Bischöfliches Gurker Ordinariat

Datenschutz

in der Katholischen Kirche in Kärnten und ihren Einrichtungen

Mai 2018, Version 1.0

Inhaltsverzeichnis

1 Kirchliche Datenschutzverordnung....2
2 Erläuterungen zum Datenschutz und zur Verwendung personenbezogener Daten....7
2.1 Einleitung....7
2.2 Datenschutz-Grundverordnung, Datenschutzgesetz, Kirchliche Datenschutzverordnung....7
2.2.1 Ziele....7
2.3 Datenschutz und Datensicherheit....7
2.3.1 Das Grundrecht auf Datenschutz....7
2.3.2 Recht auf Geheimhaltung personenbezogener Daten....7
2.4 Begriffsklärungen....8
2.4.1 Daten und Datenverwendung....8
2.4.2 Zustimmung und Information nach Artikel 13 DSGVO....9
2.4.3 Außenkommunikation....9
2.4.4 Datenschutz und Datensicherheit, technisch und organisatorisch....9
2.4.5 Social Media....10
2.4.6 Verpflichtungserklärung zum Datengeheimnis....11
2.4.7 Videoüberwachung kirchlicher denkmalgeschützter Gebäude....11
2.5. Neuaufnahme und Ergänzungen einer Datenverarbeitung....12
2.5.1 Datenschutzverantwortung in der Pfarre....12
2.6 Regelungen zum korrekten Umgang mit personenbezogenen Daten....13
2.6.1 Zugang zu personenbezogenen Daten....13
2.6.2 Einsicht in Matrikenbücher....13
2.7 Regelungen zur Übermittlung und Weitergabe von Daten, Veröffentlichungen....14
2.7.1 Datenweitergabe im kirchlichen Bereich (§ 6 kirchl. DS-VO)....14
2.7.2 Datenweitergabe an andere als kirchliche Einrichtungen (§ 7 kirchl. DS-VO)....14
2.7.3 Übergabe von Daten an einen Auftragsverarbeiter....14
2.7.4 Sammlung, Verarbeitung und Weitergabe von Daten, Beispiele....15
2.7.5 Schematismus....15
2.7.6 Weitergabe von Kirchenbeitragsdaten an pfarrliche Organe....16
2.7.7 Auskünfte an Dritte....16
2.7.8 Auskunft über eine Wohnadresse....16
2.7.9 Auskunft über Daten Verstorbener....16
2.7.10 Ahnenforschung....16
2.7.11 Bekanntgabe von Kirchenaustritten....16
2.7.12 Veröffentlichung von Bildern....16
2.7.13 Sonstige Veröffentlichungen im Pfarrblatt, Schaukasten, Internet....17
2.8 Sicherheitsmaßnahmen....17
2.8.1 Umgang mit Zugangscodes, Passwörtern, Token....17
2.8.2 Schutz der Daten vor unbefugten Zugriffen und Virenbefall....18
3 Checkliste zum Datenschutz....19

1 Kirchliche Datenschutzverordnung

Decretum Generale über den Datenschutz in der Katholischen Kirche in Österreich und ihren Einrichtungen (Kirchliche Datenschutzverordnung)

§ 1 Anwendungsbereich

(1) Dieses Dekret ist auf die Katholische Kirche in Österreich und alle ihre Einrichtungen anzuwenden, soweit diese auf Grund kirchenrechtlicher Bestimmungen eingerichtet sind und ihrem Bestande nach kirchenrechtlichen Vorschriften unterliegen. Diese Einrichtungen haben Rechtspersönlichkeit nach kanonischem Recht und nach staatlichem Recht oder sind von einer kanonischen Rechtsperson, welche auch Rechtspersönlichkeit des öffentlichen Rechts nach staatlichem Recht ist, umfasst.

(2) Dieses Dekret ist auf jene Rechtsträger nicht anzuwenden, welche ihrer tatsächlichen Geschäftsführung nach ausschließlich oder überwiegend kirchliche Zwecke verfolgen, aber nach der staatlichen Rechtsordnung eingerichtet sind und nur innerhalb dieser, nicht aber auch nach der kanonischen Rechtsordnung, Rechtspersönlichkeit genießen.

§ 2 Gegenstand des Datenschutzes im kirchlichen Bereich

(1) Der Schutz von personenbezogenen Daten stellt ein besonderes Anliegen der Katholischen Kirche in Österreich dar. In Einklang mit den in der Europäischen Union und in Österreich in Geltung stehenden Bestimmungen zum Datenschutz und in Umsetzung von Art. 91 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 („DSGVO“) enthält dieses Dekret Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten. Es schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.

(2) Gegenstand ist die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen (im Folgenden kurz als Daten“ bezeichnet).

(3) Unter personenbezogenen Daten sind alle Informationen zu verstehen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

(4) Die Verarbeitung von Daten unterliegt den geltenden datenschutzrechtlichen Bestimmungen und Vorgaben. Soweit besondere kirchliche, staatliche oder unionsrechtliche Rechtsvorschriften auf das Verarbeiten von Daten anzuwenden sind, gehen sie den Vorschriften dieses Dekretes vor.

(5) Die Verpflichtung zur Einhaltung des geistlichen Amtsgeheimnisses und dienstrechtlicher Schweigepflichten bleibt unberührt.

§ 3 Kirchliche Datenschutzkommission und Datenschutzbeauftragter gemäß DSGVO

(1) Zur Wahrung des Datenschutzes und zur Vertretung gegenüber den zuständigen staatlichen Behörden ist die Kirchliche Datenschutzkommission im Generalsekretariat der Österreichischen Bischofskonferenz eingerichtet.

(2) Die Kommission besteht aus drei Mitgliedern, von denen zwei, unter ihnen der Vorsitzende, von der Österreichischen Bischofskonferenz, das dritte von der Superiorenkonferenz der männlichen Ordensgemeinschaften Österreichs im Einvernehmen mit der Vereinigung der Frauenorden Österreichs ernannt werden.

(3) Die Kirchliche Datenschutzkommission wird namens der Katholischen Kirche in Österreich tätig. Sie ist berechtigt, sich eine Geschäftsordnung zu geben.

(4) Zur Wahrnehmung der Aufgaben iSd Art 39 DSGVO wird von der Österreichischen Bischofskonferenz der Datenschutzbeauftragte der Katholischen Kirche in Österreich ernannt. Die Ernennung bedarf der Einholung des vorherigen Einverständnisses der Superiorenkonferenz der männlichen Ordesgemeinschaften Österreichs sowie der Vereinigung der Frauenorden Österreichs.

Der Datenschutzbeauftragte ist bezüglich der Erfüllung seiner Aufgaben weisungsfrei.

(5) Die Aufgaben des Datenschutzbeauftragten ergeben sich insbesondere aus Art 39 DSGVO sowie den mit ihm dazu ergänzend getroffenen Vereinbarungen.

(6) Der Datenschutzbeauftragte und die für ihn tätigen Personen sind unbeschadet sonstiger Verschwiegenheitspflichten bei der Erfüllung der Aufgaben zur Geheimhaltung verpflichtet. Dies gilt insbesondere in Bezug auf die Identität betroffener Personen, die sich an den Datenschutzbeauftragten gewandt haben, sowie über Umstände, die Rückschlüsse auf diese Personen zulassen, es sei denn, es erfolgte eine ausdrückliche Entbindung von der Verschwiegenheit durch die betroffene Person. Der Datenschutzbeauftragte und die für ihn tätigen Personen dürfen die zugänglich gemachten Informationen ausschließlich für die Erfüllung der Aufgaben verwenden und sind auch nach Ende ihrer Tätigkeit zur Geheimhaltung verpflichtet.

§ 4 Die Katholische Kirche in Österreich und ihre Einrichtungen

(1) Für die Katholische Kirche in Österreich erfolgte die Registrierung im Datenverarbeitungsregister nach den Bestimmungen des Datenschutzgesetzes, BGBl. I 1999/165 in der zu diesem Zeitpunkt geltenden Fassung.

(2) Die Katholische Kirche in Österreich ist Verantwortliche des öffentlichen Bereiches 11 gemäß § 26 DSG idF Datenschutz-Anpassungsgesetz 2018. Sie und ihre Einrichtungen werden im öffentlichen Bereich tätig. Die Katholische Kirche in Österreich genießt öffentlich-rechtliche Stellung gemäß Artikel II Konkordat vom 5. Juni 1933 zwischen dem Heiligen Stuhl und der Republik Österreich, BGBl II Nr 2/1934. Sie und ihre Einrichtungen sind öffentliche Stellen iSd der DSGVO und des DSG idF Datenschutz-Anpassungsgesetz 2018.

(3) Es wird ein Verzeichnis von Verarbeitungstätigkeiten im Sinne des Art 30 DSGVO geführt. Das Verzeichnis wird bei der Kirchlichen Datenschutzkommission zentral verwaltet und ist nicht öffentlich zugänglich.

(4) Alle kirchlichen Einrichtungen, welche Daten verarbeiten, haben diese Verarbeitung dem Datenschutzbeauftragten der Katholischen Kirche in Österreich zu melden. Die Aufnahme der Verarbeitung ist erst dann zulässig, wenn seitens der Kirchlichen Datenschutzkommission die Registernummer samt Subnummer mitgeteilt ist und die Verarbeitung im Verzeichnis von Verarbeitungstätigkeiten gemäß Art 30 DSGVO eingetragen wurde. Anlässlich der Anführung von Registernummern ist von kirchlichen Einrichtungen in Klammer auch die jeweilige Subnummer anzuführen.

(5) Das Generalsekretariat der Österreichischen Bischofskonferenz steht der Kirchlichen Datenschutzkommission für die Erledigung ihrer Aufgaben zur Verfügung.

§ 5 Rechte betroffener Personen

(1) Die Rechte betroffener Personen ergeben sich aus Kapitel III DSGVO, den Bestimmungen des DSG in der jeweils gültigen Fassung, dies jeweils iZm den Bestimmungen dieses Dekretes.

(2) Die Bereichs-Datenschutzreferenten und die Datenschutzzuständigen der Einrichtungen nehmen die Verpflichtungen der Katholischen Kirche in Österreich wahr, die sich aus den Rechten betroffener Personen in ihrem Zuständigkeitsbereich (vgl § 9) ergeben. Die Erledigungen ergehen im Namen der Katholischen Kirche in Österreich.

§ 6 Datenweitergabe im kirchlichen Bereich

(1) Die Weitergabe von Daten an eine andere kirchliche Einrichtung ist zulässig, wenn sie zur Erfüllung des kirchlichen Auftrages erforderlich ist, welche entweder der weitergebenden Einrichtung oder der empfangenden Einrichtung obliegt.

(2) Unterliegen die weiterzugebenden Daten einem kirchlichen Dienst- oder Amtsgeheimnis, so ist die Weitergabe nur dann zulässig, wenn die empfangende kirchliche Einrichtung die Daten zur Erfüllung des gleichen Zweckes benötigt, für den sie die weiterleitende kirchliche Einrichtung ermittelt hat.

(3) Das Siegel der geistlichen Amtsverschwiegenheit und staatliche Berufsgeheimnisse sind jedenfalls zu wahren. Daten, die diesen Geheimnissen unterliegen, dürfen nur mit schriftlicher Zustimmung des Betroffenen weitergegeben werden, soweit anzuwendende Rechtsvorschriften die Weitergabe nicht absolut untersagen.

§ 7 Datenübermittlung an nicht-kirchliche Empfänger

(1) Die Weitergabe von Daten an andere als kirchliche Einrichtungen oder den Betroffenen ist nur unter Einhaltung der gesetzlichen Voraussetzungen, insbesondere jener nach Art 6 DSGVO, zulässig.

(2) Ist die Übermittlung von Daten nicht im Verzeichnis der Verarbeitungstätigkeiten (laut Artikel 30 DSGVO) erfasst, gehört die Übermittlung aber zum berechtigten Zweck 12 der kirchlichen Einrichtung oder ist die Übermittlung zur Wahrung überwiegender Interessen eines Dritten notwendig, so ist deren Genehmigung bei der Kirchlichen Datenschutzkommission zu beantragen.

(3) Werden Daten an Dritte übermittelt oder überlassen, so ist das von der Katholischen Kirche in Österreich geforderte und gesetzlich vorgegebene Datenschutzniveau weiterhin sicherzustellen. Dafür sind mit den Empfängern entsprechende Vereinbarungen und Regelungen zu treffen und deren Einhaltung gegebenenfalls auch zu auditieren und zu prüfen.

§ 8 Bereichs-Datenschutzreferenten und Datenschutzzuständige der Einrichtungen

(1) Jeder Diözesanbischof, der Militärbischof, der Territorialabt von Wettingen-Mehrerau sowie die Superiorenkonferenz der männlichen Ordensgemeinschaften Österreichs und die Vereinigung der Frauenorden Österreichs ernennen für ihren jeweiligen Bereich einen Bereichs-Datenschutzreferenten.

(2) Die Bereichs-Datenschutzreferenten unterstützen den unter § 3 (4) genannten Datenschutzbeauftragten der Katholischen Kirche in Österreich bei der Erfüllung seiner Aufgaben.

(3) Ebenso unterstützen die Bereichs-Datenschutzreferenten die unter § 3 (1) genannte Kirchliche Datenschutzkommission bei der Erfüllung ihrer Aufgaben, haben in dieser Funktion deren Empfehlungen und Richtlinien zu beachten und werden in dieser Funktion nach außen namens der Katholischen Kirche in Österreich tätig. Die Rechte der zuständigen Ordinarien bleiben unberührt.

(4) Betrifft das Tätigwerden des Bereichs-Datenschutzreferenten grundsätzliche Rechts- oder Sachfragen, so ist rechtzeitig der Datenschutzbeauftragte der Katholischen Kirche in Österreich einzubinden und die Zustimmung der Kirchlichen Datenschutzkommission einzuholen.

(5) Darüber hinaus ist für jede kirchliche Einrichtung von deren Leitung eine Person zu bestimmen, welche für die Einhaltung des Datenschutzes Sorge trägt und die damit verbundenen operativen Aufgaben erfüllt („Datenschutzzuständiger der Einrichtung"). Mehrere kirchliche Einrichtungen können auch einen gemeinsamen Zuständigen benennen. Diese Person ist in dieser Funktion an die Empfehlungen und Richtlinien des für sie zuständigen Bereichs-Datenschutzreferenten gebunden und kann diesen zu Rate ziehen. Außerdem hat diese Person in dieser Funktion ebenfalls die Empfehlungen und Richtlinien der Kirchlichen Datenschutzkommission zu beachten.

Die Rechte der zuständigen Ordinarien bleiben unberührt.

(6) Die Datenschutzreferenten berichten den für sie zuständigen Ordinarien, denen sie dienstrechtlich unterstehen, regelmäßig über ihre Tätigkeit.

§ 9 Datengeheimnis

(1) Alle Personen, denen iZm ihrer Tätigkeit für die Katholische Kirche in Österreich und ihren Einrichtungen Daten anvertraut sind oder zugänglich gemacht werden, gleich, ob dies auf Grund eines Dienstverhältnisses oder einer anderen Leistung für die kirchliche Einrichtung erfolgt, haben das Datengeheimnis iSd § 6 DSG idF Datenschutz-Anpassungsgesetz 2018 zu wahren.

Diese Personen sind vor Aufnahme ihrer Tätigkeit zur Einhaltung des Datengeheimnisses, dies auch nach Beendigung ihrer Tätigkeit, ausdrücklich vertraglich zu verpflichten.

(2) Daten dürfen nur aufgrund einer ausdrücklichen Anordnung des zuständigen dienstlichen Vorgesetzten verarbeitet werden.

§ 10 Datensicherheit

Jede kirchliche Einrichtung, welche Daten verarbeitet, hat ausreichende Datensicherheitsmaßnahmen, insbesondere jene gemäß Art 24, 25 und 32 DSGVO sowie § 54 DSG idF Datenschutz-Anpassungsgesetz 2018, zu treffen. Der Datenschutzbeauftragte der Katholischen Kirche in Österreich hat über die Durchführung ausreichender Datensicherheitsmaßnahmen zu wachen.

§ 11 Bildverarbeitung

Für die Zulässigkeit der Bildverarbeitung durch die Katholische Kirche in Österreich und ihre Einrichtungen gilt § 30 DSG idF Datenschutz-Anpassungsgesetz 2018. Nähere Bestimmungen werden durch die Kirchliche Datenschutzkommission erlassen.

§ 12 Inkrafttreten und Änderung

(1) Dieses Dekret wurde von der Österreichischen Bischofskonferenz in ihrer Herbstvollversammlung vom 6. bis 9. November 2017 beschlossen und tritt am 25. Mai 2018 in Kraft. Zum gleichen Zeitpunkt tritt die im Amtsblatt Nr. 52 der Österreichischen Bischofskonferenz vom 15. September 2010 veröffentlichte Kirchliche Datenschutzverordnung außer Kraft.

(2) Zur Abänderung oder Aufhebung dieses Dekretes ist ein Beschluss der Österreichischen Bischofskonferenz und die Veröffentlichung im Amtsblatt erforderlich. Der Beschluss ist seitens der Österreichischen Bischofskonferenz nach den Normen des can. 455 § 4 CIC 1983 zu fassen.

Die Diözesanbischöfe haben dem vorliegenden Decretum Generale über den Datenschutz in der Katholischen Kirche in Österreich und ihren Einrichtungen (Kirchliche Datenschutzverordnung) einzeln ihre Zustimmung im Sinne can. 455 § 4 CIC 1983 gegeben.

2 Erläuterungen zum Datenschutz und zur Verwendung personenbezogener Daten

2.1 Einleitung

Der Schutz der Vertraulichkeit und die Integrität der Daten haben für die Diözese Gurk, ihre Pfarren und sonstigen Einrichtungen einen hohen Stellenwert. Die Beachtung der Datenschutzbestimmungen ist deshalb besonders wichtig. Die Verletzung des Datengeheimnisses oder der unberechtigte Zugriff Dritter auf Daten verletzt die Privatsphäre und kann für die Diözese, die Pfarren und verschiedenen Einrichtungen sowie den Einzelnen großen materiellen und auch immateriellen Schaden zur Folge haben.

2.2 Datenschutz-Grundverordnung, Datenschutzgesetz, Kirchliche Datenschutzverordnung

Rechtliche Grundlagen sind die EU-Datenschutz-Grundverordnung (DSGVO) und das Datenschutzgesetz (DSG) in der geltenden Fassung. Zur konkreten Anwendung erließ die Österreichische Bischofskonferenz die Kirchliche Datenschutzverordnung, kundgemacht im Amtsblatt der Bischofskonferenz Nr. 74 vom 01.01.2018.

2.2.1 Ziele

Ein wesentliches Ziel dieser Verordnung war es, Regelungen zum korrekten Umgang mit personenbezogenen und allen anderen Daten zu schaffen, die im Rahmen des dienstlichen Auftrages erfasst und verarbeitet werden. Zusätzlich wurden Überlegungen zur Arbeitsgestaltung im Umgang mit EDV, Internet, Intranet und den Daten angestellt und durch strenge Bestimmungen soll die Datensicherheit gewährleistet werden.

2.3 Datenschutz und Datensicherheit

2.3.1 Das Grundrecht auf Datenschutz

Jeder hat Anspruch auf Achtung seiner Privatsphäre. Durch den Einsatz der EDV ist es leicht möglich Daten zu sammeln, abzurufen und zu verknüpfen. Das Datenschutzrecht regelt den Anspruch jeder Person auf Geheimhaltung der sie betreffenden personenbezogenen Daten, soweit sie daran ein schutzwürdiges Interesse hat. Die Geheimhaltungspflicht umfasst alle personenbezogenen Daten, unabhängig von einer automatisationsunterstützten Verarbeitung.

Jedermann ist daher verpflichtet, personenbezogene Daten Dritter (natürlicher und juristischer Personen, sowie Personengesellschaften) geheim zu halten. Ein schutzwürdiges Interesse ist grundsätzlich anzunehmen. Ein solches liegt jedoch nicht vor für Daten in allgemein zugänglichen Quellen, wie z.B. im Telefon- oder Firmenbuch. Beispiele für personenbezogene Daten sind der Name, die Adresse, das Geburtsdatum (sofern es nicht in öffentlich zugänglichen Quellen ersichtlich ist), der Beruf, die Bankverbindung, die Einkommensverhältnisse, Zahlungen, Matrikendaten, etc..

In ganz besonderem Maße als „sensible Daten“ sind die rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit sowie das Sexualleben geschützt. Außer dem röm.kath. Religionsbekenntnis dürfen sensible Daten grundsätzlich nicht gespeichert werden.

2.3.2 Recht auf Geheimhaltung personenbezogener Daten

Betroffen ist bereits die Ermittlung solcher Daten, sowie erst recht die Speicherung, Verwendung und Weitergabe. Erst nach einer Prüfung, ob eine Ausnahme von der Geheimhaltepflicht vorliegt, dürfen die Daten verarbeitet werden. Ausnahmen können bestehen, wenn

Daten öffentlich zugänglich sind, eine Zustimmung des Betroffenen vorliegt oder eine gesetzliche Verpflichtung bzw. die Erfüllung von Verpflichtungen gegenüber Mitgliedern gegeben ist.

Eine wichtige Rechtfertigung ist auch das Vorliegen lebenswichtiger Interessen des Betroffenen oder überwiegend berechtigter Interessen des Datenanwenders. Diese liegen z.B. vor, wenn die Daten zur Vertragserfüllung notwendig sind. Folgende Punkte sich zu beachten:

- Zweckbindungsgrundsatz
  Daten dürfen nur für (vorher) festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und verwendet werden. Das wahllose Sammeln von Daten und spätere Auswerten je nach Bedarf ist also nicht erlaubt, ebenso das spätere Verwenden für einen anderen Zweck, wobei die Zwecke eher eng zu interpretieren sind.

- Wesentlichkeitsgrundsatz
  Daten dürfen nur gesammelt und verwendet werden, soweit sie für den jeweiligen Zweck auch wesentlich sind und nicht darüber hinausgehen.

- Grundsatz der sachlichen Richtigkeit und Aktualität
  Daten müssen (nur) soweit aktuell gehalten werden, als dies für den Zweck notwendig ist.

- Grundsatz der Datenlöschung
  Die Verwendung/Aufbewahrung ist nur solange erlaubt, als dies für die Erreichung der Zwecke erforderlich ist.

- Rechtmäßigkeit / Treu und Glauben
  Rechtmäßigkeit meint die Einhaltung aller Gesetze. Treu und Glauben ist ähnlich zu verstehen wie Einhaltung der guten Sitten und des redlichen Verkehrs und verbietet in erster Linie die Irreführung des Betroffenen über die Umstände der Datenanwendung und seine Rechte.

- Relevante Bestimmungen
  Es finden die Bestimmungen der Datenschutz-Grundverordnung, des Datenschutzgesetzes, des Arbeitsverfassungsgesetzes und anderer relevanter Gesetze Anwendung.

Für die Gewährleistung des Datenschutzes, sowohl für die personenbezogenen Daten der DienstnehmerInnen, als auch der dritter Personen (KundInnen/KlientInnen), ist nach Maßgabe des Datenschutzgesetzes der Dienstgeber verantwortlich. Pflichten der DienstnehmerInnen zur Wahrung des Datengeheimnisses nach Maßgabe des § 6 Datenschutzgesetz bleiben davon unberührt. Die Übermittlung von personenbezogenen Daten an andere RechtsträgerInnen ist immer auf das berechtigte bzw. rechtliche Interesse hin zu überprüfen.

2.4 Begriffsklärungen

2.4.1 Daten und Datenverwendung

Daten sind Angaben über Personen, deren Identität bestimmt oder bestimmbar ist (= „normale“ personenbezogene Daten). Besonders schutzwürdig sind die sensiblen Daten. Anonyme Daten gelten hingegen nicht als personenbezogene Daten und werden daher auch nicht geschützt. Unter Datenverwendung versteht man sowohl das Verarbeiten (Ermitteln, Speichern, Überlassen etc.) als auch das Übermitteln (an andere Empfänger) von Daten.

Im Datenschutzgesetz gibt es drei Akteure. Der Betroffene ist jene Person, dessen Daten verwendet werden, der Auftraggeber ist jene Person oder Stelle, die die Entscheidung

getroffen hat, Daten für einen bestimmten Zweck zu verarbeiten und der Auftragsverarbeiter verwendet Daten, die ihm zur Herstellung eines aufgetragenen Werkes überlassen wurden.

2.4.2 Zustimmung und Information nach Artikel 13 DSGVO

Bei der Zustimmung handelt es sich um eine gültige, ohne Zwang abgegebene Willenserklärung des Betroffenen, dass er in Kenntnis der Sachlage in die Verwendung seiner Daten einwilligt.

Jede rechtswirksame Zustimmung bedarf der genauen taxativen Bezeichnung der Datenarten (Name, Alter, Adresse, Einkommen), die verwendet werden sollen, einer ausreichenden Information des Betroffenen über den Zweck der Übermittlung, die Benennung der Übermittlungsempfänger unter Angabe des Namens, der Firma oder der Behördenbezeichnung, sowie einen ausdrücklichen Hinweis auf einen jederzeit möglichen Widerruf der Zustimmung.

Werden personenbezogene Daten an externe Auftragsverarbeiter übermittelt (z.B. Druckerei) ist schriftlich eine Vereinbarung zu schließen.

Bei jeder Neuerhebung von Daten (z.B. bei der Anmeldung zur Taufe, zu einer Hochzeit, zur Firmung etc.) ist allen Betroffenen das Formular "Informationsschreiben gemäß Artikel 13 DSGVO" zu übergeben

2.4.3 Außenkommunikation

Gemäß § 107 TelKG (Telekommunikationsgesetz) ist die „Direktwerbung“ (Begriff sehr weit auszulegen) per E-Mail oder SMS an Verbraucher nur bei vorheriger Einwilligung und Hinweis auf die Widerrufsmöglichkeit des Empfängers gestattet. Das Gleiche gilt für die telefonische Kontaktaufnahme, welche vom Unternehmen ausgeht. Zulässig ist die Verwendung der Kontaktdaten jedoch, wenn sie im Rahmen einer konkreten Geschäftsbeziehung bekanntgegeben wurden und für diese genutzt werden.

Ein Hinweis auf die Widerrufsmöglichkeit ist per SMS aber schwer möglich. Massen-SMS an mehr als 50 Personen sind grundsätzlich unzulässig. Verstöße gegen § 107 TelKG werden mit empfindlichen Verwaltungsstrafen geahndet. Postsendungen mit Briefpost fallen nicht unter das Verbot des § 107 TelKG. Die Übertragung personenbezogener Daten auf bewegliche Speichermedien (externe Datenträger wie USB – Sticks, CDs usw.) ist auf das berechtigte bzw. rechtliche Interesse zu überprüfen.

2.4.4 Datenschutz und Datensicherheit, technisch und organisatorisch

Hier geht es darum, Daten sowie Hard- und Software vor unberechtigtem Zugriff, Missbrauch, Verlust und Zerstörung zu schützen. Die Daten sind vor unberechtigtem Lesen, Verändern, Löschen und Kopieren zu schützen. Dies gilt auch für Schriftstücke (Akte, Briefe, Listen ect.), die Matrikenbücher und Datenträger, auch beim Transport und elektronischer Übertragung. Im Wesentlichen ist bei der technischen Bearbeitung von Daten Folgendes zu beachten:

- Daten sind vor dem Entsorgen unleserlich zu machen oder es ist dies einem Fachmann zu übertragen.
- Der Zutritt und Zugriff zu den EDV-Anlagen und zu den Datenträgern ist zu regeln und zu kontrollieren. Die berechtigten Personen sind festzulegen.
- Der Datenzugriff durch Benutzer ist gut abzusichern.
- Benutzererkennungen sind regelmäßig zu ändern.
- Die Bildschirmarbeitsplätze sind bei Abwesenheit und laufendem System zu sichern.

- Interne Netze sind gegen Zugriffe von außen zu schützen.

- Es ist ausschließlich der hausinterne Cloud-Dienst zu verwenden, der alle Daten nur auf diözesanen Servern speichert, Die Speicherung in anderen Cloud-Diensten ist verboten. Alle Regelungen zum Schutz personenbezogener Daten gelten auch in diesem Umfeld.

- Mobile IT-Endgeräte müssen unter ständiger Kontrolle der berechtigten Person(en) bleiben, d.h. Sie dürfen nicht unbeaufsichtigt gelassen werden. Sie dürfen auch nicht im Auto aufbewahrt werden. Notebooks müssen mit einer Festplattenverschlüsselung versehen werden. Der Verlust oder Diebstahl eines IT-Endgerätes muss unverzüglich der IT-Abteilung der Diözese Gurk gemeldet werden.

- Synchronisation mobiler IT-Endgeräte
  Sofern eine Synchronisation von E-Mails, Kontakten, Kalendern und Aufgaben mit dem diözesanen Server erfolgt, gelten bei Verlust eines Diensthandys folgende Regeln:
  - Verlust sofort bei der IT-Abteilung melden.
  - Es erfolgt umgehend die Sperrung der SIM-Karte durch die IT-Abteilung.
  - Das Handy wird durch die IT-Abteilung auf Werkseinstellungen zurückgesetzt.
  - Sämtliche Daten (Kontaktdaten, Fotos, Apps, Mails, Kalenderdaten, Accounts, etc.) am Handy werden gelöscht.

- Es ist darauf zu achten, dass alle Schriftstücke, die personenbezogene Daten enthalten, unter Verschluss gehalten werden und die gesetzlich vorgegebenen Aufbewahrungspflichten (3 Jahre) für Protokoll- und Dokumentationsdaten beachtet werden.

- Ein Schlüsselverzeichnis ist zu führen.

- Für die Aufbewahrung von Datenträgern ist ein schriftlicher Plan zu erstellen.

- Die Mitarbeiter sind über Ihre Pflichten zu belehren.

- Die Speicherung personenbezogener und sensibler Daten auf private PCs ist generell untersagt.

- Alle Briefe, Faxnachrichten, Dokumente, Ordner, Schriftstücke und E-Mails, bei welchen aus der Adresse und/oder dem Betreff eindeutig ersichtlich ist, dass sie privaten Charakter haben, unterliegen wie persönlich adressierte Briefe dem Briefgeheimnis.

- Private Daten sind in eigenen Ordnern bzw. Verzeichnissen, die als „privat“ zu kennzeichnen sind, abzulegen. In privaten Ordnern dürfen keine Daten abgelegt werden, die dienstlichen Charakter haben und im Vertretungs- bzw. Krisenfall von anderen Personen benötigt werden.

- Die DienstnehmerInnen nehmen durch ihre Unterschrift die Datenschutzverpflichtungserklärung zur Kenntnis und verpflichten sich damit zur Einhaltung aller einschlägigen Bestimmungen. Die DienstgeberIn ihrerseits ist verpflichtet, für eine ausreichende Qualifizierung der DienstnehmerInnen zu den Datenschutzbestimmungen zu sorgen.

2.4.5 Social Media

Die Nutzung von Social Media zu dienstlichen Zwecken ist nur auf Basis der vorliegenden Richtlinie erlaubt:

- Nutzer/innen halten sich an geltendes Recht und berücksichtigen bei allen Veröffentlichungen insbesondere Persönlichkeitsrechte.

- Vertrauliche und interne Informationen werden nicht kommuniziert.

- Nutzer/innen treten ausschließlich mit eigenem Namen auf, geben Funktion an und sorgen für eine Kontaktmöglichkeit.

- Nutzer/innen akzeptieren die Meinungsfreiheit in Social Media, veröffentlichen keine beleidigenden oder diskriminierenden Inhalte und üben öffentlich keine Kritik an der Diözese und deren Partnern, Kunden und Lieferanten.

2.4.6 Verpflichtungserklärung zum Datengeheimnis

Personen, denen berufsmäßig oder ehrenamtlich personenbezogene Daten anvertraut sind, oder zugänglich gemacht werden, sind vor Aufnahme ihrer Tätigkeit zur Einhaltung des Datengeheimnisses ausdrücklich vertraglich zu verpflichten.

Wird ein Dienstvertrag über das Personalreferat der Diözese Gurk abgeschlossen, holt dieses die Verpflichtungserklärung ein. Für Priester und Diakone ist das Ordinariat zuständig. Bei ehrenamtlichen Mitarbeitern obliegt es dem Pfarrvorsteher, für den der Mitarbeiter tätig ist, diese Erklärung einzuholen.

Ein Exemplar der Verpflichtungserklärung ist im Personalakt bzw. im Pfarrarchiv abzulegen. Ein Exemplar der Verpflichtungserklärung und ein Informationsblatt ist auszuhändigen; auf Wunsch auch das Datenschutzgesetz und die kirchliche Datenschutzverordnung.

Die Verpflichtung zum Datengeheimnis besteht auch nach Ende des Dienstverhältnisses bzw. der ehrenamtlichen Tätigkeit weiter. Verstöße gegen diese Pflicht und andere Datenschutzbestimmungen können Geld- oder Freiheitsstrafen, arbeits- bzw. dienstrechtliche Folgen (z.B. Entlassung bei Dienstnehmern), sowie Schadenersatzansprüche des Geschädigten nach sich ziehen.

Daneben gelten andere Geheimhaltungsvorschriften, wie die Verpflichtung zur Wahrung des Dienstgeheimnisses nach der Dienst- und Besoldungsordnung der Diözese Gurk oder die Verpflichtung zum Amtsgeheimnis für die Pfarrgemeinderäte nach der Pfarrgemeinderatsordnung. Wenn personenbezogene Daten von diözesanen Stellen an Dritte (ehrenamtliche MitarbeiterInnen, PraktikantInnen u.ä.) zur Bearbeitung, Verwaltung usw. weitergegeben werden, unterliegen diese den gleichen Bestimmungen.

2.4.7 Videoüberwachung kirchlicher denkmalgeschützter Gebäude

<u>Wie/Was/Wann/Wer darf videoüberwacht werden?</u>

WIE: Bereits vor der geplanten Inbetriebnahme einer Videoüberwachungsanlage sind die Bauabteilung und der diözesane Datenschutzbeauftragte mit genauen Angaben zum Vorhaben zu informieren. Alle bereits aktuell bestehenden Videoüberwachungsanlagen müssen nachgemeldet werden.

WAS: Denkmalgeschützte kirchliche Gebäude im Eingangsbereich und besonders schützenswerte Gegenstände, welche sich im Innenraum dieser Gebäude befinden.

WANN: Die Videoüberwachung kann rund um die Uhr erfolgen.

WER: Alle Personen, welche das Gebäude betreten bzw. verlassen, sowie jene Personen, welche sich den überwachten Gegenständen nähern. Eine Verwendung der Überwachung zur Kontrolle allfälliger Anwesenheit oder Nichtanwesenheit, insbesondere bei Gottesdiensten oder Veranstaltungen, oder aber zur Kontrolle von Mitarbeitern, entspricht nicht dem Zweck der Videoüberwachung und ist daher unzulässig.

<u>Wozu dient die Videoüberwachung?</u>

Die Videoüberwachung dient ausschließlich dem Schutz des Eigentums und der besonders schützenswerten Gegenstände in kirchlichen denkmalgeschützten Gebäuden; sowie der Vorbeugung oder Aufklärung strafrechtlicher Handlungen.

Wozu ist der videoüberwachende kirchliche Eigentümer verpflichtet?

Findet eine Videoüberwachung statt, so ist dies mit einem Hinweis (Schild) anzuzeigen und zwar so, dass ein potenzieller Besucher die Möglichkeit hat, videoüberwachte Bereiche nicht zu betreten. Auf dem Hinweis ist der Auftraggeber der Videoüberwachung (z.B. Pfarre) anzuführen.

Zulässigkeit der Auswertung der Daten

Die Daten dürfen ausgewertet werden, wenn ein begründeter Verdacht auf das Vorliegen einer strafbaren Handlung durch die videoüberwachte Person besteht. Ein automatisierter Abgleich mit anderen Bildaufzeichnungen oder ein Durchsuchen der aufgezeichneten Daten nach sensiblen Auswahlkriterien, ist unzulässig.

Zulässigkeit der Weitergabe von Daten

Bei begründetem Verdacht sind die Daten an Sicherheitsbehörden bzw. Strafverfolgungsbehörden (Staatsanwaltschaft, Gerichte) zu übermitteln. Außerdem ist der Datenschutzbeauftragte der Diözese zu verständigen. Jede weitere Übermittlung, insbesondere eine Veröffentlichung der Daten, ist unzulässig.

Protokollierungspflicht

Jede Verwendung der Daten ist zu protokollieren. Sind sonstige Videoüberwachungen beabsichtigt, ist vorher mit der Rechtsabteilung und dem diözesanen Datenschutzbeauftragten Rücksprache zu halten.

2.5. Neuaufnahme und Ergänzungen einer Datenverarbeitung

Die Notwendigkeit einer Neuanmeldung bzw. der Erweiterung einer bestehenden Meldung besteht,

- wenn ein zusätzlicher Verarbeitungszweck hinzukommt, oder
- bei einer bestehenden Verarbeitung zusätzliche Daten erforderlich sind, oder
- zusätzliche Übermittlungsempfänger notwendig sind.

In diesem Fall ist über den Datenschutzreferenten der Diözese Gurk ein Antrag einzubringen. Dieser hat bei einer Neuanwendung zu enthalten:

- den Zweck der automatisationsunterstützten Datenverarbeitung
- die zu verarbeitenden Daten
- welche Daten an andere als kirchliche Einrichtungen weitergegeben werden dürfen
- an welche Behörden/Einrichtungen diese Daten weitergegeben werden dürfen.

Bei einer Ergänzung sind die Veränderungen gegenüber der bestehenden Anwendung anzuführen.

2.5.1 Datenschutzverantwortung in der Pfarre

In der Diözese Gurk ist jede Pfarre als Auftraggeber für Datenverarbeitungen eingerichtet. Damit bildet jede Pfarre einen eigenen Datenschutzverantwortungsbereich. Datenschutzverantwortlicher (Datenschutzzuständiger der Einrichtung) ist der jeweilige Pfarrvorsteher (sofern er nicht eine andere Person ausdrücklich und schriftlich dazu bestimmt hat), er hat dafür zu sorgen, dass alle Maßnahmen zur Gewährleistung des Datenschutzes und der Datensicherheit getroffen werden.

Ist eine Pfarre nicht besetzt, so werden diese Agenden vom zuständigen Dechant wahrgenommen. Rektoren, die personenbezogene Daten verwenden, sind für Ihren Bereich zuständig.

2.6 Regelungen zum korrekten Umgang mit personenbezogenen Daten

Alle Daten, die im Rahmen des dienstlichen Auftrages erstellt, bearbeitet, verwaltet und gespeichert werden, sind Eigentum der Diözese Gurk. Bei einem Wechsel des Arbeitsplatzes oder bei Kündigung dürfen diese Daten keinesfalls gelöscht, mittels E-Mail an private Adressen gesandt oder auf beweglichen Speichermedien mitgenommen werden.

Alle im Rahmen des Dienstes erarbeiteten Unterlagen, betriebliche Konzepte, Projektunterlagen, Daten etc. sind ordnungsgemäß zu speichern / abzulegen und der/dem unmittelbar Vorgesetzten zu übergeben. Private Notizen, Mitschriften oder Unterlagen dürfen gelöscht bzw. mitgenommen werden. Dateien und Ordner, die als privat gekennzeichnet sind und nach dem Ausscheiden der betreffenden Person aus dem diözesanen Dienst noch vorhanden sind, sind von der Abteilung für Datenverarbeitung zu löschen.

2.6.1 Zugang zu personenbezogenen Daten

Der Zugang zu personenbezogenen Daten ist beschränkt auf:

- diözesane DienstnehmerInnen
- Pfarrvorsteher, Kapläne, Diakone
- bei der Pfarre angestellte Pastoralassistenten/innen und Pfarrsekretäre/innen
- ehrenamtlich Tätige, die vom Ordinariat mit einer Funktion betraut wurden (z.B. Pfarrgemeinderäte; Beitragsberater jedoch beschränkt auf Ausdrucke von Kirchenbeitragsdaten)
- ehrenamtlich Tätige, die vom Pfarrer mit einer Funktion betraut wurden (z.B. ehrenamtliche Pfarrsekretär/in); die förmliche Bestellung mit Bestellungsdekret ist erforderlich. Diese ist jedenfalls notwendig, wenn ein Zugang zu EDV-Daten oder Matrikendaten besteht. Die Bestellung ist zu befristen, und zwar längstens bis zum Ende der Funktionsperiode für die Pfarrgemeinderäte. Verlängerungen sind möglich. Das Mindestalter beträgt 16 Jahre.
- Andere Personen, die in der Pfarre ehrenamtlich tätig sind, jedoch beschränkt auf Ausdrucke bzw. Listen von Daten für Ihren Tätigkeitsbereich (z.B. Geburtstagslisten).

Der Zugang zu Kirchenbeitragsdaten erfolgt ausschließlich gemäß § 4 Kirchenbeitragsordnung (Betrauung durch den Diözesanbischof mit den Aufgaben der Kirchenbeitragstelle). Es dürfen nur die oben angeführten Personen, sowie ehrenamtliche PfarrsekretärInnen befasst werden. Jegliche Auskunftswünsche von Dritten über ihre gespeicherten Daten sind im Amtsweg an die/den Datenschutzbeauftragte(n) weiter zu leiten und von dieser/diesem zu bearbeiten.

Jeder Katholik hat grundsätzlich den Anspruch darauf, dass unrichtige Daten oder zu Unrecht gespeicherte Daten aus eigenem oder auf begründetem Antrag richtig gestellt bzw. gelöscht werden.

2.6.2 Einsicht in Matrikenbücher

Die Matrikendaten unterliegen dem Datenschutz. Beim Recht auf Einsicht und Ausstellung von Urkunden bei Altmatriken bis 1938 kommt das Personenstandsgesetz 2013 zur Anwendung. Das Recht auf Einsicht und Ausstellung von Urkunden haben:

- Personen, auf die sich die Eintragung bezieht
- Personen, deren Personenstand durch die Eintragung berührt wird; dies sind bei den Matriken bis 1938 jedenfalls der Ehegatte, die Vorfahren und Nachkommen

- ab 1939 Eltern für ihre noch nicht volljährigen Kinder, der Ehegatte in Bezug auf Eintragungen in das Ehebuch und Kinder in Bezug auf die Eintragungen Ihrer Eltern und weiteren Vorfahren.
- Personen, die ein rechtliches Interesse glaubhaft machen, soweit kein überwiegendes schutzwürdiges Interesse der Personen, auf die sich die Eintragung bezieht, entgegensteht.
- Behörden und Körperschaften des öffentlichen Rechtes im Rahmen der Vollziehung der Gesetze
- Bei einer Inkognito-Adoption besteht dieses Recht nur für die Adoptiveltern und das Adoptivkind ab 14 Jahren.

Die Berechtigung muss sich aus einem vorgelegten urkundlichen Dokument ergeben (Geburtsurkunde, Taufschein, amtlicher Lichtbildausweis). Einschränkungen gelten nach 100 Jahren seit der Eintragung der Geburt (sofern die Eintragung nicht eine lebende Person betrifft) bzw. 75 Jahren seit der Eintragung der Eheschließung (30 Jahre ab Eintragung des Todes) als aufgehoben. Ahnen- und Familienforschung ist in diesem Rahmen zulässig. Auf die Möglichkeit der Einsichtnahme auf der Internetplattform http://www.matricula-online.eu wird verwiesen.

2.7 Regelungen zur Übermittlung und Weitergabe von Daten, Veröffentlichungen

2.7.1 Datenweitergabe im kirchlichen Bereich (§ 6 kirchl. DS-VO)

Kirchliche Einrichtungen dürfen automatisationsunterstützt verarbeitete Daten untereinander nur dann weitergeben, wenn dies zur Erfüllung des kirchlichen Auftrages erforderlich ist, welcher entweder der weitergebenden Einrichtung oder der empfangenden Einrichtung obliegt.

Unterliegen die weiterzugebenden Daten einem kirchlichen Dienst- oder Amtsgeheimnis, so ist die Weitergabe nur dann zulässig, wenn die empfangende kirchliche Einrichtung die Daten zur Erfüllung des gleichen Zweckes benötigt, für den sie die weiterleitende kirchliche Einrichtung ermittelt hat.

Ob ein kirchliches Dienst- oder Amtsgeheimnis vorliegt, ist aufgrund der geltenden kirchenrechtlichen Normen im Einzelfall zu prüfen. Beispiele sind etwa die Vorschrift zur Wahrung des Dienstgeheimnisses in der Dienst- und Besoldungsordnung der Diözese Gurk und die Verpflichtung zum Amtsgeheimnis für die Pfarrgemeinderäte nach der Pfarrgemeinderatsordnung.

2.7.2 Datenweitergabe an andere als kirchliche Einrichtungen (§ 7 kirchl. DS-VO)

Die Weitergabe von Daten an nichtkirchliche Einrichtungen ist unter Einhaltung der gesetzlichen Voraussetzungen nur dann erlaubt, wenn diese Übermittlung im Verzeichnis der Verarbeitungstätigkeit erfasst ist oder der Betroffene der Datenübermittlung schriftlich zugestimmt hat. Eine Übermittlung darf nur im erforderlichen Ausmaß erfolgen. Erfolgt mit Zustimmung des Betroffenen eine Übermittlung, die nicht erfasst ist, so muss diese dokumentiert werden.

2.7.3 Übergabe von Daten an einen Auftragsverarbeiter

Ist die Pfarre nur Auftraggeber und erfolgt die automatisationsunterstützte Verarbeitung durch einen nicht kirchlichen Dienstleister, ist ein schriftliches Übereinkommen abzuschließen. Dies ist etwa der Fall, wenn Namen und Adressen zur Adressierung des Pfarrblattes einer Druckerei übergeben werden. Für die Pfarre besteht eine Prüfungspflicht, einen Auftragsverarbeiter mit rechtmäßiger und sicherer Datenverarbeitung in Anspruch zu nehmen. Mit diesen

Maßnahmen soll sichergestellt werden, dass das Datenmaterial nicht missbräuchlich verwendet wird.

2.7.4 Sammlung, Verarbeitung und Weitergabe von Daten, Beispiele

Wer sich zu einer Veranstaltung (z. B. Wallfahrt) anmeldet, erteilt zugleich seine Zustimmung, dass für Zwecke der Durchführung und Organisation dieser Veranstaltung seine Daten verarbeitet werden. Diese Zustimmung reicht jedoch nur so weit, als die Daten zur Erfüllung des jeweils geschlossenen Vertrages gespeichert und bearbeitet werden müssen.

Mit beidseitiger Vertragserfüllung (z. B. Durchführung der Wallfahrt und Bezahlung) dürfen diese Daten, sofern der Wallfahrtsteilnehmer keine entsprechende Erklärung (z. B. im Datenblatt eines Wallfahrtsteilnehmers, der der Datenverwendung zugestimmt hat, kann die Tatsache seiner Wallfahrtsteilnahme vermerkt werden) abgegeben hat, nicht weiterverwendet werden und müssen gelöscht werden, wenn kein Rechtfertigungsgrund mehr für die Aufbewahrung gegeben ist.

Das aktive Aufmerksam machen von betroffenen Katholiken auf aus den Matriken abzuleitende Ereignisse mit rein pastoraler Bedeutung (Silberhochzeit etc.) ist als Ausfluss der Freiheit der inneren Organisation der Kirche rechtlich unbedenklich. Dies gilt auch für die Trauerbegleitung von Angehörigen, so ferne der trauernde Angehörige katholisch ist.

Soweit kirchennahe Institutionen (z. B. Schulen, Sportvereine etc.) mit kommerziellen Anbietern in Konkurrenz stehen, unterliegt die direkte Kontaktaufnahme zu Werbezwecken auf elektronischem Weg dem Verbot des § 107 TelKG. Jede Kontaktaufnahme auf Grund von Daten, welche verbotenerweise diesen Organisationen von der Kirche selbst übermittelt wurden, stellt auch einen Verstoß gegen § 1 UWG (Wettbewerbsgesetz) dar.

Daher sollte, soweit es organisatorisch, d. h. unter pastoralen Gesichtspunkten möglich ist, bei einer „Kontaktaufnahme“ zwischen der Kirche und ihren Umfeldorganisationen einerseits und den Katholiken andererseits eine Zustimmungserklärung (etwa in Form eines entsprechenden Beisatzes auf dem Anmeldeformular zu Wallfahrten etc.) eingeholt werden.

Bei Ausgetretenen sind Datensätze - mit Ausnahme der Matrikendaten und bis Ablauf der Verjährungsfrist auch der ökonomischen Daten, welche zur Ermittlung und Einhebung des Kirchenbeitrages erforderlich sind – zu löschen. Bei Ausgetretenen, die gegenüber der Kirche erklärt haben, dass sie keinerlei Kontakt mehr haben wollen, ist eine aktive Kontaktaufnahme unter Verwendung der gespeicherten Daten nicht zulässig.

Für die Sammlung von Daten über Gläubige, welche über die Stammdaten hinausgehen (z. B. Reisegewohnheiten, Teilnahme an Kirchenveranstaltungen etc.), um in weiterer Folge gezielt auf derartige Angebote aufmerksam machen zu können, ist eine Zustimmung bei Erstkontakt einholen. Die katholische Kirche hat bisher ca. 30 Datenanwendungen registriert.

Zwecke der Datensammlung sind z. B. die Matrikenführung, Personalverwaltung, pfarrliche Seelsorge, Einhebung und Verwaltung des Kirchenbeitrages, Spendenerfassung für kirchliche Zwecke, Videoüberwachung usw..

2.7.5 Schematismus

Der Schematismus ist zur Erfüllung kirchlicher Aufgaben zu verwenden. Er darf – ob als Buch oder PC-Version – nicht an Unbefugte weitergegeben werden. Er ist sorgfältig aufzubewahren und vor missbräuchlicher Einsichtnahme zu schützen. Auskünfte, Abschriften, Ablichtungen sowie Einspeicherungen auch einzelner Teile in Datenverarbeitungsanlagen dürfen an Privatpersonen sowie an wirtschaftliche Unternehmen nur bei nachgewiesenem berechtigtem, kirchlichem Interesse mit Genehmigung des Bischöflichen Ordinariats erteilt werden.

2.7.6 Weitergabe von Kirchenbeitragsdaten an pfarrliche Organe

Einkommensdaten sind in der Pfarre nicht zur Seelsorge notwendig. Die Pfarre ist kein Kirchenbeitragseinheber, außer sie wird ausdrücklich als Hilfsorgan der kirchenbeitragseinhebenden Verwaltungsstelle beauftragt und tätig. In diesen Fällen können die Kirchenbeitragsdaten samt Rückständen weitergegeben werden.

2.7.7 Auskünfte an Dritte

Oft werden Anfragen nach der Zugehörigkeit bestimmter Personen zur Katholischen Kirche gestellt. Eine Antwort darf außenstehenden Personen und Institutionen aufgrund des verfassungsrechtlich geschützten Anspruchs der Betroffenen auf Geheimhaltung nicht erteilt werden. Das Religionsbekenntnis zählt zu den sensiblen Daten und ist daher besonders geschützt.

2.7.8 Auskunft über eine Wohnadresse

Nur dann, wenn der Auskunftswerber im konkreten Fall beim Meldeamt nichts erreicht, darf die Pfarre die Daten, jedoch auch nur mit Zustimmung des Gesuchten, weitergeben.

2.7.9 Auskunft über Daten Verstorbener

Der Begriff „Person“ impliziert, dass es sich um einen lebenden Menschen handelt, Verstorbene fallen nicht unter den Personenbegriff, die Datenschutzbestimmungen sind daher nicht anwendbar. Dies bedeutet nicht, dass die Daten Verstorbener automatisch nach Belieben verwendet werden dürfen. Es gelten in der Regel andere Bestimmungen wie Amtsverschwiegenheit, das Archivgesetz udgl.

Eine Auskunftserteilung über Daten bereits Verstorbener hängt vom jeweiligen Sachverhalt ab und kann nicht allgemein beantwortet werden. Grundsätzlich kann jedoch das Argument „Datenschutz“ für eine Auskunftsverweigerung nur in den seltensten Fällen herangezogen werden. Eine Auskunftsverweigerung unter Hinweis auf den „Datenschutz“ ist bei Daten Verstorbener nur dann annehmbar, wenn durch eine bestimmte Information unmittelbar in die Interessen noch lebender Personen eingegriffen wird.

Oft werden Anfragen über Verstorbene unter Berufung auf das Auskunftspflichtgesetz (APG) gestellt. Sofern es sich dabei nicht um Rechtsnachfolger handelt, welche einen Anspruch haben, kann man uU auf das Standesamt verweisen.

2.7.10 Ahnenforschung

Dies ist grundsätzlich möglich, jedoch ist die Genehmigung des Kanzlers (derzeit delegiert an die Diözesanarchivare) für Einsichtnahme in den Pfarren einzuholen. Diese ist bei Einsichtnahme im Diözesanarchiv, für das die Archiv-Ordnung gilt, nicht erforderlich.

Bevor die Pfarre überhaupt mit der Bearbeitung einer diesbezüglichen Anfrage beginnt, soll erhoben werden, ob es eine zuständige öffentliche Behörde gibt, auf welche verwiesen werden kann.

2.7.11 Bekanntgabe von Kirchenaustritten

Die öffentliche Bekanntgabe (sei es von der Kanzel oder im Pfarrblatt) von Personen, die aus der Kirche ausgetreten sind, verletzt das Grundrecht auf Datenschutz.

2.7.12 Veröffentlichung von Bildern

Bilder von Personen dürfen ohne deren Zustimmung nicht veröffentlicht werden, wenn dadurch berechtigte Interessen des Abgebildeten (oder falls er gestorben ist naher Angehöriger) verletzt werden. Es ist auch zu klären, wer das Bild gemacht hat, das veröffentlicht werden soll.

Wenn das Bild nicht selbst gemacht wurde, besteht das Problem des Urheberrechts des Fotografen, d. h. man benötigt eine Werknutzungsgenehmigung oder eine Überlassung des Werknutzungsrechtes (entgeltlich oder unentgeltlich). Ohne Rechteeinräumung kann man

auf Zahlung der entsprechenden Beträge für die Fotonutzung geklagt werden, ebenso wenn man den Urheber nicht namentlich genannt hat.

Ohne Zustimmung dürfen Personen abgebildet werden, die von öffentlichem Interesse sind, wie z. B. Politiker, Pfarrer etc. Bei Veröffentlichungen von Einzelfotos soll im Zweifel eine mündliche Zustimmung eingeholt werden. Die Veröffentlichung von Kinderfotos (im Schaukasten, Pfarrblatt, Internet udgl.) bedarf der Zustimmung der Eltern. Ein Bericht über eine Veranstaltung, darf auch bebildert stattfinden. Wer an einer öffentlichen Veranstaltung teilnimmt muss damit rechnen, dass er abgebildet wird. Das Gleiche gilt bei Pfarrbällen, wenn in den Pfarrnachrichten oder in Kirchenzeitungen darüber berichtet wird.

2.7.13 Sonstige Veröffentlichungen im Pfarrblatt, Schaukasten, Internet

Geburtstage und Ehejubiläen

Veröffentlichungen personenbezogener Daten, also etwa runder Geburtstage, dürfen nur mit Zustimmung des Betroffenen erfolgen. Wenn Veröffentlichungen vorgenommen werden sollen, entsteht der Aufwand der Einholung und auch der Dokumentation der Zustimmung.

Es ist zulässig, zu runden Geburtstagen und Ehejubiläen persönlich (durch Vertreter der Pfarre) zu gratulieren, soweit dies pastoralen Charakter hat. Die Daten sind aus den Matriken zulässigerweise bekannt und zum Zwecke der Seelsorge auch verwendbar.

Geburten/Taufen, Hochzeiten und Todesfälle

Die Taufe ist ein Akt der Aufnahme in die Kirche. Grundsätzlich darf und soll die örtlich pfarrliche Öffentlichkeit wissen, wer ihr angehört. Andererseits gehört gerade das religiöse Bekenntnis zu den „sensiblen Daten“, die der besonderen Geheimhaltung unterliegen. Da jedoch Pfarrblätter oft über die Pfarröffentlichkeit hinausgehen, insbesondere durch Veröffentlichung im Internet, ist auch hier die Zustimmung der Betroffenen einzuholen. Ein Hinweis im Pfarrblatt, dass diejenigen, die bei den oben genannten Anlässen nicht erwähnt werden wollen, dies in der Pfarrkanzlei melden mögen, ist rechtlich letztendlich nicht ausreichend. Es kann jedoch im Fall einer Beschwerde durchaus als Argument vorgebracht werden.

Die ARGE Daten führt dazu aus, dass : „…wird die Veröffentlichung einer Geburt oder einer Trauung von den meisten Menschen akzeptiert und ist diese Form des Eindringens in die Privatsphäre in gewissem Maß gesellschaftlich erwünscht.“, und weiter: „Grundsätzlich gilt, dass alle Melde-, Verwaltungs- und Personenstandsdaten geheim zu halten sind, auch Veröffentlichungen über Geburten, Trauungen usw. nur in dem Ausmaß erlaubt sind, als die Betroffenen dem ausdrücklich zugestimmt haben oder selbst öffentlich gemacht haben.“

Das bedeutet letztlich, dass auch hier die Zustimmung zu einer Veröffentlichung erforderlich ist, wenn die Daten nicht öffentlich sind (z. B. durch Parteaushang). Dabei ist darauf zu achten, welche Daten konkret veröffentlicht werden sollen, damit diese von der Zustimmung auch erfasst sind.

2.8 Sicherheitsmaßnahmen

2.8.1 Umgang mit Zugangscodes, Passwörtern, Token

- Alle personenbezogenen Zugangsberechtigungen (Citrix, Adressdatenbank, Intranet, Token) sind ausschließlich von der betreffenden Person zu verwenden. Die Weitergabe an andere Personen ist nicht gestattet. Token müssen bei Beendigung des Dienstverhältnisses bzw. wenn die/der betreffende DienstnehmerIn diesen nicht mehr benötigt, der Informatikabteilung retourniert werden.

- Im Falle von Krankheit und Urlaub ist der Umgang mit einlangenden Mails zu regeln.

- DienstnehmerInnen, die dienstliche Laptops haben, sind grundsätzlich selbst für die sichere Verwahrung verantwortlich. Bei längerer Abwesenheit ist der Laptop auf Verlangen der DienstgeberIn der Abteilung bzw. der Dienststelle zur Verfügung zu stellen, bei Ausscheiden aus dem Betrieb unverzüglich den Dienstgebern zurückzugeben.

- Vertrauliche Unterlagen sind versperrt zu halten. Während der Bürozeiten verwendete Unterlagen sind so zu sichern, dass sie nicht von Dritten missbraucht werden können.

- Es ist für jede Dienststelle, Abteilung zu vereinbaren und festzuhalten, wer im Vertretungs- oder Krisenfall Zugang zu versperrten Daten, Unterlagen, Passwörtern und versperrten Schränken hat.

- Der Zugang zu privaten Daten und Unterlagen, die hinterlegt sind, ist nur mit Zustimmung der betreffenden Person und ersatzweise des Betriebsrates möglich.

2.8.2 Schutz der Daten vor unbefugten Zugriffen und Virenbefall

Ein Virenschutzprogramm ist unbedingt einzusetzen und ständig aktuell zu halten (am besten direkt über das Internet). Der Einsatz eines Firewall-Systems wird dringend empfohlen (zumindest die Firewall-Funktionalität des Betriebssystems).

Eine weitere Folge des Datenschutzes ist die so genannte Datensicherung, d. h. es muss gewährleistet werden, dass Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, dass ihre Verwendung ordnungsgemäß erfolgt und dass die Daten Unbefugten nicht zugänglich sind. Es sind Datensicherungsmaßnahmen zu treffen, so z. B.

- die Räume immer verschlossen zu halten,
- die Kästen zu versperren und
- es dürfen keine Schriftstücke offen herumliegen, so dass ein Unbefugter daraus Daten entnehmen könnte,
- Belehrung der Mitarbeiter,
- Sicherheitsüberprüfungen,
- komplexe zeitlich beschränkt gültige Passwörter.

So ist z. B. die Mitnachhausenahme von Akten sehr problematisch, wenn Familienmitglieder oder dgl. Einsicht nehmen könnten.
Desweitern ist die Umleitung von E-Mails, die an die dienstliche E-Mail-Adresse gehen auf eine andere (private) E-Mail-Adresse nicht zulässig. Zu beachten ist auch, dass Daten in Public Clouds (Dropbox) nicht vor Zugriffen Dritter geschützt sind. Es ist daher vor Nutzung solcher Instrumente jeweils sorgfältig zu überlegen, ob die Informationen tatsächlich für diese Nutzung geeignet sind. Personenbezogene Daten, insbesondere sensible und sonstige heikle Informationen, dürfen nicht in Public Clouds gestellt werden.

3 Checkliste zum Datenschutz

Diese Checkliste dient der Kontrolle, ob in einer Dienststelle (Pfarre) die wichtigsten Datenschutzbestimmungen eingehalten werden. Die Liste spricht anhand konkreter Fragen verschiedene Bereiche des Datenschutzes an. Sie soll alle Mitarbeiterinnen für die Anliegen des Datenschutzes sensibilisieren.

Die Fragen erheben keinen Anspruch auf Vollständigkeit. Für die sichere Einhaltung des Datenschutzes sind auf jeden Fall Schulungen und eine weiterführende Befassung mit dem Thema notwendig.

1. **Wie steht der Bildschirm am Schreibtisch?**

   Erläuterung: Am PC soll verhindert werden, dass außenstehende Personen in den Bildschirm einsehen können, da bei der Arbeit personenbezogene Daten am Bildschirm angezeigt sein können. Daher: Bildschirm so drehen, dass Besucher keinen Einblick haben.

2. **Liegen Zettel, Listen o.ä. mit personenbezogenen Daten am Schreibtisch?**

   Erläuterung: Hier gilt dasselbe wie bei der 1. Frage: Besucher dürfen keine Möglichkeit haben, personenbezogene Daten von herumliegenden Zetteln einzusehen.

3. **Wo werden Listen, Ausdrucke u. andere Zettel mit personenbezogenen Daten aufbewahrt?**

   Erläuterung: Listen, Zettel und andere Unterlagen mit personenbezogenen Daten sind prinzipiell versperrt aufzubewahren. Bei Abwesenheit der zuständigen Person ist zu gewährleisten, dass Dritte keine Daten einsehen können.

4. **Gibt es Speichersticks, CDs und andere Datenträger?**

   Erläuterung: Die Speicherung von personenbezogenen Daten auf tragbare Medien ist nur in ganz bestimmten Fällen erlaubt. Diese Speichermedien sind vor unbefugtem Zugriff zu schützen (versperren).

5. **Wer weiß die Passwörter für den Zugang zu personenbezogenen Daten?**

   Erläuterung: Persönliche Passwörter dürfen nicht weitergegeben werden. Wenn jemand Zugang zu geschützten Dateien will, so ist die Berechtigung zu prüfen; nötigenfalls bekommt die Person eine eigene Anmeldung. Im Missbrauchsfall ist die Person haftbar, deren Zugangsdaten verwendet wurden.

6. **Besitze ich einen sogenannten „Token"?**

   Erläuterung: Der Umgang mit Token ist ebenfalls streng geregelt: Token sind persönliche Zugangsberechtigungen und dürfen keinesfalls weitergegeben werden. Bei Bedarf sind für weitere Personen eigene Token anzufordern.

7. **Werden Daten auf privaten PCs abgespeichert?**

   Erläuterung: Die Speicherung personenbezogener Daten auf private PCs ist generell verboten.

8. Werden Daten gesichert? Wo werden die Sicherungen aufbewahrt?

Erläuterung: Es ist von der Dienststelle sicherzustellen, dass Daten, die nicht auf zentralen Servern liegen, regelmäßig gesichert werden. Die Sicherungen sind gegen den Zugriff durch Unberechtigte zu schützen.

9. Woher werden Daten erfasst?

Erläuterung: Die Datenerfassung ist nur im Rahmen der betrieblichen Arbeit erlaubt. Die Erfassung muss auch im Verzeichnis der Verarbeitungstätigkeit vorgesehen sein. Daten, die dort nicht vorgesehen sind, dürfen nicht erfasst werden. Für die Verarbeitung und Weitergabe von Daten gelten die Bestimmungen analog.

10. Schicken wir unverlangte Post bzw. Mails an Personen?

Erläuterung: Persönlich adressierte Post darf nur geschickt werden, wenn die betroffene Person der Zusendung zugestimmt hat. Dies gilt vor allem für Rundbriefe, Zeitungen und andere Massensendungen.

11. Welche personenbezogenen Daten werden an Dritte weitergegeben?

Erläuterung: Es ist sicherzustellen, dass die Weitergabe erlaubt ist. Es gibt Einschränkungen auf Grund verschiedenster Regelungen, wie beispielsweise dem Datenschutzgesetz, Personenstandsgesetz, kirchliche Datenschutzverordnung. Die Erlaubtheit der Weitergabe von Daten muss vorab geklärt sein.

12. Wie wird mit telefonischen Anfragen und Auskünften umgegangen?

Erläuterung: Telefonische Anfragen unterliegen wie schriftliche Anfragen dem Datenschutz. Es ist vor allem zu gewährleisten, dass die Identität der anfragenden Person eindeutig klar ist und diese Person auch wirklich das Recht auf Auskunft hat.
Tipp: Im Zweifelsfall die Anfrage schriftlich schicken lassen und mit Ausweiskopie die Identität der anfragenden Person sowie die Berechtigung zur Auskunft feststellen. Auch die Beantwortung schriftlich vornehmen. Bei Postzustellung kann die richtige Adresse noch geprüft werden.

13. Werden Dokumente o.ä. von dritten Personen persönlich abgeholt?

Erläuterung: Es kann sein, dass Ehepartner, Eltern oder andere Bekannte von Personen Dokumente abholen oder mitnehmen sollen/wollen. In diesem Fall unbedingt das Dokument oder das Schreiben in ein verschlossenes Kuvert legen und an die zuständige Person persönlich adressieren.
Tipp: Im Zweifelsfall lieber mit der Post an die Person direkt schicken oder eine Vollmacht vorlegen lassen.

14. Datenverarbeitungsregister-Nummer

Erläuterung: Das Führen der Datenverarbeitungsregisternummer ist nicht mehr vorgesehen.

15. Besitzt die Pfarre bzw. Einrichtung eine eigene Homepage?

Erläuterung: Auch auf Homepages dürfen keine personenbezogenen Daten, die über die dienstlich „normale" Datenverwendung hinausgehen, verwendet bzw. veröffentlicht werden. Erlaubt sind bei hauptamtlichen Dienstnehmerinnen Name, betriebliche Funktion, telefonische Erreichbarkeit, (dienstliche) E-Mail-Adresse. Darüber hinausgehende Informationen wie private Adressen, Telefonnummern, Geburtsdatum, Fotos etc. dürfen nur mit Zustimmung der betreffenden Person veröffentlicht werden! Bei ehrenamtlichen Personen immer die Zustimmung zur Bekanntgabe der Daten einholen!

16. Werden Fotos von Personen in irgendeiner Weise veröffentlicht?

Erläuterung: Auch hier ist der Datenschutz zu berücksichtigen. Bei Fotos von Veranstaltungen dürfen nur allgemeine Gruppenfotos veröffentlicht werden. Generelle Regel: Wenn Fotos von Einzelpersonen und kleinen Personengruppen (bis ca. 5 Personen) veröffentlicht werden sollen, ist die Zustimmung der fotografierten Personen notwendig. Dies gilt sowohl für Homepage als auch für Drucksachen (Pfarrbrief, Jahresberichte etc.)

17. Werden Daten von Kindern erfasst, verarbeitet, weitergegeben?

Erläuterung: Bei Daten von Kindern ist ein besonders strenger Maßstab anzulegen. Daten und Fotos von Kindern dürfen prinzipiell nur mit der Zustimmung der Erziehungsberechtigten erfasst, verarbeitet oder veröffentlicht werden.
Tipp: Die Zustimmung schriftlich einholen.

18. Haben ehrenamtliche Mitarbeiterinnen Zugang zu personenbezogenen Daten?

Erläuterung: Personenbezogene Daten dürfen an Ehrenamtliche nur unter bestimmten Voraussetzungen weitergegeben werden. Die Weitergabe der Daten muss zur Erfüllung des kirchlichen Auftrages notwendig sein, die ehrenamtliche Person muss im Bereich Datenschutz geschult sein und über die Konsequenzen einer Datenschutzverletzung Bescheid wissen und der/die Ehrenamtliche muss die „Verpflichtungserklärung Datenschutz" unterschrieben haben. Es gelten alle einschlägigen Bestimmungen analog. Insbesondere das Verbot der Speicherung auf privaten PCs und auf tragbaren Speichermedien ist zu beachten.

19. Wer hat Zugriff auf das Intranet und auf dienstliche E-Mails?

Erläuterung: Betriebsfremden Personen ist die Nutzung des diözesanen Intranets und E-Mails untersagt.

20. Gibt es Auskunftswünsche von Personen über die Speicherung ihrer eigenen Daten?

Erläuterung: Derartige Auskunftswünsche sind an die/den diözesane/n Datenschutzbeauftragte/n weiterzuleiten und von dieser/m zu bearbeiten.

21. Sind die datenschutzrelevanten Bestimmungen für alle damit Befassten zugänglich?

Erläuterung: Es sollen für alle (haupt- und ehrenamtlichen) Mitarbeiterinnen die einschlägigen Bestimmungen zum Nachlesen bereit stehen:

- EU-Datenschutzgrundverordnung
- Datenschutzgesetz
- Personenstandsgesetz und Personenstandsverordnung (nur für Mitarbeiterinnen in der Pfarrkanzlei)

- Matrikenwegweiser (nur für Mitarbeiterinnen in der Pfarrkanzlei)
- Decretum Generale über den Datenschutz in der Katholischen Kirche und ihren Einrichtungen