Bistum Basel
Diocèse de Bâle

Datenschutz FAQ

Vorbemerkungen zur Benutzung dieses Dokuments

Die vorliegenden FAQ (Frequently Asked Questions) werden den Pfarreien des Bistums Basel als Arbeitshilfe im Alltag zur Verfügung gestellt. Dabei kommen die sieben Prinzipien des Datenschutzrechts immer zur Anwendung. Nachfolgend wird jedoch der Versuch unternommen, die für den Sachverhalt wichtigsten Prinzipien auf den konkreten Fall anzuwenden. Es kann sich aber je nach Kontext aufdrängen, dass noch zusätzliche Pflichten jeweils zu beachten sind. Die vorliegenden FAQ sind sodann in Verbindung mit den weiteren Unterlagen zu lesen, die ebenfalls zur Verfügung gestellt werden - u. a. die Dokumente «Datenschutz: Grundlagen für die Pfarreien im Bistum Basel», «Taufbücher führen - Datenschutz einhalten» oder die erarbeiteten Vorlagen (Auftragsdatenbearbeitungsvereinbarung ADV, Datenschutzerklärungen, Bearbeitungsverzeichnis).

Nr.	FAQ	Antwort
1	**Alternative EDV-Programme:** Gibt es Alternativen zu verbreiteten Programmen?	Eine exemplarische Liste alternativer Programme findet sich im Anhang. Alle verwendeten Programme sind auf ihre Datenschutzkonformität zu prüfen. Die Hersteller stellen heute Datenschutzerklärungen sowie Vertragsdokumente zur Verfügung.
2	**Apps für die Arbeit auf privatem Phone:** Inwiefern ist es opportun, dass Mitarbeitende Apps, die sie fürs Arbeiten benutzen, auf ihren privaten Smartphones installieren und bedienen? In welchen Fällen ist davon dringend abzuraten?	Aus Sicht der Pfarrei ist dann dringend davon abzuraten, wenn die in den Apps bearbeiteten Daten (Geschäftsdaten oder Personendaten) unter Kontrolle der Pfarrei zu bleiben haben. Sofern keine technische Lösung implementiert wird, um solche Geräte zu bewirtschaften und Daten der Pfarrei, wo nötig auch auf privaten Geräten, aus der Ferne zu löschen, wenn das Gerät verloren geht oder die entsprechende Person austritt (sog. Mobile Device Management MDM mit Remote-Wipe), ist davon abzuraten. Geht es nicht darum, Inhaltsdaten zu bearbeiten, sondern organisatorische Fragen zu klären (Terminfindung usw.), kann die Pfarrei eine sichere Messenger-Lösung empfehlen und den Mitarbeitenden in einer Weisung mitteilen, wie sie diese zu verwenden haben (Beschränkung auf Organisatorisches, keine Inhaltsdaten usw.).
3	**Auftragsdatenbearbeitungsvereinbarung, ADV:** Was muss ich beachten, wenn ich Dritte mit einer Datenbearbeitung beauftrage?	Die Vorlage «Datenschutz Vorlage Auftragsdatenbearbeitungsvereinbarung (ADV) inkl. TOMs» enthält die wichtigen Inhalte eines solchen Auftrags.

Nr.	FAQ	Antwort
4	**Betroffenenrechte:** (siehe Rechte) Was beinhalten die Betroffenenrechte?	Das Datenschutzrecht sieht verschiedene Ansprüche vor, die eine von einer Datenbearbeitung betroffene Person im Zusammenhang mit ihren eigenen Personendaten bei Pfarreien oder Kirchgemeinden geltend machen kann. Dazu gehören das Auskunfts- und Einsichtsrecht, die Berichtigung oder Vernichtung unrichtiger Personendaten, Unterlassung und Feststellung widerrechtlicher Datenbearbeitung, Einschränkung und Sperrung eigener Daten.
5	**Bildrechte:** Was muss ich bei Bildern beachten?	Das Medienzentrum kath.ch hat im folgenden Blog ein Merkblatt zu den Bildrechten eingefügt (letzter Aufruf 15.02.2024): https://www.blogs-kath.ch/bilder-rechtskonform-nutzen/
6	**Cloud:** Worauf ist zu achten, wenn Dateien/Daten auf einem Cloud-Speicher abgelegt werden?	Die korrekte Nutzung von Cloud-Speichern ist aus datenschutzrechtlicher Sicht nicht immer einfach. Werden die Daten durch eine inländische Anbieterin in der Schweiz bearbeitet, braucht es ein komplettes Vertragswerk, das u. a. auch eine Auftragsdatenbearbeitungsvereinbarung ADV (siehe dazu die Vorlage) beinhaltet und adäquate technische und organisatorische Massnahmen des Datenschutzes (TOMs) vorsieht. Die gewünschte Cloud-Lösung ist technisch und vertraglich vor Vertragsschluss genau zu prüfen. Werden Daten durch die Cloud-Anbieterin im Ausland bearbeitet oder kann diese (z. B. zu Support- oder Wartungszwecken) aus dem Ausland im Einzelfall darauf zugreifen, ist die Situation etwas komplexer: Zusätzlich zum Vertragswerk ist zu prüfen, ob die ausländische Rechtsordnung ein adäquates Datenschutzniveau gewährleistet. Dies ist für EU-Länder sowie einzelne weitere Länder der Fall. Die USA gilt zum Zeitpunkt der Erstellung dieser FAQ (Dezember 2023) nicht als sicheres Drittland, der Bundesrat ist aber dabei, mit den USA ein sog. «Data Privacy Framework» abzuschliessen, das ein adäquates Datenschutzniveau für Datenbearbeitungen in/aus den USA gewährleisten soll. Gilt das Drittland nicht als adäquat, sind weitere Sicherheitsmassnahmen zu treffen, damit die Übermittlung datenschutzrechtlich zulässig ist. Dazu gehören bestimmte zusätzliche Vertragsbestimmungen sowie technische Massnahmen wie etwa die Pseudonymisierung der gespeicherten Daten, so dass der Personenbezug ausserhalb der Organisation nicht hergestellt werden kann. Dies ist oftmals technisch sehr anspruchsvoll. Unterstehen die Daten einem Amts- oder Berufsgeheimnis, empfiehlt sich die Datenhaltung in der Schweiz.
7	**Datenbearbeitung:** Was ist zu beachten, wenn Datenbearbeitungen an Dritte ausgelagert werden?	Wenn die Pfarrei bei ihrer Tätigkeit Dritte (Unternehmen oder natürliche Personen) beizieht und diese im Rahmen des Auftrags Personendaten bearbeiten, liegt eine sogenannte Auftragsdatenbearbeitung vor (bspw. Newsletter-Software oder Kollaborations-Tool von Drittunternehmen). Die Verantwortung für die Einhaltung des Datenschutzes bleibt dabei stets bei der Pfarrei (sie ist sog. Verantwortliche). Die Pfarrei muss sicherstellen, dass die Dritten (sog. Auftragsbearbeitende) die Daten nur gemäss ihren Weisungen und für die von ihr vorgegebenen Zwecke bearbeiten. Dazu muss die Pfarrei einen schriftlichen Vertrag mit den Auftragsbearbeitenden (eine sog. Auftragsdatenbearbeitungsvereinbarung, ADV) abschliessen, in welchem sie die notwendigen datenschutzrechtlichen Pflichten regelt und überbindet. Das Bistum Basel stellt eine Vorlage für eine ADV zur Verfügung, die die Pfarreien nutzen können.
8	**Datenbearbeitungsverzeichnis:** Was muss in einem Datenbearbeitungs-verzeichnis aufgeführt werden?	Ein Datenbearbeitungsverzeichnis enthält eine kurze Beschreibung aller Datenbearbeitungsvorgänge (d. h. aller Geschäftsprozesse, bei denen Personendaten bearbeitet werden), die innerhalb einer Organisation vorgenommen werden. Eine Vorlage dafür (inkl. Vorbemerkungen) findet sich auf der Webseite des Bistums Basel.

Nr.	FAQ	Antwort
9	**Datenherausgabe:** Was mache ich, wenn jemand seine Daten erhalten will?	Die Person in der Pfarrei oder Kirchgemeinde, welche für Datenschutzfragen zuständig ist (sofern vorhanden), ist zunächst darüber zu informieren. Die gesuchstellende Person ist korrekt zu identifizieren, damit Daten nicht der falschen Person herausgegeben werden. Dies kann durch den persönlichen Kontakt (bei mündlichen Gesuchen), durch Abfragen zusätzlicher Informationen (bei telefonischen Gesuchen) oder durch Einreichen einer (ggf. teilweise geschwärzten) Kopie der ID geschehen. Intern müssen alle Datenbestände auf die Daten der betroffenen Person abgesucht werden. Dies kann je nach Umfang des Gesuchs z. B. auch Logdaten umfassen. Dann kann die Liste der Daten zusammengestellt und (ggf. in Absprache mit der intern zuständigen Person) der Gesuchstellerin zur Verfügung gestellt werden (Auskunftsrecht, Betroffenenrechte). Achtung: Es müssen nicht ganze Dokumente herausgegeben werden, nur die Liste der Personendaten, über die die Pfarrei verfügt. Die Auskunft ist innerhalb von 30 Tagen zu erteilen. Liegen überwiegende Interessen der Pfarrei oder von Dritten vor oder wird das Auskunftsgesuch klar zu missbräuchlichen Zwecken gestellt (d. h. nicht um effektiv Auskunft zu den eigenen Daten zu erhalten, sondern um z. B. Prozesschancen im Falle einer Klage gegen die Pfarrei abzuklären), kann die Auskunft eingeschränkt oder verweigert werden. Gemäss Gesetz kann die betroffene Person über Folgendes Auskunft verlangen: a. die Identität und die Kontaktdaten des Verantwortlichen (d. h. der Organisation, die die Daten verarbeitet, sowie ggf. einer Datenschutzkontaktperson); b. die bearbeiteten Personendaten als solche; c. der Bearbeitungszweck; d. die Aufbewahrungsdauer der Personendaten oder, falls dies nicht möglich ist, die Kriterien zur Festlegung dieser Dauer; e. die verfügbaren Angaben über die Herkunft der Personendaten, soweit sie nicht bei der betroffenen Person beschafft wurden; f. gegebenenfalls das Vorliegen einer automatisierten Einzelentscheidung sowie die Logik, auf der die Entscheidung beruht; g. gegebenenfalls die Empfängerinnen und Empfänger oder die Kategorien von Empfängerinnen und Empfängern, denen Personendaten bekanntgegeben werden, sowie weitere Informationen (Staat und Schutzmassnahmen), sofern Personendaten ins Ausland bekanntgegeben werden.
10	**Datenschutzrecht: Anwendungspflicht** Wann muss das Datenschutzrecht beachtet werden?	Das Datenschutzrecht ist immer dann anwendbar, wenn *Personendaten bearbeitet* werden. Bei Personendaten handelt es sich um Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Bestimmt ist eine Person, wenn die Daten sie direkt identifizieren (z. B. Name und Vorname). Bestimmbar ist eine Person, wenn Daten aus Perspektive der Datenbearbeitenden oder in Kombination mit weiteren verfügbaren Informationen die Identifikation dieser Person ermöglichen (bspw. Datenbankidentifikationsnummer in Verbindung mit einer Datenbank

Nr.	FAQ	Antwort
		oder Telefonnummern mit Zugang zu tel.search.ch). Das Bearbeiten umfasst alle Handlungen im Zusammenhang mit Personendaten, z. B. das Erheben, Speichern, Verändern, Versenden, Löschen oder Anonymisieren. Also: Auch Daten, die auf einem Server unbenutzt «liegen», werden bearbeitet! Allgemein gilt, dass die Begriffe «Personendaten» und «Bearbeiten» sehr breit sind. *Das heisst, dass das Datenschutzrecht in den meisten Fällen im Pfarreialltag zur Anwendung kommen wird.*
11	**Datenschutzrecht: Zweck** Was bezweckt das Datenschutzrecht?	Jede Person hat ein Anrecht darauf, dass ihre personenbezogenen Daten geschützt werden. Der Datenschutz stellt den Schutz der Privatsphäre beim Umgang mit Personendaten als Grundrecht aller Menschen sicher. Dazu sieht das Datenschutzrecht diverse Regeln für Datenbearbeitende (Unternehmen, öffentliche Organe oder Privatpersonen) im Umgang mit Personendaten vor. Weiter gibt es den betroffenen Personen, über die Daten bearbeitet werden, eine Reihe von Instrumenten in die Hand, um die Hoheit über ihre Daten zu behalten.
12	**Datenschutz: Grundprinzipien** Welche Grundprinzipien sind stets zu beachten?	Das Datenschutzrecht sieht eine Reihe von Grundprinzipien vor, die bei jeder Datenbearbeitung beachtet werden müssen. Man kann sich diese als eine Art «Dach» über allen Datenbearbeitungen vorstellen. Diese Prinzipien werden in diversen Ausführungsbestimmungen im Datenschutzgesetz weiter konkretisiert. Die sieben Grundprinzipien lauten wie folgt: - Rechtmässigkeit: Datenbearbeitungen müssen rechtmässig erfolgen und dürfen nicht gegen geltendes Recht verstossen. Für öffentliche Organe bedeutet es zudem, dass die Bearbeitung gewöhnlicher Personendaten nur basierend auf einer gesetzlichen Grundlage erlaubt ist (oder in gewissen Kantonen: die Datenbearbeitung muss zur Erfüllung einer gesetzlichen Aufgabe notwendig sein). - Datensparsamkeit: Es sollen nur so viele Personendaten wie nötig erfasst und bearbeitet werden! Wenn Daten nicht mehr gebraucht werden, sind sie zu anonymisieren oder zu löschen. - Zweckbindung: Die Personendaten dürfen nur für Zwecke bearbeitet werden, die der betroffenen Person angegeben werden oder die für sie erkennbar sind bzw. die mit dem ursprünglichen Zweck vereinbar sind (Zweckänderungsverbot). Bspw. dürfen Personendaten, die von Bewerbenden erhoben werden (z. B. Kontaktdaten, Referenzen, CV) nur für den Zweck der Rekrutierung und nicht zusätzlich für einen Newsletter-Versand usw. verwendet werden. Transparenz: Die betroffenen Personen werden über die Datenbearbeitungen informiert. - Datenrichtigkeit: Unrichtige Daten müssen korrigiert oder gelöscht werden. - Sicherheit: Personendaten müssen vor Verlust, Verfälschung oder unbefugtem Zugriff geschützt werden. Dies geschieht meist durch sogenannte technische und organisatorische Schutzmassnahmen (TOMs). - Rechenschaftspflicht: Organisationsintern müssen nötige Prozesse und Verfahren zur Sicherstellung und zum Nachweis der Datenschutzkonformität umgesetzt werden.
13	**Datenschutz: Folgenabschätzung** Was ist eine Datenschutz-Folgenabschätzung und wie wird sie durchgeführt?	Wie der Name sagt, ist die Datenschutz-Folgenabschätzung (DSFA) ein Nachdenken über die Risiken einer Datenbearbeitung, die man dokumentiert und zu reduzieren versucht. Das Datenschutzgesetz sieht vor, dass die Auswirkungen einer Datenbearbeitung auf die betroffenen Personen immer vorab zu prüfen sind, und zwar bei jedem neuen Projekt,

Nr.	FAQ	Antwort
		das die Bearbeitung von Personendaten mit sich bringt, sowie wenn eine bestehende Datenbearbeitung angepasst wird. Die Einführung einer neuen Software zur Verwaltung umfangreicher Datensätze (CRM, Mitgliederregister) oder die Installation einer Überwachungskamera auf dem Pfarreigelände sind Beispiele von Sachverhalten, bei denen eine DSFA durchzuführen ist. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) stellt ein Merkblatt zur Verfügung, das Hilfestellungen bietet: https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/grundlagen/dsfa.html
14	**Datenschutzbestimmungen:** Was geschieht, wenn Datenschutzbestimmungen missachtet werden?	Der Schutz der Personendaten ist nicht freiwillig, sondern gesetzlich vorgeschrieben. Zuständige Datenschutzaufsichtsbehörde für die Pfarreien ist der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB), für die Kirchgemeinden sind es die kantonalen Datenschutzbehörden. Sie überwachen die Anwendung der Datenschutzvorschriften und haben Kontrollbefugnisse (z. B. Recht auf Auskunft oder Einsichtnahme), können Empfehlungen abgeben oder die Anpassung oder Einstellung von Datenbearbeitungen verfügen. Neben Aufsichtsmassnahmen können die betroffenen Personen Datenschutzverletzungen auf zivil- oder verwaltungsrechtlichem Weg direkt bei der Pfarrei geltend machen und bspw. die Beendigung oder Beseitigung widerrechtlicher Datenbearbeitungen verlangen. Bei finanziellem Schaden oder schwerer Persönlichkeitsverletzung hat die betroffene Person Anspruch auf Schadenersatz oder Genugtuung. Gemäss DSG drohen sodann strafrechtliche Sanktionen für private Personen und Bussen von bis zu CHF 250'000.00. Diese dürften in erster Linie die Leitung der Pfarrei betreffen, da diese als Exekutive der Pfarrei für die Einführung und Durchsetzung der nötigen Prozesse und Pflichten verantwortlich ist. Die Strafbarkeit ist jedoch nur für gewisse Datenschutzpflichten vorgesehen und verlangt mindestens Eventualvorsatz. Eventualvorsatz bedeutet, dass die Datenschutzverletzung zwar nicht bewusst angestrebt, jedoch in Kauf genommen wird. Nebst diesen rechtlichen Sanktionen kann die Nichteinhaltung des Datenschutzrechts schwere Reputationsrisiken mit sich bringen.
15	**Datensicherheit:** Was versteht man unter Datensicherheit? Was sind TOMs?	Die Datensicherheit ist ein Teilbereich des Datenschutzes. Sie regelt die Verfügbarkeit, Vertraulichkeit, Integrität der bearbeiteten Personendaten sowie die Nachvollziehbarkeit der Datenbearbeitungsvorgänge. Dazu müssen Organisationen geeignete technische und organisatorische Massnahmen (sogenannte «TOMs») ergreifen. Beispiele solcher Massnahmen sind Zugriffskonzepte, Anonymisierungen, Passwort-Schutz, 2-Faktoren-Authentifizierung, Schulungen, Weisungen, usw. Je sensitiver die Personendaten sind, umso höher sind die Anforderungen an die Sicherheitsmassnahmen («Angemessenheit»). Nebst dem Erfordernis der Datensicherheit im Datenschutz gibt es auch ein breiteres Arbeitsfeld der «Informationssicherheit». Auch hier ist das Ziel, die Verfügbarkeit, Vertraulichkeit und Integrität sicherzustellen; im Gegensatz zum Datenschutz ist der Anwendungsbereich aber breiter. Es geht nicht nur um Personendaten, sondern um alle geschäftsrelevanten Informationen. Praxistipp: Es empfiehlt sich, die Informationssicherheit und den Datenschutz miteinander so zu verbinden, dass Synergien genutzt und Doppelspurigkeiten vermieden werden können.

Nr.	FAQ	Antwort
16	**Datensicherheit:** Was ist bei einer Verletzung der Datensicherheit zu tun?	Eine Verletzung der Sicherheit liegt vor, wenn die Integrität, Vertraulichkeit, Verfügbarkeit oder Nachvollziehbarkeit der Daten nicht mehr gewährleistet ist und Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden. Das ist bspw. der Fall, wenn ein USB-Stick oder Geschäfts-Computer verloren geht oder liegen gelassen wird, bei Cyberangriffen (DDoS-Attacke, Phishing) oder Datenzugriffen durch unberechtigte Personen. Pfarreien müssen Verletzungen der Datensicherheit intern analysieren und der eidgenössischen Datenschutzaufsichtsbehörde (bzw. bei gemeinsam mit der Kirchgemeinde verantworteten Tätigkeiten auch der kantonalen Datenschutzaufsichtsbehörde) im Normalfall dann melden, wenn daraus ein hohes Risiko für die Grundrechte der betroffenen Personen resultiert (sog. Data breach notification). Notabene: In gewissen kantonalen Gesetzen ist die Schwelle etwas tiefer angesetzt und Datenschutzvorfälle sind immer zu melden. Alle Mitarbeitenden der Pfarrei müssen jeden Verdacht auf einen Datenschutzvorfall intern bei einer dafür designierten Stelle – idealerweise die Sicherheitsbeauftragte oder der Datenschutzberater - sowie auch bei der Pfarreileitung und der Kirchgemeindeleitung unverzüglich (!) melden. Zudem kann der Generalvikar des Bistums kontaktiert werden, der beratend zur Seite steht. Intern ist dann zu analysieren und zu dokumentieren, ob ein Datenschutzvorfall im Sinne des Gesetzes vorliegt. Ist dies der Fall, sind folgende Schritte notwendig: • Ergreifen von Massnahmen zur Risikoeindämmung • Unverzügliche Meldung an Datenschutzaufsichtsbehörde (innert 72 Stunden gemäss Praxis bzw. je nach kantonalen datenschutzrechtlichen Bestimmungen), beim EDÖB kann folgendes Formular genutzt werden: https://databreach.edoeb.admin.ch/report • Information an die betroffene Person, wenn der Datenschutzvorfall für sie ein grosses Risiko bedeutet oder sie selber Schutzmassnahmen treffen muss (bspw. Wechsel des Passwortes).
17	**Gruppierungen:** Was ist bei Listen von Gruppierungen zu beachten?	Mitgliederlisten (ML) von Gruppierungen sind mit adäquaten Massnahmen vor Verlust oder unbefugter Einsichtnahme zu schützen. Grundsätzlich dürfen sie nur für die rechtmässige Aufgabenerfüllung der Pfarrei oder der Kirchgemeinde geführt werden (Rechtmässigkeitsprinzip) und die Datenschutzgrundsätze sind einzuhalten (insb. Verhältnismässigkeit: restriktive Zugriffsrechte, Erfassung nur der nötigen Daten, und Sicherheit: Ablage in geschützter Umgebung, ggf. Passwortschutz beim Versand usw.). Die Mitglieder müssen bei der Erhebung ihrer Daten über den Umgang mit der ML informiert werden (Transparenzprinzip, Einwilligung der betroffenen Personen). Werden ML weitergegeben, sind sie z. B. mit Passwort zu sichern, insbesondere dann, wenn sie viele Personendaten enthalten. Es ist vor der Weitergabe zu prüfen, ob die empfangende Person/Organisation befugt ist, die Daten zu erhalten. Wenn nicht (z. B. weil die Person/Organisation nicht mit der Erfüllung kirchlicher Aufgaben betraut ist), ist das Einverständnis der betroffenen Personen einzuholen.

Nr.	FAQ	Antwort
		Bei Pfarrei internen Versänden sind die Listen nicht einer E-Mail als Anlage beizulegen, sondern es ist stattdessen ein Link auf die gemeinsame Ablage zu setzen. Die Verantwortung für den Datenschutz kommt primär der Leitung der Pfarrei zu.
18	**Internetseite:** Was muss zwingend in das Impressum einer Pfarrei-Internetseite?	Ein Impressum sollte die Kontaktdaten der für die Internetseite verantwortlichen Organisation enthalten: Voller Name der Organisation sowie ggf. eine Ansprechperson oder -stelle innerhalb der Pfarrei, Postadresse, E-Mail-Adresse, idealerweise auch eine Telefonnummer.
19	**Katechese/Religionsunterricht:** Dürfen Schülerlisten (mit Angaben wie Wohnadresse, Telefonnummern, E-Mail der Eltern, zusätzliche Versandadressen) angelegt werden? Müssen die Eltern zustimmen, dass diese Daten gespeichert werden?	Sofern diese Listen für die Durchführung von Religionsunterricht und Katechese erforderlich sind, dürfen sie angelegt werden. Es ist darauf zu achten, dass nur erforderliche Daten erhoben werden und dass Massnahmen zur Einhaltung der Sicherheit (Ablage in sicherer Umgebung, Verzicht auf das Anlegen von Dateikopien, Passwortschutz beim Versand usw.) und Verhältnismässigkeit (auf das Nötigste beschränkte Zugriffsrechte innerhalb der Pfarrei) umgesetzt werden.Wenn die Erhebung der Daten für Religionsunterricht/Katechese zulässig ist (weil die Eltern die Daten freiwillig zu diesem Zweck gegeben haben oder das kantonale Recht die Weitergabe der Personendaten der Konfessionsangehörigen zu diesem Zweck an die Pfarrei vorsieht), darf die Pfarrei diese Daten zu demselben Zweck auch speichern. Will die Pfarrei später über diesen Zweck hinausgehen und die Daten nutzen, um die Schülerinnen und Schüler oder deren Eltern zu weiteren Anlässen einzuladen oder Newsletter zu verschicken, empfiehlt es sich, dazu die Einwilligung einzuholen.
20	**Katechese/Religionsunterricht:** Dürfen Schülerlisten an die Eltern einer Klasse abgegeben werden? Welche Angaben dürfen sie in diesem Fall enthalten, welche nicht?	Dies ist ein Graubereich, in dem es zwar sinnvoll (und oft nützlich) sein kann, Schülerlisten abzugeben (z. B. damit sich die Eltern organisieren können), es ist aber nicht immer im datenschutzrechtlichen Sinne *erforderlich* für die Durchführung von RU/Katechese. Entsprechend reagieren Betroffene manchmal mit wenig Verständnis. Im Zweifelsfall empfiehlt es sich, bei der Anmeldung (z. B. mittels Formular) die Eltern darauf hinzuweisen, dass Schülerlisten abgegeben werden, und ihnen die Möglichkeit zu geben, entweder aktiv ihr Einverständnis zu geben (z. B. durch Ankreuzen) oder sie darauf hinzuweisen, dass sie sich bei der Pfarrei melden können, wenn sie nicht wollen, dass ihr Kind auf einer solchen Liste erscheint. Bei Protest kann dann das entsprechende Kind - oder auch nur bestimmte Kontaktangaben wie z. B. Telefonnummern - von der Liste entfernt werden. In jedem Fall sind Angaben auf ein Minimum zu beschränken, um den gewünschten Zweck zu erreichen (z. B. Telefonnummer der Eltern, keine Geburtsdaten o.ä. Zusatzangaben, die nicht benötigt werden).
21	**Listen** (siehe auch Gruppierungen, Vereine): Wie ist mit Listen von Klienten im weitesten Sinne (z. B. regelmässige Krankenkommunion, Sozialdienste) zu verfahren?	Das Prinzip der Datensparsamkeit muss beachtet werden. Alle, die Zugriff auf die Listen haben, sind dafür verantwortlich, dass diese datenschutzkonform verwendet und nicht an Dritte herausgegeben werden (Rechtmässigkeitsprinzip).
22	**Listen:**	Grundsätzlich darf dies zu Zwecken der Nachvollziehbarkeit festgehalten werden. Informationen über eine Person, welche soziale Hilfe erhält, gehören zu den besonders schützenswerten Personendaten und sind entsprechend gut zu schützen.

Nr.	FAQ	Antwort
	Darf festgehalten werden, wer, wann und in welcher Form z. B. vom Sozialdienst unterstützt wird?	
23	**Listen mit Kontaktdaten:** Wie ist der Zugang zu diesen Angaben zu regeln?	Die Zugriffsrechte auf die entsprechenden Unterlagen sind auf ein Minimum zu reduzieren. Sie sind in einer sicheren Umgebung zu speichern (in der intern freigegebenen Ablage der Pfarrei, nicht auf Dropbox oder auf dem privaten Arbeitsgerät usw.) und wieder zu löschen, wenn sie nicht mehr gebraucht werden. Wenn sie verschickt werden müssen, sollte die entsprechende Datei mit Passwortschutz versehen werden. Es muss definiert werden, wer in der Pfarrei (oder Kirchgemeinde) Zugang zu diesen Informationen haben muss, um seine rechtmässige Aufgabe erfüllen zu können (Need-to-know-Prinzip). Nach den relevanten Datenschutzgesetzen handelt es sich bei Angaben über soziale Hilfe um besondere Personendaten, welche besonders geschützt werden müssen. Es empfiehlt sich daher, diese Listen in einem Ordner abzulegen, zu dem nur wenige Personen Zugriff haben. Ggf. sind Dateien mit Passwortschutz zu versehen.
24	**Listen wiederkehrender Anlässe:** Darf ich Listen über Jahre weiterführen (z. B. einer jährlichen Fachtagung)?	Solche Listen dürfen geführt werden. Vorschlag für die entsprechende Datenschutzerklärung: *Die Personendaten, die Sie uns mit der Anmeldung für [Anlass] mitgeben, werden von der [Organisation] in einer Liste geführt und laufend aktualisiert. Zweck der Liste ist es, Sie an zukünftige Fachtagungen mit derselben oder ähnlichen Ausrichtung einladen zu können [sowie Sie ggf. für praktische Mithilfe anfragen zu können]. Diese Liste ist nur für [Organisatoren sowie an der Organisation des [Anlasses] beteiligte Dritte] zugänglich, wird mit adäquaten Massnahmen geschützt und von uns ggf. mit Beizug von Dritten in einer gesicherten Umgebung in der Schweiz oder in der EU gespeichert. Sie können Ihre Personendaten jederzeit von der Liste löschen lassen. Bei Fragen oder Anliegen steht Ihnen XY@xyz.ch zur Verfügung.* Aus diesen Daten darf für die jeweilige Veranstaltung eine Teilnehmerliste mit Vorname, Name und Ort erstellt werden.
25	**Mail-Verkehr:** In welchen Fällen verbietet der Datenschutz unverschlüsselten Mailverkehr?	Unverschlüsselter Mailverkehr an Empfängerinnen und Empfänger ausserhalb der eigenen Organisation ist ungeeignet für besonders schützenswerte Personendaten oder Daten, die aus anderen Gründen vertraulich zu behandeln sind (z. B. Daten, die dem Amts- oder Berufsgeheimnis unterliegen).
26	**Messenger:** Welche Messenger-Dienste können im Rahmen des pfarreilichen Umfelds bedenkenlos genutzt werden? Von welchen sollte man die Finger lassen?	Grundsätzlich empfiehlt es sich aus Datenschutzsicht, Threema oder Signal anderen Messenger-Diensten wie WhatsApp oder Telegram vorzuziehen. Die Pfarrei kann mit dem Erlass einer Weisung dafür sorgen, dass auch bei einer Nutzung etwa von WhatsApp durch die Mitarbeitenden keine Inhaltsdaten aus den Tätigkeiten der Pfarrei weitergegeben werden, sondern dass sich die Nutzung der App auf Organisatorisches beschränkt (z. B. Terminfindung usw.).
27	**Office-Programme:** Können Microsoft-Produkte heutzutage gemäss Schweiz. Datenschutzgesetz weiter	Zum Zeitpunkt des Verfassens dieser FAQ (Dezember 2023) bedingt die rechtskonforme Nutzung von Microsoft Cloud-Diensten a) vertragliche Garantien, die teilweise zusätzlich mit Microsoft abzuschliessen sind, b) zusätzliche vertragliche und technische Sicherheitsmassnahmen, um das Risiko einzugrenzen, das mit Datenbearbeitungen durch

Nr.	FAQ	Antwort
	bedenkenlos im Rahmen der Pfarrei eingesetzt werden? Wo gibt es Bedenken? Was wären die Alternativen?	Microsoft in den USA einhergeht und c) eine interne Datenklassifikation, die Daten in verschiedene Schutzstufen einteilt und die für deren Bearbeitung unterschiedliche Vorgaben macht (z. B. keine Daten, die einem Amts- oder Berufsgeheimnis unterstehen, die in der Microsoft-Cloud abgespeichert werden). Mit dem erwarteten Abschluss des «Data Privacy Framework» des Bundesrates mit der US-Regierung dürften sich einige dieser Probleme entschärfen, wobei den Daten, die Amts- oder Berufsgeheimnissen unterstehen, nach wie vor besondere Sorge zu tragen ist. Sollen Microsoft-Cloud-Dienste eingesetzt werden, empfiehlt es sich, mit spezialisierter Unterstützung die obigen Schritte einzuhalten und mit internen Weisungen sicherzustellen, dass Daten unter Amts- oder Berufsgeheimnis separat abgelegt werden (u. a. CMI Axioma für Behördenunterlagen).
28	**Personaldaten (Angestellte):** Welche Vorgaben gibt es?	Es geht hier um: Arbeitszeugnisse, Zwischenzeugnisse, Arbeitsvertrag, Stellenbeschrieb, Mitarbeitergespräche. Die Unterlagen werden bei der Anstellungsbehörde, (teilweise auch) bei den kirchlichen Vorgesetzten (Pfarrei) abgelegt, aufbewahrt. Es ist zu definieren, wer diese Unterlagen haben, wer sie einsehen darf. Es gilt das Need-to-know-Prinzip. Unnötige Doppelspurigkeiten bei der Ablage sind zu vermeiden. Es gelten die allgemeinen Vorgaben mit besonderem Fokus auf die Verhältnismässigkeit (restriktive Zugriffsrechte) und die Sicherheit (Ablage in geeigneter Umgebung, restriktive Zugriffsrechte). Das staatliche Recht, das auf die Kirchgemeinde zur Anwendung kommt (landeskirchliches oder kantonales Personalrecht sowie das Obligationenrecht), ist auch für die Pfarrei zu beachten.
29	**Personaldaten (Angestellte):** Wie lange darf aufbewahrt werden?	Die Rechtsordnung sieht verschiedenste Aufbewahrungs- und Verjährungsfristen vor, die für die Aufbewahrung von Personalunterlagen relevant sein können. Für das Arbeitsverhältnis stehen zwei Arten von gesetzlichen Aufbewahrungsfristen im Vordergrund: a. Die Aufbewahrungsfristen für Geschäftsbücher, die die Nachvollziehbarkeit von Lohnzahlungen über 10 Jahre sicherstellen sollen (und aufgrund derer bestimmte Angaben aus dem Arbeitsverhältnis, z. B. der Vertrag, während dieser Dauer aufbewahrt werden sollten) b. Verjährungsfristen für Lohnforderungen (z. B. fünf Jahre für Forderungen aus dem Arbeitsverhältnis, wenn das Obligationenrecht direkt oder als subsidiäres kantonales Recht zur Anwendung kommt). Es empfiehlt sich, gestaffelt vorzugehen und 5-6 Jahre nach dem Weggang das zu löschen, was nicht für die Nachvollziehbarkeit der Geschäftsbücher nötig ist (Evaluationen aus Mitarbeitergesprächen, Lohnbelege, sofern nicht relevant für die Geschäftsbücher, Unterlagen im Zusammenhang mit Leistungen und Beiträgen der Sozialversicherungen sowie der beruflichen Vorsorge). Der übrigbleibende Grundstock an Stammdaten wird dann nach Ablauf von 10-11 Jahren gelöscht.
30	**Personaldaten (Angestellte):** Umgang beim Stellenwechsel	Geschieht der Stellenwechsel innerhalb der Organisation, können die Unterlagen, die zur vormaligen Stelle gehören, aufbewahrt werden, sofern dies nötig ist. Verlässt die Person die Organisation, gilt das oben Gesagte.

Nr.	FAQ	Antwort
31	**Personendaten:** Was sind besonders schützenswerte Personendaten?	Besonders schützenswerte Personendaten haben aufgrund ihrer Sensitivität für die betroffene Person einen erhöhten Schutzbedarf. Dies ist der Fall, wenn Daten einen besonders tiefen Einblick in die Persönlichkeit und das Leben einer Person erlauben (z. B. persönliche Informationen aus Seelsorgegesprächen oder Sozialarbeitergesprächen sowie Informationen zu Angestellten, wenn sie auf risikoreiche Art bearbeitet werden oder wenn viele Daten miteinander kombiniert werden. Das DSG nennt folgende Beispiele: • Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, • Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie, • genetische Daten, • biometrische Daten, die eine natürliche Person eindeutig identifizieren, • Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen, • • Daten über Massnahmen der sozialen Hilfe.
32	**Personendaten:** Was ist bei der Bearbeitung besonders schützenswerter Personendaten zu beachten?	Aufgrund der sensitiven Natur der Daten sind sie *besonders gut zu schützen* - mit anderen Worten ist den technischen und organisatorischen Schutzmassnahmen (TOMs) der *Datensicherheit* besonderes Augenmerk zu geben. Zudem ist die Bekanntgabe von besonders schützenswerten Personendaten an Dritte (d.h. die Weitergabe oder das Zugänglichmachen von Personendaten an eine andere Organisation oder Person, die diese zu eigenen Zwecken nutzt) nur zulässig, wenn dafür ein Rechtfertigungsgrund vorliegt; d.h. es braucht dafür eine *gesetzliche Grundlage*, ein *überwiegendes Interesse* der Pfarrei oder einer Drittperson oder die *explizite Einwilligung* der betroffenen Personen. Als explizite Einwilligung gilt eine Einwilligung, bei der die betroffene Person selbst aktiv wird, etwa durch Ankreuzen eines Häkchens oder durch Unterschrift.Wichtig: Die Kirchgemeinden als Körperschaften des kantonalen Rechts brauchen für die Bearbeitung besonders schützenwerter Personendaten meist eine explizite Grundlage in einem Gesetz.
33	**Personendaten:** Wie müssen Listen mit Personendaten (z. B. per Mail) versendet werden?	Wenn es möglich ist, statt dem Versenden als Anlage zur E-Mail mit einer Verlinkung auf eine gemeinsame interne Ablage zu arbeiten, ist dies zu bevorzugen. So kann vermieden werden, dass dieselbe Liste vervielfacht wird, was aus Sicht des Datenschutzes nicht empfehlenswert ist. Ist es nicht möglich, auf eine gemeinsame interne Ablage zu verlinken, empfiehlt es sich, die Datei mit einem Passwortschutz zu versehen und der Empfängerin oder dem Empfänger das Passwort zur Datei in einer separaten E-Mail oder via einen anderen Kanal (Telefon, SMS) zu übermitteln. Eine generelle E-Mail-Verschlüsselung wird empfohlen.
34	**Personendaten:** Was ist zu beachten, wenn Personendaten ins Ausland übermittelt werden?	Eine Übermittlung von Personendaten liegt vor, wenn diese physisch im Ausland gespeichert werden (bspw. ausländischer Hosting-Provider) oder Personen aus dem Ausland Zugriff (*Remote Access)* auf lokal gespeicherte Daten haben (bspw. ausländischer Software-Anbieter in Support-Fällen). Wenn Personendaten ins Ausland übermittelt werden, so ist ausländische Gesetzgebung auf die Datenbearbeitung anwendbar. Ist diese Gesetzgebung nicht gleichwertig mit dem lokalen Datenschutzrecht, so müssen zusätzliche Schutzmassnahmen getroffen werden und es ist eine Risikobeurteilung vorzunehmen. Zusammenfassend gilt also folgende Kaskade:

Nr.	FAQ	Antwort
		1. **Sicherer Drittstaat**: Als Land mit genügendem Datenschutzniveau gelten z. B. alle Staaten des EWR-Raums (sichere Drittstaaten), nicht aber die USA (zum Zeitpunkt des Verfassens dieser FAQ im Dezember 2023), China oder Russland (unsichere Drittstaaten). Bei Übermittlung in sichere Drittstaaten sind keine Zusatzmassnahmen notwendig. 2. **Geeignete Schutzmassnahmen**: Bei Übermittlung in unsichere Drittstaaten müssen zusätzliche Massnahmen getroffen werden, bspw. sind von der Datenschutzaufsicht genehmigte Datenschutzklauseln oder die Standard-datenschutzklauseln der EU-Kommission abzuschliessen. 3. **Ausnahmegrund**: Ohne geeignete Schutzmassnahmen können Daten nur in Ausnahmefällen ins Ausland übermittelt werden. Dies, wenn bspw. eine ausdrückliche Einwilligung vorliegt oder die Bekanntgabe zur Wahrung überwiegender Interessen notwendig ist.
35	**Personendatenbank:** Welche Daten darf ich speichern?	Es dürfen nur die Personendaten gespeichert werden, die für die Erfüllung der Aufgaben der Pfarrei oder der Kirchgemeinde erforderlich sind (Rechtmässigkeitsprinzip, Verhältnismässigkeitsprinzip, Zweckbindungsprinzip). Es dürfen keine zusätzlichen Informationen zweckfrei auf Vorrat erfasst werden. Was die effektiv zulässigen Personendaten für die Verwaltung der Mitglieder (meist mit dem Programm «KiKartei») anbelangt, so gibt das kantonale Recht vor, welche Daten (Attribute) die Pfarrei aus dem kantonalen Einwohnerregister beziehen kann (Rechtmässigkeitsprinzip).
36	**Personendatenbank:** Wie lange darf ich diese Daten speichern?	Die Personendaten dürfen nur so lange gespeichert werden, wie sie für die Erfüllung des Zwecks nötig sind (Zweckbindungsprinzip). Danach sollten die Daten gelöscht werden. Dies ist im Einzelfall nicht ganz einfach zu bestimmen, weil gewisse Daten zur Nachvollziehbarkeit kirchlicher Handlungen (Taufbuch, Erhebung Kirchensteuer) von der Pfarrei oder der Kirchgemeinde unter Umständen über lange Zeit aufbewahrt werden müssen. Sieht man aber, dass gewisse Daten nicht mehr benötigt werden (z. B. eine alte Adresse), so sind sie zu löschen. Damit diese Pflichten nicht vergessen gehen, ist mindestens einmal pro Jahr mit allen Angestellten ein Datenbereinigungstag anzusetzen. EDV-Programme haben automatische Löschprogrammierungen.
37	**Personendatenbank:** Bei welchen Ereignissen muss ich diese Daten löschen?	Es gibt grundsätzlich zwei Situationen, in denen Daten gelöscht werden müssen: 1. Wenn sie für den ursprünglichen Bearbeitungszweck nicht mehr benötigt werden. 2. Wenn die betroffene Person die Löschung verlangt und die Pfarrei der Löschung keinen überwiegenden Grund für die Aufbewahrung entgegenhalten kann. Ein überwiegender Grund für die Aufbewahrung kann in der Führung kirchlicher Register liegen, wenn ansonsten die Nachvollziehbarkeit gewisser Handlungen (z. B. Taufdatum) nicht mehr gewährleistet ist.
38	**Pfarrblatt:** Darf ich Taufen, Ehen, Verstorbene im Pfarrblatt publizieren? Benötige ich eine Einwilligung?	Es geht die Mitglieder der gesamten Pfarrei an, zu wissen, wer in die Pfarrei neu aufgenommen wird, dort heiratet oder verstirbt, weil es sie als Gemeinschaft betrifft. Eine Ausnahme ist das Aufgebot zur Eheschliessung. Von diesem darf mit Dispens verzichtet werden. Die Dispens wird im Rahmen des Ehevorbereitungsgesprächs erteilt. Nichtmitglieder der Pfarrei haben kein Recht auf die Information. In den Vorbereitungsgesprächen werden die Betroffenen über die

Nr.	FAQ	Antwort
		Publikation informiert. Will jemand keine Veröffentlichung, wird das respektiert. CIC/1983: cc. 747 Verkündigungsrecht, c. 220 Persönlichkeitsschutz, c. 1067 Dispens vom Aufgebot.
39	**Rechte** (siehe Betroffenenrechte): Welche Rechte haben betroffene Personen?	Das DSG gibt den Personen, die von der Bearbeitung ihrer Personendaten betroffen sind (sog. betroffene Personen), gewisse Rechte. In erster Linie besteht ein Recht auf Einsicht, bzw. Auskunft, ferner ein Recht auf Berichtigung unrichtiger Personendaten sowie unter Umständen ein Recht auf Widerspruch oder Löschung. Ein Recht auf Herausgabe von Personendaten in einem gängigen elektronischen Format besteht dann, wenn die Daten automatisiert bearbeitet werden und dies auf Basis der Einwilligung der betroffenen Person oder zur Erfüllung eines Vertrags geschieht.
40	**Schaukasten:** Darf ich Taufen, Ehen, Verstorbene (Begräbnisfeiertermine) durch öffentlichen Aushang publizieren? Benötige ich eine Einwilligung?	Es geht die Mitglieder der gesamten Pfarrei an, zu wissen, wer in die Pfarrei neu aufgenommen wird, dort heiratet oder verstirbt, weil es sie als Gemeinschaft betrifft. Die Veröffentlichung der Informationen an die Pfarreimitglieder im Rahmen von Gottesdiensten ist zulässig (vgl. auch Verkündigungen). In den Vorbereitungsgesprächen werden die Betroffenen darüber informiert. Will jemand keine Veröffentlichung (im Schaukasten, Pfarrblatt), wird das respektiert. Eine Ausnahme ist das Aufgebot zur Eheschliessung. Von diesem darf mit Dispens verzichtet werden. Die Dispens wird im Rahmen des Ehevorbereitungsgesprächs erteilt.
41	**Social Media:** Worauf ist zu achten bei der Verwendung von Social-Media (Bsp. Instagram, Facebook, TikTok, SnapChat, usw.)? Kann man die ohne Bedenken benutzen? Wo ist Vorsicht geboten?	Es wird empfohlen, das Datenschutzniveau und die Nutzungsbestimmungen von Social-Media-Kanälen zu kennen und entsprechend zu entscheiden, ob man einen bestimmten Kanal nutzen will (Wer ist der Betreiber des Kanals, welche Daten werden gesammelt, wo werden die Daten gespeichert?). Datenschutzfreundliche Einstellungen kennen und vornehmen. Es empfiehlt sich, intern eine Richtlinie darüber zu erstellen, wie die Pfarrei einen Kanal nutzen will und wie die Mitarbeitenden den Kanal nutzen dürfen. Ohne Einwilligungen der betroffenen Personen dürfen keine Posts von Videos, Fotos oder anderen personenbezogenen Daten veröffentlicht werden. Instagram, Facebook, TikTok und SnapChat kann man nicht ohne Bedenken nutzen. Diese Kanäle verbreiten Hassreden, sammeln übermässig viele Daten zum Zwecke der Profilbildung und verkaufen Daten an Datenbroker zwecks Schaltung von personalisierter Werbung usw. Es ist nicht ausgeschlossen, dass die Betreiber dieser Kanäle zwecks Überwachung mit Behörden kooperieren.
42	**Taufbuch:** Dürfen die Taufbücher weiterhin ausgefüllt werden?	Die Taufbücher dürfen weiterhin ausgefüllt werden, da die Informationen als Nachweis der Taufe und weiterer empfangener Sakramente (Eheschliessung, Weihe usw.) erforderlich sind. Vgl. cc. 535; 849; 473 § 1 CIC/1983
43	**Taufbuch:** Wem darf ich welche Daten aus dem Taufbuch bekannt geben?	Die Daten dürfen dem/der Gläubigen selbst, Erziehungsberechtigten, gesetzlichen Vertretern sowie in begründeten Fällen anderen kirchlichen Stellen mitgeteilt werden. Die Auskunft ist gratis und schriftlich in Form einer Fotokopie, eines digitalen Dokuments oder eines Ausdrucks zu erteilen. Eine Einsichtnahme ins Originaldokument ist nicht vorgesehen. Damit soll vermieden werden, dass der Schutz fremder Daten verletzt wird. Betroffen sind die Eintragungen über Taufe, Firmung, Eheschliessung, Weihe und Ordenseintritt (c. 220 CIC/1983).

Nr.	FAQ	Antwort
44	**Taufbuch:** Muss auf dem Taufanmeldeformular stehen, dass diese Daten gespeichert werden? Und wofür?	Der CIC/1983 geht automatisch davon aus, dass die Daten ins Taufbuch aufgenommen werden. Die Betroffenen (Täufling, Erziehungsberechtigte) werden über diesen Vorgang informiert. Die offiziellen Formulare enthalten eine entsprechenden Hinweis.
45	**Taufbuch:** Müssen die Eltern zustimmen, dass diese Daten gespeichert werden?	Den CIC/1983 geht automatisch davon aus, dass diese die ins Taufbuch aufgenommen werden. Mit der Anmeldung zur Taufe geht der CIC/1983 implizit davon aus, dass die Eltern bzw. der Täufling der Speicherung der Daten einverstanden sind.
46	**Vereine:** Wie ist mit Mitgliederlisten zu verfahren?	Mitgliederlisten (ML) von Vereinen sind mit adäquaten Massnahmen vor Verlust oder unbefugter Einsichtnahme zu schützen. Grundsätzlich dürfen sie nur für die rechtmässige Aufgabenerfüllung der Pfarrei oder der Kirchgemeinde geführt werden (Rechtmässigkeitsprinzip) und die Datenschutzgrundsätze sind einzuhalten (insb. Verhältnismässigkeit: restriktive Zugriffsrechte, Erfassung nur der nötigen Daten, und Sicherheit: Ablage in geschützter Umgebung, ggf. Passwortschutz beim Versand usw.). Die Mitglieder müssen bei der Erhebung ihrer Daten über den Umgang mit der ML informiert werden (Transparenzprinzip, Einwilligung der betroffenen Personen). Werden ML weitergegeben, sind sie z. B. mit Passwort zu sichern, insbesondere dann, wenn sie viele Personendaten enthalten. Es ist vor der Weitergabe zu prüfen, ob die empfangende Person/Organisation befugt ist, die Daten zu erhalten - wenn nicht (z. B. weil die Person/Organisation nicht mit der Erfüllung kirchlicher Aufgaben betraut ist), ist das Einverständnis der betroffenen Personen einzuholen. Bei pfarreiinternen Versänden sind die Listen nicht einer E-Mail als Anlage beizulegen, sondern es ist stattdessen ein Link auf die gemeinsame Ablage zu setzen.Die Verantwortung für den Datenschutz kommt primär dem Verein selbst zu.
47	**Verkündigungen:** Darf im Gottesdienst mündlich verkündigt werden, dass NN verstorben ist und am …. um …. auf dem Friedhof beigesetzt wird?	Es geht die Mitglieder der gesamten Pfarrei an, zu wissen, wer in die Pfarrei neu aufgenommen wird, dort heiratet oder verstirbt, weil es sie als Gemeinschaft betrifft. Gottesdienstliche Feiern sind prinzipiell öffentlich. Eine mündliche Verkündigung ist zulässig. In den Vorbereitungsgesprächen werden die Betroffenen darüber informiert. Will jemand keine Verkündigung, wird das akzeptiert.
48	**Videokonferenzen:** Gibt es Bestimmungen im Umgang mit Videokonferenz-Diensten (Bsp. Zoom, Teams usw.)?	Die Datenschutzparameter der verschiedenen Angebote variieren ganz erheblich. Dasselbe gilt auch für die Art und Weise der Nutzung eines bestimmten Angebots, das mit Einstellungen im Administratorenkonto und dem Abschluss einer Auftragsdatenbearbeitungsvereinbarung (ADV) bedeutend verbessert werden kann. Dies ist meist etwas aufwändig und bedingt eine sorgfältige Auseinandersetzung mit der technischen Funktionsweise des Dienstes sowie den dazugehörigen Vertragsbestimmungen. Unter den grösseren Videokonferenz-Diensten wird etwa Webex (von Cisco) als besonders sicher eingestuft. Datenschutzfreundliche Einstellungen sind auf jeden Fall vorzunehmen. Es empfiehlt sich, Regeln im Umgang zu definieren, z. B. keine besonderen Personendaten besprechen, keine Aufzeichnung von Gesprächen.

Verantwortlich:	Generalvikariat
Erstveröffentlichung:	01.03.2024
Zuletzt aktualisiert:	