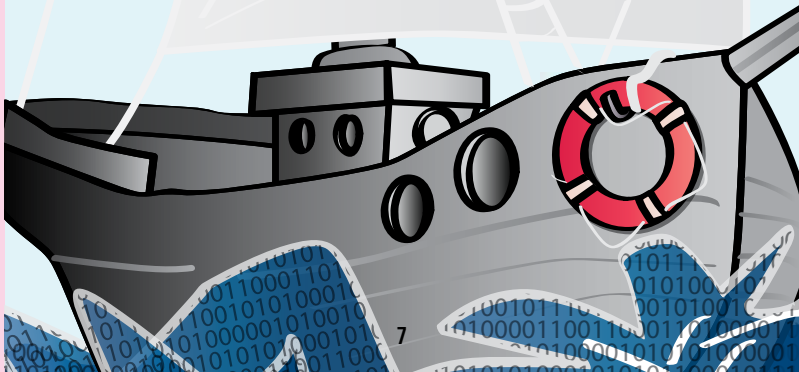
Für weitere Betroffenenrechte wie **Berichtigung, Löschung, Widerspruch** etc. holen Sie sich Unterstützung bei Ihrer Datenschutzaufsicht. Basteln Sie keine Eigenlösungen auf Gemeindeebene!

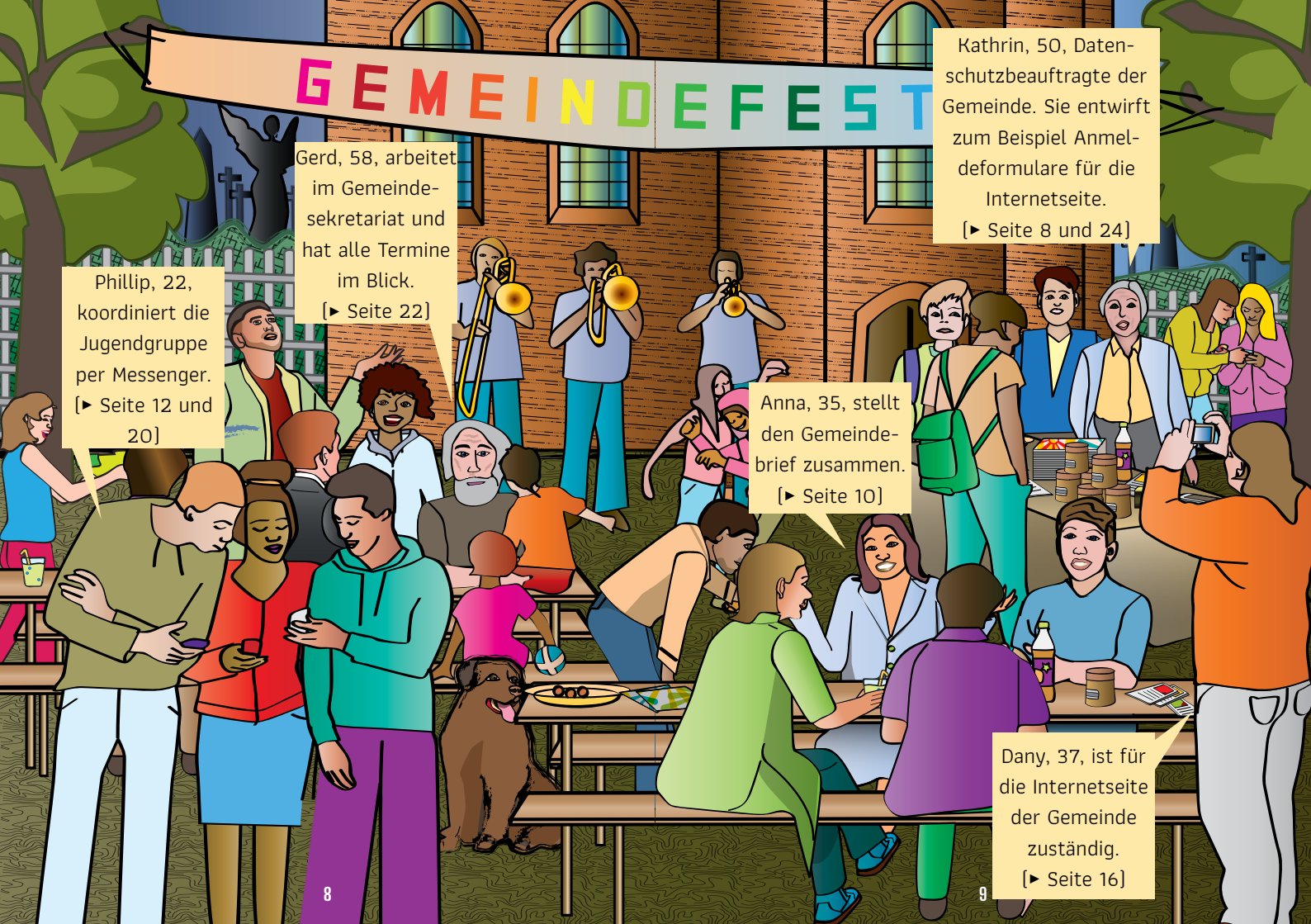
Lästig, aber hilfreich: Das Verfahrensverzeichnis

Jede datenverarbeitende Einrichtung ist zum Führen eines Verfahrensverzeichnisses verpflichtet. Darin wird dokumentiert, wer warum was wie lange auf welche Weise speichert. Betrachten Sie das nicht als lästige Pflicht, sondern als Ihren persönlichen Rettungsring. Ein gutes Verfahrensverzeichnis hilft Ihnen zu navigieren, wenn Gewässer mal unruhig werden.

Sie sparen viel Zeit, wenn Sie darin Rollen wie „die Chorleitung“ statt Namen wie „Manfred Moll“ benennen, denn Herr Moll wird vielleicht bald durch Frau Dur ersetzt, und wenn Sie Rollen vergeben haben, muss das Verzeichnis nicht geändert werden.

Muster für Verfahrensverzeichnisse finden Sie auf den Websites Ihrer kirchlichen Datenschutzeinrichtungen.




GEMEINDEFEST
Kathrin, 50, Datenschutzbeauftragte der Gemeinde. Sie entwirft zum Beispiel Anmeldeformulare für die Internetseite. [► Seite 8 und 24]
Gerd, 58, arbeitet im Gemeindesekretariat und hat alle Termine im Blick. [► Seite 22]
Phillip, 22, koordiniert die Jugendgruppe per Messenger. [► Seite 12 und 20]
Anna, 35, stellt den Gemeindebrief zusammen. [► Seite 10]
Dany, 37, ist für die Internetseite der Gemeinde zuständig. [► Seite 16]

Der Gemeindebrief

Für die Veröffentlichung von Taufen und Beerdigungen, Alters- und Ehejubiläen usw. müssen Sie in der Regel nicht um Erlaubnis fragen – wenn der Gemeindebrief eine **mitgliederinterne** Publikation ist.

Wenn der Gemeindebrief allerdings **öffentlich im Schaukasten** hängt oder in Apotheken ausliegt, ist er nicht mehr gemeindeintern. Beschränken Sie sich dann auf Name und Datum und nennen Sie keine Anschriften.

Streng genommen müssen die Betroffenen gewichtige Gründe vorbringen, wenn sie mit der Veröffentlichung nicht einverstanden sind. Aber: **Seien Sie kulant und respektieren Sie ein einfaches Nein.**

Sobald Ihr Gemeindebrief im Internet steht, als Klartext oder als PDF, dürfen Sie kirchliche Amtshandlungen nur mit **vorheriger (!) schriftlicher (!) Einwilligung** der Betroffenen veröffentlichen. Setzen Sie nicht darauf, zur Not tricksen zu können. Das funktioniert spätestens bei Beerdigungen nicht.

Vorsicht bei privaten Kontaktdaten Ihrer Ehrenamtlichen! Die Sozialberaterin der Geflüchtetenhilfe möchte sicher nicht ins Visier von Rassist.innen geraten.

Anmeldeformulare

- Unterscheiden Sie deutlich zwischen Pflicht- und freiwilligen Angaben.
- Nehmen Sie „Pflichtangaben“ wörtlich. Setzen Sie das nur ein, wenn Sie Ihr Angebot ohne diese Angaben nicht umsetzen können. Das ist etwas Anderes als: „Es wäre praktisch, wenn wir es wüssten.“
- Holen Sie sich nur für die freiwilligen Angaben eine Einwilligung. [Muster finden Sie auf den Websites Ihrer Datenschutzaufsicht.] Bei Pflichtangaben reicht der Hinweis, dass und wozu Sie diese erheben.
- Halten Sie den Datenschutzhinweis knapp und aussagekräftig.
- Bewahren Sie Daten nur so lange auf, wie laut kirchlichem Datenschutzrecht notwendig. Hinweise, wer welche Medikamente benötigt, wollen Sie schnellstmöglich wieder vergessen.
- Seien Sie zurückhaltend mit Teilnahmelisten von Veranstaltungen für staatliche Zuschüsse. Wer sich an die Beratungsstelle für Suchtkranke gewendet hat, geht niemanden etwas an. Nach außen muss es reichen, wenn Sie die Teilnahmezahl angeben und auf Nachfrage belegen können.

Messenger

- Vermeiden Sie WhatsApp und Telegram für die gemeindeinterne Kommunikation (siehe rechts).
- Der Messenger Signal ist zwar aus technischer Sicht gut geeignet, wirft aber wegen des Firmensitzes und des Serverstandorts in den USA rechtliche Schwierigkeiten auf.
- Matrix-basierte Messenger wie Element bieten zwar gute Verschlüsselung, haben aber ein Problem mit Metadaten sowie dem datenschutzkonformen Löschen von Konten.
- Suchen Sie am besten einen Messengerdienst mit Firmensitz und Serverstandort in der EU oder einem sicheren Drittstaat. Geeignet sind zum Beispiel Threema und Wire aus der Schweiz.
- Sorgen Sie für abgeschlossene Auftragsdatenverarbeitungs-Verträge mit dem Messengerdienst. [▸ Seite 26]

Für alle digitalen Angebote gilt:
Schaffen Sie Anreize zur Nutzung Ihres datenschutzkonformen Webdienstes. Sorgen Sie für interessante (!) Inhalte, die nur dort vorkommen. Ziehen Sie so Ihre Gemeindemitglieder mit.

Warum soll ich WhatsApp oder Telegram nicht nutzen?

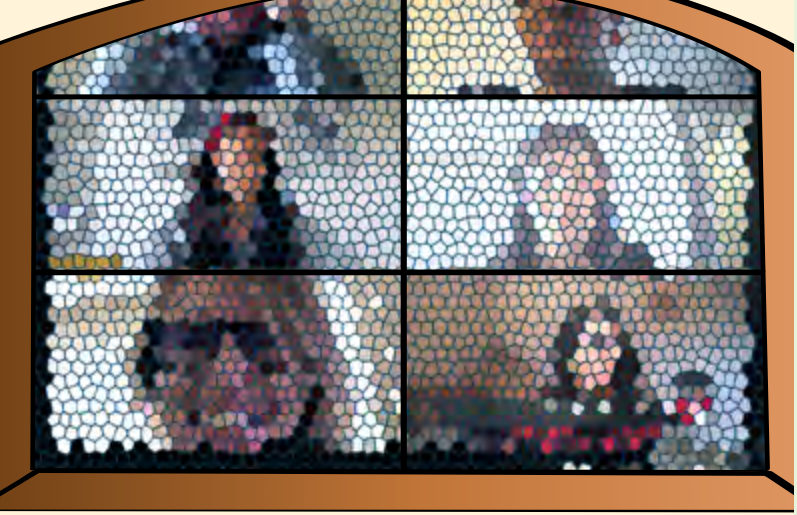
Beide Messengerdienste verarbeiten personenbezogene Daten in unsicheren Drittstaaten.

Aber ich nutze WhatsApp und sehe genau, dass alle anderen aus der Gemeinde auch da sind.

Das ist ein Zeichen für ein zweites Problem: Insbesondere das Hochladen des Adressbuchs ist problematisch, weil hier ungefragt auch die Telefonnummern von Personen in Ihrem Bekanntenkreis gemeldet werden, die den Messenger gar nicht nutzen.

Aber wir besprechen doch gar nix Geheimes! Kann doch jeder wissen, wann wir Samstag den Flohmarkt aufbauen wollen.

Bei Chats sind schon Metadaten problematisch, also wer wann mit wem kommuniziert. Soziale Kontakte sind schützenswert, z. B. wenn Menschen in Selbsthilfegruppen auf Anonymität angewiesen sind.



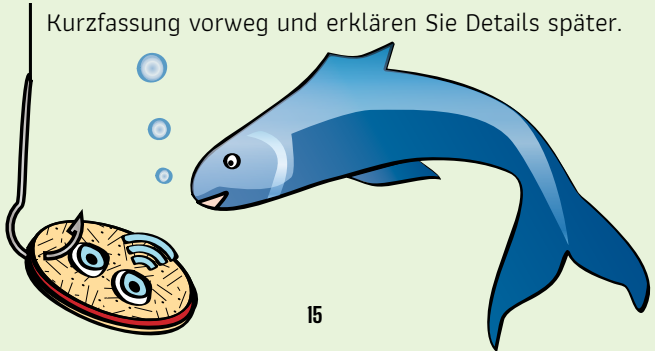
Videokonferenzen

- Vermeiden Sie aus rechtlichen Gründen in den USA ansässige Dienste wie Zoom, Microsoft Teams oder Skype. Wählen Sie nach Möglichkeit Anbieter aus der EU oder sicheren Drittstaaten.
- Empfehlenswert sind in der EU gehostete Systeme von BigBlueButton, Jitsi oder Nextcloud-Talk. Dafür gibt es auch freie öffentliche Anbieter. Mehr Infos: 🔗digitalcourage.de/videokonferenzen
- Sorgen Sie für abgeschlossene Auftragsdatenverarbeitungs-Verträge mit dem Videokonferenzanbieter. [▸Seite 26]

Cookies

Achten Sie auf rechtskonforme Cookiebanner. Sie sollten

- nicht mit allen möglichen Tricks versuchen, die Besucher.innen zum Klick auf „Alles akzeptieren“ zu verleiten.
- das Ablehnen genau so einfach wie das Annehmen gestalten, also gut sichtbar und mit einem Mausklick erreichbar.
- nicht ein halbes Dutzend Cookies in der Kategorie „berechtigtes Interesse“ verstecken. Am besten bauen Sie Ihre Website von vornherein so auf, dass sie gar keine Cookiebanner benötigen. [▸Seite 16ff.]
- sich nicht in fein ziseliertem juristischem Fachjargon ergehen, sondern in klarer, verständlicher und einfacher Sprache sagen, was Sie warum und wie lange speichern und an wen Sie es weitergeben. Sollte der Text zu lang werden, schreiben Sie eine knackige Kurzfassung vorweg und erklären Sie Details später.



Checkliste für die Website

So verlockend es sein mag, bei Facebook oder Instagram präsent zu sein – Datenschutzbehörden warnen vor diesen Plattformen. Sie legen umfangreiche Nutzer.innen-Profile an und speichern sie in einem unsicheren Drittstaat (USA). Solche Probleme können Sie mit einer eigenen, in der EU gehosteten Website umgehen.

Für die Programmierung

- ☑ Der **Datenschutzhinweis** sollte wie das Impressum von jeder Unterseite aus direkt erreichbar sein.
- ☑ Untersuchen Sie Ihre Website auf **Trackingmechanismen**, löschen sie diese, wenn möglich, oder führen Sie alle in Ihrem Datenschutzhinweis auf.
- ☑ Das gilt insbesondere für von Google geladene Zeichensätze (Google-Fonts). Halten Sie **Fonts lokal** auf Ihrem Server vor, um Ärger durch Abmahnungen zu vermeiden.
- ☑ Achten Sie darauf, den Datenverkehr Ihrer Website mit **HTTPS** abzusichern. Das ist zwar nicht überall zwingend vorgeschrieben, aber Sie gewinnen auch nichts, wenn Sie es nur dort einschalten, wo Sie es unbedingt müssen.
- ☑ Sorgen Sie für abgeschlossene **Auftragsverarbeitungsverträge** mit allen an der Website beteiligten externen Unternehmen (▸Seite 26). Das umfasst insbesondere den Webhoster, den Newsletter-Versand, die Webdesign-Agentur, den Maildienstleister und Analysedienste.
- ☑ Verwenden Sie statt Google Analytics auf **kircheneigenen Infrastrukturen** betriebene Dienste wie Matomo. Da bei Google Analytics personenbezogene Daten in die USA übertragen werden, gibt es auch hier Datenschutzbedenken.
- ☑ Versetzen Sie sich in die Lage, das **Bestellen und Abbestellen von Newslettern** zu belegen. Die Anmeldung sollte über ein Double-Opt-In-Verfahren laufen. Das heißt, die Interessierten geben auf der Website eine Mailadresse an, an die dann ein Bestätigungslink geschickt wird, der angeklickt werden muss.
- ☑ Löschen Sie **Logfiles**, wenn sie nicht mehr gebraucht werden. Löschfristen finden Sie im Kirchen-Datenschutzrecht.
- ☑ Nutzen Sie **kein Facebook oder Instagram**. Setzen Sie kein TikTok (auch nicht in der Kinder- und Jugendarbeit) ein. Die Argumentation ist die gleiche wie bei der Messenger-Nutzung (▸Seite 12).

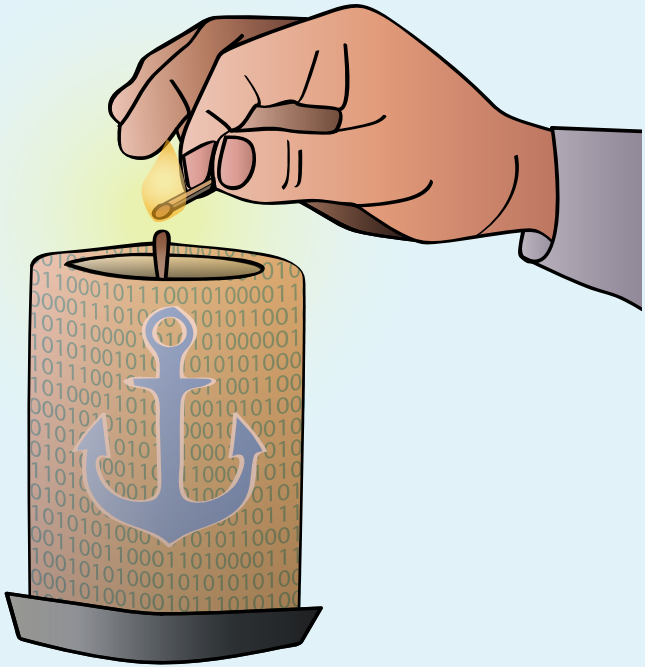
Details zu dieser Liste finden Sie auch im kurz&mündig Nr. 3 „Faire Websites“ 🔗digitalcourage.de/kum

Korrekte Datenschutzhinweise

- Achten Sie im Datenschutzhinweis auf den korrekten Gesetzestext. Textbausteine aus dem Internet berücksichtigen Kirchenrecht meistens nicht. Auf kirchlichen Websites gilt das kirchliche Datenschutzgesetz, nicht die Datenschutzgrundverordnung (DSGVO) oder das Bundesdatenschutzgesetz (BDSG).
- Ebenso ist für Sie nicht die Landes- oder Bundesdatenschutzaufsicht zuständig, sondern die kirchliche Datenschutzbehörde.
- Nennen Sie in Ihrem Datenschutzhinweis nicht nur die verantwortliche Stelle (in der Regel die Kirchengemeinde), sondern auch die Kontaktdaten der örtlichen Datenschutzbeauftragten. (►Seite 24)
- Führen Sie auch eingebundene externe Dienste wie Video- und Kartendienste auf.

Für die Gestaltung Ihrer Internetseite

- Achten Sie bei Fotos und Videos darauf, die Persönlichkeitsrechte der abgebildeten Personen geklärt zu haben. Das gilt insbesondere für z. B. Konfirmations- oder Firmungsfotos und wenn Sie den Gemeindebrief zum Download bereitstellen wollen (►Seite 10). Urheberrechte der Menschen an der Kamera müssen Sie auch beachten, aber das ist in diesem Buch nicht das Thema (►Seite 4).
- Verzichten Sie der Einfachheit halber auf die Veröffentlichung von kirchlichen Amtshandlungen auf der Internetseite. (►Seite 10)
- Vorsicht bei als PDF hochgeladenen Gemeindebriefen. Diese enthalten häufig kirchliche Amtshandlungsdaten, für die Sie meist keine Genehmigung für Veröffentlichung im Internet haben.



Hinweise für Ehrenamtliche

Unterschreiben Sie nicht einfach die Verpflichtungserklärung auf den Datenschutz. Sie sollten wissen, was Sie tun, was Sie dürfen und wie bestimmte Abläufe von der Kirchengemeinde geregelt und gewünscht werden. Gerade wenn Sie Gruppen leiten, speichern Sie womöglich zum Beispiel Telefonnummern in Ihrem privaten Handy.

Bestehen Sie auf regelmäßige Informationsveranstaltungen zum Datenschutz, um immer auf dem aktuellen Stand zu sein. Lassen Sie sich nicht mit der Verpflichtung abspeisen, sich selbst zu informieren, z. B. Im Intranet.

Lassen Sie sich eine kirchliche Mailadresse geben. Mischen Sie die Ehrenamts-Kommunikation nicht mit Ihren privaten Accounts. Wir wissen, dass das in vielen Gemeinden noch völlig utopisch ist – aber wenn z. B. Ihr privater Mailaccount angegriffen wird, haften Sie persönlich für das Datenleck, nicht Ihre Gemeinde.

Gemeindedaten haben auf Diensten wie Google Drive nichts verloren.

WhatsApp ist kein geeigneter Messenger für die gemeindeinterne Kommunikation. Manche Bistümer und Landeskirchen verbieten sogar WhatsApp für dienstliche Kommunikation. [▸Seite 12]

Verschlüsseln Sie die dienstlichen Daten auf ihrem Privatrechner. Wir empfehlen Veracrypt [Software und Anleitung gibt es im Internet].

Verschlüsseln Sie externe Datenträger wie USB-Platten oder Sticks.

Hinweise für Gemeinden

Erstellen Sie ein **Datenschutzkonzept**. Ein paar Tipps dafür:

- Verpflichten Sie Ihre Haupt- und Ehrenamtlichen auf den Datenschutz. Mustererklärungen finden Sie bei Ihren kirchlichen Datenschutzstellen.
- Sorgen Sie mindestens einmal jährlich für verpflichtende Datenschutz-Infoveranstaltungen für die Haupt- und Ehrenamtlichen.
- Alle Mitarbeitenden haben ihr eigenes Passwort, das sie mit niemandem teilen.
- Sorgen Sie für verschlüsselte Daten auf den Dienstrechnern.
- Lassen Sie im Gemeindebüro keine Akten offen herumliegen, insbesondere dann, wenn es außerhalb der Dienstzeiten frei zugänglich ist. Die meisten Aktenschränke kann man übrigens abschließen. :-)

- Statten Sie Ihre Haupt- und Ehrenamtlichen mit Kirchen-Mailadressen aus. Zum Beispiel Presbyter.innen haben Kontakt mit Bewerbungs-, Disziplinar- und Personaldaten und müssen sie auf gesicherten Wegen transportieren können.
  Pastorin.mueller_kreuzkirche@umsonstmail.de ist nicht geeignet. Pastorin.mueller@kreuzkirche.de wirkt nicht nur seriöser, sondern ist es auch.
- Statten Sie Ihre Mitarbeiter.innen mit professionell gewarteten Dienstrechnern aus, auf denen nur die IT-Abteilung Adminrechte hat, nicht die Pastorin oder der IT-kundige Küster. Klare Aufgaben- und Verantwortungstrennung sorgt für Rechtssicherheit.
- Treffen Sie verbindliche und klare Absprachen zur privaten Nutzung dienstlicher Geräte. Dienstrechner sind keine Familienrechner.
- Richten Sie Funktionspostfächer ein. Außenstehende wollen nicht Gerd Schulze, sondern das Sekretariat der Kreuzkirche erreichen – egal, wer das ist.
- Erstellen Sie ein Verfahrensverzeichnis [▸Seite 7].
- Nehmen Sie Selbstauskunftsanfragen ernst [▸Seite 24]. Es gibt Abmahnmaschen, die auf verschleppt, falsch, unvollständig oder gar nicht beantwortete Anfragen zielen.

Datenschutzbeauftragte vor Ort und ihre Aufgaben

- Benennen Sie eine Person, der/die offiziell als Datenschutzbeauftragte.r fungiert.
- Sorgen Sie dafür, dass der/die Betreffende sich wirklich dafür interessiert und nicht nur ein Name auf der Liste ist. Eine engagierte Ehrenamtliche kann das genausogut wie ein Anwaltsbüro, wenn sie von Ihnen gut unterstützt wird (bezahlen Sie Schulungen, Literatur etc.).
- Sorgen Sie dafür, dass die beauftragte Person mindestens per Mail oder postalisch erreichbar ist. Veröffentlichen Sie die Kontaktdaten, insbesondere auf der Website und im Impressum des Gemeindebriefs.
- Anfragen laufen nicht über das Gemeindebüro, sondern direkt. Wenn jemand nach Kontaktdaten zur beauftragten Person fragt, geben Sie diese einfach freundlich und ohne Rückfragen heraus.
- Vermeiden Sie Interessenskonflikte. Der Pastor eignet sich nicht als Beauftragter, weil er dann seine eigenen Weisungen kontrollieren müsste.
- Binden Sie Ihre beauftragte Person so früh wie möglich in alles ein, was ihren Aufgabenbereich betrifft. Je später sie eingebunden wird, desto teurer ist es, begangene Fehler zu korrigieren.

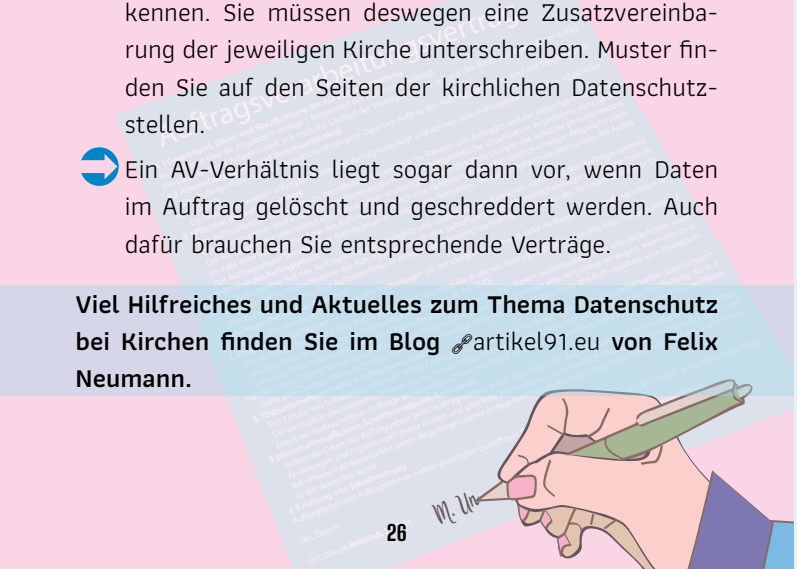
- Die beauftragte Person ist Ihre kritische Partnerin, nicht Ihre Gegnerin, auch wenn Sie Ihnen manchmal auf die Nerven geht.
- Sie verhindert, dass Ihnen andere auf die Nerven gehen, die ernsthaft Geld kosten können.
- Die beauftragte Person gibt Ihnen Hinweise, wie Sie am besten den Datenschutz umsetzen. Für die Umsetzung dieser Hinweise sind Sie selbst verantwortlich.
- Ihre Rolle besteht darin, Sie zu beraten und sie vor finanziellen sowie rechtlichen Risiken zu warnen. Ihre Rolle ist nicht, ergeben alles abzunicken und Ihnen möglichst wenig Arbeit zu machen.
- Informieren Sie Ihre Beauftragte auch und gerade dann, wenn etwas schiefgelaufen ist. Wenn sie von einem Datenleck erst dann erfährt, wenn die Anwaltsschreiben mit Schadensersatzforderungen auf Ihrem Tisch liegen, sind ihre Möglichkeiten sowie ihre Bereitschaft, die Situation zu retten, begrenzt.
- Sie soll Ihre Mitarbeiter.innen schulen und beraten. Fordern Sie das ein.
- Geben Sie der beauftragten Person die Möglichkeit, sich regelmäßig fortzubilden. Planen Sie dafür einen Etat ein.

Datenverarbeitung im Auftrag

Immer wenn Sie die Verarbeitung personenbezogener Daten auslagern, gehen Sie ein Auftrags-Datenverarbeitungs-Verhältnis ein [kurz AV]. So beispielsweise, wenn Sie eine Druckerei mit dem Erstellen und Versenden von Spendenaufrufen beauftragen und dafür Mitgliederadressen herausgeben. Ein anderes typisches Beispiel ist Ihr Webhoster oder der Versender Ihres Mail-Newsletters.

- Sorgen sie für geklärte AV-Verträge. Die im Auftrag Daten Verarbeitenden müssen sich der kirchlichen, nicht der staatlichen Datenschutzaufsicht unterwerfen. Meistens werden sie nur die staatlichen Verträge kennen. Sie müssen deswegen eine Zusatzvereinbarung der jeweiligen Kirche unterschreiben. Muster finden Sie auf den Seiten der kirchlichen Datenschutzstellen.
- Ein AV-Verhältnis liegt sogar dann vor, wenn Daten im Auftrag gelöscht und geschreddert werden. Auch dafür brauchen Sie entsprechende Verträge.

Viel Hilfreiches und Aktuelles zum Thema Datenschutz bei Kirchen finden Sie im Blog artikel91.eu **von Felix Neumann.**



Denken Sie darüber nach, Ihre Systeme selbst zu hosten?

Sie brauchen keinen Auftragsverarbeitungsvertrag, wenn Sie es schaffen, sich um Ihre Computer selbst zu kümmern und dabei keine fremden Auftragsfirmen einsetzen.

Es gibt inzwischen ein breites Angebot, wie Sie ohne Zoom, Microsoft, Google oder andere Digitalkonzerne auskommen. Denn diese US-Firmen müssen die Daten von Nicht-US-Bürger.innen den US-Geheimdiensten zur Verfügung stellen. Wenn Sie mehr wissen wollen, können Sie zum Beispiel bei Wikipedia nach den Stichworten CLOUD Act und FISA suchen.

Ihre Computervernetzung mit selbst verantworteter [gehosteter] Software zu organisieren, erspart Ihnen viele Fallstricke. Auf der nächsten Doppelseite schlagen wir Ihnen einige Programme vor.

„Die Zeit wird kommen, da ihr euch entscheiden müsst zwischen dem, was richtig und dem, was bequem ist.“

[Albus Dumbledore,
Schulleiter von Harry Potter]

Pro und Contra Selbst-Hosting

Admin werden ist nicht schwer. Die meisten modernen Dienste lassen sich selbst von Laien mit wenigen Mausklicks aufsetzen.

Admin sein dagegen sehr. Die größere Schwierigkeit ist, einen Dienst dauerhaft zu betreiben, bei Problemen schnell zur Stelle zu sein, Hilfe zu leisten, Aktualisierungen einzuspielen, Dokumentationen zu pflegen, Konfigurationen sicherer zu machen und Anpassungen vorzunehmen. Überlegen Sie im Vorfeld, ob Sie das über mehrere Jahre leisten können, und wer einspringt, wenn Sie nicht [mehr] zur Stelle sind.

Unser Tipp: Es gibt inzwischen IT-Dienstleister, die Ihnen Systeme aus freier Software aufsetzen. Dann brauchen Sie zwar wieder einen Auftragsverarbeitungsvertrag [▸Seite 26], aber Sie sind immerhin unabhängig von den Großkonzernen und gehen mit gutem Beispiel voran.

Unsere Software-Empfehlungen

Jitsi oder **BigBlueButton** für Videokonferenzen

Matomo zur Nutzungsanalyse der Webseite

Nextcloud als Datenablage und Terminkalender

Onlyoffice [innerhalb einer Nextcloud], um Texte und Tabellen gleichzeitig gemeinsam zu bearbeiten

Mastodon zum Microblogging wie bei Twitter

Moodle für den Konfirmations- oder Firm-Unterricht

Linux als Betriebssystem – schauen Sie mal bei 🔗luki.org vorbei

LUKi .ORG Linux User im Bereich der Kirchen e.V.

Über den Autor

Jochim Selzer ist Administrator und engagiert sich ehrenamtlich beim Chaos Computer Club. Er hält Seminare zu netzpolitischen Themen bei DGB-Gewerkschaften und hat seit 2013 unter dem Namen „Crypto-party“ mehrere hundert Seminare zur digitalen Selbstverteidigung durchgeführt. Seit 2008 ist er ehrenamtlich Datenschutzbeauftragter mehrerer Einrichtungen der Evangelischen Kirche im Rheinland sowie zweier gemeinnütziger Vereine.

Weitere kurz&mündig-Broschüren passend zum Thema:

Faire Websites – Kompaktwissen für Programmierung und Redaktion [Band 3]

Digitale Angriffe im Büro – Tipps für alle, die beruflich Geheimnisse wahren müssen [Band 9]

Einfach. Linux. – Freies Betriebssystem für freie Menschen [Band 17]

Die kurz&mündig-Reihe wird herausgegeben von:

digitalcourage e.V. engagiert sich seit 1987 für Grundrechte, Datenschutz und eine lebenswerte Welt im digitalen Zeitalter. Seit 2000 verleihen wir die BigBrotherAwards. Digitalcourage ist gemeinnützig, finanziert sich durch Spenden und lebt von viel freiwilliger Arbeit.

Mehr zu unserer Arbeit finden Sie auf 🔗digitalcourage.de und 🔗bigbrotherawards.de

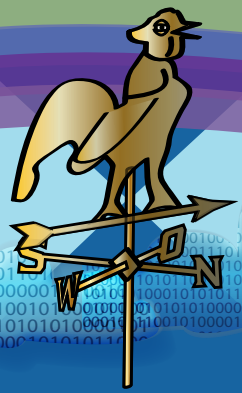
In der kurz&mündig-Reihe sind bisher erschienen:

01 **Digitale Mündigkeit**
02 **Datenschutzrechte in Schulen durchsetzen**
03 **Faire Websites**
04 **Leitlinien für digitale Bildung in Schulen**
05 **Uploadfilter**
06 **Stalking, Hass, Kontrolle**
07 **Homeoffice**
08 **Digitale Bildungsangebote selbst erstellen**
09 **Digitale Angriffe im Büro**
10 **Digitale Sicherheit für Frauenhäuser**
11 **Versammlungsfreiheit**
12 **Nichts zu verbergen?**
13 **Apps selbst prüfen und bewerten**
14 **Überwachung in China**
15 **Solidarität im Netz**
16 **Fediverse. So geht Social Media**
17 **Einfach. Linux.**
18 **Smart Toys und Kinder-Tracking-Apps**
19 **Datenschutzbeschwerden richtig einreichen**
20 **Datenschutz in Kirchengemeinden**

Dieses KURZ&MÜNDIG-Minibuch ist auch als komfortables interaktives PDF erhältlich. Es kostet nur 5,00 Euro und ist wie alle KURZ&MÜNDIG-Ausgaben (auch als Printversion) erhältlich unter: 🔗digitalcourage.de/kum

Geburtstage in der Kinderbibelgruppe, Telefonnummern vom Posaunenchor, Ankündigung von Beerdigungen, Fotos vom Sommerfest der Beratungsstelle – persönliche Daten schwirren überall im kirchlichen Kontext umher.

Checklisten für die Gemeindearbeit
Tipps für Haupt- und Ehrenamtliche



Digitalcourage e.V.
Marktstraße 18 | 33602 Bielefeld
mail@digitalcourage.de | digitalcourage.de
T: +49 521 1639 1639

9 783934 636514 >
5,00 Euro
5,00 CHF
ISBN 978-3934636-51-4
digitalcourage
k&m 20 Datenschutz in Kirchengemeinden