Handlungsempfehlungen zum **Kirchlichen Datenschutz**

im Ehrenamt

Bischöfliches Generalvikariat Trier
Betrieblicher Datenschutz

BISTUM
TRIER

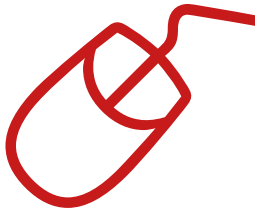
Bischöfliches Generalvikariat Trier
Betrieblicher Datenschutz

Inhalt

Was bedeutet Datenschutz?

Zweck und Ziel des Datenschutzes ist die **Sicherung des Grundrechts auf informationelle Selbstbestimmung** der Einzelperson. Jeder[1] soll selbst bestimmen können, wann er wem welche seiner Daten und zu welchem Zweck zugänglich macht.
Datenschutz soll den gläsernen Menschen verhindern und die **Privatsphäre** des Einzelnen **schützen**.

Auch für alle ehrenamtlich Engagierten im Bistum Trier ist die datenschutzkonforme Ausübung ihrer Tätigkeit sowohl Verantwortung als auch Selbstverständlichkeit. Zuständig für die Umsetzung der rechtlichen Anforderungen sind die Verantwortlichen vor Ort, z. B. die Pfarrer, Leitungsteammitglieder, Abteilungsleiter im Bischöflichen Generalvikariat und alle anderen Einrichtungsleiter.
Ehrenamtlich tätige Personen sind lt. KDG-DVO ebenfalls „Beschäftigte/Mitarbeiter" im Sinne von § 4 Ziffer 24 KDG.



1 Im Interesse einer besseren Lesbarkeit wird nicht ausdrücklich in geschlechtsspezifischen Personenbezeichnungen differenziert. Die gewählte männliche Form schließt alle anderen Formen gleichberechtigt ein.

Das Kirchliche Datenschutzgesetz

In allen deutschen Bistümern ist zum 24.05.2018 das Gesetz über den Kirchlichen Datenschutz (KDG) in Kraft getreten. **Das KDG gilt für alle kirchlichen Rechtsträger**, unabhängig von der Organisationsform; also Bistümer, Kirchengemeinden, Kirchengemeindeverbände, Kirchenstiftungen, Caritas, …

Das Gesetz steht mit der EU-DSGVO im Einklang.

Besondere kirchliche oder staatliche Rechtsvorschriften z. B. Strafgesetzbuch oder das Kunsturhebergesetz zum Umgang mit Fotos gehen dem KDG vor, sofern sie dessen Datenschutzniveau nicht unterschreiten.

Das KDG (KA 2018 Nr. 65) sowie die Durchführungsverordnung zum Gesetz (KDG-DVO – KA 2019 Nr. 9) sind auf der Homepage des Bistums Trier zu finden.
www.bistum-trier.de/datenschutz
Darüber hinaus kann es im zuständigen Pfarrbüro bzw. in der für Sie zuständigen Abteilung im Bischöflichen Generalvikariat eingesehen oder bei Bedarf in Papierform angefordert werden.

Der Pfarrer oder Einrichtungsleiter muss ehrenamtlich Tätige über die Datenschutzregeln informieren und darauf sensibilisieren, wie sie die ihnen anvertrauten Daten schützen. Das erfolgt in Form von **Online-Schulungen, Präsenzschulungen oder durch diese Handreichung**. So kann der Ehrenamtliche bei seiner Arbeit für die kirchliche Stelle datenschutzkonform handeln.


SECURITY

Haben Sie Fragen zum Datenschutz?

Dann wenden Sie sich an...

... Ihren zuständigen Verantwortlichen oder
... an den zuständigen betrieblichen Datenschutzbeauftragten im Bistum Trier

Bischöfliches Generalvikariat
Betrieblicher Datenschutz
Mustorstraße 2
54290 Trier

E-Mail	Telefon
datenschutz-pfarreien@bgv-trier.de	
Visitationsbezirk Koblenz	0651 7105 - 148
Visitationsbezirk Saarbrücken	0651 7105 - 478
Visitationsbezirk Trier	0651 7105 - 339
datenschutz@bgv-trier.de	0651 7105 - 468
datenschutz-lebensberatung@bgv-trier.de	0651 7105 - 339
datenschutz-telefonseelsorge@bgv-trier.de	0651 7105 - 339

Was sind personenbezogene Daten?

Datenschutzklasse 1

- Namens- und Adressangaben **ohne Sperrvermerk** (nach dem Bundesmeldegesetz)
- Berufsbezeichnung

Datenschutzklasse 2

- Handynummer
- Daten über Mietverhältnisse, Geschäftsbeziehungen, Vertragsdaten
- Geburts- und Jubiläumsdaten

Datenschutzklasse 3

- Namens- und Adressangaben **mit Sperrvermerk** (nach dem Bundesmeldegesetz)
- Bankdaten
- Gesundheitsdaten/ Krankheiten/Allergien und/oder Daten zum Sexualleben
- Angaben zur religiösen Überzeugung und/oder politische Meinungen
- Arbeitsrechtliche Rechtsverhältnisse
- Daten über strafbare Handlungen/Disziplinarverfahren

Was sind personenbezogene Daten?

Jegliche Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen, bezeichnet man als personenbezogene Daten. Dazu zählen Name, Anschrift, Geburtsdatum, Nationalität, Religionszugehörigkeit, Gesundheits- und Krankheitsdaten, Allergien, körperliche Merkmale, Daten zum Arbeitsverhältnis, …. und auch Fotos.

Diese personenbezogenen Daten werden in drei Datenschutzklassen unterteilt. In der Praxis haben sich hierfür klar definierte Schutzklassen etabliert, welche ein adäquates, hohes oder sehr hohes Schutzniveau festlegen.

Besondere personenbezogene Daten, die einem hohen oder sehr hohen Schutzniveau unterliegen:

- müssen noch stärker geschützt werden und
- dürfen nur unter bestimmten Bedingungen verarbeitet werden.
- Das Merkmal der Zugehörigkeit zu einer Kirche oder Religionsgemeinschaft (z.B. rk) gehört nicht dazu.

Je höher die Datenschutzklasse ist, umso intensiver sind die technischen und organisatorischen Maßnahmen durch den Verantwortlichen zu gestalten, damit das Schutzniveau der personenbezogenen Daten gewährleistet ist.

Vgl. die beiliegende Tabelle «Berührungspunkte mit personenbezogenen Daten für Mitarbeitende im Ehrenamt». Eine ausführliche Version inkl. Handlungsempfehlungen finden Sie unter: www.bistum-trier.de/datenschutz

Wie werden Daten verarbeitet?

- Erhebung
  Erfassung
- Abgleich
  Verknüpfung
- Abfrage
  Auslese
- Verwendung
- Speicherung
- Organisation
- Einschränkung
  Sperrung
- Offenlegung
  Übermittlung
- Veränderung
  Anpassung
- Verbreitung
  Veröffentlichung
- Ordnung
- Löschung
  Vernichtung

Verarbeitung von personenbezogenen Daten

Über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden verantwortliche Personen oder Stellen.

Dazu gehören im kirchlichen Bereich:

- der Generalvikar/der leitende Direktor
- Leitungen von Abteilungen und Einrichtungen
- der Pfarrer oder der Vorsitzende des Verwaltungsrates, der Verbandsvertretung oder des Verbandsausschusses einer Kirchengemeinde oder eines Kirchengemeindeverbandes, andere Entscheidungsträger
- der Vorstand eines kirchlichen Vereins

Zur Erfüllung der in der jeweiligen Zuständigkeit der Einrichtung/Dienststelle/Gemeinde liegenden kirchlichen Aufgaben dürfen personenbezogene Daten verarbeitet werden *(Beispiel: Einladungen von Kirchenmitgliedern, Durchführung von Hausbesuchen und Veranstaltungen, Zustellung des Pfarrbriefs, Besuchsdienst, Jugendarbeit)*.

Die Weiterleitung von den hierzu benötigten personenbezogenen Daten an Mitarbeiter ist nur zur Erfüllung kirchlicher Aufgaben erlaubt. Keine kirchliche Aufgabe ist z. B. die Weiterleitung von Daten (etwa die Liste der Kommunionkinder) an die Presse, Banken, Einzelhandel oder politische Parteien.

Verarbeitung umfasst jede Form des Umgangs mit personenbezogenen Daten, beginnend mit der Erfassung bis zur Löschung – unabhängig davon, ob eine manuelle oder elektronische Verarbeitung erfolgt. Es gilt das **Verbot mit Erlaubnisvorbehalt**. Jede Verarbeitung personenbezogener Daten ist unzulässig, es sei denn es gibt eine rechtliche Grundlage oder es liegt eine Einwilligung vor.

Wann wird eine Einwilligung benötigt?

Dort wo keine Rechtsnorm eine Verarbeitung personenbezogener Daten erlaubt, benötigen die Einrichtungen auch die Einwilligung von ehrenamtlich tätigen Mitarbeitern zur rechtmäßigen Verarbeitung ihrer personenbezogenen Daten, egal ob es sich um die Verwendung von Namen, Anschriften, E-Mail-Adressen, Jahrestagen, Bankdaten… oder um die Veröffentlichung von Fotos/Videos handelt. Diese kann jederzeit bei der jeweils verantwortlichen Stelle für die Zukunft widerrufen werden.

Die personenbezogenen Daten von z. B. Lektoren, Kommunionhelfern, Mitarbeitenden in den Empfangsdiensten, Gremien, Arbeitsgruppen, Besuchsdiensten, Orga-Teams, Ministranten-/Kinder-/Jugendbetreuung, der Pfarrbriefverteilung usw. werden durch die Kirchengemeinde verarbeitet (Listen, Planungen, Einsatzpläne), die hierzu eine Einwilligung benötigt.

Die entsprechenden → Einwilligungsformulare sind bei der zuständigen Einrichtung oder dem Betrieblichen Datenschutz erhältlich.

Einwilligung von Minderjährigen

Wenn die Einrichtung die Einwilligung eines Kindes/Jugendlichen vor Vollendung des 16. Lebensjahres erwirken möchte, so bedarf es zusätzlich auch der Einwilligung des/der Personensorgeberechtigten. Im Gegensatz zu Grundsatzentscheidungen legt die verantwortliche Stelle bei Alltagsentscheidungen (z. B. Teilnahme an einer Ferienfreizeit) fest, ob die Unterschriften aller personensorgeberechtigten Personen vorliegen müssen. Für kostenfreie kirchliche Beratungsangebote (z. B. Telefonseelsorge) an Minderjährige nach Vollendung des 13. Lebensjahres gilt hinsichtlich der Zustimmungspflicht eine Ausnahmeregelung, denn hier ist keine Zustimmung erforderlich.

Wann wird eine Verpflichtungserklärung benötigt?

Wie im Falle hauptamtlicher Mitarbeiter schreibt das KDG auch für ehrenamtliche Mitarbeiter, die personenbezogene Daten verarbeiten (verwenden) vor, diese Mitarbeiter auf die Einhaltung der datenschutzrechtlichen Bestimmungen schriftlich zu verpflichten, sowie diese individuell auch auf andere für ihre Tätigkeit geltende Datenschutzvorschriften hin zu belehren.

Im Falle von minderjährigen Ehrenamtlichen (z. B. Pfarrbriefausträgern) liegt es in der Verantwortung des Pfarrers bzw. der Abteilungs- oder Einrichtungsleitung zu entscheiden, in welcher Form die Verpflichtung erfolgt, ggf. reicht eine mündliche Unterweisung aus.

Die Verpflichtung auf das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.

Jeder, der einer kirchlichen Stelle seine Daten anvertraut, hat einen Anspruch darauf, dass mit diesen Daten verantwortungsbewusst umgegangen wird. Hier wird nicht zwischen dem geschriebenen oder gesprochenen Wort unterschieden.

Auch sollte niemand die Verpflichtung als Ausdruck grundsätzlichen Misstrauens verstehen, sondern als Qualitätsmerkmal für die geleistete Arbeit.

Welche Aufgaben hat der betriebliche Datenschutzbeauftragte?

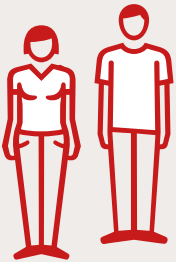
Zur Unterstützung und Beratung der verantwortlichen Personen oder Stellen sind im Bistum betriebliche Datenschutzbeauftragte tätig. Kirchliche Stellen sind gemäß § 36 KDG verpflichtet, einen betrieblichen **Datenschutzbeauftragten schriftlich zu benennen**. Die Benennung ist der Datenschutzaufsicht anzuzeigen.

Der betriebliche Datenschutzbeauftragte...

... berät und **unterrichtet Verantwortliche**.

... berät und **unterstützt bei Datenpannen**.

... **informiert haupt- und ehrenamtliche Mitarbeiter** über den Datenschutz.



... arbeitet mit den **Aufsichts-behörden** zusammen.

... **überwacht die ordnungs-gemäße Anwendung der Systeme**, die datenschutz-relevante Angaben verarbeiten.

... nimmt **Beschwerden** von Betroffenen entgegen und leitet diese an die Aufsichtsbehörde weiter.

Wichtige Regeln zum Datenschutz und Handlungsempfehlungen anhand von Fallbeispielen

1. Rechtmäßigkeit

Regel: **Grundsätzlich ist die Verarbeitung von personenbezogenen Daten verboten, es sei denn eine Rechtsnorm erlaubt es oder die betroffene Person willigt ein.**

Beispiel Rechtmäßigkeit: Im Vorfeld zur Pfarrgemeinderatswahl dürfen die Namen, Anschriften, Alter und Berufsbezeichnungen der Bewerber in ortsüblicher Weise veröffentlicht werden, wenn eine schriftliche Einwilligung der Bewerber vorliegt.

Beispiel unrechtmäßige Verarbeitung: Die Vorsitzende des Wahlausschusses veröffentlicht ohne Einwilligung die Fotos und Namen von allen Bewerbern auf der Homepage der Pfarreiengemeinschaft.

! Risiko: Gegebenenfalls können Schadensersatzansprüche gegen die kirchliche Einrichtung als verantwortliche Stelle geltend gemacht werden.

➥ Handlungsempfehlung: Im Vorfeld der Pfarrgemeinderatswahlen können die Modalitäten einer Veröffentlichung/Bekanntgabe auf der Homepage oder in anderen Medien mit den Beteiligten besprochen und schriftliche Einwilligungen erbeten werden.

2. Zweckbindung

Regel: **Personenbezogene Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke verarbeitet werden.**

Beispiel Zweckbindung: Es braucht die schriftliche Einwilligung der Eltern, bevor ein Foto ihres Kindes veröffentlicht werden darf. Sie müssen im Vorfeld genau darüber informiert werden, in welchen Medien (Pfarrbrief, Kindergartenzeitung, Tageszeitung, Homepage etc.) das Foto zu sehen ist. In privaten Social-Media-Accounts dürfen Fotos ebenfalls nur mit Zustimmung der Abgebildeten hochgeladen werden.

Beispiel Zweckentfremdung: Ein Katechet findet im Internet ein Gewinnspiel für Firmlinge. Als Preis winkt ein verlängertes Wochenende in einem Ferienpark für alle Firmlinge. Der Katechet lädt alle Namen und Anschriften sowie ein Gruppenbild aller Firmlinge auf der Gewinnspiel-Plattform hoch.

! Risiko: Der Katechet verstößt gegen das Gebot der Zweckbindung, da die Daten nur zur Firmvorbereitung und -durchführung erhoben wurden. Des Weiteren haben die Eltern nicht der Weiterleitung der Daten an Dritte zugestimmt, die diese nun für Werbezwecke etc. verwenden können.

➥ Handlungsempfehlung: Beim Elternabend der Firmbewerber können die Katecheten Aktionen, die sie mit den Jugendlichen durchführen möchten, vorstellen. Eltern entscheiden dann, ob sie das für ihre Kinder wünschen und geben dazu ihre schriftliche Einwilligung, damit die Kirchengemeinde ihrer Nachweispflicht nachkommen kann.

3. Datenminimierung

Regel: **So wenige Daten wie möglich, so viele Daten wie nötig verarbeiten!**

Beispiel Datenminimierung: Zur Durchführung einer Ferienfreizeit werden im Anmeldebogen Fragen zu Allergien und Ernährungsgewohnheiten abgefragt, allerdings auch die Kontaktdaten der Eltern, Krankheiten, Medikamentengaben, Kleidergröße für das Teilnehmer-Shirt, der Hinweis ob Schwimmer oder Nichtschwimmer, Bankdaten usw.

Beispiel Verstoß gegen den Grundsatz der Datensparsamkeit:
Die erhobenen Daten werden allen Betreuern und auch dem Küchenpersonal zur Verfügung gestellt, obwohl eine genaue Abgrenzung möglich wäre, wer welche Informationen zur Erledigung seiner Aufgaben benötigt.

! Risiko: Die Liste ist der Datenschutzklasse III zuzuordnen und bedarf damit eines besonders hohen Schutzes. Bei Verlust der Liste ist eine Datenpanne zu melden (→ Seite 38), denn eine missbräuchliche Verwendung dieser Daten kann zu einem erheblichen Schaden für die davon betroffenen Personen führen.

➥ Handlungsempfehlung: Eine Datenerhebung und Weitergabe ist dem Zweck angemessen durchzuführen und auf das notwendige Maß zu beschränken. Die Daten werden dementsprechend sortiert und nur den für den jeweiligen Aufgabenbereich zuständigen Mitarbeitern zur Verfügung gestellt.

4. Integrität und Vertraulichkeit

Regel: **Daten müssen geschützt und sicher aufbewahrt werden; nur zuständige Mitarbeiter dürfen auf die Daten zur Erfüllung ihrer Aufgaben zugreifen.**

Beispiel für Vertraulichkeit: Zur Organisation des Besuchs- und Gratulationsdienstes gibt es Namenslisten der zu besuchenden/gratulierenden Gemeindemitglieder. Diese Listen dürfen nur in die Hände des Besuchsdienstes gelangen.

Beispiel Verstoß gegen die Vertraulichkeit: Die Dame des Besuchsdienstes hat die Liste des gemeindlichen Besuchsdienstes offen im Wohnzimmer liegen lassen. Die Gäste ihres monatlichen Kaffeekränzchens finden die Liste während sie in der Küche ist und beschließen unangemeldet zur Geburtstagsfeier eines begehrten Junggesellen zu gehen.

! Risiko: Ungebetene Gäste bei der Feier oder Einbruchsgefahr in der Wohnung während der Abwesenheit des Geburtstagskindes.

➥ Handlungsempfehlung: Die Liste sollte im verschließbaren Schrank aufbewahrt werden, sodass unberechtigte Dritte keine Einsicht erlangen können. Für den Fall, dass ein Unberechtigter Einblick in die Liste erhält, sollte derjenige darauf hingewiesen werden, dass die Informationen vertraulich zu behandeln sind und nicht weiter verwendet werden dürfen. Ggf. ist es erforderlich, die betroffene Person zu benachrichtigen und in kritischen Fällen bedarf es sogar der Meldung einer Datenpanne an die Datenschutzaufsicht. Die Listen sind nach Gebrauch datenschutzkonform zu vernichten.

5. Transparenz

Regel: **Auskunftsrechte der Betroffenen und Informationspflichten der Verantwortlichen beachten.**

Sollte an ehrenamtliche Mitarbeiter ein Auskunftsersuchen herangetragen werden, sollte dieses Anliegen zur Erledigung unverzüglich an die zuständige Einrichtung/Abteilung/das zuständige Pfarrbüro weitergeleitet werden.

Informationspflicht der verantwortlichen Stelle:

Wenn die verantwortliche Stelle personenbezogene Daten erhebt, hat diese die betroffene Person umfassend über den Umgang mit ihren personenbezogenen Daten zu informieren. Dieser Informationspflicht kann z. B. über die Datenschutzerklärung auf der jeweiligen Homepage nachgekommen werden.

6. Speicherbegrenzung

Regel: **Begrenzung der Speicherdauer von Daten auf die notwendige Verarbeitungsdauer.**

Beispiel für Speicherbegrenzung: Teilnehmerlisten sind nach den abschließenden Arbeiten einer Veranstaltung, d. h. nach Erfüllung des Zwecks, zu vernichten, sofern die Zweckbestimmung keine zweite Einwilligung der Betroffenen für eine längere Verwahr- und Nutzungsmöglichkeit enthält und keine gesetzlichen Fristen eine längere Aufbewahrung erfordern.

Beispiel Verstoß gegen Speicherbegrenzung (Datenminimierung):
Eine Teilnehmerliste (Name/Anschrift/Geburtsdatum/Berufsbezeichnung) wird nach Beendigung der Veranstaltung ohne Einwilligung der Betroffenen für andere Zwecke (z. B. Organisation weiterer Veranstaltungen) im Büro der Katholischen Erwachsenenbildung archiviert.

! Risiko: Die personenbezogenen Daten aus der Liste fallen unter die Datenschutzklasse II, deren missbräuchliche bzw. unrechtmäßige Verarbeitung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann.

➥ Handlungsempfehlung: Zur rechtmäßigen Verarbeitung sind alle Daten, die einen Rückschluss auf die betroffenen Personen zulassen, zu löschen, es sei denn, der verantwortlichen Stelle liegt eine Einwilligung der Betroffenen für eine längere Nutzung vor.

Für den Fall, dass die verantwortliche Stelle Daten aus vergangenen Veranstaltungen statistisch auswerten möchte (z. B. Anzahl Teilnehmer, männlich/weiblich, Alter, Familienstand), empfiehlt es sich, durch Schwärzung aller personenbezogenen sowie personenbeziehbaren Daten, die Teilnehmerliste zu anonymisieren. Ein Rückschluss auf die seinerzeit betroffenen Personen darf nicht mehr möglich sein.

Anonymisierte Daten unterliegen nicht dem Datenschutz!

Rechte der betroffenen Person anhand von Fallbeispielen

Recht auf Auskunft

Möchte eine Person von einer kirchlichen Einrichtung/Dienststelle wissen, ob sie personenbezogene Daten von ihr verarbeitet, hat die Person das Recht, unverzüglich, spätestens jedoch innerhalb einen Monats, darüber Auskunft durch die verantwortliche Stelle zu erhalten.

Recht auf Widerruf der datenschutzrechtlichen Einwilligungserklärung

Für den Fall, dass die Verarbeitung personenbezogener Daten auf einer Einwilligungserklärung beruht, kann diese jederzeit, allerdings nur für die Zukunft, widerrufen werden.

Beispiel: *Die neuen ehrenamtlichen Mitarbeiter der Telefonseelsorge werden namentlich und bildlich auf der Homepage der Telefonseelsorge vorgestellt. Ein Mitarbeiter widerruft seine Einwilligung zur Bildveröffentlichung und das Bild ist umgehend von der Homepage zu löschen.*

Recht auf Berichtigung

Falsche Daten sind auf Verlangen der betroffenen Person zu berichtigen. Daneben besteht das Recht unvollständige Daten zu vervollständigen.

Beispiel: *Der Vorname der Gruppenleiterin auf der Homepage der Jugendgruppe hat einen Rechtschreibfehler. Die Gruppenleiterin hat ein Recht auf Berichtigung ihres Vornamens.*

Recht auf Löschung

Die betroffene Person hat das Recht unter den in § 19 KDG genannten Voraussetzungen, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden.

Beispiel: *Zur Planung einer Fahrgemeinschaft werden die Adressen der Teilnehmer gesammelt. Nach Beendigung der Fahrt erhält der Teilnehmer weiterhin postalisch Werbematerial zur Durchführung der nächsten Fahrt. Er hat das Recht auf Löschung seiner Anschrift, da er diese nur zum Zweck der Planung einer Fahr-gemeinschaft weitergeleitet hat.*

Recht auf Einschränkung der Verarbeitung

Unter das Recht auf Einschränkung der Verarbeitung fällt nicht die Löschung dieser Daten. Es bezeichnet vielmehr eine **Markierung personenbezogener Daten**, damit die Verarbeitung nicht mehr in vollem Umfang möglich ist. Dies erfolgt z.B. durch Sperrung der markierten/gekennzeichneten Daten oder Auslagerung auf ein anderes Speichermedium. Es könnte sein, dass gewisse Daten korrigiert oder angepasst werden.

Beispiel: *Ein ausgeschiedener ehrenamtlicher Vorsitzender eines Verwaltungsrates verlangt von seinem Nachfolger, dass seine personenbezogenen Daten nach seinem Austritt aus dem Verwaltungsrat (z. B. Ablauf der regulären Amtszeit) endgültig im Verwaltungssystem gelöscht werden. Das System sieht aber aufgrund von Löschungs-/Aufbewahrungsfristen keine Löschung vor. Der ehemalige Vorsitzende kann eine Einschränkung der Verarbeitung der Daten verlangen, um sicherzustellen, dass diese nicht unbeabsichtigt für unerwünschte Zwecke verwendet werden (z. B. Verwendung der Adresse für Sammeleinladungen zu pfarrlichen Veranstaltungen).*

Recht auf Datenübertragbarkeit

Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die dem Verantwortlichen bereitgestellt wurden, in einem **strukturierten, gängigen und maschinenlesbaren Format** zu erhalten.

Beispiel: *Der Kirchenchor hat seit Jahren eine Bankverbindung zur Bank A. Da dort keine kostenlose Kontoführung mehr gewährt wird, möchte der Vorstand die Bankverbindung zur Bank B verlegen. Da aber eine Vielzahl von SEPA-Lastschriftmandaten bei den Kontodaten hinterlegt ist, scheut der Vorstand den Aufwand alles manuell zu ändern. Der Kontoinhaber (hier der Kirchenchor) hat das Recht, die kostenfreie Übermittlung aller relevanten Daten von Bank A nach Bank B zu verlangen.*

Recht auf Widerspruch

In bestimmten Fällen, die in § 23 KDG näher beschrieben sind, haben betroffene Personen das Recht, gegen die Verarbeitung, der sie betreffenden personenbezogenen Daten, Widerspruch einzulegen.

Beispiel: *Ein Jubilar wird vom Förderverein einer Kirchengemeinde zum Spendenaufruf postalisch angeschrieben. Die Adresse hat der Förderverein vom Pfarrbüro erhalten. Der Jubilar hat das Recht, der Verwendung seiner Daten, um Direktwerbung und Fundraising (z. B. zur Spendenbeschaffung) zu betreiben, zu widersprechen.*

Datenschutz konkret

Fotos und Videos

Sobald Fotos oder Videos von Personen gemacht werden, ist neben dem KDG das **Recht am eigenen Bild** (§ 22 Kunsturhebergesetz – KUG) zu beachten.
Das Anfertigen und Veröffentlichen von Fotos ist regelmäßig nur zulässig, wenn die abgebildete Person, bzw. bei Kindern und Jugendlichen der Sorgeberechtigte, in das Fotografieren und die Veröffentlichung eingewilligt hat. Den abgelichteten Personen ist mitzuteilen, in welchen Medien (Pfarrbrief, Webseite, Social Media, Flyer/ Broschüre, etc.) das Foto/Video veröffentlicht werden soll.

Eine Einwilligung entfällt, wenn z.B. die Kirchengemeinde ein **berechtigtes Interesse an der Veröffentlichung** des Fotos hat und die Interessen des Abgelichteten an einer Nichtveröffentlichung nicht überwiegen.

Im Rahmen dieser Interessenabwägung sind die Grundsätze des **§ 23 Kunsturhebergesetz** (KUG) heranzuziehen: Der Veranstalter eines Festes hat etwa ein berechtigtes Interesse an der Veröffentlichung von Fotos, die bei einer Veranstaltung von allgemeinem gesellschaftlichem Interesse gemacht wurden.

Dazu können Veranstaltungen wie etwa eine Fronleichnamsprozession, ein Sommerfest oder die Sternsinger-Aktion gehören. In jedem Fall muss eine Abwägung erfolgen zwischen dem Interesse an der Veröffentlichung und den Interessen der abgebildeten Personen. Das Interesse an einer Nichtveröffentlichung überwiegt z.B. dann, wenn die Person im Fokus eines Fotos steht, das sie in einer Situation zeigt, die zur inneren Privatsphäre gehört (z.B. stilles Gebet in der Kirche).

Ein besonderes Augenmerk sollte auf die Anfertigung und Veröffentlichung von **Fotos Minderjähriger** gelegt werden. Relevant sind hier unter anderem das Alter der Kinder, die Gruppengröße und der Verarbeitungszweck. Lt. Beschluss der Diözesandatenschutzkonferenz (DDSK) ist es aber ausreichend, wenn die Einwilligung für konkret benannte Veranstaltungen vor bzw. zu Beginn eines Jahres für das jeweilige Veranstaltungsjahr eingeholt wird. Die Einwilligung kann entweder unmittelbar im Anmeldeprozess oder zu Beginn des Veranstaltungsjahres eingeholt werden.

Es ist nicht mehr erforderlich, die Veröffentlichung jedes einzelnen Fotos von den Personensorgeberechtigten genehmigen zu lassen.

Hinweis: *Im Rahmen der ersten Hl. Kommunion gehört die Beauftragung eines Fotografen nicht zu den kirchlichen Aufgaben der Pfarrei. Daher sollte eine Beauftragung des Fotografen direkt durch die Eltern erfolgen. In diesem Fall liegt die Verantwortung, die erforderlichen Einwilligungen einzuholen, bei den Sorgeberechtigten bzw. dem Fotografen.*

Externe Speicher (USB-Stick, externe Festplatte)

Sticks zum Speichern oder Weitergeben von personenbezogenen Daten sollten vermieden werden. Wenn es sich nicht vermeiden lässt, sollten Speichermedien wie externe und interne Festplatten, Sticks und Speicherkarten von Digitalkameras selbst oder die sich darauf befindlichen Dateien verschlüsselt werden.

Darüber hinaus sind USB-Sticks auch verstärkte Viren-Träger für Schadsoftware und damit eine große Gefahr für die Datensicherheit.

E-Mail-Versand

Trennen Sie Ihre E-Mail-Adressen! Mitarbeiter des Bistums Trier müssen sich an die Nutzungsbedingungen für die IT-Systeme des Bistums Trier halten, damit ist die Nutzung der privaten E Mail-Adresse für dienstliche Zwecke ausgeschlossen. Kirchengemeindliche Mitarbeiter (auch Ehrenamtliche) mögen sich im Bedarfsfall mit ihrem Pfarrer bzw. dem Einrichtungsleiter darauf verständigen, ob die Einrichtung einer (personalisierten) dienstlichen E-Mail-Adresse oder einer Funktionsadresse ermöglicht werden kann. In diesem Fall gelten die Nutzungsbedingungen des Anbieters.

Der Zugriff auf Funktionspostfächer sollte nur über einen personalisierten Zugang für jeden einzelnen Berechtigten möglich sein. So wird sichergestellt, dass jeder Zugriff nachvollzogen werden kann. Bei Beendigung der Tätigkeit bzw. Ausscheiden aus einem Amt sind selbstverständlich die entsprechenden Zugriffsberechtigungen zurück zu geben.

Stellen Sie sicher, dass **kein Unbefugter** (z. B. Ehepartner, Kinder, Kollegen) Zugriff auf das E-Mail-Konto bzw. auf die Daten aus der ehrenamtlichen Tätigkeit hat.

Dateien, die personenbezogene Daten der Datenschutzklasse II und III enthalten, sollten immer als **vertrauliche Anlage** zur E-Mail (z.B. als verschlüsselte PDF) versendet werden. *(Anleitungen zur Verschlüsselung und zur Vertraulichkeitsklassifizierung bei Bistumsaccounts sind beim Betrieblichen Datenschutz erhältlich.)*

E-Mail-Verteiler mit privaten E-Mail-Adressen werden grundsätzlich als **Blindkopie (BCC)** versendet, es sei denn die Mitglieder eines/r Gremiums/Gruppierung haben ihre Einwilligung zur transparenten Versandform erteilt. Dies sollte z. B. im Protokoll dokumentiert werden. Damit klar ist, wer konkret die E-Mail-Benachrichtigung erhält, können Sie am Textanfang einen Verteiler einfügen (z. B. „An alle Mitglieder PGR/VR)“ oder formulieren Sie eine eindeutige Anrede (z. B. „Liebe Teilnehmer des Senioren-Treffs“).

SPAM-Mails sind nicht mehr durch die Schreibweise oder gar den Absender problemlos zu erkennen. Oftmals sind es bekannte Absenderadressen aus dem eigenen Adressbuch. Der Anhang bzw. ein enthaltener Link sollte niemals geöffnet werden. **SPAM-Mails unbedingt** im Posteingang und im Gelöscht-Ordner/Papierkorb **löschen!**

Messenger-Dienste

Messenger-Dienste sind ein beliebtes Hilfsmittel zur Kommunikation und Organisation. Leider sind gerade die bekanntesten Anbieter nicht datenschutzkonform, weshalb z. B. WhatsApp für die dienstliche Nutzung nicht zu empfehlen ist. Bitte überlegen Sie bei Verwendung von WhatsApp oder anderen nicht datenschutzkonformen Messengern, Ihre Konversation inhaltlich einzuschränken, um sensible Daten möglichst nicht dort zu kommunizieren, z. B. Krankmeldungen über andere Wege kundtun.

Passwörter

Passwörter nicht personalisieren, d.h. keine Kombination aus Anfangsbuchstaben, des Namens und Geburtsdatums etc. verwenden. **Für ein starkes Passwort braucht es mindestens 10 Stellen. Es enthält Groß- und Kleinbuchstaben, mindestens zwei Zahlen und mindestens ein Sonderzeichen.** Merken Sie sich das Passwort anhand eines einprägsamen Satzes.

Beispiel: *Datenschutz im Bistum Trier ist uns nicht erst seit dem 24.5.18 wichtig!*
Passwort: „DiBTiunesd24.5.18w!“

Bitte beachten Sie auch gerne die Hinweise des Bundesamtes für Sicherheit in der Informationstechnik (BSI) → https://www.bsi.bund.de

Tipps und Hinweise im Alltag und im Büro

- ✓ Im Zuge von Sakramentsspendungen (Taufe – Beerdigung), beim Empfangsdienst, bei Besuchen im Pfarrbüro, auf der Bank, im Umfeld der Kirche oder bei Ausübung des kirchlichen Ehrenamtes kommt man mit personenbezogenen Daten in Wort und Schrift in Kontakt (z. B. Urkunden, familieninterne Informationen, Namen, Anschriften, Verwaltungsratsinformationen, aus Gesprächen, kirchengemeinde-spezifische Auskünfte). **Diese Informationen dürfen nicht an unberechtigte Dritte weitergegeben werden.**
- ✓ Türen bei eigener Abwesenheit immer abschließen.
- ✓ Keine sensiblen Unterlagen bei eigener Abwesenheit offen liegen lassen.
- ✓ Keine Gäste und Besucher alleine im Gebäude oder unbeaufsichtigt im Büro zurücklassen.
- ✓ Schlüssel und/oder Transponder nicht verleihen.
- ✓ Unterlagen mit personenbezogenen Daten dürfen nicht in den Hausmüll gelangen, sondern müssen datenschutzgerecht entsorgt werden.
- ✓ Mitgliedsverzeichnisse jeglicher Art unter Verschluss halten.

- Installation und stetige Aktualisierung eines Virenschutzprogrammes auf PC oder Laptop.
- Klare Trennung von dienstlichen und privaten Inhalten.
- Kein Zugriff auf E-Mail-Adressen oder Ablageordner durch andere Familienmitglieder oder Arbeitskollegen.
- Datensparsam im Internet agieren, denn es ist sehr leicht möglich, im Internet Daten zu verknüpfen und aus scheinbar harmlosen Informationen ein Raster/Profil zu entwickeln.
- Scheinbar kostenlose Angebote im Internet werden häufig mit der Preisgabe personenbezogener Daten bezahlt, die dann zu Werbezwecken verwendet werden.
- Nach Beendigung der ehrenamtlichen Tätigkeit sind Arbeitsmaterialien und Dokumente mit dienstlichen Inhalten zurückzugeben und von allen privaten Endgeräten datenschutzkonform zu löschen, ggf. überlassene Endgeräte sind ebenfalls zurückzugeben.

Wurde der Datenschutz verletzt? Aufgaben der Aufsichtsbehörden

Was tun bei einer Datenpanne?

Die Leitung bzw. ein Mitarbeiter der Einrichtung/Dienststelle oder die betroffene Person meldet die Datenpanne direkt nach Bekanntwerden dem Betrieblichen Datenschutz im Bistum Trier. In enger Zusammenarbeit zwischen Verantwortlichen und dem zuständigen betrieblichen Datenschutzbeauftragten erfolgt die Entscheidung, ob eine Meldung an die überdiözesane Datenschutzaufsicht **(Frist: innerhalb von 72 Stunden)** erfolgen muss.

→ Notfallplan unter www.bistum-trier.de/datenschutz

Aufgaben der Aufsichtsbehörde

Die Datenschutzaufsicht kontrolliert und überprüft u.a. die Einhaltung datenschutzrechtlicher Gesetze und Vorschriften. Sie fungiert als neutrale Beschwerdestelle, wenn sich eine betroffene Person nicht richtig behandelt fühlt. Außerdem nimmt sie Meldungen von Datenschutzverletzungen entgegen und wirkt auf Abstellung von Fehlern hin. Sie hat das Recht, Prüfungen vor Ort vorzunehmen.

Das Katholische Datenschutzzentrum Frankfurt/M., Roßmarkt 23, 60311 Frankfurt (Telefon 069 58 99 755–10, Fax 069 58 99 755–11, E-Mail: info(at)kdsz-ffm.de) wacht als Datenschutzaufsicht gemäß § 44 Abs. 1 KDG über die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz.
Sie ist zuständig für die (Erz-)Bistümer Freiburg, Fulda, Limburg, Mainz, Rottenburg-Stuttgart, Speyer und Trier.

BISTUM
TRIER

Impressum

Bischöfliches Generalvikariat Trier
S 1.7 Betrieblicher Datenschutz
Mustorstraße 2, 54290 Trier

Redaktion Cornelia Wagner und Anna Matussek
Betriebliche Datenschutzbeauftragte

Stand Januar 2025

Diese Informationsschrift ist beispielhaft und erhebt keinen Anspruch auf Vollständigkeit.