KATHOLISCH
Bistum Mainz

05



Datenschutzkonzept der Kirchengemeinde St. Maria Magdalena Ingelheim

einfach & sicher

Datenschutz im Bistum Mainz

Betriebliche Datenschutzstelle
Stand: Juni 2024

Änderungshistorie Dokument

Änderungsgrund	Datum	Geändert durch
Inkraftsetzung	31.12.2025	Christine Wüst-Rocktäschel
Aktualisierung	01.09.2026	Christine Wüst-Rocktäschel
Aktualisierung nach Unterweisung	11/2026	Christine Wüst-Rocktäschel

In Anlehnung an § 1 KDG-DVO zum Verzeichnis der Verarbeitungstätigkeiten empfiehlt es sich das Konzept bei jeder Veränderung eines Verfahrens bzw. in regelmäßigen Abständen von höchstens zwei Jahren durch den Verantwortlichen zu überprüfen und bei Bedarf zu aktualisieren. Die Überprüfung ist in geeigneter Weise zu dokumentieren (Dokumentenhistorie) – *Die Dokumentation wird durch die Verantwortliche Person in der Leitung gewährleistet.*

Bearbeitungshinweis:
Bitte füllen Sie die gekennzeichneten Felder aus -> ✎ bitte ausfüllen

Hinweis: Bitte stimmen Sie das DS- Konzept mit Ihrer zuständigen MAV ab. – *Für die Kirchengemeinde St. Maria Magdalena Ingelheim ist derzeit keine MAV gemeldet.*

„Niemand darf den guten Ruf, den jemand hat, rechtswidrig schädigen und das persönliche Recht eines jeden auf den Schutz der eigenen Intimsphäre verletzen.“
Can 220 CIC/1983

Inhalt

Präambel 4
01 Ziele des Datenschutzkonzeptes 9
02 Geltungsbereich 9
03 Datenverarbeitung 10
04 Zuständigkeiten in der Kirchengemeinde ..... Fehler! Textmarke nicht definiert.
05 Datenschutzordner / -dokumentation 11
06 Verzeichnis von Verarbeitungstätigkeiten (VVT) 12
07 Verpflichtung auf das Datengeheimnis 12
08 Sensibilisierung der Mitarbeitenden 13
09 Auftragsverarbeitung (AVV) 14
10 Risikoanalyse / Datenschutz-Folgenabschätzung (DSFA) 14
11 Umgang mit Datenschutzverletzungen 15
12 Betroffenenrechte 15
13 Verarbeitung personenbezogener Daten 16
13.1 Gemeindemitgliederverzeichnis (e-Mip) 17
13.2 Kirchenbücher 17
13.3 Führen von Personalakten 18
13.4 Listen für Freizeiten, Chöre, Seniorennachmittage, Telefonlisten,… 18
13.5 VR-Protokolle 19
14 Öffentlichkeitsarbeit 20
14.1 Webpräsenz 20
14.2 SocialMedia 21
14.3 Foto- und Filmaufnahmen 21
15 Daten- und Informationssicherheit 22
15.1 Dokumentation der IT-Systeme 23
15.2 Passwortmanagement, Digitaler Nachlass 23
15.3 Datensicherung 24
15.4 Datenverschlüsselung 25
15.5 Schutz vor Schadprogrammen 27
15.6 Absicherung Windows-Endgeräte 28
15.7 Absicherung Mobiltelefone / Smartphones 29
15.8 Absicherung der lokalen Netzwerke der kirchlichen Einrichtungen 30
15.9 Absicherung Internet-Zugang 31
15.10 Zutritts- / Zugangs- / Zugriffskontrolle 31
15.11 Eingabekontrolle 33

15.12 Nutzung dienstlicher IT zu privaten Zwecken 33
15.13 Nutzung privater IT zu dienstlichen Zwecken 33
16 Löschung und Vernichtung von Daten 34
16.1 Löschkonzept 34
16.2 Vernichtung von Schriftgut 35

Präambel

Die folgenden Ausführungen des Datenschutzkonzeptes der Katholischen Kirchengemeinde St. Maria Magdalena Ingelheim beschreibt unsere Aufgaben, die Erhebung der dazu notwendigen Daten und wie wir damit umgehen. Weiterhin werden die sich daraus ergebenden Sicherheitsmaßnahmen und die „Betroffenen Rechte“ beschrieben. Der Schutz der Daten aller Menschen, die mit uns im Kontakt stehen, hat für uns erste Priorität. Auf Basis des Kirchlichen Datenschutzgesetzes (KDG) haben wir für unsere Pfarrei ein detailliertes Datenschutzkonzept entwickelt.

Unser Handeln hat zum Ziel, den Einzelnen davor zu schützen, dass er durch die Verarbeitung seiner personenbezogenen Daten in seinem Persönlichkeitsrecht nicht beeinträchtigt wird und um den freien Verkehr solcher Daten zu ermöglichen.

Datenschutzverantwortlichkeiten in der Pfarrei: Verwaltungsrat (vertreten durch Herrn VWR Christian Wellner), und Pfr. Christian Feuerstein, Datenschutzbeauftragte und für diesen Bereich in Leitungsverantwortung: Pfarreikoordinatorin Christine Wüst-Rocktäschel.

Datenschutz meint zum einen, dass alle personenbezogenen Daten dann gespeichert und verarbeitet (genutzt) werden können, wenn der/die Rechteinhaber/in zugestimmt hat. Zum anderen, dass die übertragenen Daten nur nach bestimmten Grundlagen verwendet werden dürfen. Diese regelt das KDG (Kirchliche Datenschutzgesetz). Wir gewährleisten also, dass jede/r zustimmt, dass seine Daten gespeichert u. verarbeitet werden dürfen (bed. auch Weitergabe!) und andererseits, dass alle, die diese Daten nutzen, verantwortungsvoll nach KDG damit umgehen. Ferner kann es ggf. erforderlich sein, dass Daten veröffentlicht werden. Dieser Form der Nutzung ist ebenfalls zuzustimmen. (Unterkategorie)

Die beiden Seiten einer Medaille sind zur Übersichtlichkeit in zwei Kategorien (X: Zustimmung zu Speicherung/Nutzung/Weitergabe und Y: Verantwortungsvoller Umgang mit den Daten) unterschieden. Da auch nicht volljährige Personen der Pfarrei Daten übertragen bzw. mit ihnen umgehen gibt es hierfür die Kategorien XX und YY.

Für alle Kategorien gewährleistet die Pfarrei, dass die jeweils unterwiesene Person durch Ausfüllen und Unterzeichnen einer entsprechenden Erklärung (je nach Kategorie), dem Umgang zuzustimmen. Alle Erklärungen werden im Original verwahrt und digital erfasst. Sie gelten bis auf Widerruf. Das Vorgehen gilt für Haupt- und Ehrenamtliche tätige Personen. Es umfasst auch den verantwortungsvollen Umgang mit sensiblen Daten von Auftragnehmern und Dienstleistern.

Durch regelmäßige Unterweisungen ist gewährleistet, dass den handelnden Personen in Haupt- und Ehrenamt hinlänglich bekannt gemacht wird, welche Vorgaben einzuhalten sind. Dazu gehört u.a. eine Online-Schulung, die alle HA Mitarbeitenden absolviert haben. Sie wird von EA Personen, die mit besonders sensiblen Daten arbeiten ebenfalls absolviert. Alle anderen EA sind informiert, dass sie diese Schulung machen können, aber nicht müssen.
Das Datenschutzkonzept sowie anhängige Informationen sind transparent einsehbar (Homepage). Die Ablage der Original-Erklärungen und der digitalen Erfassung erfolgt durch die Sekretärin der Pfarreileitung im Pfarrhaus, Belzerstraße 8, 55218 Ingelheim.

Aufgaben

Eine besondere Herausforderung entsteht, wenn freiwilliges Engagement auf gesetzliche Rahmenbedingungen trifft. Die Rahmenbedingungen sind so zu gestalten, dass die Rechte der Betroffenen gewahrt werden.

Als Kirchengemeinde sind wir dem christlichen Grundauftrag verpflichtet, alle Menschen unabhängig von ihrer Herkunft zu den Grundvollzügen der Kirche einzuladen. Dazu zählen

1. die gemeinsamen **gottesdienstlichen Feiern** (Liturgie),
2. der **Dienst am Mitmenschen** (Diakonie),
3. die **Weitergabe der Reich-Gottes-Botschaft** an die Menschen (Verkündigung) sowie
4. die **gelebte Gemeinschaft** (Koinonia).

In diesen Bereichen setzt die Katholische Kirche Schwerpunkte, die den Bedürfnissen der Menschen entsprechen.

Insbesondere in den folgenden Aufgaben werden personenbezogene Daten verarbeitet

- Die Feier und Spendung von Sakramenten (Taufe, Kommunion, Firmung, Eheschließung)
- Die Feier von Gottesdiensten (in Frage der Organisation im Vorfeld)
- Beerdigungen
- Führen von verpflichtenden Kirchenbüchern (Taufbuch, Trauungsbuch…)
- Die Verwaltung der Gemeinden und deren Mitglieder
- Spendenverwaltung
- Beteiligungen an Organisationen und öffentlichen Einrichtungen

Darüber hinaus erfüllen wir eine Vielzahl von pastoralen (sozialen) Tätigkeiten, die unter anderem in Zusammenarbeit mit Behörden oder anderen kirchlichen Einrichtungen und sozialen Organisationen durchgeführt werden. Viele Aufgaben werden von ehrenamtlich tätigen Personen ausgeführt.

Hierzu zählen zum Beispiel Angebote für Kinder (Ministranten), Seniorennachmittage, Büchereiarbeit oder musikalische Angebote und Gruppierungen.

Rechtsgrundlagen des Datenschutzes

Für unsere Kirchengemeinde sind Anforderungen der folgenden Rechtsgrundlagen unbedingt zu beachten:

- Gesetz über den Kirchlichen Datenschutz (KDG) in der Fassung des einstimmigen Beschlusses der Vollversammlung des Verbandes der Diözesen Deutschlands vom 20. November 2017 ab dem 25. Mai 2018
- Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO) in der Fassung des einstimmigen Beschlusses der Vollversammlung des Verbandes der Diözesen Deutschlands vom 19. November 2018 ab dem 01. März 2019.
- § 29 KDG Gesetz in der Fassung des Beschlusses der Vollversammlung des Verbandes der Diözesen Deutschlands vom 23. November 2020
- KAO -> Anordnung über die Sicherung und Nutzung der Archive der katholischen Kirche (Kirchliche Archivordnung) vom 10.01.2014
- KMAO -> Kirchliche Meldewesenanordnung (KMAO) in der Fassung des Beschlusses der Vollversammlung des Verbandes der Diözesen Deutschlands vom 20./21.06.2005, zuletzt geändert am 22.06.2015
- Ausführungsdekret zum Gesetz über den Kirchlichen Datenschutz zur Veröffentlichung von Sakramentsspendungen sowie Alters- und Ehejubiläen, Geburten, Weihe-, Priester- und Ordensjubiläen und Sterbefällen (Jubiläumserlass) vom 22.04.2024

Weitere Rechtsgrundlagen sind wichtig (keine abschließende Aufzählung):

- zum Sozialdatenschutz, Teile des Sozialgesetzbuchs, zum Beispiel das erste Buch, neunte Buch und zehnte Buch (im Folgenden: SGB I, SGB IX, SGB X),
- zur Verletzung von Privatgeheimnissen das Strafgesetzbuch (StGB)
- für die Telekommunikation das Telekommunikationsgesetz (TKG), zum Beispiel zum unerlaubten Abhören,
- für Medien das Digitale-Dienste-Gesetz (DDG), zum Beispiel in Bezug auf die Internetpräsenz unserer Kirchengemeinde,
- für den Datenschutz und den Schutz der Privatsphäre das Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG),
- zum Umgang mit Bildern das Kunst-Urhebergesetz (KunstUrG),
- für den Arbeitnehmendendatenschutz das Betriebsverfassungsgesetz (BetrVG), zum Beispiel für Mitarbeiter/-innenvertretungen
- für das Aufbewahren von Daten die Pflichten zur Aufbewahrung, zum Beispiel aus der Abgabenordnung (AO, steuerrechtlich) und dem Handelsgesetzbuch (HGB, handelsrechtlich).

Datenschutzgrundsätze

Begriffsbestimmungen

Im § 4 des KDG sind zahlreiche Begriffe für das Datenschutzrecht definiert (siehe: Kirchliches Amtsblatt Mainz 2018 Nr. 3, Seite 23ff). Sie helfen, das Recht zu verstehen.
Wesentliche Punkte sind hier vereinfacht beschrieben.

Eine „betroffene Person“ ist eine natürliche Person, von der Daten verarbeitet werden.

Der „Verantwortliche“ ist eine natürliche oder juristische Person, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (§ 4 Nr. 9 KDG).
In der Kirchengemeinde ist die verantwortliche Stelle die Kirchengemeinde selbst, vertreten durch den Verwaltungsratsvorsitzenden.

„Personenbezogene Daten“ sind die Informationen einer natürlichen Person. Mit den Daten kann man die Person identifizieren. Das kann direkt durch den Namen passieren, aber auch einzelne Informationen ohne Namen können auf eine Person schließen lassen, zum Beispiel eine Adresse.

Zu den „Besonderen Kategorien personenbezogener Daten“ zählen nach § 9 KDG unter anderem Gesundheitsdaten.

„Verarbeiten“ bedeutet das Vorgehen im Zusammenhang mit den personenbezogenen Daten. Das kann digital und in Papierform sein. Dazu zählt zum Beispiel, wenn personenbezogene Daten:

- erfasst werden,
- gespeichert werden,
- gedruckt werden,
- weitergeleitet werden,
- gelöscht werden.

„Pseudonymisierung“ bedeutet, dass die personenbezogenen Daten ohne zusätzliche Informationen (eine Art Schlüssel) nicht mehr eindeutig einer betroffenen Person zugeordnet werden können. Diese zusätzlichen Informationen müssen nach den Anforderungen des Datenschutzes aufbewahrt werden.

Bei der „Anonymisierung“ werden personenbezogene Daten so verändert, dass sie nicht mehr einer Person zugeordnet werden können. Anonymisierte Daten unterliegen nicht dem Datenschutz.

„Sozialdaten“ sind personenbezogene Daten, die von einer Stelle, die dem Sozialgeheimnis unterliegt, im Hinblick auf ihre Aufgaben nach dem Sozialgesetzbuch verarbeitet werden (siehe § 67 Absatz 2 Satz 1 SGB X).

Grundsätze

Die Grundsätze (§7 KDG) sind wie ein Fundament, worauf unser Handeln im Datenschutz aufbaut.
Die wesentlichen Punkte sind:

- Rechtmäßigkeit, d. h. es muss grundsätzlich eine Erlaubnis geben für das Verarbeiten (zum Beispiel eine Einwilligung, berechtigtes Interesse).

- Transparenz, d. h. das Arbeiten mit den personenbezogenen Daten muss nachvollziehbar sein (zum Beispiel, woher kommen Daten, wo werden sie gespeichert, wohin werden sie weitergeleitet).
- Zweckbindung, d. h. es ist für jede Verarbeitung ein Grund zu bestimmen. Daten dürfen nicht für einen anderen Zweck verwendet werden.
- Datenminimierung, d. h. dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (so viel wie nötig und so wenig wie möglich).
- Richtigkeit, d. h. die Daten müssen stimmen. Sind sie falsch, müssen sie berichtigt oder gelöscht werden.
- Speicherbegrenzung, d. h. die Daten müssen gelöscht werden, wenn sie nicht gebraucht werden.
- Integrität, d. h. die Daten dürfen nicht von Unbefugten verändert werden.
- Vertraulichkeit, d. h. die Daten müssen vertraulich behandelt werden. Unbefugte dürfen sie nicht einsehen.
- Rechenschaftspflicht, d. h. der Verantwortliche muss die genannten Punkte zum Umgang mit den Daten einhalten und dies nachweisen können.

01 Ziele des Datenschutzkonzeptes

Der Schutz von personenbezogenen Daten ist für unsere Katholische Kirchengemeinde wichtig. Mit Datenschutz wird das Recht auf informationelle Selbstbestimmung geschützt. Dieses Grundrecht ist als Ausprägung des allgemeinen Persönlichkeitsrechts nach Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen. Dafür sind Regelungen zum Umgang mit den Daten nötig.
Das Erheben, Verarbeiten und Nutzen personenbezogener Daten ist im Gesetz über den kirchlichen Datenschutz (KDG) geregelt.

Das Datenschutzkonzept hat zum Ziel, in einer zusammenfassenden Dokumentation die datenschutzrechtlichen Aspekte darzustellen. Es kann auch als Grundlage für datenschutzrechtliche Prüfungen genutzt werden. Dadurch soll die Einhaltung des KDG nicht nur gewährleistet, sondern auch der Nachweis der Einhaltung geschaffen werden.

Dazu gehört:

- wer etwas tun muss (zum Beispiel: Mitarbeitende oder Verantwortlicher),
- was die Person für den Datenschutz tun muss (welche Aufgaben und Maßnahmen),
- was alle Mitarbeitende beachten müssen (Regeln).

Ziel ist es, bei den Regeln

- die aktuellen Gesetze zum Datenschutz zu erfüllen und
- auf die Arbeit in unseren Tätigkeitsbereichen zu übertragen und anzuwenden.

02 Geltungsbereich

Die Regeln gelten für alle Mitarbeitenden (Haupt- und Ehrenamtliche) unserer Kirchengemeinde mit allen entsprechenden Einrichtungen.

Nachstehend sind die unselbstständigen Gruppierungen und Einrichtungen aufgeführt, in denen das Datenschutzkonzept Anwendung findet; insbesondere bei Körperschaften mit einer Vielzahl Gruppierungen und Einrichtungen ist das von Bedeutung (Bsp.: Kirchengemeinde mit x Pfarrbüros, x Kindergärten, x Kirchenchören, x Büchereien,) und gibt allen Beteiligten die erforderliche Klarheit. Die vollständige Übersicht enthält das VVT.

Unselbständige Gruppierungen und Einrichtungen:
Das zentrale Pfarrbüro Ingelheim
Außenstellen des Pfarrbüros (wöchentlich stundenweise besetzt) in Gau-Algesheim und Heidesheim
Kirchenchöre in Ober-Ingelheim, Ockenheim, Gau-Algesheim, Heidesheim, Wackernheim
Kinder- und Jugendchöre in Wackernheim und Gau-Algesheim
Kantorei Ingelheim
Katholische Kirchenmusik Gau-Algesheim, Heidesheim, Ockenheim, Welzbachtal,
Musikgruppe Heidesheim

KÖB Heidesheim, Gau-Algesheim und Ockenheim

Die Kindertagesstätten auf Terrain der Pfarrei sind unter der Rechtsträgerschaft von Unikathe und haben ein eigenes Datenschutzkonzept; die Pfarrei ist hier lediglich für die religionspädagogische Versorgung verantwortlich.

03 Datenverarbeitung

Datenerhebung

Als Kath. Kirchengemeinde verfolgen wir ausschließlich und unmittelbar kirchliche Zwecke. Unsere Aufgaben sind die Seelsorge nach der katholischen Glaubenslehre sowie die Verwaltung dieses pastoralen Raumes als rechtliche und organisatorische Größe innerhalb des Bistum Mainz nach allgemeinem Kirchenrecht.
Wir erheben und verarbeiten ausschließlich personenbezogene Daten, die unmittelbar zu unserer Aufgabenerfüllung notwendig sind. Die Erhebung und Verwendung personenbezogener Daten erfolgt gemäß dem KDG, hauptsächlich aufgrund einer gesetzlichen Grundlage, einer rechtlichen Erlaubnis (Vertrag/Beauftragung) oder einer rechtlichen Verpflichtung (Rechenschaftspflichten; Meldepflichten), sowie nach Einwilligung des Betroffenen oder seiner gesetzlichen Vertreter.

Datenkategorien

Wir verarbeiten folgende Kategorien mit personenbezogenen Inhalten in einem Umfang, der ausschließlich durch den damit verbundenen Auftrag bestimmt i.d.R. gehören hierzu:

- Kontakt- Identitätsdaten: Name, Anschrift, Kommunikationsdaten, Alter und Geschlecht
- Bankdaten: Kontonummer, IBAN, BIC, Bank, Name des Kontoinhabers
- Sozialdaten: Nationalität, Glaubenszugehörigkeit, Familienstatus, Beruf, Steuer- und Sozialversicherungsdaten (bei Hauptberuflichen), Führungszeugnis
- Gesundheitsdaten: Daten zur körperlichen und seelischen Gesundheit
- Mobilitätsdaten: Dokumentation des Vorhandenseins eines Führerscheins (keine Kopien)
- Daten von Dritten: Daten, die im Rahmen der Auftragserfüllung über Dritte Personen anfallen und gespeichert werden müssen

Art der Datenverarbeitung

Im Wesentlichen erheben und verarbeiten wir Daten

☑ zur Erfüllung unserer amtlichen Aufgaben durch Übermittlung entsprechender Dateien, Dokumente und Unterlagen
- ✓ seitens unseres Bistums
- ✓ durch staatliche kommunale Stellen
- ✓ durch die von dem Betroffenen beauftragte Organisation (z.B. Beerdigungsinstitut, etc.)

☑ zur Erfüllung unserer pastoralen Aufgaben
- ✓ durch die erlaubte Überlassung durch die jeweilige Person oder deren rechtmäßigen Vertreter
- ✓ aufgrund gesetzlicher Vorgaben (z. Bsp. Spendenverwaltung)
- ✓ zusätzlich zur Kommunikation mit den Gemeindemitgliedern (Einladungen, allgemeine Informationen und Ankündigungen) sowie zur Koordination unserer Aktivitäten

✓ bei Bild- und Filmmaterial durch Einwilligung der Beteiligten und weitere Schutzbefohlene

☑ zur Erfüllung unserer verwaltungstechnischen Aufgaben für die Pfarrei
✓ zur Erfüllung unserer z. B. Miet- u. Pachtangelegenheiten
✓ Zur Erfüllung von rechtlich erforderlichen Tätigkeiten wie bspw. Zahlungsvorgänge

Zuständigkeitsbereich	Kontaktdaten	Benennungsdatum
Verantwortlicher im Sinne des § 4 KDG	Pfr. Christian Feuerstein Ottonenstr. 3, 55218 Ingelheim christian.feuerstein@bistum-mainz.de	Mit Wirkung zum 01.01.2024
Gemeinsame Betriebliche Datenschutzbeauftragte für die Kirchengemeinden	Michaela Beiersdorf Bischöfliches Ordinariat Mainz Betriebliche Datenschutzstelle Weißliliengasse 2d, 55116 Mainz Postfach 1560, 55005 Mainz Tel. 06131/253-821 datenschutz.kirchengemeinden@bistum-mainz.de	Mit Wirkung zum 01.07.2022 Veröffentlichung im kirchl. Amtsblatt 14/2022
Interner IT-Sicherheitsbeauftragte(r) (oder Kontaktdaten des betreuenden IT-Fachbetriebs	IT Support und Service durch Bistums-IT Abteilung	
Ggf. zuständige Ansprechperson für das Thema Datenschutz (Datenschutz-Koordinator)	Pfarreikoordinatorin Christine Wüst-Rocktäschel Ottonenstr. 3, 55218 Ingelheim christine.wuest-rocktaeschel@bistum-mainz.de	Mit Wirkung zum 01.01.2024
Aufsichtsbehörde	Kath. Datenschutzzentrum Frankfurt/M., Frau Ursula Becker-Rathmair, Roßmarkt 23, 60311 Frankfurt/M. Tel.: 069 / 58 99 755 -10 Fax: 069 / 58 99 755 -11 info@kdsz-ffm.de	Mit Wirkung zum 01.01.2023 für weitere fünf Jahre zur Diözesandatenschutz-beauftragten

05 Datenschutzordner / -dokumentation

Die Dokumente (z. B. Verzeichnis für Verarbeitungstätigkeiten, AV-Verträge, Einwilligungen, etc.), die zur Erfüllung der Nachweis- und Rechenschaftspflicht erforderlich sind, müssen für den Verantwortlichen und die zuständigen Mitarbeitenden direkt verfügbar sein. Die obigen Dokumente sind in einem zentral verfügbaren digitalen Ordner
Speicherort: **Laufwerk O, Rheinhessen//Ingelheim//PWII/Datenschutz**
und in einem „analogen“ Ordner (=Datenschutzordner), Standort: Büro Christine Wüst-Rocktäschel, Pfarrhaus, Belzerstraße 8, 55218 Ingelheim abgeschlossener Schrank abgelegt.

Zuständig für die Durchführung ist: Christine Wüst-Rocktäschel (CWR), Pfarreikoordinatorin

06 Verzeichnis von Verarbeitungstätigkeiten (VVT)

Gem. § 31 Abs. 1 KDG hat jeder Verantwortliche ein Verzeichnis von Verarbeitungstätigkeiten, kurz VVT zu führen. Das VVT dient als wesentliche Grundlage für eine strukturierte Datenschutzdokumentation und hilft dem Verantwortlichen dabei, gemäß § 7 Abs. 2 KDG nachzuweisen, dass die Vorgaben aus dem KDG eingehalten werden (Rechenschaftspflicht).

Thema	Rahmenbedingungen	Trifft zu	Trifft nicht zu	ToDo / Bemerkungen
Erstellung	Das VVT basiert auf einer Vorlage, welche in Zusammenarbeit mit der KPMG, einer Kirchengemeinde und der Betrieblichen Datenschutzstelle erarbeitet wurde. Es ist an unsere Gegebenheiten angepasst und vollständig ausgefüllt.	✓		
Aufbewahrung	Das VVT ist zentral im „Datenschutzordner“ abgelegt, so dass es für den Verantwortlichen der Einrichtung im Bedarfsfall schnell verfügbar ist.	✓		
Überprüfung	Gem. § 1 Abs. 5 KDG-DVO ist das Verzeichnis bei jeder Veränderung eines Verfahrens zu aktualisieren. Im Übrigen wird es in regelmäßigen Abständen von höchstens zwei Jahren einer Überprüfung durch den Verantwortlichen unterzogen und bei Bedarf aktualisiert sowie der Datenschutzbeauftragten übermittelt. Die Überprüfung ist in geeigneter Weise zu dokumentieren (Änderungshistorie des Dokuments VVT).	✓		

Zuständig für die Durchführung ist: Christine Wüst-Rocktäschel, Christian Wellner (Verwaltungsrat)

07 Verpflichtung auf das Datengeheimnis

Alle, bei der Verarbeitung personenbezogener Daten tätigen Mitarbeitenden der Einrichtung, haben in nachweisbar dokumentierter Form eine Verpflichtungserklärung abzugeben. Neben den hauptberuflichen Mitarbeitenden gilt dies auch für die Ehrenamtlichen. Das Bistum hat Verpflichtungserklärungen für die jeweiligen Mitarbeitenden erstellt.

Thema	Rahmenbedingungen	Trifft zu	Trifft nicht zu	To-do / Bemerkungen
Mitarbeiterbestand verpflichten	Die Belehrung und Verpflichtung auf das Datengeheimnis nach § 5 KDG in Verbindung mit § 2 KDG-DVO erfolgt durch den Verantwortlichen oder einen von ihm Beauftragten. ▪ Verweis auf Datenschutzhinweise ▪ Verpflichtungserklärung ▪ Online Schulung Datenschutz und Datenschutz im Pfarrbüro	✓		
Neue Mitarbeiter verpflichten	Der Punkt „Belehrung und Verpflichtung auf das Datengeheimnis“ wird im Einarbeitungsprozess für neue	✓		

	hauptberufliche und ehrenamtliche Mitarbeiter berücksichtigt.			
Aufbewahrung	Die Verpflichtungserklärungen der hauptberuflichen Mitarbeitenden werden in den Personalakten aufbewahrt. Die Verpflichtungserklärungen der neben- und ehrenamtlichen Mitarbeitenden werden im „Datenschutzordner“ aufbewahrt.	✓		Es gibt mehrere Ordner mit den erforderlichen Dokumenten; Datenschutz-konzept; alphabethische Sortierung aller abgegebenen Datenschutzerklär-ungen, tw. sortiert nach Anlass wg. Kategorisierung, digitale Version
Einwilligung zu Fotos oder Filmaufnahmen	Solche Einwilligungen werden eingeholt, wenn aktueller Bedarf besteht	✓		s.o. Kategorisierung

Zuständig für die Durchführung ist: Christine Wüst-Rocktäschel, Christian Feuerstein

08 Sensibilisierung der Mitarbeitenden

Die/Der Datenschutzbeauftragte bietet sowohl im allgemeinen Fortbildungsprogramm des Bistums als auch auf Nachfrage Schulungen für Mitarbeitende an. Die Schulungen behandeln allgemeine datenschutzrechtliche Fragestellungen, werden bei Bedarf aber auch auf besondere datenschutzrechtliche Anforderungen ausgerichtet, die durch die Tätigkeit der Teilnehmende bedingt sind.

Da sich Gesetze, Richtlinien, Rechtsgrundlagen oder auch Bedrohungslagen ändern können, sind die Themen der Schulung und Sensibilisierung nicht als einmalige Angelegenheit zu betrachten. Von daher ist die Einrichtung gefordert, regelmäßig und unter Berücksichtigung des geeigneten Mediums ihre Mitarbeitenden für die Themen zu sensibilisieren und mit geeigneten Handlungsanweisungen auszustatten.

Zusätzlich werden zur Sensibilisierung im Team nach Erfordernis Unterweisungen schriftlich eingegeben. Die Themen der Unterweisung, Empfänger*innen sowie Zeitpunkt der Unterweisung wird dokumentiert und ist einsehbar.

Thema	Rahmenbedingungen	Trifft zu	Trifft nicht zu	To-do / Bemerkungen
Grundschulung	Alle Beschäftigten erhalten eine Grundschulung Datenschutz (KDG). Die Schulung erfolgt für Mitarbeitende der Kirchengemeinde i.d.R. durch die Onlineschulung, durch Präsenzschulungen oder andere geeignete Schulungsformate.	✓		
Sensibilisierung	Regelmäßige Schulungen zur Sensibilisierung der Beschäftigten werden sichergestellt.	✓		Erfolgte Online-Schulungen aller HA MA 2026

Dokumentation	Die durchgeführten Schulungsmaßnahmen bzgl. Datenschutz und IT-Sicherheit werden dokumentiert.	✓		Erfolgt für die Schulung 2026

Zuständig für die Durchführung ist: Christine Wüst-Rocktäschel

09 Auftragsverarbeitung (AVV)

Gem. § 29 KDG ist mit allen Auftragsverarbeitern (= natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet) ein schriftlicher AVV nach den Vorgaben des § 29 KDG zu schließen.

Thema	Rahmenbedingungen	Trifft zu	Trifft nicht zu	To-do / Bemerkungen
AV-Vertrag schließen	Es wurde mit allen Auftragsverarbeitern ein AVV abgeschlossen (bspw. bei Wartungsvertrag mit IT-Firmen)	✓		IT Dienstleistungen laufen über das Bistum
Aufbewahrung	Alle AV-Verträge sind im „Datenschutzordner“ der Kirchengemeinde abgelegt.	✓		
§ 29-KDG-Gesetz	Die Verarbeitung personenbezogener Daten durch eine kirchliche Stelle für eine andere kirchliche Stelle regelt das § 29-KDG-Gesetz und die § 29-KDG-Gesetz-DVO	✓		

Zuständig für die Durchführung ist: Pfr. Christian Feuerstein, Jörg Beuter (Verwaltungsleiter)

10 Risikoanalyse / Datenschutz-Folgenabschätzung (DSFA)

Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche gem. 35 Abs. 1 KDG vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.
Ein Praxisbeispiel könnte, je nach Umfang, eine geplante Videoüberwachung für die Erforderlichkeit einer DSFA sein. Bei Unklarheiten oder Fragen steht die zuständige betriebliche Datenschutzbeauftragte zur Verfügung.
In der Pfarrei St. Maria Magdalena Ingelheim werden neue Technologien nur zur Anwendung gebracht, wenn sie durch das Bistum als Dienstleistung angeboten werden. Insofern können hier keine aktuellen DSFA wiedergegeben werden. Sollte sich dieser Zustand ändern, wird das im Konzept niedergeschrieben werden.

Thema	Rahmenbedingungen	Trifft zu	Trifft nicht zu	To-do / Bemerkungen
DSFA durchführen	Es wurde für alle Verarbeitungen, die ein hohes Risiko für die Betroffenen zur Folge haben, eine Risikoanalyse / Datenschutz-Folgenabschätzung durchgeführt.			Keine Erfordernis zum aktuellen Zeitpunkt

Aufbewahrung	Das Ergebnis der Bewertung einer (möglicherweise erforderlichen) DSFA und die Verfahrensschritte im Falle einer DSFA sind dokumentiert und im Datenschutzordner abgelegt.			Keine DSFA zu verwahren
Kontaktaufnahme bDSB	Kontaktaufnahme mit zuständigem bDSB ist erfolgt.			Nicht erforderlich

Das Kirchliche Datenschutzmodell (KDM) bietet, unter folgendem Link, weitere Hinweise zur Durchführung einer Risikoanalyse an:

Richtlinie_Risikoanalyse-und-Risikobehandlung_KDM.pdf (kirchliches-datenschutzmodell.de)

Zuständig für die Durchführung ist: Christine Wüst-Rocktäschel, Christian Feuerstein

11 Umgang mit Datenschutzverletzungen

Kommt es bei der Verarbeitung personenbezogener Daten zu einer Datenschutzverletzung gemäß §§ 33 und 34 KDG (z.B. Diebstahl, Hacking, Fehlversendung, Verlust von Geräten mit unverschlüsselten Daten) so besteht, wenn diese Verletzung eine Gefahr für die Rechte und Freiheiten natürlicher Personen darstellt, eine gesetzliche Meldepflicht durch den Verantwortlichen. Im Falle einer Meldepflicht an das Kath. Datenschutzzentrum in Frankfurt (KDSZ) ist eine Frist von 72 Stunden vorgesehen.

Meldeweg / Verfahren bei einer Datenschutzverletzung:

- Datenschutzverletzung wird festgestellt
- Information an den Verantwortlichen und den betrieblichen Datenschutzbeauftragten (Anzeigeformular im Anhang)
- Durch das Ausfüllen des Anzeigeformulars erfolgt die erforderliche Dokumentation und das Risiko für die Betroffenen wird ermittelt
- Die Datenschutzverletzung wird an das Katholische Datenschutzzentrum in Frankfurt (KDSZ) gemeldet.
  Katholisches Datenschutzzentrum » Meldungen (kath-datenschutzzentrum-ffm.de)
- Die Anlaufstelle für das KDSZ ist mit der Meldung anzugeben. Es ist sicherzustellen, dass die angegebene Stelle informiert und in der Sache sprachfähig ist.
- Die Dokumentation erfolgt durch Speichern des Anzeigeformulars in einem unveränderbaren Dateiformat (z. B. pdf.) oder durch ausdrucken.

Um Datenschutzverletzungen entgegenzuwirken, ist die Sensibilisierung der Mitarbeitenden wichtig.

Zuständig für die Durchführung ist: Christine Wüst-Rocktäschel, Christian Feuerstein 12

Betroffenenrechte

Die Rechte der betroffenen Person sind in den §§ 17 bis 25 KDG geregelt, diese sind:
§ 17 Auskunftsrecht
§ 18 Recht auf Berichtigung
§ 19 Recht auf Löschung

§ 20 Recht auf Einschränkung der Verarbeitung
§ 21 Mitteilungspflicht im Zusammenhang mit der Berichtigung, Löschung oder Einschränkung
§ 22 Recht auf Datenübertragbarkeit
§ 23 Widerspruchsrecht
§ 24 Automatisierte Entscheidung im Einzelfall einschl. Profiling
§ 25 Unabdingbare Rechte der betroffenen Personen

Nach § 17 KDG haben Betroffene das Recht zu erfahren, ob und welche bei den Verantwortlichen Daten zu ihrer Person verarbeitet werden. Im Arbeitsalltag wird das Recht am häufigsten in Anspruch genommen.

Vorgehen bei einem Auskunftsersuchen:

- Ein Auskunftsersuchen kann über viele Kommunikationskanäle und Mitarbeitende eingehen. Die Weiterleitung erfolgt unverzüglich per Mail an den Datenschutzverantwortlichen und in Kopie an den Datenschutzbeauftragten.
- Eingangsbestätigung an Auskunftsersuchenden schreiben, und bei Unklarheit Nachweis der Identität und Anhaltspunkte für das Auffinden der Daten abfragen (Mustertext im Anhang).
- Die gespeicherten Daten werden unter Mitwirkung aller Dienststellen und Einrichtungen zusammengetragen.
- Negativ-Auskunft, wenn keine Daten vorliegen
  Positiv-Auskunft, wenn Daten vorliegen, gemäß § 17 Abs. 1 lit. a-h KDG
  (Mustertexte im Anhang)
  -

Für die Beantwortung von Anfragen gilt die Fristregelung des § 14 Abs. 3 KDG. Hiernach werden der betroffenen Person Informationen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung gestellt.

Zuständig für die Durchführung ist: Christine Wüst-Rocktäschel, Christian Feuerstein

13 Verarbeitung personenbezogener Daten

Der zentrale Ort der Verwaltung ist in der Regel das Pfarrbüro, hier laufen meist „alle Fäden" zusammen. Für die Durchführung verschiedenster alltäglicher Vorgänge der Organisation, Kommunikation und Zusammenarbeit werden unterschiedlichste personenbezogene Daten verarbeitet. Insbesondere: Führen von Kirchenbüchern und Gemeindemitgliederverzeichnis, Terminkalender, Terminplanung, Übersicht der Aktivitäten, Ansprechpartner und engagierten der Kirchengemeinde, Schlüsselvergabe und Materialverleih, Spenden und Fundraising, Informationsweitergabe per E-Mail-Verteiler oder Briefe, …

Bei der Verarbeitung von personenbezogenen Daten muss aber darauf geachtet werden, dass nicht alles, was wünschenswert oder technisch möglich ist, auch erlaubt ist! Manche pragmatische Lösung entpuppt sich im Nachhinein als datenschutzrechtlich bedenklich oder gar unzulässig.

Bei dieser Verarbeitung sind die Grundsätze für die Verarbeitung personenbezogener Daten §7 KDG zu berücksichtigen.

13.1 Gemeindemitgliederverzeichnis (e-Mip)

Das Gemeindemitgliederverzeichnis ist die wirksame und gleichzeitig notwendige Grundlage für eine ordnungsgemäße pastorale Versorgung in den Kirchengemeinden. Sein möglichst vollständiger und richtiger Inhalt ist für kirchliches Handeln daher von entscheidender Bedeutung.

Nach § 42 Abs. 1 BMG hat die katholische Kirche als öffentliche Religionsgesellschaft gegenüber den Einwohnermeldeämtern Anspruch auf Übermittlung der Daten ihrer Mitglieder. Zudem dürfen ihr nach § 42 Abs. 2 BMG ein Teil der Meldedaten von Familienmitgliedern, die einer anderen oder gar keiner Kirche angehören ebenfalls übermittelt werden (Familienverbund).

Nach § 42 Abs. 5 BMG ist die Übermittlung nur zulässig, wenn sichergestellt ist,
dass beim Datenempfänger (Kirchengemeinde) ausreichende Datenschutzmaßnahmen getroffen sind.

Thema	Rahmenbedingungen/ Empfehlungen	Trifft zu	Trifft nicht zu	To-do / Bemerkungen
Sperrvermerk	Übermittlungs- und Auskunftssperren sind zu beachten	✓		
Listen erstellen	Zustellung Pfarrbrief, Jubiläen, EK, Firmung,… Helfer haben Verpflichtungserklärung unterschrieben Helfer sind unterwiesen, dass die Unterlagen datenschutzkonform entsorgt werden Helfern wird ermöglicht, an den online-Schulungen des Bistums teilzunehmen	✓		
Ausgetretene	Ausgetretene Gemeindemitglieder dürfen lediglich unmittelbar nach Kenntnisnahme angeschrieben werden.	✓		
Auskunftsersuchen	Zur Beantwortung des Auskunftsersuchen wird das aus eMip generierte Dokument mit einbezogen.	✓		

Zuständig für die Durchführung ist: Christine Wüst-Rocktäschel, Christian Feuerstein

13.2 Kirchenbücher

Für die Verwaltung der Kirchenbücher mit den Matrikeldaten und die Urkundensammlung der Pfarrei gilt can. 535 CIC sowie die hierzu erlassenen Partikularnormen der Bischofskonferenz und ggf. des Diözesanbischofs. Ältere Bücher sind gemäß den Regelungen zum Archivwesen der katholischen Kirche sorgfältig und datenschutzkonform aufzubewahren. Diese Vorschriften sind als bereichsspezifische Normen dem KDG vorrangig (§ 2 Abs. 1 KDG).

Thema	Rahmenbedingungen / Empfehlungen	Trifft zu	Trifft nicht zu	To-do / Bemerkungen
Eintragung Sakrament	Beachtung von Partikularnom Sorgfaltspflicht bei Eintragung auf Richtigkeit, damit kein Antrag auf Berichtigung des Betroffenen gestellt werden muss.	✓		

Einsichtnahme in Kirchenbücher	Berücksichtigung der Nutzungs- und Gebührenordnung sowie der KAO	✓		

Zuständig für die Durchführung ist: Christian Feuerstein, Pfarrbüro

13.3 Führen von Personalakten

Die Personalakten werden im Auftrag der Kirchengemeinde im Bischöflichen Ordinariat geführt.

Personalakten sind Sammlungen von Urkunden und Vorgängen, die die persönlichen und dienstlichen Verhältnisse von Mitarbeitenden betreffen und in einem inneren Zusammenhang mit dem Dienstverhältnis stehen.
Das Führen der Personalakte liegt allerdings im Organisationsermessen des Arbeitgebers, das heißt, es muss keine einheitliche Akte geführt werden; es können auch Beiakten angelegt werden. Unabhängig davon, wo sich einzelne Unterlagen befinden, die persönliche oder dienstliche Verhältnisse von Beschäftigten beinhalten, gehören diese aber zur Personalakte.

Für die Verarbeitung personenbezogener Daten findet das Gesetz über den Kirchlichen Datenschutz (KDG) insbesondere § 53 Abs. 1 KDG (Beschäftigtendatenschutz) Anwendung.

Typische Daten, die in einer Personalakte (unter Beachtung der Aufbewahrungsfristen) verarbeitet werden dürfen, sind:

- Nachweise über die Aus- und Fortbildung
- Zeugnisse, soweit sie für die Durchführung des Arbeitsverhältnisses noch von Bedeutung sind
- der Arbeitsvertrag
- Beurteilungen
- Zeugnisse über Fortbildungsmaßnahmen
- Abmahnungen, Ermahnungen, Rügen
- Vereinbarungen über Darlehen und Gehaltsvorschüsse, Pfändungs- und Überweisungsbeschlüsse sowie Lohnabtretungen
- das Arbeitsverhältnis betreffender Schriftverkehr

Für die Führung von Personalakten von Klerikern und Kirchenbeamten gilt die Personalaktenordnung (PAO).

Zuständig/Verantwortlich für die Personalverwaltung (Beiakten) in der Kirchengemeinde sind: Christian Feuerstein, Christine Wüst-Rocktäschel, Jörg Beuter

13.4 Listen für Freizeiten, Chöre, Seniorennachmittage, Telefonlisten,…

Für den Pfarreirat, Kommunion- und Firmvorbereitungskreise, Seniorenkreise, Jugendgruppen und viele andere Bereiche sind Telefon-, Kontakt-, und Teilnahmelisten wichtig und notwendig.

Datenschutzrechtlich ist eine solche Weitergabe von Privatdaten aber nur dann zulässig, wenn eine Rechtsvorschrift sie erlaubt oder anordnet, die betroffene Person eingewilligt hat oder die Verarbeitung personenbezogener Daten erforderlich ist (§ 6 Abs. 1 KDG).
Unabhängig davon, wie die Liste erstellt wird (ChurchDesk, Excel, handschriftlich,..).

Thema	Rahmenbedingungen/ Empfehlungen	Trifft zu	Trifft nicht zu	To-do / Bemerkungen
Telefon- / Kontaktliste	§6 Abs. 1 lit. b KDG vorbereitete leere Liste auslegen, in der sich der TN selbst einträgt und somit einwilligt			Telefonlisten werden nicht geführt
Teilnahmeliste (Zuschuss)	§6 Abs. 1 lit. g KDG Zuschussliste des Zuschussgebers verwenden, Vorschriften sind zu beachten	✓		Betr. Zuschusslisten Förderung Stadt Ing
Besuchsliste	§6 Abs. 1 lit. f KDG Listenempfänger unterzeichnet Verschwiegenheitserklärung	✓		Erl. 10/25 an alle EA Besuchsdienste
Kontaktlisten in der Sakramentenkatechese (Taufe, Erstkommunion, Firmung)	§6 Abs. 1 lit. f KDG Listenempfänger unterzeichnet Verschwiegenheitserklärung	✓		Wegbegleiter*innen Firmung, EKO werden unterwiesen
Kontaktlisten in der Arbeit der nicht eigenständigen Gruppierungen	§6 Abs. 1 lit. f KDG Listenempfänger unterzeichnet Verschwiegenheitserklärung	✓		Gruppierungen sind informiert

Zuständig für die Durchführung ist: Christine Wüst-Rocktäschel, Pfarrbüro

13.5 VR-Protokolle

Über jede Kirchenverwaltungsratssitzung ist ein Protokoll zu erstellen gemäß §13 des Kirchenvermögensverwaltungsgesetzes (KVVG).

Dieses enthält unter anderem regelmäßig personenbezogene Daten, z. B. bei Beschlüssen zu Einstellungen von Mitarbeitenden oder Änderungen im Beschäftigungsverhältnis bis hin zu dokumentierten Problemfällen. Gemäß § 13 KVVG sind die Beschlüsse in ein Protokollbuch aufzunehmen. Jedes Verwaltungsratsmitglied kann unter Wahrung der datenschutzrechtlichen Bestimmungen eine Abschrift des Protokolls erhalten. Nicht selten werden die Protokolle elektronisch (z. B. als Word-Dokument oder als PDF-Datei) erzeugt und gespeichert. Die Protokolle als Datei unverschlüsselt (!) per E-Mail über öffentliche Netze an die Verwaltungsratsmitglieder zu versenden, ist auf Grundlage der datenschutzrechtlichen Bestimmungen nicht erlaubt!
Alternativen, z. B. ein geschützter Bereich für Verwaltungsratsmitglieder auf einer Internetplattform, können nur dann in Betracht gezogen werden, wenn die datenschutzrechtlichen Bestimmungen eingehalten werden. Das heißt unter anderem, dass die Vertraulichkeit des Inhalts von Verwaltungsratsprotokollen gewahrt bleiben und die Speicherung auf privaten Geräten ausgeschlossen sein muss.

Thema	Rahmenbedingungen/ Empfehlungen	Trifft zu	Trifft nicht zu	To-do / Bemerkungen
Versand des Protokoll	per Mail verschlüsselt		✓	Kein Versand per Mail; Abruf über nextcloud-Zusammen
Speicherung /Aufbewahrung	Grundsätzlich muss die Vertraulichkeit des Inhalts von Verwaltungsratsprotokollen	✓		

	gewahrt werden (sicherer Aufbewahrungsort) Speicherung auf privaten Geräten ist ausgeschlossen (nur lesender Zugriff)			

Zuständig für die Durchführung ist: Pfr. Christian Feuerstein, Jörg Beuter

14 Öffentlichkeitsarbeit

14.1 Webpräsenz

In der Regel betreiben viele Kirchengemeinden eine eigene Webpräsenz. Daraus ergeben sich eine Reihe von Fragen aus den Bereichen des Datenschutz- und Urheberrechts. Hierzu veröffentlichte das Sekretariat der Deutschen Bischofskonferenz eine ausführliche Arbeitshilfe (Internetpräsenz - Arbeitshilfe Nr. 234 vom 22. Juni 2009).
Diese Schrift sollte in jedem Fall ausführlich zur Kenntnis genommen werden. Sie ist auf der Webseite der Deutschen Bischofskonferenz als Printversion bestellbar oder hier heruntergeladen werden.
Link: Internetpräsenz | Arbeitshilfen | Deutsche Bischofskonferenz (dbk-shop.de)

Unsere Webadresse lautet: https://bistummainz.de/region-rheinhessen/pfarrei/Ingelheim/start/
Mit dieser Homepage informieren wir die Öffentlichkeit über unsere Dienste und Aktivitäten.

Thema	Rahmenbedingungen	Trifft zu	Trifft nicht zu	To-do / Bemerkungen
Impressum	Beachtung von § 5, 7 und 8 DDG sowie § 18 Abs.2 MStV	✓		
Datenschutzerklärung	Offenlegung von transparenten Informationen zum Betrieb der Homepage. Hierzu zählen ua. Nennung von: Verantwortlichen, Datenschutzbeauftragter, Aufsichtsbehörde, Betroffenenrechte, technischen Details, Rechtsgrundlage und Zweck der Verarbeitung, …, Beachtung des KDG und § 25 TDDDG	✓		
Bildrechte	Beachtung des Urheberrechts, schriftl. Einwilligung bei Fotos	✓		Wir verwenden nur Fotos, die uns für diesen Zweck zur Verfügung gestellt werden.
Pfarrbrief auf der Website	Bei Veröffentlichung von personenbezogenen Daten (Taufen, Kommunion, Firmung, Hochzeit…) liegt die Einwilligung zur Veröffentlichung vor oder die Seite mit den personenbezogenen Daten wird ersetzt.	✓		Bspw. zwei Versionen der Gottesdienstordnung (Druck/Online)
Abo Newsletter	Die Einwilligung liegt von allen Empfängern vor.	✓		Mit ihrer Anmeldung erklären sie sich mit dem Empfang einverstanden

Zuständig für die Durchführung: Christine Wüst-Rocktäschel, Webmasterin ist: Gertrud Wellner

14.2 SocialMedia

Weiterhin betreiben wir die SocialMedia Kanäle
Instagram: minis.pfarrei.mariamagdalena
Instagram: st_maria_magdalena_ingelheim_
Facebook: St. Maria Magdalena Ingelheim
Mit diesen Plattformen informieren wir die Öffentlichkeit zusätzlich über unsere Dienste und Aktivitäten.

Thema	Rahmenbedingungen	Trifft zu	Trifft nicht zu	To-do / Bemerkungen
Impressum	Beachtung von § 5, 7 und 8 DDG, sowie § 18 Abs.2 MStV	✓		
Datenschutzerklärung	Offenlegung von transparenten Informationen zum Betrieb der Kanäle. Hierzu zählen u.a. Nennung von: Verantwortlichen, Datenschutzbeauftragter, Aufsichtsbehörde, Betroffenenrechte, technischen Details, Rechtsgrundlage und Zweck der Verarbeitung, …, Beachtung des KDG und § 25 TDDDG	✓		
Social Media Konzept	Konzept wurde erarbeitet und liegt vor	✓		

Zuständig für die Durchführung ist: Christine Wüst-Rocktäschel;
Administratoren sind: Stefanie Anders, Kirsten Huber

14.3 Foto- und Filmaufnahmen

Film- und Fotoaufnahmen von Menschen stellen grundsätzlich personenbezogene Daten dar, da die abgebildeten Personen direkt oder indirekt identifiziert werden können.

Für die Verarbeitung dieser personenbezogenen Daten, insbesondere für die Anfertigung der Fotografien, Filme und Videos, bedarf es nach dem KDG einer gesetzlichen Grundlage. Maßgeblich hierfür sind die § 6 Abs. 1 lit. b (Einwilligung), lit. c (Vertrag) und lit. f (kirchliches Interesse) KDG. Darüber hinaus ist der Betroffene transparent zu informieren.

Für die Veröffentlichung benötigen Fotografierende laut dem Kunsturhebergesetz (§ 22 KUG) die Zustimmung der aufgenommenen Personen. Diese Zustimmung kann in Ausnahmefällen aber auch mündlich oder durch entsprechendes Verhalten (z.B. in Pose stellen, Nicken …) erteilt werden.
Das KUG sieht nach § 23 folgende Ausnahmen zur Einwilligung vor:

1. Bildnisse aus dem Bereich der Zeitgeschichte;
2. Bilder, auf denen die Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen;
3. Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben;

Die Ausnahmen erstrecken sich jedoch nicht auf eine Verbreitung und Schaustellung, durch die ein berechtigtes Interesse des Abgebildeten oder, falls dieser verstorben ist, seiner Angehörigen verletzt wird.

Wer auf der sicheren Seite sein will, sollte sich vorab von allen abgebildeten Personen eine schriftliche Einverständniserklärung ausstellen lassen.

Die Einwilligungserklärung und Information für Foto- und Filmaufnahmen (siehe Anhang) werden im Datenschutzordner abgeheftet und somit dokumentiert (Dokumentationspflicht).

Bei öffentlichen Veranstaltungen werden Schilder mit datenschutzrechtlichen Hinweise aufgehängt bzw. sichtbar aufgestellt.

Thema	Rahmenbedingungen	Trifft zu	Trifft nicht zu	To-do / Bemerkungen
Foto/Filmaufnahmen von Hauptberuflichen	Die Betroffenen sind nach §§ 14, 15 KDG informiert und die Einwilligung liegt von allen vor.	✓		Werden je im gg. Fall eingeholt
Foto/Filmaufnahmen von Ehrenamtlichen	Die Betroffenen sind nach §§ 14, 15 KDG informiert und die Einwilligung liegt von allen vor.	✓		Werden je im gg. Fall eingeholt
Foto/Filmaufnahmen von Teilnehmenden und Gästen	Die Betroffenen sind nach §§ 14, 15 KDG informiert und die Einwilligung liegt von allen vor.	✓		Werden je im gg. Fall eingeholt
Foto/Filmaufnahmen bei Veranstaltungen	Datenschutzrechtliche Hinweise werden sichtbar ausgehängt.	✓		Werden je im gg. Fall eingeholt

Zuständig für die Durchführung ist: Christine Wüst-Rocktäschel

15 Daten- und Informationssicherheit

Zur Erfüllung kirchlicher Aufgaben ist die Informations- und Kommunikationstechnik (IT) ein zentrales Instrument. Die IT-Sicherheit ist ein wichtiger Bestandteil der Informationssicherheit. Die Sicherheit von IT-Systemen und der darin gespeicherten Daten wird durch die Realisierung und Aufrechterhaltung geeigneter technischer und organisatorischer Maßnahmen (TOMs) gewährleistet, um die Schutzziele der IT-Sicherheit im Sinne des § 26 Abs. 1 KDG (Vertraulichkeit, Integrität, Verfügbarkeit) zu gewährleisten.

Die den Datenschutz betreffenden TOMs sind in diesem Kapitel beschrieben. Die betriebliche Datenschutzbeauftragte überprüft im Rahmen ihrer Beratung und Betreuung die TOMs regelmäßig.

Bei der Bearbeitung die folgenden Punkte ist ggf. der Systemadministrator oder der betreuende IT-Dienstleister zu Rate zu ziehen.

✎ Zuständig für die Durchführung ist: Bistums IT

✎ Systemadministrator (wenn vorhanden) ist: Bistums IT

15.1 Dokumentation der IT-Systeme

Alle, in der kirchlichen Einrichtung vorhandenen IT-Systeme und Softwarekomponenten, sind in Bestandsverzeichnissen und speziellen Übersichten aufgelistet. Dies ermöglicht u.a. auch ein schnelles, effektives und erfolgreiches Handeln bei Ausfall oder Störungen einzelner Komponenten. Die Dokumentation ist stets auf dem neusten Stand zu halten.

Thema	Rahmenbedingungen	Trifft zu	Trifft nicht zu	To-do / Bemerkungen
Dokumentation der IT-Systeme	Die IT-Dokumentation enthält sensible Informationen und ist deshalb an einem zugriffsgeschützten Speicherort abgelegt, der den handelnden Personen bekannt und zugänglich ist.	✓		
IT-Infrastruktur (Desktop-Systeme, Mobile Geräte, sonstige IT-Systeme	Die Beschreibung der IT-Infrastruktur (incl. Telekommunikations-Einrichtungen) ist erstellt und umfasst die Auflistung der Hardware mit Standortangabe, Installationsanleitungen, Angaben zu Support, Konfigurationsänderungen sowie Sicherheitseinstellungen und vorhandene Verträge.	✓		
Netz (LAN, WLAN, Internetanbindung, Netzkomponenten, Telekommunikation)	Die Beschreibung der Netz-Infrastruktur (incl. TK-Einrichtungen) ist erstellt und umfasst die Auflistung der Hardware mit Standortangabe bzw. Netzplänen, Installationsanleitungen, Angaben zu Support, Konfigurationsänderungen sowie Sicherheitseinstellungen.	✓		
Anwendungen	Die Beschreibung der Anwendungen (incl. TK-Anwendungen) ist erstellt und umfasst die Auflistung der Anwendungen mit Angaben zu Support, Lizenzangabe und Angaben zur Benutzer- und Rechteverwaltung.	✓		

Zuständig für die Durchführung ist: Christine Wüst-Rocktäschel

15.2 Passwortmanagement, Digitaler Nachlass

Passwörter sind idealerweise in einem elektronischen Passwortmanagement-System zu hinterlegen, wie zum Beispiel Keepass. Alternativ ist auch ein verschlossener Umschlag in einem abschließbaren Schrank/Tresor möglich. Hierunter fallen alle Arten von Passwörtern (System, Online-Accounts u.ä.)

Für den Fall des offiziellen Ausscheidens oder Ausschlusses des Systemadministrators oder dessen/deren Ablebens oder dessen/deren andauernden Handlungsunfähigkeit wird eine Vollmacht über den „Digitalen Nachlass“ hinterlegt (siehe Muster).

Diese Vollmacht gilt nur für digitale Inhalte, Benutzerkonten, Zugangsdaten und zugehörige Informationen und elektronische Konversationen, die im Auftrag der Kirchengemeinde erstellt, betreut und genutzt wurden/werden und die in der Übersicht der Dokumentation aufgeführt sind. Diese Vollmacht erstreckt sich nicht auf die privaten Internetkonten und Rechner.

Der Systemadministrator verpflichtet sich gleichzeitig, die Übersicht sachgerecht, vollständig und aktuell zu führen.
Durch diese Maßnahmen sollen

- Ausfälle, Unsicherheiten, Sicherheitsprobleme, wie z.B. im Büchereibetrieb, vermieden werden
- Integrität, Datenschutz, Reputation und Verlässlichkeit der Einrichtung gewahrt werden
- dem Kirchenverwaltungsrat ermöglichen, die Kirchengemeinde im Rechtsverkehr zu vertreten und das Vermögen der Kirchengemeinde zu verwalten
- etwaige Kosten und Abbuchungen von Nachfolgern/Erben vermieden werden
- die grundsätzlichen Datenschutzrechte Dritter, mit denen über die Online-Konten kommuniziert wurde, berücksichtigt werden
- hoher Zeitaufwand und Kosten einer eventuellen „Nachlass-Recherche“ (Konten, Passwörter etc.) vermieden werden
- postmortale Persönlichkeitsrechte angemessen berücksichtigt werden

Thema	Rahmenbedingungen	Trifft zu	Trifft nicht zu	To-do / Bemerkungen
Passwortmanagementsystem im Einsatz	Nutzung und Speicherort von Software und Daten festgelegt. Benutzer sind informiert	✓		Es gibt eine Liste aller PW, die nicht personengebunden sind; die Liste lagert im Tresor der Pfarrei und wird bei Änderung mit Unterschrift versehen.
Master-Passwort ist hinterlegt	Im Umschlag, eindeutig gekennzeichnet und gesichert aufbewahrt			Nicht erforderlich
Vollmacht „Digitaler Nachlass“ ist vorhanden	Im Umschlag, eindeutig gekennzeichnet und gesichert aufbewahrt	✓		Werden automatisch in Altarchiv übertragen (MeWe)

Zuständig für die Durchführung ist: Christine Wüst-Rocktäschel

15.3 Datensicherung

Das KDG fordert vom Verantwortlichen gemäß § 26 Abs. 1 lit. c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen. Um die Verfügbarkeit und die Wiederherstellbarkeit zu gewährleisten, sind regelmäßige, vollständige Backups der personenbezogenen Daten notwendig. Die Backupmedien sind einem anderen Standort abzulegen, d. h. nicht an dem gleichen physischen Standort wie die Daten.

Eine der größten Bedrohungen bei der Nutzung von IT-Systemen und Datenträger sind unwiderrufliche Datenverluste. Solche Datenverluste können aus technischen Defekten des Systems, durch Diebstahl, Verlust aber auch durch versehentliches Löschen oder Überschreiben von Daten entstehen. Laut den letzten IT-Sicherheitsreports des BSI nimmt die Bedrohung durch Ransom-Software (Verschlüsselungssoftware) weiterhin zu und stellt eine der größten Cyperbedrohungen dar.

Durch regelmäßige Backups können Schäden zwar nicht verhindert werden, aber deren Auswirkung in Grenzen gehalten werden.
Alle in der Kath. Kirchgemeinde St. Maria Magdalena Ingelheim erhobenen und gespeicherten Daten liegen auf dem Server des Bistums Mainz; einen eigenen Server betreibt die Pfarrei nicht. Insofern liegen die beschriebenen Maßnahmen und Intervalle im Bereich Backup der Datensicherheit in der Hoheit der IT des Bistums Mainz und können von uns nur dahingehend unterstützt werden, dass wir versichern, keine Daten, besonders keine personenbezogenen Daten, zur Erfüllung unserer Aufgaben in Verwaltung und Pastoral auf anderen Servern zu hinterlegen.

Thema	Rahmenbedingungen	Trifft zu	Trifft nicht zu	To-do / Bemerkungen
Backup-Daten definieren	Es ist festgelegt, welche Daten aus welchen Datenquellen das Backup umfassen muss Beispiele: Zentrale(r) Datenspeicher der Einrichtung, individuelle Datenspeicher, E-Mail-Daten, Daten mobiler Geräte, etc.			Liegt im Ermessen und in der Durchführung bei der Bistums IT
Backup-Medien festlegen	Unter Berücksichtigung von zeitlicher Beständigkeit (Persistenz), geringer Fehleranfälligkeit (Lesbarkeit), Robustheit, etc. wurden die geeigneten Backup-Medien festgelegt. Die Datensicherung ermöglicht eine hinreichende Historie, d. h. es existieren mehrere Sicherungsstände auf mehreren Sicherungsmedien (Mehrgenerationenprinzip).			Liegt im Ermessen und in der Durchführung bei der Bistums IT
Backup-Zyklus festlegen	Die Datensicherung hat eine ausreichende Aktualität um den potentiellen Datenverlust zu minimieren. Die Backup-Intervalle sind definiert.			Liegt im Ermessen und in der Durchführung bei der Bistums IT
Aufbewahrung der Backup-Medien festlegen	Die Backup-Datenträger werden verschlossen und räumlich getrennt von den gesicherten IT-Systemen aufbewahrt. Sie sind auch bei Notlagen, wie z. B. Brand oder Hochwasser verfügbar.			Liegt im Ermessen und in der Durchführung bei der Bistums IT
Vertraulichkeit sicherstellen	Das Backup-Medium ist verschlüsselt/passwortgeschützt, damit ein unrechtmäßiger Zugriff bei Verlust oder Diebstahl nicht möglich ist.			Liegt im Ermessen und in der Durchführung bei der Bistums IT

Zuständig für die Durchführung ist: IT Bistum Mainz

15.4 Datenverschlüsselung

Verschlüsselung ist eines der wesentlichen Werkzeuge, um die Vertraulichkeit und Integrität von Daten sicherzustellen und wird daher als eine der wenigen Maßnahmen zur IT-Sicherheit explizit in § 26 KDG genannt. Die Voraussetzung für eine Verschlüsselung der Daten ist die Einteilung der personenbezogenen Daten in Schutzklassen.

Übersicht Datenschutzklassen:

Datenschutzklasse I: Personenbezogene Daten, deren Missbrauch keine besonders schwerwiegende Beeinträchtigung des Betroffenen erwarten lässt.

Bsp.: Namens- und Adressangaben, die so auch in Telefonbüchern oder anderen öffentlichen Quellen stehen.

Datenschutzklasse II: Personenbezogene Daten, deren Missbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann. Bsp.: Daten zum Beschäftigungsverhältnis, Kontaktdaten von haupt- und ehrenamtlichen Mitarbeitenden, z. B. Handynummer, Vertragsdaten, Mietverhältnisse, Geburts- und Jubiläumsdaten.

Datenschutzklasse III: Personenbezogene Daten, deren Missbrauch die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen erheblich beeinträchtigen kann. Bsp.: Daten zur Gesundheit, alle Bank- und Kreditkartendaten, politische Meinungen, rassische und ethnische Herkunft, religiöse und philosophische Überzeugungen, Hinweise oder Angaben zu Ordnungswidrigkeiten oder Straftaten.

Verschlüsselung bei Übermittlung personenbezogener Daten

Gemäß §§ 12, 13 KDG-DVO hat die Übermittlung personenbezogener Daten der Datenschutzklassen II + III außerhalb eines geschlossenen und gesicherten Netzwerks (auch über automatisierte Schnittstellen) grundsätzlich verschlüsselt zu erfolgen. Das Verschlüsselungsverfahren ist dem aktuellen Stand der Technik und dem jeweiligen Sicherheitsbedarf entsprechend angemessen auszuwählen.

Die Kath. Kirchengemeinde St. Maria Magdalena Ingelheim übermittelt personenbezogene Daten nur auf Wegen der durch das Bistum Mainz und ihre IT-Abteilung zugebilligten elektronischen Wegen, beispielhaft ist die Nutzung von personalisierten Mailaccounts zur Übertragung von pb Daten zu nennen. Auch funktionale Mailadressen, bspw. für die Verwaltung, das Pfarrbüro oder die Pfarreileitung operieren ausschließlich über die vom Bistum bereitgestellten elektronischen Wege.

Thema	Rahmenbedingungen	Trifft zu	Trifft nicht zu	To-do / Bemerkungen
Schnittstellen identifizieren	Die Schnittstellen über die pb. Daten der Datenschutzklassen II+III nach Außen übermittelt werden, sind identifiziert. Beispiele: ▪ E-Mail-Kommunikation mit den Verrechnungsstellen, ▪ Gemeindemitgliedern, Stiftungsräten, etc. ▪ Automatisierte Übertragungen pb. Daten innerhalb genutzter Programme ▪ Übertragung pb. Daten in Cloud-Systeme			Liegt im Ermessen und in der Durchführung bei der Bistums IT
Verfahren festlegen, implementieren und Arbeitsanweisung zur Verfügung stellen	Für die ermittelten Schnittstellen sind geeignete Verschlüsselungsverfahren, die dem aktuellen Stand der Technik und dem jeweiligen Sicherheitsbedarf entsprechen, ausgewählt. Beispiele: ▪ Ende-zu-Ende-Verschlüsselung mit den Verfahren S/MIME und OpenPGP.			Liegt im Ermessen und in der Durchführung bei der Bistums IT

	Bei der Auswahl des Verschlüsselungs-verfahrens ist auf eine hohe Verschlüsselung zu achten: Die AES-256-Verschlüsselung gilt derzeit als sehr sicher und sollte bevorzugt genutzt werden. ▪ Auch Kompressionsprogramme wie 7-Zip oder WinZip bieten angemessene Verschlüsselungsverfahren an. ▪ Passwortgesicherte Datei (z. B. in Word o. Excel) Arbeitsanweisung ist erstellt.			

Zuständig für die Durchführung ist: IT Bistum Mainz

Verschlüsselung bei Speicherung personenbezogener Daten

Gemäß § 13 KDG-DVO sind Daten der Datenschutzklasse III, die aus dienstlichen Gründen zwingend erforderlich sind, auf mobilen Geräten im Sinne des § 4 Absatz 2 KDG-DVO nur passwortgeschützt abzuspeichern.
Ein hohes Diebstahl- und Verlustrisiko besteht hauptsächlich bei mobilen Datenträgern (USB-Festplatten, USB-Sticks, Laptops, etc.). Deshalb sind die Dateien oder besser die gesamten Datenträger mit einem Passwort vor unbefugtem Zugriff zu schützen.
Die Kath. Kirchengemeinde St. Maria Magdalena Ingelheim speichert personenbezogene Daten nur auf mobilen Endgeräten, die vom Mainz und ihrer IT-Abteilung ausgegeben und zugewiesen sowie kontrolliert und unterhalten werden.

Thema	Rahmenbedingungen	Trifft zu	Trifft nicht zu	To-do / Bemerkungen
Verfahren festlegen, implementieren und Arbeitsanweisung zur Verfügung stellen	Das Verschlüsselungsverfahren ist dem aktuellen Stand der Technik und dem jeweiligen Sicherheitsbedarf entsprechend ausgewählt und installiert. Arbeitsanweisung ist erstellt.	✓		Wird über die Bistumscloud bzw. deren Datenschutz gewährleistet

Zuständig für die Durchführung ist: IT Bistum Mainz

15.5 Schutz vor Schadprogrammen

Der Einsatz diverser Sicherheitssoftware und Sicherheitshardware sind geeignete technische Maßnahmen, um diesem Verlangen nachzukommen und Zugriffsmöglichkeiten auf die personenbezogenen Daten durch unbefugte Dritte zu verhindern.
Wenn IT-Systeme mit Schadsoftware (Viren, Würmer, Trojanische Pferde usw.) befallen werden, kann dies die Verfügbarkeit, Integrität und Vertraulichkeit der Systeme und der darauf gespeicherten Daten gefährden. Die IT-Systeme (z. B. PC, Laptop) müssen deshalb auf verschiedenen Ebenen gegen Schad-Software geschützt werden:

Thema	Rahmenbedingungen	Trifft zu	Trifft nicht zu	To-do / Bemerkungen
Virenschutz	Die eingesetzte Virenschutz-Software entspricht dem aktuellen Stand der Technik.			Liegt im Ermessen und in der

				Durchführung bei der Bistums IT
Schutz vor Ransom-ware	Eine Schutzsoftware gegen Ransomware (Erpressungstrojaner) wurde auf allen betroffenen Systemen installiert.			Liegt im Ermessen und in der Durchführung bei der Bistums IT
Schutz vor SPAM-Mails	Es werden SPAM-Filter genutzt.			Liegt im Ermessen und in der Durchführung bei der Bistums IT
Patch-Management	Die eingesetzten Betriebssysteme, Programme, Virenscanner, Webbrowser, etc. aller betroffenen Systeme und eingesetzter Systeme werden generell durch das Einspielen aktueller, sicherheitsrelevanter Firmware, Updates und Patches auf dem neuesten Stand gehalten.			Liegt im Ermessen und in der Durchführung bei der Bistums IT
Sensibilisierung Mitarbeiter	Alle Mitarbeiter werden regelmäßig hinsichtlich der Gefahren von Schadsoftware sensibilisiert. Es wird darauf hingewiesen, - dass keinesfalls E-Mail-Anhänge geöffnet werden dürfen, wenn nicht sicher ist, dass deren Inhalt unbedenklich ist - dass infizierte IT-Systeme (falls der Worst-Case eintreten sollte) unverzüglich von allen Datennetzen zu trennen sind und bis zur vollständigen Bereinigung nicht mehr produktiv genutzt werden dürfen.			Liegt im Ermessen und in der Durchführung bei der Bistums IT, Unterweisung unterstützt durch Datenschutzveranwortliche CWR der Pfarrei

Zuständig für Durchführung ist: Bistum Mainz, IT, Unterstützung: Christine Wüst-Rocktäschel

15.6 Absicherung Windows-Endgeräte

Nach § 6 Abs. 2 KDG-DVO hat der Verantwortliche für die Verarbeitung personenbezogener Daten in elektronischer Form, technische und organisatorische Maßnahmen zur Zugangs-, Zugriffs- und Verfügbarkeitskontrolle zu treffen.

Dies geschieht durch entsprechende Konfiguration der Windows-Endgeräte.

Thema	Rahmenbedingungen	Trifft zu	Trifft nicht zu	To-do / Bemerkungen
Trennung in Admin- und Benutzerkonten	Im Netzwerk- und im Einzelplatzbetrieb gibt es eine abgestufte Rechteverwaltung, Anwender- und Administrationsrechte sind getrennt. Die Windows-Benutzer sind entsprechend konfiguriert. Jedem Benutzer wird ein eigenes Windowskonto zugeordnet.	✓		Liegt im Ermessen und in der Durchführung bei der Bistums IT
Gebrauch von Benutzer-Passwörtern	Alle Windows-Systeme können nur nach Eingabe von Systembenutzer und zugehörigem Passwort genutzt werden (Zugangskontrolle).	✓		Liegt im Ermessen und in der Durchführung bei der Bistums IT

	Alle Mitarbeitenden haben für ihren Benutzer ein persönliches und geheim zu haltendes Passwort vergeben.			
Anpassen System-Datenschutzein-stellungen	Die Assistenz- und Unterstützungs-funktionen von Windows wurden so konfiguriert, dass die Zugriffe deaktiviert oder auf ein Minimum reduziert sind (Diagnose- und Telemetriedaten).	✓		Liegt im Ermessen und in der Durchführung bei der Bistums IT
Aktivieren zusätzlicher Windows-Sicherheits-funktionen	Zum Schutz der Windows-Systeme vor unbefugtem Zugriff wurden weitere Sicherheitsfunktionen aktiviert. Beispiele: - Sperren des Bildschirms nach Inaktivität - Deaktivieren der automatischen Wiedergabe (Autostart) von Programmen auf Wechseldatenträgern - etc.	✓		
Anpassung Internet-Browser	Im Browser wurden verschiedene Sicherheitsfunktionen zum Schutz der Privatsphäre und des IT-Systems vor Schadprogrammen aktiviert und entsprechend konfiguriert.	✓		Liegt im Ermessen und in der Durchführung bei der Bistums IT

Zuständig für die Durchführung ist: IT Bistum Mainz, Christine Wüst-Rocktäschel

15.7 Absicherung Mobiltelefone / Smartphones

Mobiltelefone und Smartphones sind alltäglicher Bestandteil der kirchlichen Kommunikation geworden. Neben der Möglichkeit von Telefongesprächen bieten die Geräte meist noch weitere Funktionen an, wie das Verschicken von SMS, MMS, E-Mails, die Nutzung des Internets über WLAN oder Mobilfunk.
Für dienstliche Zwecke dürfen nur Diensttelefone zum Einsatz kommen. Sollten in Ausnahmefällen doch private Handys genutzt werden, müssen die Regelungen nach § 20 KDG-DVO umgesetzt werden.
Die Geräte verfügen über eine Option zur Speichergrundverschlüsselung (Einschalt- bzw. Display-Kennwort). Dies ist eine Verschlüsselungstechnik, die auf dem jeweiligen Gerät bereits integriert ist und das komplette Gerät inklusive gespeicherter Daten verschlüsselt.

Thema	Rahmenbedingungen	Trifft zu (ja)	Trifft nicht zu (nein)	To-do / Bemerkungen
Zugangskontrolle	Identifizierungsmaßnahmen wie Einschaltkennwort oder PIN werden verwendet.	✓		
Daten-verschlüsselung	Die Datenspeicher der Smartphones werden verschlüsselt.			Liegt im Ermessen und in der Durchführung bei der Bistums IT
Apps	Es werden nur datenschutzkonforme Apps (Messenger-Dienste, etc.) eingesetzt. Die Apps müssen dafür zumindest eine Datenschutzerklärung enthalten.	✓		

Datensicherung	Es wird auch bei Mobilgeräten eine regelmäßige Datensicherung durchgeführt Die automatische Datensicherung der Gerätehersteller wird nicht verwendet (Um die Übermittlung von Daten in Drittländer zu verhindern). Details siehe Kapitel „Datensicherung“.			Liegt im Ermessen und in der Durchführung bei der Bistums IT
Außerbetriebnahme	Vor Weitergabe oder Entsorgung des Gerätes muss sichergestellt sein, dass alle gespeicherten pb. Daten vollständig gelöscht werden.			Liegt im Ermessen und in der Durchführung bei der Bistums IT

Zuständig für die Durchführung ist: Bistum Mainz IT, Christine Wüst-Rocktäschel

15.8 Absicherung der lokalen Netzwerke der kirchlichen Einrichtungen

Netzwerkanschlüsse ermöglichen den Zugriff auf alle Systeme und Daten, die sich im Netzwerk befinden. Der Zugang zum eigenen Netzwerk kann sowohl über physische Netzwerkzugänge (LAN) als auch über Funknetzwerke (WLAN) erfolgen. Diese Zugänge können von einrichtungsfremden Personen genutzt werden, wenn sie sich über eine freie Netzwerkdose oder über WLAN verbinden. Zudem kann Schadsoftware in das eigene Netzwerk eingeschleust werden.
Daher müssen für den Zugriffschutz auf das Netzwerk (LAN / WLAN) bestimmte Maßnahmen ergriffen werden.

Thema	Rahmenbedingungen	Trifft zu	Trifft nicht zu	To-do / Bemerkungen
WLAN-Zugriff	Der Zugriff auf die IT-Systeme über WLAN ist nur nach Eingabe eines (hinsichtlich Länge und Zusammensetzung) geeigneten Kennwortes möglich. Voreingestellte Standardpasswörter für die Netzwerk-Komponenten (z.B. DSL-Router, etc.) werden gewechselt. Die neu vergebenen Passwörter sind in einem geschützten Bereich aufbewahrt und sind nur der zuständigen Person zugänglich.	✓		
WLAN-Gastzugriff	Ein eigener WLAN-Gastzugang ist eingerichtet und das Passwort wird regelmäßig geändert.	✓		
WLAN-Verschlüsselung	Die Kommunikation im WLAN-Netzwerk erfolgt verschlüsselt. Der Verschlüsselungsstandard entspricht dem aktuellen Stand der Technik.	✓		
Außerbetriebnahme	Bei der Aussonderung von Netzwerk-Komponenten werden sämtliche Authentifizierungsinformationen (Zugangsdaten Internetanschluss, etc.) entfernt.	✓		

Zuständig für die Durchführung ist: Christine Wüst-Rocktäschel

15.9 Absicherung Internet-Zugang

Die Nutzung des Internets ist ein wichtiger Bestandteil des Arbeitsalltags. Die Nutzung von E-Mails, Informationsangeboten, Internet-Dienstleistungen, Online-Banking und -Einkauf ist für die meisten Organisationen selbstverständlich. Es muss verhindert werden, dass durch die Anbindung der eigenen Geräte an das Internet Risiken für die Organisation entstehen. Firewalls sind eine geeignete technische Maßnahme, um Zugriffsmöglichkeiten auf die personenbezogenen Daten durch unbefugte Dritte zu verhindern.
Der Provider unseres Internetzugangs (Vodafone) regelt die Absicherung des Internetzugangs.
https://www.vodafone.de/de/datenschutz/

Thema	Rahmenbedingungen	Trifft zu	Trifft nicht zu	To-do / Bemerkungen
Einsatz einer Firewall	Die Entscheidung, welche Firewall-Variante die richtige ist, orientiert sich an den Grundsätzen aus § 27 Abs. 1 KDG: „Unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche […] technische und organisatorische Maßnahmen, die geeignet sind, die Datenschutzgrundsätze wirksam umzusetzen und […] und die Rechte der betroffenen Personen zu schützen.“ In der Regel reicht hierfür der vom Provider zur Verfügung gestellte Router (zB. FritzBox), der immer auf dem aktuellen Patchstand gehalten werden muss.	✓		

Zuständig für die Durchführung ist: Christine Wüst-Rocktäschel

15.10 Zutritts- / Zugangs- / Zugriffskontrolle

Thema	Rahmenbedingungen	Trifft zu	Trifft nicht zu	To-do / Bemerkungen
Zutrittskontrolle	Unbefugter Zutritt zum Gebäude und zu den Räumen, in denen pb. Daten aufbewahrt werden, wird verhindert. Es werden technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle ergriffen: ▪ Gebäudetüren sind verschlossen, Einsatz Klingel + elektrischer Türöffner ▪ Fenster und Türen in Büros generell verschließen, wenn ein Raum nicht besetzt ist.	✓		

	▪ Datenträger und Papierunterlagen, welche sensible pb. Daten enthalten, sind in verschließbaren Aktenschränken. ▪ Einsatz einer Schlüsselliste ▪ Abschließbares Archiv ▪ Besuchermanagement (kein offener Zutritt, nur nach Anmeldung oder Klingel)			
Zugangskontrolle	Das Eindringen Unbefugter in die IT-Systeme wird verhindert. Hierzu werden u.a. technische und organisatorische Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung getroffen: • Einrichtung eines Benutzerkontos pro User (Einzelaccount) • Festlegen einer Passwortrichtlinie (durch das Bistum)	✓		Unterliegt der Kontrolle der Bistums IT
Zugriffskontrolle, Berechtigungskonzept	Bei der Umsetzung des Berechtigungskonzepts wird immer nach dem „Need-to-know-Prinzip“ vorgegangen. Die zur Benutzung eines IT-Systems Berechtigten können nur auf die ihrer Zuständigkeit unterliegenden personenbezogenen Daten zugreifen; personenbezogene Daten dürfen nicht unbefugt gelesen, kopiert, verändert oder entfernt werden (Zugriffskontrolle). Nach dem Ausscheiden von Mitarbeitenden wird der personalisierte Zugang deaktiviert und zu gegebener Zeit gelöscht.	✓		
Umgang mit pd Daten im Rahmen des Beicht- und Seelsorgegeheimnis §14 KDG-DVO	▪ Das Beichtgeheimnis nach cc. 983 ff. CIC ist zu wahren; personenbezogene Daten, die dem Beichtgeheimnis unterliegen werden nicht verarbeitet. ▪ Personenbezogene Daten, die dem Seelsorgegeheimnis unterliegen oder die Seelsorge in Form einer Online-Beratung erfolgt, werden nur verarbeitet, wenn technische und organisatorische Maßnahmen mindestens das Schutzniveau der Datenschutzklasse III ergriffen werden.	✓		

Zuständig für die Durchführung ist: IT Bistum Mainz, Christine Wüst-Rocktäschel, Christian Feuerstein

15.11 Eingabekontrolle

Gem. § 6 Abs. 2 f) KDG-DVO ist grundsätzlich sicher zu stellen, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in IT-Systemen verarbeitet worden sind (Eingabekontrolle).

Thema	Rahmenbedingungen	Trifft zu	Trifft nicht zu	To-do / Bemerkungen
Eingabekontrolle	Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist gewährleistet. Dazu gehören Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind.		✓	Nach Überleitung aller Daten in die Zusammen Nextcloud u.U. möglich, derzeit technisch nicht darstellbar

Zuständig für die Durchführung ist: Bistums IT

15.12 Nutzung dienstlicher IT zu privaten Zwecken

Thema	Rahmenbedingungen	Trifft zu	Trifft nicht zu	To-do / Bemerkungen
Regelung	Die Nutzung dienstlicher IT-Systeme (PC, Internet, E-Mail-Account, etc.) durch Mitarbeiter zu privaten Zwecken ist verboten oder geregelt.	✓		Unterwiesen in Teams Pastoral und Verwaltung

Zuständig für die Durchführung : Christine Wüst-Rocktäschel

15.13 Nutzung privater IT zu dienstlichen Zwecken

Thema	Rahmenbedingungen	Trifft zu	Trifft nicht zu	To-do / Bemerkungen
Regelung	Die Nutzung privater IT-Systeme zu dienstlichen Zwecken ist verboten. In Ausnahmefällen gelten die Regelungen nach §20 KDG-DVO. Die Zulassung gemäß KDG-DVO ist schriftlich zu vereinbaren und beinhaltet: a) die Angabe der Gründe, aus denen die Nutzung des privaten IT-Systems erforderlich ist, b) eine Regelung über den Einsatz einer zentralisierten Verwaltung von Mobilgeräten (z. B. Mobile Device Management) auf dem privaten IT-System des Mitarbeiters, c) das Recht des Verantwortlichen zur Löschung durch Fernzugriff aus wichtigem und unabweisbarem Grund; ein wichtiger und unabweisbarer Grund liegt insbesondere vor, wenn der Schutz personenbezogener Daten Dritter nicht auf andere Weise sichergestellt werden kann,	✓		Unterwiesen in Teams Pastoral und Verwaltung

	d) eine jederzeitige Überprüfungs-möglichkeit des Verantwortlichen, e) die Dauer der Nutzung des privaten IT-Systems für dienstliche Zwecke, f) das Recht des Verantwortlichen festzulegen, welche Programme verwendet oder nicht verwendet werden dürfen sowie g) die Verpflichtung zum Nachweis einer Löschung der zu dienstlichen Zwecken verarbeiteten personenbezogenen Daten, wenn die Freigabe der Nutzung des privaten IT-Systems endet, das IT-System weitergegeben oder verschrottet wird.			

Zuständig für die Durchführung ist: Christine Wüst-Rocktäschel

16 Löschung und Vernichtung von Daten

Schriftstücke, Akten und sonstige EDV-Ausdrucke mit personenbezogene Daten, die entsorgt werden sollen, sind so zu vernichten, dass sie vor Missbrauch geschützt sind.

16.1 Löschkonzept

Nach dem KDG dürfen Daten nicht auf unbestimmte Zeit aufbewahrt werden. Daten sind zu löschen, wenn diese nicht mehr erforderlich sind, bzw. wenn der Zweck für die Datenerhebung entfällt. Vor der Löschung sind gesetzliche / kirchliche Aufbewahrungsfristen zu beachten (Löschungssurrogat, KAO).

Das Löschkonzept der Pfarrei hat die gängigen Aufbewahrungsfristen für Dokumente, die rechtlich gefordert sind, zur Grundlage.
Aufbewahrungsfrist 8 Jahre: Rechnungen (Ein- und Ausgangsrechnungen), Quittungen, Kontoauszüge, buchungsrelevante Lieferscheine, Lohn- und Gehaltslisten, Reisekostenabrechnungen, Steuerbescheide.

Aufbewahrungsfrist 10 Jahre: Handelsbücher, Inventare, Eröffnungsbilanzen, Jahresabschlüsse, Lageberichte, Konzernabschlüsse, Kontoauszüge

Aufbewahrungsfrist 6 Jahre: Handelsbriefe und einfache Lieferscheine ohne Buchungsfunktion.
Nach Ablauf der Aufbewahrungsfrist werden die Daten entsprechend der Vorgaben vernichtet bzw. gelöscht, so sie digital archiviert oder vorgehalten wurden.

Für personenbezogene Daten gilt, dass sie

- Gemäß den Bestimmungen des KDG nur so lange gespeichert und genutzt werden, wie die konkrete Aufgabe es erfordert.
- Nach Ablauf dieses Zeitraums werden die Daten gelöscht bzw. vernichtet, wenn sie entsprechend vorgelegen haben.
- Sollten Datensätze aufgrund von Widerspruch bereits vorher nicht mehr gespeichert und/oder genutzt werden dürfen, werden sie unverzüglich vernichtet.

Thema	Rahmenbedingungen/ Empfehlungen	Trifft zu	Trifft nicht zu	To-do / Bemerkungen
Löschkonzept	▪ Es ist geklärt, in welchen Intervallen und in welchen Zuständigkeiten die pb Daten gelöscht werden. ▪ Die Vernichtung ist dokumentiert (Nachweispflicht). ▪ Löschkonzept ist erstellt.	✓		

16.2 Vernichtung von Schriftgut

Es ist dafür zu sorgen, dass bei der Vernichtung der Schriftstücke die Daten nicht mehr lesbar sind. Die entsprechende DIN-Norm 66399 unterscheidet zwischen drei Schutzklassen:

Schutzklasse 1:	Normaler Schutzbedarf für interne Daten (Telefonlisten, Notizen, etc.)
Schutzklasse 2:	Hoher Schutz für vertrauliche Daten (Personal- und Finanzdaten)
Schutzklasse 3:	Sehr hoher Schutzbedarf für besonders vertrauliche und geheimer Daten

Hierzu gibt es verschiedene Möglichkeiten:

Aktenvernichter

Um eine datenschutzgerechte sichere Vernichtung der papiernen Dokumente zu gewährleisten, sind Normen zu beachten, die sich an der Sensibilität der Daten orientieren. Kernstück der Norm nach DIN 66399 ist die Definition von Schutzklassen und Sicherheitsstufen. Wir empfehlen einen Aktenvernichter mit mind. Sicherheitsstufe 4 zu benutzen.

Datentonne

Bei der Datentonne handelt es sich um einen speziellen Behälter für sensible oder geheime Unterlagen, die zum Zwecke der Aktenvernichtung transportiert werden. Diese kann bei einem Aktenvernichtungsunternehmen angemietet werden. Es gibt unterschiedliche Tonnen je nach Menge bzw. Schutzklasse der Daten, die vernichtet werden sollen. Die Entsorgung kann einmalig oder in regelmäßigen Abständen erfolgen.

Thema	Rahmenbedingungen/ Empfehlungen	Trifft zu	Trifft nicht zu	To-do / Bemerkungen
Vernichten von Daten	Nicht mehr benötigte Papier-Unterlagen/ Datenträger (mit pb. Daten) müssen vernichtet (z.B. geschreddert) werden. Die dafür eingesetzten Aktenvernichter müssen die geforderte Schutzstufe (P-4) gem. DIN-Norm 66399 erfüllen. Die Vernichtung ist dokumentiert (Nachweispflicht).			Unterlagen mit personenbezogenen Daten werden je nach Schutzklasse vor Ort geschreddert oder zur Vernichtung an entsprechende Unternehmen verbracht.
Entsorgung PC-Systeme / Drucker, Multifunktions - Geräte	Festplatten sowohl in PC-Systemen als auch von Druckern müssen vernichtet werden. Die Vernichtung ist dokumentiert (Nachweispflicht).			Vernichtung über Bistums IT bei Rückgabe der Geräte vorausgesetzt; Festplatten alter IT

				Geräte sind im Tresor verwahrt

Literaturverweise:

- Deutsche Bischofskonferenz, Grundordnung des kirchlichen Dienstes, Entwurfsfassung vom 06.05.2022 https://www.dbk.de/fileadmin/redaktion/diverse_downloads/presse_2022/2022-086a-Grundordnung-des-kirchlichen-Dienstes-Entwurfsfassung-vom-06.05.2022.pdf
- activeMind.AG, Muster: Datenschutzkonzept nach DSGVO
- https://www.activemind.de/datenschutz/dokumente/datenschutzkonzept/
- Bistum Limburg, Grundlagen zum kirchlichen Datenschutz, 02/2020
- Broschuere_Grundlagen_zum_kirchlichen_Datenschutz_2020.pdf (bistumlimburg.de)
- Ullrich, Matthias, 2022, Beschäftigtendatenschutz der katholischen Kirche
- Bundesamt für Sicherheit in der Informationstechnik, 2023, Die Lage der IT-Sicherheit in Deutschland 2022
- Schläger und Thode (Hrsg.), 2018. Handbuch Datenschutz und IT-Sicherheit, 1. Aufl.
- Erzbischöfliches Ordinariat Freiburg, Referat Datenschutz, 2021, Datenschutzkonzept

Ersteller der Mustervorlage:

Bischöflichen Ordinariat Mainz

KATHOLISCH Bistum Mainz

Betriebliche Datenschutzstelle im Bistum Mainz
☎ 06131-253857
✉ Postfach 1560, 55005 Mainz
datenschutz@bistum-mainz.de
https://bistummainz.de/service/datenschutzstelle

Redaktion: Wolfgang Knauer, Michaela Beiersdorf, Alexandra Glinka
Mitwirkung: Willi Weiers