Katholische Kirche
in Oberösterreich

Datenschutz & Datensicherheit in der Diözese Linz

Leitfaden und Richtlinien

Jänner 2023

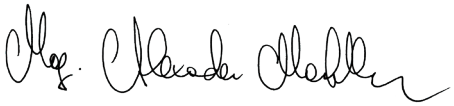
LIEBE MITARBEITENDE DER DIÖZESE LINZ,

ein Blick in die täglichen Schlagzeilen genügt, um festzustellen, wie sehr das Thema Datenschutz in den Blickpunkt einer breiten Öffentlichkeit gerückt ist (Datenverluste, Datendiebstahl, Umgang mit Gesundheitsdaten) – und dies verstärkt seit der Einführung der viel diskutierten und auch heftig kritisierten EU-Datenschutzgrundverordnung (EU-DSGVO) im Mai 2018. Umso wichtiger ist es daher, Mitarbeiter:innen für dieses komplexe Thema zu sensibilisieren.

Aufgrund der Fülle an Informationen, die sich im Zuge datenschutzrechtlicher Bestimmungen ergeben, ist es nicht möglich, auf sämtliche gesetzliche Vorgaben im Detail einzugehen. Mit dieser Handreichung möchte ich Ihnen aber eine Übersicht über die wesentlichsten Themen geben, wie wir alle in unseren unterschiedlichen Aufgabenbereichen mit den uns anvertrauten Daten rechtskonform umgehen.

Für Fragen zum Thema Datenschutz und dessen Umsetzung stehe ich Ihnen selbstverständlich zur Verfügung!

Vielen Dank für Ihre gewissenhafte Mitarbeit!



Mag. Alexander Marktler
Datenschutzreferent der Diözese Linz
Mitarbeiter der Kirchlichen Datenschutzkommission

JÄNNER 2023

KONTAKT:
Mag. Alexander Marktler
Datenschutzreferent der Diözese Linz
Hafnerstraße 18 | 4021 Linz
Tel. +43 732 79800-1424
E-Mail datenschutz@dioezese-linz.at

Formulare und Muster-Vorlagen finden Sie im diözesanen Mitarbeiter:innen-Portal „DiALog“ im Bereich „Datenschutz“!

INHALT

„Datenschutz will nicht den Einsatz der ADV[1] verhindern, aber er will dafür sorgen, dass dieser Einsatz dort endet, wo unsere Privatsphäre beginnt, wo wir schutzwürdige Interessen auf Geheimhaltung von Informationen geltend machen können.

Datenschutz ist der Schutz einer fairen Informationsumwelt, er ist Bürgerschutz gegenüber dem Staat, Konsumentenschutz gegenüber Unternehmern, Arbeitnehmerschutz gegenüber dem Arbeitgeber.

Datenschutz will die Rechtsstellung des Bürgers gegenüber allen Stellen, die seine Daten verarbeiten, verbessern."

(Aus „Die Bundesregierung informiert – Datenschutzgesetz", herausgegeben vom Bundeskanzleramt, Wien 1980)

[1] ADV = automationsunterstützte Datenverarbeitung

I. WAS MUSS ICH WISSEN, UM DIE BESTIMMUNGEN DES DATENSCHUTZES UMSETZEN ZU KÖNNEN?

1.1. RECHTSGRUNDLAGEN

Rechtliche Grundlage ist die EU-Datenschutzgrundverordnung (**EU-DSGVO** oder auch nur **DSGVO**), welche seit 25.5.2018 in allen Mitgliedsstaaten der Europäischen Union gilt.

Diese europarechtliche Grundlage wird in Österreich durch das nationale Datenschutzgesetz **(DSG)** in der jeweils geltenden Fassung ergänzt. Die Katholische Kirche in Österreich ist zur selbstständigen Verwaltung und Ordnung ihrer inneren

Angelegenheiten berechtigt (Artikel 15 Staatsgrundgesetz über die allgemeinen Rechte der Staatsbürger:innen). Sie ist aber auch den staatlichen Gesetzen unterworfen.

Die DSGVO sowie nationale Datenschutzbestimmungen gelten daher auch für die Einrichtungen der Katholischen Kirche in Österreich!

Zur konkreten Anwendung des Datenschutzrechts im Bereich der Katholischen Kirche in Österreich erließ die Österreichische Bischofskonferenz die **Kirchliche Datenschutzverordnung** („Decretum Generale über den Datenschutz in der Katholischen Kirche in Österreich und ihren Einrichtungen"), kundgemacht im Amtsblatt der Österreichischen Bischofskonferenz Nr. 74 vom 1. Jänner 2018.

Beachten Sie bitte, dass datenschutzrechtliche Einzelbestimmungen auch in Betriebsvereinbarungen und Kollektivverträgen enthalten sein können!

Konkret für die Diözese Linz siehe dazu die diözesane Betriebsvereinbarung „Datenschutz" im Mitarbeiter:innen-Portal „DiALog"!

Den Text des Decretum Generale, die Datenschutzgrundverordnung sowie das österreichische Datenschutzgesetz finden Sie auf der diözesanen Website unter **https://www.dioezese-linz.at/datenschutz**.

I.2. GRUNDLEGENDES

GRUNDBEGRIFFE: BETROFFENE PERSON, VERANTWORTLICHER, AUFTRAGSVERARBEITER, EMPFÄNGER[2] (ARTIKEL 4 DSGVO)

- Die **betroffene Person** (bzw. der **Betroffene**) ist jene lebende, individuelle Person, deren personenbezogene Daten verarbeitet werden. Die **Kategorien betroffener Personen** („Betroffenenkreise") sind die entsprechenden Personengruppen, die dem Einzelnen zugeordnet werden können.
  Beispiele für Kategorien betroffener Personen: Katholik:innen, Mitarbeiter:innen, Mitglieder, Abonnent:innen, Teilnehmer:innen, Schüler:innen etc.
- Der **Verantwortliche** ist jene Person oder Stelle, die die Entscheidung getroffen hat, Daten für einen bestimmten Zweck zu verarbeiten.

In unserem Fall ist der Verantwortliche die Katholische Kirche in Österreich.

- Der **Auftragsverarbeiter** (alt „Dienstleister“) verarbeitet personenbezogene Daten, die ihm zur Herstellung eines aufgetragenen Werkes vom Verantwortlichen überlassen wurden. Der Auftragsverarbeiter ist nicht von selbst tätig, sondern ausschließlich **im Auftrag** des Verantwortlichen.
  Beispiel: Eine Druckerei, die zum Versenden des Pfarrblattes Adressetiketten (= personenbezogene Daten) erhält, ist für die Pfarre als Auftragsverarbeiter tätig.
- Ein (Übermittlungs-)**Empfänger** ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt („übermittelt“) werden. Als **Kategorien von Empfängern** werden wiederum entsprechende Gruppen zusammengefasster Empfänger bezeichnet (z. B. „Gerichte“, „Gemeinden“, „Finanzämter“).
  Beispiel: Aufgrund diverser gesetzlicher Vorgaben müssen gewisse Personaldaten dem Sozialversicherungsträger übermittelt werden. Datenschutzrechtlich fungiert somit der konkrete Träger (z. B. die ÖGK) als Übermittlungsempfänger.

WAS BEDEUTET DAS GRUNDRECHT AUF DATENSCHUTZ (§ 1 DSG)?

Datenschutz ist in Österreich[3] ein **Grundrecht** (§ 1 DSG ist eine Verfassungsbestimmung) und fußt auf der Achtung der **Privatsphäre** (Privat- und Familienleben, siehe etwa Artikel 8 der Europäischen Menschenrechtskonvention).

„Das österreichische Datenschutzgesetz (DSG) schützt nicht nur die Daten (d. h. die gespeicherten Informationen), sondern eigentlich das Recht jedes Bürgers auf Selbstbestimmung und auf Achtung seiner persönlichen Sphäre, die er durch schutzwürdige Interessen an der Geheimhaltung von Daten umschreiben kann.“

(„Die Bundesregierung informiert – Datenschutzgesetz“, herausgegeben vom Bundeskanzleramt, Wien 1980)

[2] Diese Bezeichnungen werden in Artikel 4 DSGVO (Ziffern 1, 7, 8 und 9) definiert und sind geschlechtsneutral zu verstehen. Sie werden in weiterer Folge daher **nicht gegendert**.
[3] Österreich war einer der ersten Staaten, in dem ein Grundrecht auf Datenschutz der Verfassung angehörte!

Jede natürliche Person hat grundsätzlich ein Recht auf die Geheimhaltung der sie betreffenden personenbezogenen Daten.

- Bei **schutzwürdigem Interesse:** Dieses ist grundsätzlich anzunehmen, außer die Daten sind allgemein verfügbar (z. B. Daten aus einem öffentlich einsehbaren Register wie etwa dem Grundbuch) oder anonymisiert (Statistik).
- **Unabhängig** von der Verarbeitung der Daten, also bei **automationsunterstützter** (PC, USB-Stick) und manueller (Karteikarten, Matrikenbücher) Verarbeitung.
- Als höchstpersönliches Recht **endet der Datenschutz mit dem Tod**. Dennoch sind bei etwaigen Veröffentlichungen auch die berechtigten Interessen Angehöriger zu beachten, wenn diese Interessen die Wahrung des Lebensbildes des/der Verstorbenen betreffen.

GRUNDREGEL: Personenbezogene Daten dürfen NICHT verarbeitet werden, es sei denn, die Verarbeitung ist gesetzlich erlaubt. Die gesetzlichen „Erlaubnistatbestände“ siehe Seite 13 (Artikel 6 DSGVO).

WAS VERSTEHT MAN UNTER PERSONENBEZOGENEN DATEN?

Nach europäischem Recht sind personenbezogene Daten all jene Informationen, die sich auf eine natürliche Person beziehen oder zumindest beziehbar sind und so **Rückschlüsse auf deren Persönlichkeit** erlauben.

Die Arten personenbezogener bzw. auf Personen beziehbarer Daten sind zahlreich und vielfältig – im Folgenden als grober Überblick einige Beispiele:

- allgemeine Personendaten (Name, Geburtsdatum, Alter, Geburtsort, Anschrift, E-Mail-Adresse, Telefonnummer, Beruf, Personenstand usw.)
- besondere Personendaten (Religionsbekenntnis, Gesundheitsdaten, Einkommensverhältnisse, Ausbildung, Bonität usw.)
- Kennnummern (Sozialversicherungsnummer, Steueridentifikationsnummer, Personalausweisnummer, Beitragsnummer, Matriken-Nummer usw.)
- Bankdaten (Kontonummern, Kreditinformationen, Kontostände usw.)
- Online-Daten (IP-Adresse, Standortdaten usw.)

- physische Merkmale (Geschlecht, Haut-, Haar- und Augenfarbe, Statur, Kleidergröße usw.)
- Besitzmerkmale (Fahrzeug- und Immobilieneigentum, Grundbucheintragungen, Kfz-Kennzeichen, Zulassungsdaten usw.)
- Kundendaten (Bestellungen, Adressdaten, Kontodaten usw.)
- Werturteile (Schul- und Arbeitszeugnisse, „ist ein schlechter Zahler" usw.)

Die einzelnen Felder (Name, Alter etc.) werden auch **„Datenarten"** genannt, die konkrete Ausprägung (Maximilian Mustermann, 48 Jahre) **„Dateninhalt"**.

Als **Kategorien personenbezogener Daten** bezeichnet man Gruppen „zusammengehörender" Daten, z. B. „Adressdaten" (bestehend wiederum aus den Datenarten Straße, Hausnummer, Postleitzahl, Ort).

Die Katholische Kirche in Österreich verarbeitet im Wesentlichen die Daten der **Gläubigen**, das sind jene, die durch die Taufe eingegliedert wurden (Laien und Kleriker), die Daten der **Katechumenen** (jene, die um Aufnahme in die Kirchengemeinschaft bitten), die Daten von **Abonnent:innen**, **Kurs-/Veranstaltungsteilnehmer:innen** und **Spender:innen** sowie die Daten von Personen, die in einem **Beschäftigungs- und/oder Ehrenamtsverhältnis** mit der Katholischen Kirche in Österreich oder einer ihrer Einrichtungen stehen. Weitere Möglichkeiten einer kirchlichen Datenverarbeitung liegen etwa im Bereich der **Bildungs- und Kindertageseinrichtungen**, der **Klient:innen-Verwaltung** sowie im Bereich der **Liegenschaftsverwaltung** (Mieter:innen, Pächter:innen).

In den Anwendungsbereich der DSGVO fallen auch **pseudonymisierte** personenbezogene Daten. Darunter versteht man Daten, die einer bestimmten Person zuordenbar sind, aber die Zuordnung nur mit zusätzlichen Informationen möglich ist.
Dies ist z. B. der Fall, wenn die Zuordnung nur mittels eines Zuordnungsschlüssels möglich ist.

NICHT in den Anwendungsbereich der DSGVO fallen **anonyme** Daten. Bei anonymen Daten handelt es sich um Daten, die nicht einer bestimmten natürlichen Person zugeordnet werden können. Die Zuordnung ist nicht bloß erschwert (wie bei den pseudonymisierten Daten), sondern **unmöglich**.

WAS VERSTEHT MAN UNTER „VERARBEITUNG" (ARTIKEL 4 ZIFFER 2 DSGVO)?

Das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung im Zusammenhang mit personenbezogenen Daten.

DIE 7 GRUNDSÄTZE FÜR DIE VERARBEITUNG PERSONENBEZOGENER DATEN (ARTIKEL 5 DSGVO):

- **Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz:** Eine Datenverarbeitung ist nur **rechtmäßig**, wenn eine entsprechende **Rechtsgrundlage** (siehe dazu Seite 13, Artikel 6 DSGVO) dafür vorliegt. Die betroffene Person muss zusätzlich in umfassender, transparenter Form über die sie betreffende Datenverarbeitung informiert werden.
- **Zweckbindung:** Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

Der Zweckbindungsgrundsatz ist DIE zentrale Grundlage des österreichischen bzw. europäischen Datenschutzrechts!
Das Sammeln von Daten auf „Vorrat" oder „Verdacht" ist somit nicht gestattet.

Beispiele für Verarbeitungs-Zwecke (auch **„Datenanwendungen"** genannt) in der Katholischen Kirche in Österreich:
„Matrikenführung", „Pfarrliche Seelsorge", „Kirchenbeitragswesen", „Personalverwaltung", „Finanzbuchhaltung" bis hin zu „Liegenschaftsverwaltung" oder „Erziehung und Betreuung natürlicher Personen in Schulen, Kindertageseinrichtungen und Internaten".

Auch Videoüberwachungen sind Datenanwendungen!
Die Verarbeitungszwecke müssen im (diözesanen) Verzeichnis der Verarbeitungstätigkeiten erfasst und dokumentiert werden.

- **Datenminimierung, Datensparsamkeit:** Es dürfen nur jene Daten verarbeitet werden, die für die Zweckerreichung unvermeidbar sind. Daten, die für die Erreichung des Verarbeitungszweckes keine Notwendigkeit darstellen, sind von der Verarbeitung auszuschließen bzw. überhaupt nicht zu erheben.
  Beispiel: Für den Zweck „Matrikenführung" wäre das Erheben und Speichern der Augenfarbe unzulässig.

Die Mitarbeiter:innen eines Verantwortlichen oder eines Auftragsverarbeiters dürfen nur auf jenen Datenbestand Zugriff haben, der für die Erfüllung ihrer Aufgaben unabdingbar ist.

- **Datenrichtigkeit**: Die erhobenen Daten sollen sachlich richtig und, soweit erforderlich, auf dem neuesten Stand sein.
- **Speicherbegrenzung:** Die Speicherdauer von Daten ist auf das unbedingt erforderliche Mindestmaß zu beschränken – Daten dürfen (in personenbezogener Form) nur so lange aufbewahrt werden, wie es für den Verarbeitungszweck erforderlich ist.
  Beispiel: Bewerbungsunterlagen müssen (außer es liegt eine Zustimmung für eine längere Evidenzhaltung durch den sich Bewerbenden vor) 7 Monate („6+1") nach der Stellenentscheidung vernichtet werden.

  Sonderfall: Matrikendaten –> siehe dazu Kapitel III, Seite 38

  Im Einzelfall (also für bestimmte Datenarten) sind allerdings auch gesetzliche **Aufbewahrungsfristen** bzw. **Aufbewahrungspflichten** zu berücksichtigen und es ist zu überlegen, ob andere rechtliche Interessen (z. B. die Abwehr von Ansprüchen) eine längere Aufbewahrung rechtfertigen.
  Beispiele:
  - Steuerrechtliche Aufbewahrungspflicht (Belege): 7 Jahre
  - Anspruch auf Ausstellung eines Dienstzeugnisses: 30 Jahre
  - Geltendmachung von Ansprüchen wegen Diskriminierung bei Beförderung/Bewerbung: 6 Monate

Um die Löschung der Daten nach Fristablauf zu gewährleisten, sollte innerhalb jeder Einrichtung ein Löschkonzept überlegt und implementiert werden.
Hierfür sind auch eventuelle Aufbewahrungspflichten zu beachten.
Nicht mehr benötigte Daten sind unwiederbringlich zu löschen bzw. zu vernichten.

- **Integrität und Vertraulichkeit:** Daten dürfen **weder** von Unbefugten oder sonst unbeabsichtigt **verändert** oder **gelöscht** werden noch von diesen **gelesen** oder **verarbeitet** werden. Dies ist durch geeignete technische und organisatorische Maßnahmen („TOMs“) zu gewährleisten (siehe Seite 26).
- **Rechenschaftspflicht:** Der Verantwortliche muss in der Lage sein, das Einhalten der DSGVO-Bestimmungen nachweisen zu können. Daraus folgt eine umfassende Dokumentationspflicht.

WAS VERSTEHT MAN UNTER DEM „VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN“ (ARTIKEL 30 DSGVO) UND WER FÜHRT ES?

Im Verzeichnis der Verarbeitungstätigkeiten sind alle **Datenanwendungen**, also jeder „Zweck der Verarbeitung“ (siehe Seite 10) eines Verantwortlichen mit den jeweiligen Betroffenenkreisen, den Datenarten und etwaigen Übermittlungs-Empfängern sowie den dafür eingesetzten Datensicherheitsmaßnahmen anzuführen.

Dieses Verzeichnis erstellt im Falle der Katholischen Kirche in Österreich der/die jeweilige Bereichs-Datenschutzreferent:in für seinen/ihren Bereich, im Falle einer Diözese also der/die **diözesane Datenschutzreferent:in** und nicht die einzelne Einrichtung oder Pfarre. Dieses Verzeichnis entspricht in etwa dem früheren Datenverarbeitungsregister (DVR), welches im Zuge der DSGVO-Einführung aufgelassen wurde und nun dem Verantwortlichen die Aufgabe der **Dokumentation** überträgt (Motto: „Weg von der Behörde, hin zum Verantwortlichen“). Aktuell (Stand 2023) sind 67 solcher Verarbeitungs-Zwecke im Verzeichnis der Verarbeitungstätigkeiten der Diözese Linz erfasst bzw. registriert!

- Änderungen, Korrekturen, Ergänzungen bzgl. Datenanwendungen oder Sicherheitsmaßnahmen sind dem/der diözesanen Datenschutzreferenten/

-referentin zu melden und von ihm/ihr – nach Prüfung der Rechtmäßigkeit – im Verzeichnis einzutragen.
- Daten sind nur für den ursprünglichen und im Verzeichnis der Verarbeitungstätigkeiten dokumentierten Zweck zu verwenden!

DIE GRUNDSÄTZE RECHTMÄSSIGER DATENVERARBEITUNG (ARTIKEL 6 DSGVO):

Personenbezogene Daten dürfen nicht einfach willkürlich erhoben, gespeichert oder weitergegeben werden. Eine Datenverarbeitung ist nur dann rechtmäßig, wenn sie auf einer rechtlichen Grundlage (Rechtsgrundlage) beruht („Erlaubnistatbestände").

Die Verarbeitung ist nur **rechtmäßig**, wenn

- die betroffene Person ihre **Einwilligung** zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte **Zwecke** gegeben hat (Artikel 6 Absatz 1 lit. **a** DSGVO).

Eine Einwilligung nach Artikel 6 Absatz 1 lit. a DSGVO kann jederzeit ohne Angabe von Gründen von der betroffenen Person widerrufen werden!

- die Verarbeitung zur **Erfüllung eines Vertrages**, dessen Vertragspartei die betroffene Person ist, erforderlich ist bzw. erforderlich zum Zwecke vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen (Artikel 6 Absatz 1 lit. **b** DSGVO).

  – Im Zuge eines **Dienstverhältnisses** etwa werden personenbezogene Daten des Dienstnehmers/der Dienstnehmerin verarbeitet. Die Verarbeitung, Speicherung und Weitergabe unterschiedlicher Daten (z. B. an Lohnverrechnung, Sozialversicherung, AMS, Mitarbeiter:innen-Vorsorgekasse) ist für die Erfüllung des Dienstvertrages erforderlich.
  – Die **auf ein Vertragsverhältnis gestützte Datenverarbeitung** bietet den Vorteil, dass die Rechtmäßigkeit – anders als bei der Einwilligung der betroffenen Person – nicht durch Widerruf entfallen kann!

- die Verarbeitung zur **Erfüllung einer rechtlichen Verpflichtung** erforderlich ist, der der Verantwortliche unterliegt (Artikel 6 Absatz 1 lit. **c** DSGVO).

  – Derartige Verpflichtungen sind z. B. im **Arbeitsrecht** normiert (Datenfluss Katholische Kirche/Personalabteilung –> Extern).
  – „Umgekehrt" sind etwa die Bürgermeister:innen gemäß **§ 20 Absatz 7 Meldegesetz** verpflichtet, den gesetzlich anerkannten Religionsgesellschaften auf Verlangen die Meldedaten all jener in der Gemeinde angemeldeten Menschen zu übermitteln, die sich zu diesen Religionsgesellschaften bekannt haben (Datenfluss Extern –> Katholische Kirche/Fachbereich Kirchenbeitrag).

- die Verarbeitung erforderlich ist, um **lebenswichtige Interessen** der betroffenen Person oder einer anderen natürlichen Person zu schützen (Artikel 6 Absatz 1 lit. **d** DSGVO).

  Der Gesetzgeber hat dabei an Katastrophenschutz bei Naturkatastrophen und ähnlichen unabwendbaren Großereignissen gedacht.

- die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im **öffentlichen Interesse** liegt bzw. in Ausübung **öffentlicher Gewalt** erfolgt, die dem Verantwortlichen übertragen wurde (Artikel 6 Absatz 1 lit. **e** DSGVO).

  Hier ist z. B. an Archivzwecke zu denken.

- die Verarbeitung zur Wahrung der **berechtigten Interessen des Verantwortlichen** oder eines Dritten erforderlich ist, sofern nicht die Interessen der betroffenen Person überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt (Artikel 6 Absatz 1 lit. **f** DSGVO).

In diesem Fall ist eine **Interessenabwägung** zwischen den Interessen der betroffenen Person und den Interessen des Verantwortlichen vorzunehmen (z. B. bei einer geplanten Videoüberwachung [wegen häufiger Einbrüche oder Vandalenakte] oder bei Direktwerbung).

BESONDERE KATEGORIEN PERSONENBEZOGENER DATEN (BISHER „SENSIBLE DATEN", ARTIKEL 9 DSGVO)

Besonders geschützt ist die Verarbeitung von Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung oder weltanschauliche Überzeugung, Gewerkschaftszugehörigkeit, **RELIGIÖSE ÜBERZEUGUNG**, Gesundheitsdaten, genetische und biometrische Daten, Daten zum Sexualleben oder der sexuellen Orientierung.

Als Mitarbeiter:innen der Katholischen Kirche in Österreich haben wir in den meisten Bereichen auch mit der religiösen Überzeugung unserer Mitglieder zu tun, selbst wenn nicht in jedem Fall das Religionsbekenntnis verarbeitet wird. Aus diesem Grund bewegen wir uns quasi fast immer im Bereich sensibler Daten.

Artikel 9 DSGVO regelt die Verarbeitung („Erlaubnistatbestände") für den Bereich der sensiblen Daten.

Eine **Verarbeitung** ist **erlaubt** ...

- mit **ausdrücklicher Einwilligung** der betroffenen Person für einen oder mehrere festgelegte Zwecke (Artikel 9 Absatz 2 lit. **a** DSGVO).
- wenn sie im Bereich des **Arbeitsrechts** und dem Recht der sozialen Sicherheit bzw. des Sozialschutzes erforderlich ist (Artikel 9 Absatz 2 lit. **b** DSGVO).
- wenn sie zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich ist (Artikel 9 Absatz 2 lit. **c** DSGVO).
- wenn Daten durch die betroffene Person selbst veröffentlicht wurden (Artikel 9 Absatz 2 lit. **e** DSGVO).

- wenn sie zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist (Artikel 9 Absatz 2 lit. **f** DSGVO).
- wenn ein erhebliches öffentliches Interesse vorliegt (z. B. ein Katastrophenfall) (Artikel 9 Absatz 2 lit. **g** DSGVO).
- wenn sie für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin erforderlich ist (Artikel 9 Absatz 2 lit. **h** DSGVO)
- wenn sie aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren, erforderlich ist (Artikel 9 Absatz 2 lit. **i** DSGVO).
- wenn sie für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke erforderlich ist (Artikel 9 Absatz 2 lit. **j** DSGVO).
- wenn sie auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, **religiös** oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht **im Rahmen ihrer rechtmäßigen Tätigkeiten** und unter der Voraussetzung erfolgt, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die personenbezogenen Daten **nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden** (Artikel 9 Absatz 2 lit. **d** DSGVO).

§

Bekenntnis für religiöse Zwecke innerhalb (!) der Katholischen Kirche in Österreich –> darf nicht ohne Einwilligung der betroffenen Person nach außen offengelegt werden!
Daten betreffend den Ein- oder Austritt einer Person in die bzw. aus der Katholischen Kirche in Österreich stellen sensible Daten dar!

→ Besonderes Augenmerk ist hier auch jenen zu schenken, die im Zuge ihrer Tätigkeit mit Kranken, Gefangenen, Obdachlosen etc. arbeiten.

→ Im Zuge der COVID-19-Pandemie ist dem Thema „Verarbeitung von **Gesundheitsdaten** im Unternehmen“ besondere Bedeutung zugekommen (Stichwort „Contact-Tracing“).

WIE IST EINE RECHTSWIRKSAME EINWILLIGUNG ZU GESTALTEN (ARTIKEL 4 ZIFFER 11 DSGVO UND ARTIKEL 7 DSGVO)?

Einwilligungen bzw. Zustimmungserklärungen stehen immer wieder auf dem Prüfstand der Aufsichtsbehörden. Eine Einwilligung muss **freiwillig**, für einen **konkreten Fall**, nach **ausreichender Information** der betroffenen Person und **unmissverständlich** abgegeben werden.

Die betroffene Person gibt mit einer Erklärung oder einer sonstigen eindeutigen, aktiv bestätigenden Handlung zu verstehen (Willensbekundung), dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten für einen bestimmten Zweck einverstanden ist.

Damit eine Einwilligung **freiwillig** ist, muss die betroffene Person eine echte Wahl haben. Zusätzlich gilt das sogenannte **„Kopplungsverbot“** – so darf ein Vertragsabschluss bzw. die Erbringung einer Dienstleistung nicht von der Einwilligung zur Verarbeitung weiterer personenbezogener Daten abhängig gemacht werden, die für die Durchführung des Geschäftes **nicht** nötig sind. Zudem muss die Einwilligung an einen oder mehrere bestimmte **Zwecke** gebunden sein, die dann ausreichend erläutert sind. Soll die Einwilligung die Verarbeitung von besonderen personenbezogenen Daten (z. B. Gesundheitsdaten) legitimieren, muss sie sich **ausdrücklich** auf diese beziehen. Die betroffene Person muss in allen Fällen über die Möglichkeit zum **Widerruf** ihrer Einwilligung aufgeklärt werden. Der Widerruf muss dabei genauso leicht möglich sein wie die Abgabe der Einwilligungserklärung selbst.

Es besteht kein Formerfordernis (schriftlich/mündlich) für die Einwilligung. Sie kann daher auch in elektronischer Form erfolgen. Dabei ist zu beachten, dass eine Einwilligung nur durch eine **ausdrückliche („aktive“) Handlung** zustande kommt (**„Opt-in“**, z. B. durch das Setzen eines Häkchens in einem Kästchen). Eine Besonderheit in diesem Zusammenhang stellt die Einwilligung bei Kindern und Jugendlichen in Bezug auf **Dienste der Informationsgesellschaft** dar (siehe Seite 19).

Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es **von den anderen Sachverhalten klar zu unterscheiden ist** (Transparenzgebot und Trennungsgrundsatz).

Es empfiehlt sich, **Einwilligungserklärungen schriftlich einzuholen, zu archivieren und aufzubewahren**, um das Vorliegen der Einwilligung nachweisen zu können (Rechenschaftspflicht des Verantwortlichen).

Durch Stillschweigen, eine versteckte Einwilligung (z. B. in allgemeinen Geschäftsbedingungen) oder eine sogenannte Opt-out-Möglichkeit (bei der eine Einwilligung vom Verantwortlichen angenommen wird, wenn die betroffene Person der Verarbeitung der personenbezogenen Daten nicht widerspricht) kann **keine wirksame Einwilligung** gemäß DSGVO erteilt werden.

Kurzcheck zur Einwilligung:

Die Einwilligung ist:

o dokumentiert (nachweisbar)
o freiwillig
o klar, verständlich formuliert
o für den konkreten Fall formuliert
o durch eine aktive Handlung bestätigt
o widerrufbar (Widerrufshinweis)
o nicht an einen Vertragsschluss gekoppelt
o separat (sofern schriftlich erteilt)

Beispiele für das Einholen einer Zustimmungserklärung:

- Newsletterversand, Zusendung von Info-Materialien (z. B. Kursbücher)
- Veröffentlichen von personenbezogenen Daten (im Pfarrblatt, auf der Website, im Internet bzw. auf Social-Media-Plattformen), z. B. im Zuge von **Sakramenten** (Taufe, Hochzeit, Firmung)!
- **Veröffentlichung von Messstipendien (Messintentionen)**: Werden die Na-

men derer, die ein Messstipendium bezahlen, veröffentlicht (im Pfarrblatt, im Internet etc.) und/oder an die Familie des/der Verstorbenen weitergegeben, dann bedarf es dazu einer Einwilligung, einer Zustimmung. Diese kann schriftlich oder mündlich erfolgen.

- **Veröffentlichung von Bildern (Fotos):** Da hier mehrere Rechtsgebiete (Urheberrecht/Recht am eigenen Bild, Datenschutzrecht und Medienrecht) betroffen sind, ist eine abschließende Erörterung an dieser Stelle nicht möglich. Da wir uns im kirchlichen Umfeld allerdings fast immer im Bereich sensibler Daten bewegen (z. B. Foto beim Kommunionempfang), ist in den allermeisten Fällen eine **Zustimmung** der betroffenen Person oder des gesetzlichen Vertreters/der gesetzlichen Vertreterin bzgl. Foto-Veröffentlichung einzuholen! Siehe dazu detaillierter auch Kapitel VIII, Seite 42.

ACHTUNG: Oftmals ist eine Zustimmung der betroffenen Person als Rechtsgrundlage für die Datenverarbeitung nicht nötig, da ein Vertragsverhältnis als Rechtsgrundlage vorliegt (z. B. bei einer Anmeldung zu einer Wallfahrt)!

EINWILLIGUNG EINES KINDES (ARTIKEL 8 DSGVO)

Kinder werden aufgrund ihrer geringeren Einsichts- und Urteilsfähigkeit für die Tragweite eigenen Handelns vom Datenschutzrecht besonders geschützt. Artikel 8 DSGVO regelt die Bedingungen für die Einwilligung eines Kindes in Bezug auf Angebote von **Diensten der Informationsgesellschaft**, die einem Kind **direkt** gemacht werden. Für **unter Vierzehnjährige** besteht bei diesen ein zusätzliches Einwilligungs- bzw. Zustimmungserfordernis durch die/den Erziehungsberechtigte:n (laut DSGVO *„Träger der elterlichen Verantwortung für das Kind“*).

Folgende Elemente machen eine Dienstleistung zu einem „Dienst der Informationsgesellschaft“:

Die Dienstleistung

- wird in der Regel gegen **Entgelt** erbracht,
- wird im **Fernabsatz** erbracht, d. h. ohne gleichzeitige (physische) Anwesenheit der Vertragsparteien,

- wird **elektronisch** erbracht und
- wird auf **individuellen Abruf** eines Empfängers erbracht, d. h. die Übertragung von Daten findet auf individuelle Anforderung hin statt.

BEISPIELE: Social Media, andere Kommunikationsnetzwerke, Online-Verkauf von Waren, Online-Informationsdienste;

„die einem Kind direkt gemacht werden“: Das schließt jene Dienste aus, die **nicht** für Kinder oder Jugendliche bestimmt sind, sondern nur von diesen genutzt werden (z. B. Dating-Apps oder soziale Netzwerke speziell für Erwachsene). Umgekehrt sollen aber solche Dienstleistungen erfasst werden, die Kindern und Erwachsenen **gleichsam** offenstehen (wie z. B. Facebook).

Österreich hat von der Öffnungsklausel in Artikel 8 Abs. 1 DSGVO Gebrauch gemacht und das Alter von 16 Jahren gemäß DSGVO auf **14 Jahre** gesenkt (§ 4 Absatz 4 DSG)!

Unabhängig von datenschutzrechtlichen Bestimmungen sind bei Einwilligungen Minderjähriger auch immer die entsprechenden zivilrechtlichen Bestimmungen bzgl. Einsichtsfähigkeit/Geschäftsfähigkeit zu beachten! Dies spielt vor allem im Zuge von Vertragsverhältnissen eine Rolle!

PRAXISTIPP:

- **Unter 14-Jährige:** Hier ist **immer** die Einwilligung eines/einer Erziehungsberechtigten einzuholen. Empfohlen wird dies übrigens auch bzgl. der Teilnahme des Kindes an kirchlichen **Social-Media-Gruppen** (z. B. bei WhatsApp)!
- **Zwischen 14 und 18 Jahren** empfiehlt sich, für rein **datenschutzrechtliche** Belange (z. B. die Erlaubnis zur Veröffentlichung von Fotos) die Einwilligung von der betroffenen (minderjährigen) Person einzuholen. Hier kann durchaus mit der Religionsmündigkeit (in Österreich ab 14 Jahren) argumentiert werden – wer ab 14 Jahren die eigene Religionszugehörigkeit selbst entscheiden kann, wird wohl auch Entscheidungen in Bezug auf die eigenen Bildnisse treffen können.
  HINWEIS: Die Anmeldung zu einem Sommercamp etwa ist **keine**

datenschutzrechtliche Fragestellung –> hier wird in den allermeisten Fällen die Zustimmung („Unterschrift“) des/der Erziehungsberechtigten eingeholt werden müssen!

- Ab **Volljährigkeit (18 Jahre)** ist **immer** die Einwilligung der betroffenen Person einzuholen.

WAS BEDEUTET DIE INFORMATIONSPFLICHT (ARTIKEL 13 UND 14 DSGVO)?

Die Datenschutzgrundverordnung (DSGVO) hat die Betroffenenrechte im Datenschutz massiv gestärkt. So sieht die DSGVO nun umfangreiche Informationspflichten vor. Dies bedeutet, dass Verantwortliche grundsätzlich in der Pflicht sind, betroffene Personen „im Zeitpunkt der Erhebung der Daten“ umfassend darüber zu **informieren**, wenn personenbezogene Daten **erhoben** werden.

Die Angaben zur Informationspflicht haben in präziser, transparenter und leicht zugänglicher Form und Sprache zu erfolgen. Das Gesetz unterscheidet dabei zwischen zwei Fällen: zum einen, wenn die personenbezogenen Daten bei der betroffenen Person **direkt** erfasst/erhoben werden (Artikel 13 DSGVO), und zum anderen, wenn diese **nicht** bei der betroffenen Person erhoben werden (Artikel 14 DSGVO).

Wenn also Daten erhoben werden, müssen Sie über bestimmte Tatsachen informieren, insbesonders über folgende:

- Name und Kontaktdaten des Verantwortlichen
- Kontaktdaten der/des Datenschutzbeauftragten
- den **Zweck** und die **Rechtsgrundlage** der gegenständlichen Datenverarbeitung
- allenfalls berechtigte Interessen des Verantwortlichen
- Empfänger von personenbezogenen Daten
- Absicht zur Übermittlung in ein Drittland
- die **Speicherdauer**
- Belehrung über die Rechte der betroffenen Person

Ein allgemeines Muster für ein Informationsblatt gemäß Artikel 13 DSGVO steht im Mitarbeiter:innen-Portal „DiALog“ zur Verfügung! Auch bei der Nutzung einer Website werden in der Regel personen-

bezogene Daten erhoben (Cookies, Tracking etc.) – die Information gemäß Artikel 13 DSGVO im Bereich einer Website wird üblicherweise als „Datenschutzerklärung“ bezeichnet.

HINWEIS: U. a. für die Bereiche „Pastoral allgemein“, „Betrieb einer Videoüberwachungsanlage“, „Contact-Tracing“ und „Verträge & Vereinbarungen“ finden sich die Informationen gemäß Artikel 13 DSGVO auf der diözesanen Website unter „https://www.dioezese-linz.at/datenschutz“.

WELCHE RECHTE HAT EINE BETROFFENE PERSON GEMÄSS DSGVO?

Die Pflichten des Verantwortlichen wären zahnlos, wenn die betroffene Person keine Mittel hätte, um die Grundsätze der Datenverarbeitung überprüfbar zu machen und deren Durchsetzbarkeit sicherzustellen.

- **Recht auf Auskunft (Artikel 15 DSGVO)**
  Jede betroffene Person hat das Recht, eine Bestätigung (Auskunft) darüber zu verlangen, ob und wenn ja welche Daten von ihr vom Verantwortlichen verarbeitet werden.
  „Der Bürger soll wissen, wer welche Informationen über ihn verarbeitet und wofür sie verwendet werden.“
  (Aus „Die Bundesregierung informiert – Datenschutzgesetz“, herausgegeben vom Bundeskanzleramt, Wien 1980)

- **Recht auf Berichtigung unrichtiger Daten (Artikel 16 DSGVO)**
  Verarbeitet der Verantwortliche unrichtige personenbezogene Daten, so ist die jeweils betroffene Person berechtigt, zu verlangen, dass der Verantwortliche die Daten berichtigt.

- **Recht auf Löschung („Recht auf Vergessenwerden“) (Artikel 17 DSGVO)**
  Die betroffene Person hat **unter bestimmten Voraussetzungen** das Recht, dass der Verantwortliche personenbezogene Daten von ihr **unverzüglich** löscht. Als Voraussetzung für das Löschen personenbezogener Daten muss einer der folgenden Gründe vorliegen:
  - Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben

oder verarbeitet wurden, nicht mehr notwendig.
- Die betroffene Person widerruft ihre Einwilligung, welche die Rechtsgrundlage der Verarbeitung dargestellt hat.
- Die betroffene Person legt Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor.
- Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
- Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich.
- Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft bei einem Kind erhoben.

Die Löschung bestimmter Datensätze aus **Backups** ist oft wirtschaftlich oder technisch schwierig. Die Löschung von Daten aus Backups muss daher nicht unverzüglich erfolgen. Es muss allerdings sichergestellt werden, dass durch den Zugriff auf Backup-Dateien nicht jene Daten wieder in das System eingespielt werden können, hinsichtlich welcher die Löschung begehrt wurde.

EXKURS: Löschung aus Matrikenbüchern (siehe Seite 38)

- **Recht auf Einschränkung der Verarbeitung (Artikel 18 DSGVO)**
  Das Recht auf Einschränkung der Verarbeitung ist ein temporärer Behelf, mit dem erreicht werden soll, dass der Verantwortliche alle Verarbeitungstätigkeiten mit Ausnahme der Datenspeicherung unterlassen muss. Die Einschränkung ist jeweils für die Dauer der Prüfung der Ansprüche der betroffenen Person aufrecht.

- **Recht auf Datenübertragbarkeit (Artikel 20 DSGVO)**
  Um im Falle der Verarbeitung personenbezogener Daten mit automatisierten Mitteln eine bessere Kontrolle über die eigenen Daten zu haben, hat die betroffene Person unter bestimmten Voraussetzungen das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Weiters hat sie das Recht, zu erwirken, dass die perso-

nenbezogenen Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar und die Datenweitergabe zulässig ist. Mit dieser Bestimmung soll sichergestellt werden, dass Daten durch die Speicherung auf bzw. in bestimmten Formaten nicht unbrauchbar gemacht werden können.

- **Widerspruchsrecht (Artikel 21 DSGVO)**
  Die betroffene Person hat das Recht, gewissen Verarbeitungen ihrer personenbezogenen Daten zu widersprechen. Die Regelung konzentriert sich auf Datenverarbeitungsverfahren, die zwar zulässig sind, gegen die aber die betroffene Person aus besonderen Gründen (*„die sich aus ihrer persönlichen Situation ergeben"*) ein Widerspruchsrecht besitzen soll. Der Verantwortliche muss abwägen, ob die Gründe der betroffenen Person schwerer wiegen als die Interessen des Verantwortlichen an der Datenverarbeitung. Ist der Widerspruch erfolgreich, darf der Verantwortliche die Daten nicht mehr verarbeiten. Werden personenbezogene Daten verarbeitet, um **Direktwerbung** zu betreiben, besteht gegen diese Nutzung **jederzeit** und ohne besondere Begründung ein Widerspruchsrecht (Artikel 21 Absatz 2 und 3 DSGVO).

- **Recht auf „menschliche Entscheidung" (Artikel 22 DSGVO)**
  Die betroffene Person hat (mit gewissen Einschränkungen) das Recht, nicht einer **ausschließlich** auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

- **Recht auf Beschwerde an die Datenschutzbehörde (Artikel 77 DSGVO, § 24 Absatz 1 DSG)**
  Jede betroffene Person hat das Recht auf Beschwerde bei einer Aufsichtsbehörde, insbesondere in dem Mitgliedsstaat ihres gewöhnlichen Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DSGVO oder gegen § 1 oder Artikel 2 erstes Hauptstück des Datenschutzgesetzes (DSG) verstößt.

Sobald ein Ersuchen obiger Art (also eines, welches sich konkret auf die DSGVO stützt) bei Ihnen in der Einrichtung/Pfarre eingeht, ist dieses **umgehend** an die/den diözesane:n Datenschutzreferentin/-referenten weiterzuleiten. Beantworten Sie das jeweilige Begehren bitte **nicht** selbstständig!

DATENWEITERGABE („ÜBERMITTLUNGEN“):

Die Weitergabe („Übermittlung“, **„Offenlegung“**) von personenbezogenen Daten ohne Zustimmung der betroffenen Person an andere Empfänger als die betroffene Person selbst ist nur in wenigen Fällen möglich (etwa aufgrund einer gesetzlichen Verpflichtung oder im Zuge einer Auftragsverarbeitung). § 6 der Kirchlichen Datenschutzverordnung regelt die Datenweitergabe im kirchlichen Bereich – aber auch hier sind enge Grenzen gesetzt.

Im Zweifelsfall ist immer Rücksprache mit dem/der diözesanen Datenschutzreferenten/-referentin zu halten, da Übermittlungen im Verzeichnis der Verarbeitungstätigkeiten dokumentiert werden müssen!
Bei Genehmigung sind Übermittlungen zu protokollieren.

VERPFLICHTUNG ZUR EINHALTUNG DES DATENGEHEIMNISSES (§ 6 DSG)

§ 6 DSG regelt, dass der Verantwortliche, der Auftragsverarbeiter und deren Mitarbeiter:innen personenbezogene Daten aus Datenverarbeitungen, die ihnen **ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind,** unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim zu halten haben, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen personenbezogenen Daten besteht **(Datengeheimnis)**. Das Datengeheimnis gilt auch nach Dienstende bzw. nach Beendigung des Arbeitsverhältnisses (Dienstverhältnisses).

Aus diesem Grund ist (zumeist bei Dienstantritt) eine entsprechende Verpflichtungserklärung zu unterzeichnen, die im Personalakt abgelegt wird.

Achtung: Auch **ehrenamtliche** Mitarbeiter:innen, denen im Zuge ihrer Tätigkeit personenbezogene Daten anvertraut oder zugänglich gemacht werden, müssen VOR Aufnahme ihrer Tätigkeit eine Verpflichtungserklärung auf das Datengeheimnis (eben jene für Ehrenamtliche) unterzeichnen! Die Ablage findet in der jeweiligen Einrichtung/Pfarre statt.

DATENSICHERHEIT – WAS VERSTEHT MAN UNTER „TOMS“?

In der DSGVO finden sich nicht nur Bestimmungen zum Datenschutz im engeren Sinn, sondern auch zu **Datensicherheitsmaßnahmen**. Der Verantwortliche und der Auftragsverarbeiter haben geeignete **T**echnische und **O**rganisatorische **M**aßnahmen **(„TOMs“)** zu treffen, um die Datensicherheit zu gewährleisten, z. B. durch Pseudonymisierung und Verschlüsselung personenbezogener Daten bzw. grundsätzlich durch Maßnahmen zur Sicherung der IT-Systeme.

Artikel 24 DSGVO: „Verantwortung des für die Verarbeitung Verantwortlichen“

Artikel 25 DSGVO: „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“

- **Konsequente Datenminimierung:** Wird die erhobene oder verarbeitete Information wirklich für den konkreten, zu erreichenden Zweck benötigt?
- Der Verantwortliche trifft **geeignete technische und organisatorische Maßnahmen**, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Das gilt
  - für die Menge der erhobenen personenbezogenen Daten,
  - den Umfang ihrer Verarbeitung,
  - ihre Speicherfrist (Wie lange wird die Information benötigt?),
  - ihre Zugänglichkeit („Need-to-know-Prinzip“ für die jeweiligen Stellen).

Um sicherzustellen, dass Mitarbeiter:innen nur Zugriff auf jene Daten haben, die sie zur Erfüllung ihrer dienstrechtlichen Aufgaben benötigen, sind entsprechende Berechtigungen in den EDV-Systemen zu erteilen (Berechtigungskonzept).

Artikel 32 DSGVO: „Sicherheit der Verarbeitung“

„TOMs“ sind technische und organisatorische Maßnahmen, die eine angemessene Sicherheit bei der Verarbeitung personenbezogener Daten gewährleisten sollen, einschließlich Schutz vor **unbefugter** und **unrechtmäßiger** Verarbeitung und vor unbeabsichtigtem **Verlust**, **Zerstörung** oder **Schädigung**.

Die Daten müssen daher vor unberechtigtem Lesen, Verändern, Löschen und Kopieren geschützt werden. Dies gilt auch für Schriftstücke (Akte, Briefe, Listen etc.), Matrikenbücher und Datenträger. Werden Datenträger (z. B. auf Festplatten in PCs) nicht mehr weiterverwendet bzw. entsorgt, sind sämtliche darauf befindliche Daten unter Zuhilfenahme entsprechender Programme und/oder befugter Unternehmen komplett und UNWIEDERBRINGLICH zu löschen. Bei der Entsorgung von Schriftstücken in Papierform, die personenbezogene Daten enthalten, sind diese zu schreddern. Weiters sind der **Zutritt** zu den und der **Zugriff** auf die EDV-Anlagen und zu den Datenträgern zu regeln und zu kontrollieren (Berechtigungskonzepte).

Passwörter sind im Bedarfsfall zu ändern und dürfen nicht weitergegeben werden.
Personalisierte Zugänge und Accounts (z. B. E-Mail-Adresse, Zugangsdaten zum V4-Programm, Bankzugriffe etc.) dürfen nicht an Dritte weitergegeben werden!

Weitere Datensicherheitsmaßnahmen:

- Räume sind verschlossen zu halten, wenn sich niemand darin aufhält.
- Kästen, die zur Aufbewahrung personenbezogener Daten (Karteien, Akte, Matrikenbücher) verwendet werden, sind zu versperren (Schlüssel abziehen).
- Es dürfen keine Schriftstücke offen herumliegen, sodass Unbefugte daraus Daten entnehmen könnten (Drucker!).
- Beim Verlassen des Arbeitsplatzes ist der Bildschirm zu sperren (Strg + Alt + Entf oder Windows-Taste + L).
- PC so aufstellen, dass Besucher:innen/Unbefugte nicht auf den Bildschirm schauen können.
- Geeignete Passwörter wählen und NICHT öffentlich notieren oder weitergeben.

- Ein aktueller Virenschutz und eine aktuelle Firewall-Software sollten auf den Computern installiert sein.
- Regelmäßige Sicherheitsupdates der installierten Software sind durchzuführen.
- Die Benutzerberechtigungen an Computern sind an die entsprechenden Tätigkeiten der Benutzer:innen anzupassen.
- Mobile Geräte, Laptops, Handys und Tablets sind in einer Weise abzusichern, dass im Falle eines Verlustes oder Diebstahls der Zugriff auf personenbezogene Daten verhindert werden kann.
- Belehrung der Mitarbeiter:innen über Datenschutzregelungen und Sicherheitsüberprüfungen

Sollten im Einzelfall berufliche **Akte**, die personenbezogene Daten enthalten, zur weiteren Bearbeitung mit nach Hause genommen werden, ist sorgfältig darauf zu achten, wer dadurch Zugang zu diesen Daten haben könnte. Auch **zu Hause** muss die entsprechende Sicherheit der personenbezogenen Daten gewährleistet werden. Analoges gilt natürlich auch für **ehrenamtliche Mitarbeiter:innen** (z. B. Nicht-Einsehbarkeit von Listen für Unbefugte).

Im **Homeoffice** sind aus Datensicherheitsgründen ausschließlich die von der Dienstgeberin bereitgestellten bzw. von der Diözesanen IT (DIT) gewarteten digitalen Arbeitsmittel (Hardware), jedoch keine Privatgeräte zu benutzen (siehe dazu die entsprechende Betriebsvereinbarung **„Homeoffice und mobile Arbeitsformen in der Diözese Linz“**).

Weiters ist die (automatische) Weiterleitung von E-Mails, welche an die dienstliche E-Mail-Adresse gehen, auf eine andere Adresse nicht – bzw. nur aufgrund einer Sondergenehmigung – zulässig. E-Mails mit personenbezogenen Daten dürfen von Mitarbeiter:innen nicht an deren private E-Mail-Adresse weitergeleitet werden. Weiters darf die dienstliche E-Mail-Adresse nur für dienstliche Zwecke verwendet werden.

E-Mails an größere Adressatenkreise – vor allem bei Verwendung **externer** Adressen – sollten per **„Bcc“-Feld** versendet werden.

HISTORISCHER EXKURS: Bereits im Jahre 1979 (!) wurden im Zuge der Einführung des nationalen Datenschutzgesetzes zehn Datensicherheitsmaßnahmen („Kontrollen“) definiert, die auch heute noch ihre Gültigkeit haben:

Die „10 Gebote zur Datensicherung“

Werden personenbezogene Daten automatisiert verarbeitet, sind zur Ausführung der Vorschriften dieses Gesetzes Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind,

1. Unbefugten den Zugang zu den Datenverarbeitungsanlagen, in denen personenbezogene Daten verarbeitet werden, zu verwehren **(Zugangskontrolle)**,
2. Personen, die bei der Verarbeitung personenbezogener Daten tätig sind, daran zu hindern, dass sie Datenträger unbefugt entfernen **(Abgangskontrolle)**,
3. die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten zu verhindern **(Speicherkontrolle)**,
4. die Benutzung von Datenverarbeitungssystemen, aus denen oder in die personenbezogene Daten durch selbsttätige Einrichtungen übermittelt werden, durch unbefugte Personen zu verhindern **(Benutzerkontrolle)**,
5. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten durch selbsttätige Einrichtungen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können **(Zugriffskontrolle)**,
6. zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch selbsttätige Einrichtungen übermittelt werden können **(Übermittlungskontrolle)**,
7. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind **(Eingabenkontrolle)**,
8. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können **(Auftragskontrolle)**,

9. zu gewährleisten, dass bei der Übermittlung personenbezogener Daten sowie beim Transport entsprechender Datenträger diese nicht unbefugt gelesen, verändert oder gelöscht werden können **(Transportkontrolle)**,
10. die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird **(Organisationskontrolle)**.

WAS IST EINE DVR-NUMMER?

Bis zur Einführung der DSGVO im Mai 2018 wurde von der österreichischen Datenschutzbehörde das sogenannte Datenverarbeitungsregister **(DVR)** geführt, in dem Datenverarbeitungen („Zwecke der Verarbeitung") nach Genehmigung durch die Behörde **registriert** wurden (z. B. „Pfarrliche Seelsorge", „Matrikenführung", „Personalverwaltung" usw.). Der Datenverantwortliche erhielt eine DVR-Nummer, die bei Kontakten mit betroffenen Personen (z. B. im Mail- oder Schriftverkehr) angedruckt werden musste. Für die Katholische Kirche in Österreich wurde diese Nummer folgendermaßen dargestellt:

DVR: 0029874 (Sub-Nr. der Einrichtung)

Der Andruck ist seit Mai 2018 nun nicht mehr notwendig, allerdings wird das Datenschutz-Subnummernsystem **kirchenintern** weitergeführt, um einen Überblick über datenverarbeitende Einrichtungen gewährleisten zu können. Neue kirchliche Einrichtungen müssen daher – wenn sie personenbezogene Daten verarbeiten – eine solche Subnummer beantragen (siehe Seite 34).

BEISPIEL: Die Datenschutz-Subnummer der Katholischen Privat-Universität Linz lautet 1739.

DATENSCHUTZRECHTLICHE VERANTWORTLICHKEITEN IN DER KATHOLISCHEN KIRCHE IN ÖSTERREICH

- **Datenschutzbeauftragte:r der Katholischen Kirche in Österreich und ihrer Einrichtungen (DS-Beauftragte:r)**
  Diese:r ist gemäß Artikel 37 DSGVO verpflichtend zu benennen, wird von der Österreichischen Bischofskonferenz zur Wahrnehmung der Aufgaben

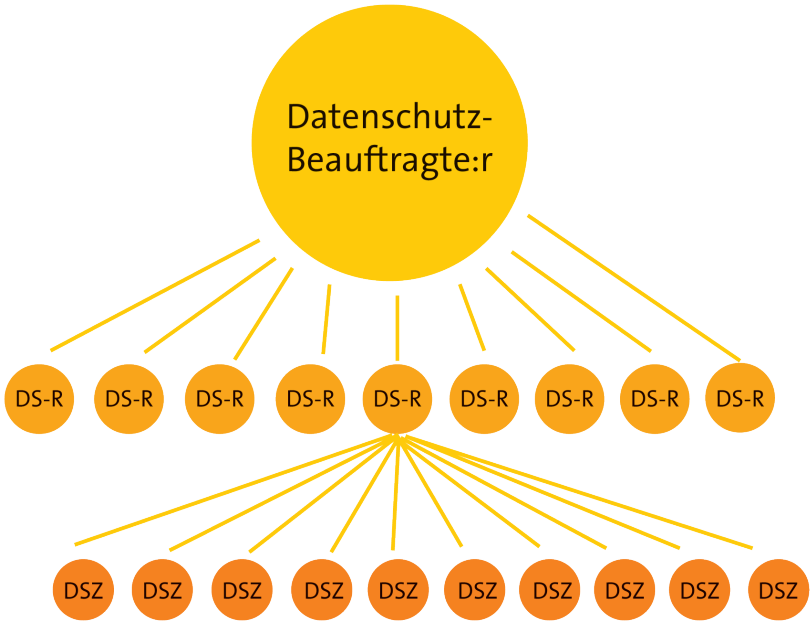
laut EU-DSGVO ernannt, tritt nach außen auf und ist Kontaktperson für die Aufsichtsbehörde. Zur Wahrung des Datenschutzes und zur Vertretung gegenüber staatlichen Behörden hat die Katholische Kirche Österreichs weiters eine **Kirchliche Datenschutzkommission** eingerichtet.

- **Bereichs-Datenschutzreferent:in (DS-R)**
  Auf Ebene der Diözesen bzw. der Orden wird ein:e Bereichs-Datenschutzreferent:in ernannt. Diese:r unterstützt die/den Datenschutzbeauftragte:n und steht ihrem/seinem Bereich als Ansprechpartner:in in datenschutzrechtlichen Fragen zur Verfügung.
- **Einrichtungs-Datenschutzzuständige:r (DSZ)**
  Gemäß § 8 Absatz 5 der kirchlichen Datenschutzverordnung ist für jede kirchliche Einrichtung von deren Leitung eine Person zu bestimmen, welche die Aufgabe hat, für die Einhaltung des Datenschutzes in der betreffenden Einrichtung Sorge zu tragen, und die damit verbundenen notwendigen Aufgaben erfüllt. Aus datenschutzrechtlicher Sicht betrifft dies vor allem folgende Fragen:
  - Welche Daten werden verarbeitet?
  - Dürfen diese Daten verarbeitet werden (Rechtsgrundlage)?
  - Welche Schutzmaßnahmen muss ich treffen?
  - Welche Pflichten treffen mich gegenüber den betroffenen Personen?
  - Ist der Webauftritt (Website) datenschutzkonform gestaltet?
  - Wurden etwaige Videoüberwachungsanlagen beim/bei der DS-R gemeldet?
  - Haben alle Mitarbeiter:innen (auch ehrenamtliche) die Verpflichtungserklärung auf das Datengeheimnis unterzeichnet?

Jede:r Datenschutzzuständige hat die für den Datenschutz notwendigen Maßnahmen umzusetzen.
Gerne bespricht der/die diözesane Datenschutzreferent:in anhand einer Datenschutz-Checkliste die wichtigsten Punkte mit Ihnen persönlich!

Mehrere kirchliche Einrichtungen können auch eine:n gemeinsame:n Zuständige:n benennen. In einer **Pfarre** übernimmt grundsätzlich der geistliche Leiter mit Übernahme seines Amtes auch die Aufgabe des Datenschutzzuständigen (Beschluss der Kanzlerkonferenz 2/2002).

In der **Diözese Linz** kann diese Aufgabe allerdings auch **delegiert** werden (Pfarrassistent:innen, Verwaltungsvorständ:innen)



II. PROZESSE: WAS IST ZU TUN, WENN ...

... EIN AUSKUNFTSBEGEHREN, LÖSCHUNGSBEGEHREN IN DER EINRICHTUNG/PFARRE ETC. EINLANGT?

Auskunftsbegehren gemäß Artikel 15 DSGVO, Löschbegehren gemäß Artikel 17 DSGVO bzw. sonstige Begehren, die sich auf die DSGVO stützen, sind ausnahmslos an die/den diözesane:n Datenschutzreferentin/-referenten weiterzuleiten und **nicht** von der Einrichtung/Pfarre zu beantworten.

... JEMAND EINE ADRESSÄNDERUNG ODER SONSTIGE ÄNDERUNGEN SEINER PERSONENBEZOGENEN DATEN BEKANNT GEBEN MÖCHTE?

Wenn möglich, vergewissern Sie sich, dass es sich wirklich um die betreffende Person handelt **(Feststellung der Identität)** – etwa durch Kontrollfragen (Geburtsdatum, alte Adresse, Beitragsnummer), oder Sie ersuchen um eine schriftliche Eingabe per Mail.

Wenn keine Zweifel an der Legitimität bestehen, dokumentieren Sie für sich, wann diese Anforderung bei Ihnen eingegangen ist, und **führen Sie die gewünschte Änderung durch**. Die Korrektur der Daten hat unverzüglich zu erfolgen.

... JEMAND EINEN NEWSLETTER ODER EIN ABO ABBESTELLEN MÖCHTE?

Wenn möglich, vergewissern Sie sich, dass es sich wirklich um die betreffende Person handelt **(Feststellung der Identität)** – etwa durch Kontrollfragen (Geburtsdatum, Beitragsnummer), oder Sie ersuchen um eine schriftliche Eingabe per Mail.

Wenn keine Zweifel an der Legitimität bestehen, dokumentieren Sie für sich, wann diese Anforderung bei Ihnen eingegangen ist, und **löschen** Sie anschließend die Adresse, E-Mail, Telefonnummer etc. aus Ihrer Newsletter-/Verteiler-/Abo-Liste. Stellen Sie sicher, dass **keine weiteren Zusendungen** an die betroffene Person mehr erfolgen (Ausnahme: Die betroffene Person wünscht eine Bestätigung über die erfolgte Löschung). Die Korrektur der Daten hat unverzüglich zu erfolgen.

... EINE NEUE DATENANWENDUNG („DATENVERARBEITUNG“) EINGESETZT WERDEN SOLL?

Eine neue Datenanwendung (siehe Seite 10, „Zweck der Verarbeitung“) darf ohne Zustimmung des/der zuständigen Bereichs-Datenschutzreferenten/-referentin nicht in Betrieb genommen werden. Bei der Aufnahme neuer bzw. der Ausweitung/Änderung bestehender Datenanwendungen ist daher neben dem/der Datenschutzzuständigen der Einrichtung auch der/die diözesane Datenschutzreferent:in zu informieren und einzubeziehen, insbesondere sind ihm/ihr von der betreffenden Einrichtung die geplanten Verarbeitungstätigkeiten zu nennen.
Die Datenanwendung ist vom/von der diözesanen Datenschutzreferenten/-referentin zu prüfen und ggf. im Verzeichnis der Verarbeitungstätigkeiten zu dokumentieren.

... EINE NEUE KIRCHLICHE EINRICHTUNG ENTSTEHEN SOLL?

Im Zuge der Errichtung einer neuen kirchlichen Einrichtung (Stiftung etc.) ist der bei Aufnahme einer neuen Datenverarbeitung beschriebene Prozess einzuhalten (siehe Seite 33). Wenn der/die Bereichs-Datenschutzreferent:in die Inbetriebnahme der Datenverarbeitung für zulässig erachtet und diese im Verzeichnis der Verarbeitungstätigkeiten dokumentiert hat, übermittelt er/sie der Kirchlichen Datenschutzkommission (BIKO) den Antrag auf Bewilligung einer **Datenschutz-Subnummer**.

Die Bewilligung erfolgt auf Grundlage des Antrags durch die Kirchliche Datenschutzkommission. Die Datenschutz-Subnummer ist der Einrichtung mitzuteilen.

... EINE DATENSCHUTZVERLETZUNG (DATA BREACH, DATENLECK) AUFTRITT?

Eine **„Verletzung des Schutzes personenbezogener Daten“** ist jede Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig,

- zur Vernichtung,
- zum Verlust (Diebstahl!),
- zur Veränderung oder
- zur unbefugten Offenlegung von bzw. zum
- unbefugten Zugang zu

personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden (Artikel 4 Ziffer 12 DSGVO).

Sollte es also trotz aller Vorsicht passieren, dass Daten unbefugt in die Hände Dritter gelangen (Hackerangriff) oder verloren gehen (USB-Stick, Laptop etc.) sind folgende Schritte durchzuführen:

1. Benachrichtigen Sie bitte umgehend Ihre:n Vorgesetzte:n bzw. die/den Datenschutz-Zuständige:n Ihrer Einrichtung/Pfarre.
2. In weiterer Folge ist so rasch wie möglich und sehr detailliert das Formular „Meldung einer Datenschutz-Verletzung“ auszufüllen und an den/die diözesane:n Datenschutzreferenten/-referentin zu übermitteln.
3. Bei Verlust von dienstlichen IT-Geräten ist zusätzlich der DIT-Helpdesk zu verständigen (helpdesk@dioezese-linz.at).

TIPP: Drucken Sie sich das entsprechende Formular für den Ernstfall aus und halten Sie es „griffbereit"! Dieses steht im diözesanen Mitarbeiter:innen-Portal „DiALog" im Bereich Datenschutz zur Verfügung.

Rechtlicher Hintergrund (Artikel 33 und 34 DSGVO):
Treffen bestimmte Voraussetzungen zu, so muss der/die Datenschutzbeauftragte der Katholischen Kirche in Österreich innerhalb von 72 Stunden diesen Vorfall der Datenschutzbehörde melden bzw. kann es sein, dass jede von der Datenschutzverletzung betroffene Person über den Vorfall informiert werden muss!

... PERSONENBEZOGENE DATEN VERÖFFENTLICHT WERDEN SOLLEN?

Personenbezogene Daten wie z. B. Namen, Geburtsdaten, Telefonnummern unterliegen natürlich dem Datenschutz. **VOR** der Veröffentlichung personenbezogener Daten in Pfarrblättern (Taufen, Geburtstage, Erstkommunion, Firmung, Trauungen, Jubiläen ...) bzw. öffentlich zugänglichen Listen bzw. auf Websites ist daher immer die **Zustimmung** der betroffenen Person (bzw. des/der Erziehungsberechtigten) einzuholen.
Die Zustimmung sollte direkt beim Erst-Kontakt (z. B. einer Sakramenten-Anmeldung im Pfarrbüro) – jedenfalls aber vorab – am besten schriftlich eingeholt werden. Für den/die Unterzeichner:in muss erkenn- und abschätzbar sein, mit welcher Veröffentlichung er/sie rechnen muss (Medium, Internet, Social Media etc.).

Besonders Veröffentlichungen im **Internet** sind heikel, da diese Daten und Bilder dann allgemein zugänglich sind und sie oft nicht mehr gänzlich gelöscht werden können. Über Suchmaschinen sind die Daten weltweit abrufbar – es könnten somit Profile erstellt werden, die für verschiedene Zwecke – auch missbräuchlich – verwendet werden könnten.

... PERSONENBEZOGENE DATEN AN EINEN AUFTRAGSVERARBEITER (ALT „DIENSTLEISTER") ÜBERGEBEN WERDEN?

Der Verantwortliche hat sicherzustellen, dass auch beim Auftragsverarbeiter die datenschutzrechtlichen Bestimmungen eingehalten werden. Daher muss mit dem Auftragsverarbeiter (Dienstleister) ein **Auftragsverarbeitungsvertrag**

gemäß Artikel 28 DSGVO abgeschlossen werden. Ein diesbezügliches Vertragsmuster steht als Download im diözesanen Mitarbeiter:innen Portal „DiALog“ zur Verfügung oder kann beim/bei der diözesanen Datenschutzreferenten/-referentin angefordert werden.

BEISPIEL: Eine Pfarre lässt das Pfarrblatt von einer Druckerei drucken und gleichzeitig versenden. Hierzu müssen die Adressdaten der Pfarrblattbezieher:innen an die Druckerei übermittelt werden. Die Druckerei wird nun für die Pfarre als Auftragsverarbeiter gemäß Artikel 4 Ziffer 8 DSGVO tätig, da personenbezogene Daten **im Auftrag der Pfarre** verarbeitet werden –> Die Pfarre muss einen Vertrag mit der Druckerei abschließen, in welchem sich die Druckerei zur Einhaltung des Datenschutzes verpflichtet.

... DIE EINRICHTUNG/PFARRE EINE VIDEOÜBERWACHUNG INSTALLIEREN MÖCHTE?

Geplante Videoüberwachungsanlagen sind ausnahmslos beim/bei der diözesanen Datenschutzreferenten/-referentin zu **beantragen** und dürfen nur im Falle einer Genehmigung installiert bzw. betrieben werden! Im Falle der Genehmigung müssen die Vorgaben der diözesanen **Videoüberwachungsordnung** unbedingt eingehalten werden (Kennzeichnung, Speicherdauer etc.)!

Diese Vorgabe gilt für alle Arten von geplanten Überwachungsanlagen, also auch für Echtzeitüberwachungen („Verlängertes Auge“) und Kamera-Attrappen!

§ **Eine Bildaufnahme darf niemals in den höchstpersönlichen Lebensbereich einer Person eingreifen (WC, Umkleideraum) oder der Arbeitnehmer:innen-Kontrolle dienen!**

§ **HINWEIS: Bzgl. „Bildverarbeitung“ sind auch § 12 DSG („Zulässigkeit der Bildaufnahme“) und § 13 DSG („Besondere Datensicherheitsmaßnahmen und Kennzeichnung“) zu beachten!**

... EINSICHT IN BZW. AUSKUNFT AUS MATRIKENBÜCHERN VERLANGT WIRD?

Da bei derlei Anfragen neben dem Datenschutzrecht auch regelmäßig das **Personenstandsgesetz** (PStG) und dessen **Sperrfristen** (§ 52 Absatz 5 Ziffern 1–3 PStG 2013) eine Rolle spielt, wurden diesbezüglich detaillierte Vorgaben, der sogenannte „Matrikenwegweiser“, erarbeitet.

Den **„Wegweiser zur Führung der Pfarrmatriken“** finden Sie im diözesanen Mitarbeiter:innen-Portal „DiALog“ im Bereich „Ordinariatsamt“!

Zusätzlich gibt es die Vorgabe (LDBl. 162/3, 2016, Art. 30), dass – bei Unklarheiten – Anfragen (z. B. von Historikerkanzleien, Ahnenforscher:innen) ausnahmslos an das **Diözesanarchiv** (archiv@dioezese-linz.at) weiterzuleiten sind und dort entschieden wird, **ob** und **welche** Auskunft zu geben ist.

Im Zuge einer Auskunftserteilung bedenken Sie bitte immer auch Folgendes:

- Der/Die Anfragende muss seine/ihre Berechtigung nachweisen (Legitimierung durch Urkunde, Ausweis oder Vollmacht)!
- Es darf nur der entsprechende Matrikenfall beauskunftet werden, nicht „darüber hinaus“.

... WENN EIN GOTTESDIENST LIVE ÜBERTRAGEN WERDEN SOLL („STREAMING“)?

Bei Messfeiern handelt es sich um die Ausübung einer religiösen Tätigkeit – wir befinden uns daher datenschutzrechtlich im Bereich sensibler Daten, die einem erhöhten Schutz unterliegen!

- Mit dem Pfarrer und den liturgischen Diensten (Ministrant:innen, Chor, Organist:in ...) ist im Vorfeld abzuklären, dass der Gottesdienst übertragen wird (auch das WO = in welchem Medium) –> Die Zustimmung der Beteiligten ist einzuholen.
- Bei religiösen Feiern bzw. Gottesdiensten aus einmaligem Anlass (Taufe, Firmung, Erstkommunion, Trauung) klären Sie bitte **vorab** mit den Betroffenen, wie die Feier gestaltet werden soll (Streaming, Fotograf:in).
- Bzgl. Besucher:innen empfiehlt es sich, dass mittels **Ansage zu Beginn** der Messe darauf hingewiesen wird, dass diese übertragen wird (Informationspflicht gemäß DSGVO) – so können Besucher:innen, die das nicht wünschen, rechtzeitig das Kirchengebäude oder den gefilmten Bereich verlassen. Auch ein dementsprechender Aushang am Eingang ist zusätzlich angeraten – allerdings kann man hierbei nicht 100%ig davon ausgehen, dass der Aushang von allen gesehen/gelesen wird –> daher auf jeden Fall die Information zu Beginn über die Ansage!

TIPP: Die Einstellung bzw. die Auflösung der Kamera sollte so gewählt werden, dass einzelne (Gottesdienstbesucher:innen) nicht identifizierbar sind („Filmen von hinten“) und somit gar keine personenbezogenen Daten entstehen!

- Es wird dringend davon abgeraten, den **Kommunionempfang** (als höchst sensiblen, persönlichen Bereich) zu filmen bzw. zu übertragen – für diese Zeitspanne empfiehlt sich etwa ein Standbild (Altar).
- Es ist zu überlegen, ob die Aufzeichnung nur einem **geschlossenen, also nicht öffentlichen**, Kreis zur Verfügung gestellt werden kann (z. B. über einen Passwort-Zugang).
- Bitte beachten Sie, dass beim Streamen auch **medien-** und vor allem **urheberrechtliche** Fragestellungen betroffen sind (Verbreitung der Inhalte, evtl. Löschpflicht für Zugriffe von außen)! Sinnvoll ist somit, vorab zu klären, ob eine „echte“ Übertragung stattfinden soll (also ein Livestream **ohne** Aufzeichnung) oder ob eine **Aufzeichnung** stattfindet, die dann z. B. als Link für eine gewisse Zeit zur Verfügung gestellt wird. Datenschutzrechtlich wäre hier Ersteres zu bevorzugen.

III. LÖSCHUNG AUS MATRIKENBÜCHERN / DATEN NACH KIRCHENAUSTRITT

Aufgrund eines Rechtssatzes der Datenschutzkommission (jetzt Datenschutzbehörde) aus dem Jahr 2007 besteht kein Recht auf Löschung aus kirchlichen Matrikenbüchern (K121.309/0010-DSK/2007)!

Die Katholische Kirche in Österreich hat aufgrund Artikel 15 StGG (Staatsgrundgesetz) das Recht, ihre inneren Angelegenheiten selbstständig zu ordnen und zu verwalten. Dieses Recht stellt eine **Grenze der Löschungsverpflichtung** dar: Personenbezogene Daten, anhand derer sich nachvollziehen lässt, ob ein bestimmtes **Sakrament** (z. B. die Taufe) stattgefunden hat (also Matrikendaten), müssen bzw. dürfen **nicht** gelöscht werden! Durch die Löschung kann insbesondere nicht

erreicht werden, dass bestimmte Ereignisse „ungeschehen“ gemacht werden – z. B. kann bei einem Kirchenaustritt **nicht** die Löschung des Taufeintrages aus dem Taufbuch begehrt werden. Die **Matrikenführung** dient nämlich u. a. **Dokumentationszwecken**.

Die in den Matriken enthaltenen Daten müssen bei einem Kirchenaustritt nicht gelöscht werden. Es ist ausreichend, den jeweiligen Eintrag mit einem Hinweis auf den Austritt zu versehen.

Bei der Verarbeitung der Daten Ausgetretener ist jedoch **besondere Sorgfalt** geboten – insbesondere dürfen Daten von Ausgetretenen nicht wie aktuelle Daten verarbeitet oder gar übermittelt werden! Eine Veröffentlichung in jeder Form (Verlesung, Aushang, Pfarrblatt) ist **nicht zulässig**. Ebenso dürfen die Eintragungen nicht mehr aktualisiert oder zur Kontaktaufnahme verwendet werden (außer auf ausdrücklichen Wunsch der betroffenen Person und Dokumentation desselbigen)!

IV. POSTALISCHE ZUSENDUNGEN FÜR INFORMATIONS- UND WERBEZWECKE

Wie bereits weiter oben ausgeführt, kann die Rechtmäßigkeit der Datenverarbeitung im **berechtigten Interesse** des Verantwortlichen liegen. Dieses liegt z. B. vor, wenn eine **maßgebliche Beziehung zwischen dem Verantwortlichen und der betroffenen Person** besteht oder wenn die betroffene Person vernünftigerweise mit der Verarbeitung ihrer Daten rechnen kann (z. B. Information, Direktwerbung und Direktmarketing).

Der Begriff der Direktwerbung ist weit auszulegen; darunter fallen auch Informationsschreiben, Marketingmaßnahmen und Werbungen für bestimmte Ideen, weiters auch Informationen über Veranstaltungen (z. B. Jahresfeiern, Adventmärkte, heilige Messen, Lesungen, Seminare, Kurse) und sonstige Ereignisse (z. B. Priesterweihe, erster Tag des neuen Jungscharjahres), weil mit diesen Zusendungen versucht wird, die Adressat:innen zur Teilnahme zu bewegen und die Reputation der Katholischen Kirche in Österreich zu steigern.
Bei Schreiben zum Zweck der Information, Direktwerbung oder des Direktmarke-

tings **per Post** ist der Eingriff in die Privatsphäre gering und im Sinne eines berechtigten Interesses des Verantwortlichen in den allermeisten Fällen zulässig (z. B. Schreiben einer Pfarre an die Pfarrangehörigen aufgrund „pastoraler Zwecke“).

Bei der Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung besteht ein absolutes Widerspruchsrecht! Die betroffene Person kann jederzeit ohne Angabe von Gründen dieser Datenverarbeitung widersprechen und der Verantwortliche darf dann die Daten nicht mehr weiter für diesen Zweck verarbeiten (Artikel 21 Absatz 2 und Absatz 3 DSGVO).

V. ANRUFE, SMS, E-MAILS UND E-MAIL-NEWSLETTER ZU WERBEZWECKEN

Auch für Telefonanrufe und den Versand von SMS bzw. E-Mails werden personenbezogene Daten, nämlich Name, Telefonnummer und E-Mail-Adresse, verarbeitet.

ACHTUNG: Hierfür ist zusätzlich zu den datenschutzrechtlichen Regelungen § 174 Telekommunikationsgesetz 2021 (TKG 2021) bzgl. „unerbetener Nachrichten“ zu beachten!

E-Mail-Newsletter etwa fallen unter Online-Direktwerbung und es gelten für diese weiterhin die Bestimmungen des Telekommunikationsgesetzes (TKG) unter Berücksichtigung der DSGVO. Dies bedeutet, dass die Verarbeitung von personenbezogenen Daten rechtmäßig sein muss.

Grundsätzlich ist festzuhalten, dass der Versand von E-Mails und SMS-Nachrichten zulässig ist, wenn eine Einwilligung vorliegt.

ACHTUNG: Auch bei Zulässigkeit muss der/die Empfänger:in klar und deutlich die Möglichkeit erhalten, eine solche Nutzung der elektronischen Kontaktinformation bei deren Erhebung und zusätzlich bei jeder Übertragung kostenfrei und problemlos abzulehnen (Widerrufsmöglichkeit)!

VI. INTERNETSEITEN – VERWENDUNG VON COOKIES

Cookies sind Textinformationen, die von einer besuchten Internetseite auf dem Computer des Nutzers/der Nutzerin hinterlegt werden. Sie dienen dazu, den/die Nutzer:in später „wiederzuerkennen", und bieten dem/der Nutzer:in eine an seine/ihre Benützung angepasste Website (z. B. durch Werbebanner, bei Suchmaschinen, bevorzugte Sprache).
Betreiber:innen öffentlicher Kommunikationsmittel und Anbieter:innen eines Dienstes der Informationsgesellschaft sind dazu verpflichtet, den/die Benutzer:in zu informieren, welche personenbezogenen Daten verarbeitet werden, auf welcher Rechtsgrundlage, für welche Zwecke und mit welcher Speicherdauer (–> Datenschutzerklärung der Website!).

Cookies dürfen in der Regel nur verwendet werden, wenn der/die Nutzer:in dazu seine/ihre ausdrückliche Einwilligung erteilt hat. In Österreich ist dies (vom/von der jeweiligen Webmaster:in) durch eine „Opt-in"-Variante umzusetzen („OK"-Klicken, Häkchen setzen).

Siehe dazu auch § 165 Absatz 3 Telekommunikationsgesetz 2021!

VII. VERÖFFENTLICHUNG VON TODESFÄLLEN UND BEGRÄBNISSEN

Wie bereits einleitend erwähnt, endet der Datenschutz als höchstpersönliches Recht mit dem Tod der betroffenen Person. Veröffentlichungen von Todesfällen und Begräbnissen sind daher in der Regel **zulässig** und **unproblematisch** (auch im Internet).

Somit **dürfen** z. B. Name und Bild des/der Verstorbenen (Totengedenkbild) sowie das Datum des Begräbnisses veröffentlicht werden, ohne eine Zustimmung Hinterbliebener einholen zu müssen. Natürlich wird man aber den Wunsch Angehöriger akzeptieren, wenn diese keine Veröffentlichung wünschen.

Viele Pfarren melden zurück, dass sie bei Verstorbenen nicht mehr die genaue Adresse angeben (sondern nur noch den Ort oder Ortsteil), da es Betrüger gibt, die leerstehende Häuser oder Witwen gezielt aufsuchen. Informationen, welche die Privatsphäre der Hinterbliebenen berühren, dürfen (ohne Zustimmung) nicht veröffentlicht werden (z. B. „hat sich umgebracht").

Etwas anders stellt sich die Situation bei **Parten** dar: Da auf einer Parte auch personenbezogene Daten von Hinterbliebenen ersichtlich sind, ist in diesem Fall die Veröffentlichung der Parte nur mit vorheriger Zustimmung (z. B. des für die Begräbnis-Abwicklung Zuständigen) zulässig. Eventuell kann auch das Bestattungsunternehmen eine diesbezügliche Zustimmung einholen und an die Pfarre weiterleiten.

VIII. DIE VERWENDUNG VON FOTOS UND VIDEOS („BILD-, TON- UND FILMMATERIAL")

Rechtlich geschützt ist ganz allgemein die **Privatsphäre** jedes Menschen, unabhängig von dessen Alter (Anspruch auf Achtung seines Privat- und Familienlebens gemäß Artikel 8 der Europäischen Menschenrechtskonvention [EMRK]).

BEI DER VERWENDUNG VON FOTOS UND VIDEOS SIND IM WESENTLICHEN DREI FRAGESTELLUNGEN ZU BEACHTEN:

1. ***Stimmt die auf dem Foto oder im Video abgebildete Person der Aufnahme und deren Veröffentlichung zu?***

   Grundsätzlich dürfen Fotos und Videos von Personen gemacht werden. Sie dürfen jedoch nicht öffentlich ausgestellt oder öffentlich zugänglich gemacht werden („*Recht am eigenen Bild*", Bildnisschutz gemäß § 78 Urheberrechtsgesetz), wenn dadurch **berechtigte Interessen** des/der Abgebildeten oder seiner/ihrer nahen Angehörigen verletzt werden. Das Bildnisrecht ist eine Ausprägung des im § 16 ABGB normierten **Persönlichkeitsrechts**. Der Bildnisschutz dient somit dem Persönlichkeitsschutz und ist ein Interessenschutz für abgebildete Personen, kein Schutz gegen Bildaufnahmen an sich. Im Zweifel ist eine Einwilligung der abgebildeten Person einzuholen.
   Wenn mit dem Foto bzw. dem Video direkt in die Privat- oder Intimsphäre

der/des Abgebildeten eingegriffen wird, ist jedenfalls eine Zustimmung vor dem Fotografieren erforderlich.
Bei der Verletzung schutzwürdiger Interessen, z. B. der Preisgabe des Privatlebens, bestehen zivilrechtliche Ansprüche (u. a. Unterlassung, Beseitigung, Schadenersatz).

Prüffrage: Wirft das Foto ein negatives Licht auf die/den Abgebildete/n? Könnte ihr/ihm die Abbildung unangenehm sein?

2. ***Stimmt der/die Fotograf:in der Verwendung des Fotos oder des Videos zu?***

Mit dem Fotografen/der Fotografin sollte jedenfalls eine schriftliche Vereinbarung getroffen werden, ob und in welchem Ausmaß dessen/deren Fotos und Videos verwendet werden dürfen und ob ein Hinweis auf den/die Urheber:in (z. B. Copyright) angebracht werden soll. Widrigenfalls droht die Durchsetzung zivilrechtlicher Ansprüche (z. B. Unterlassung, Beseitigung, Schadenersatz).

VORSICHT: Sie sollten bei der Verwendung fremder Aufnahmen besonders vorsichtig sein – der/die Fotograf:in ist der/die Urheber:in des Fotos oder Videos und kann Nutzungsrechte einräumen. Die Verwendung von Fotos oder Videos, die nicht selbst hergestellt wurden, ist daher von der Zustimmung des Urhebers/der Urheberin zur Nutzung abhängig!

3. ***Sind allenfalls Erklärungen aufgrund datenschutzrechtlicher Bestimmungen (DSGVO, DSG) einzuholen?***

Fotos und Videos sind personenbezogene Daten, wenn die Identität der betroffenen Person bestimmt oder bestimmbar ist (= die betroffene Person ist **erkennbar**).

Es kommt nicht auf die Anzahl der abgebildeten Personen an („Märchen der 5"), sondern auf deren Erkenn- bzw. Identifizierbarkeit!

Solche Fotos und Videos dürfen im Internet, Zeitschriften o. Ä. nur dann verarbeitet und veröffentlicht werden, wenn dafür eine **Rechtsgrundlage** besteht. In den meisten Fällen ist die Veröffentlichung nur dann zulässig, wenn eine **Einwilligung** der betroffenen Person vorliegt. Diese ist **vor** der Veröffentlichung einzuholen.

Eine Zustimmung zur Veröffentlichung ist immer dann notwendig, wenn berechtigte Interessen des/der Abgebildeten betroffen sind.

In der Judikatur werden diese „berechtigten Interessen" bzw. das „Recht am eigenen Bild" sehr streng (d. h. zugunsten der betroffenen Person) ausgelegt (Stichwort „Persönlichkeitsrechte"). Bei der Beurteilung, ob das Recht am eigenen Bild verletzt ist, ist nach ständiger Rechtsprechung nicht nur auf das Bild selbst, sondern auch auf den in Zusammenhang mit dem Bild veröffentlichten **Begleittext** abzustellen.

- Berechtigte Interessen können verletzt werden durch **Bloßstellung, Entwürdigung, Klischees, Herabsetzung** oder **Preisgabe des Privatlebens (der Intimsphäre),** jedenfalls aber durch Verwendung zu **Werbezwecken**.
- Je besser erkennbar eine Person auf dem Foto ist, desto eher besteht die Gefahr, dass die Aufnahme ihre **Privatsphäre** berührt! Auch ist zu prüfen, ob die dargestellte Person das Foto als faire und wahrheitsgemäße Darstellung empfinden würde.

Die Privatsphäre betrifft jeden Menschen höchstpersönlich. Einem Eingriff in die Privatsphäre – und sei es auch „nur" durch das Veröffentlichen eines Fotos – kann daher an sich auch nur jede:r selbst zustimmen. Das ist bei Kindern bis zu einem bestimmten Alter in der Praxis nicht durchführbar. Bis zum vollendeten 14. Lebensjahr wird daher in der Regel die Zustimmung der/des Erziehungsberechtigten ausreichend sein, aber grundsätzlich sollten auch immer die Abgebildeten einverstanden sein.

Kinder und Jugendliche sind besonders schutzwürdig – es ist darauf zu achten, dass diese nicht nachteilig dargestellt werden.

§ **AUSNAHMSLOS VERBOTEN sind Aufnahmen, welche die Intimsphäre betreffen, wie z. B. Aufnahmen in Umkleidekabinen, Nacktbilder oder Ähnliches!**

Prüffrage: Möchte ich, dass mein eigenes Kind oder ich selbst so dargestellt wird oder werde?

Bei Fotos/Videos von öffentlichen Versammlungen und Personen des öffentlichen Lebens (z. B. Prominente, Politiker:innen, Funktionsträger:innen bei Ausübung ihrer Tätigkeit) **im öffentlichen Raum** ist eine Zustimmungserklärung im Regelfall nicht erforderlich.
Gleiches gilt, wenn von einer **schlüssigen Zustimmung** ausgegangen werden kann (z. B. durch bewusstes Posieren), oder wenn die Person nur als „Beiwerk" zum Motiv aufscheint.

Bei der Veröffentlichung ist auf den Kontext, in welchem die Bilder/Videos gemacht wurden, zu achten. Zeigen diese Personen z. B. beim Sakramentenempfang, so enthalten die Bilder/Videos **sensible Daten** (nämlich über die religiöse Ausrichtung der betroffenen Person). Gleiches gilt, wenn Fotos von Patient:innen, etwa im Rahmen der Seelsorge, gemacht werden – hier handelt es sich allenfalls um Gesundheitsdaten. Das Veröffentlichen von derlei Fotos kann berechtigte Interessen verletzen!

Ist das Ziel eines Fotos, dass darauf bestimmte Personen (also nicht „die Menge") abgebildet werden und werden in der Bildunterschrift auch noch deren Namen genannt (Gruppenfoto der Erstkommunionkinder, Firmlinge etc.), ist vor der Veröffentlichung jedenfalls eine Zustimmung der Personen oder ihrer gesetzlichen Vertreter:innen einzuholen.

TIPP: Die Einstellung bzw. die Auflösung der Kamera sollte so gewählt werden, dass einzelne Gottesdienstbesucher:innen nicht identifizierbar sind („Aufnahme von hinten") und somit gar keine personenbezogenen Daten entstehen!

Fotos und Videos von **öffentlich zugänglichen Veranstaltungen** (Pfarrball, Adventmarkt etc.) und vom Gottesdienst dürfen mit bestimmten Vorbehalten auch ohne ausdrückliche Einwilligung veröffentlicht werden. Dies gilt aber nur dann, wenn die Bild- und Tonaufnahmen für alle Besucher:innen sichtbar sind (= kein „heimliches" Fotografieren, Filmen) und Bilder von diesen Vorgängen dabei grundsätzlich nicht gezielt **einzelne Personen** hervorheben, sondern das **Gesamtgeschehen dokumentieren**.
Es wird daher dringend empfohlen, zu Beginn der Veranstaltung bzw. des Gottesdienstes auf allfällige Aufnahmen **hinzuweisen** (Informationspflicht

gemäß DSGVO) bzw. zusätzlich mittels Aushängen an den Eingängen **(entsprechende Muster sind im Mitarbeiter:innen-Portal „DiALog“ vorhanden)** darüber zu **informieren**.

Bilder dürfen auch nur im ursprünglichen Kontext verwendet werden. BEISPIEL: Die Bilder eines Pfarrfaschings dürfen nur für die konkrete Berichterstattung darüber verwendet werden, nicht aber z. B. für eine spätere Bewerbung eines Spielenachmittages.

- Auch hier ist auf die berechtigten Interessen des/der Abgebildeten zu achten – wird z. B. ein:e Teilnehmer:in eines Pfarrfestes in unvorteilhafter Pose (etwa betrunken) abgebildet, kann sein/ihr Recht am eigenen Bild verletzt sein!
- **Im Zweifel ist vor der Veröffentlichung eine Einwilligung einzuholen!** Sie können das z. B. bereits bei der Anmeldung zur Veranstaltung bzw. bei der Anmeldung des Sakraments im Pfarrbüro tun – holen Sie das Einverständnis zur Nutzung bzw. Veröffentlichung von Fotos/Videos am besten schriftlich ein und achten Sie darauf, dass sowohl die Veranstaltung als auch die möglichen Formen der Veröffentlichung (Pfarrblatt, Website, YouTube etc.) **genau** benannt sind!

Für die Veröffentlichung von Fotos und Videos von nicht **öffentlich zugänglichen Veranstaltungen** (z. B. wöchentliche Treffen des Seniorenclubs, Gruppenstunden, Seminare & Workshops) ist die Einwilligung der betroffenen Person(en) vor Veröffentlichung einzuholen.

Zu guter Letzt sei im Zusammenhang mit Bildveröffentlichungen auch noch auf das Medienrecht hingewiesen – z. B. auf § 6 MedienG („Üble Nachrede, Beschimpfung, Verspottung und Verleumdung“) und § 7 MedienG („Verletzung des höchstpersönlichen Lebensbereiches“).

FAZIT: Vor der Veröffentlichung von Fotos mit erkennbaren Personen sollte nach Möglichkeit deren Zustimmung eingeholt werden (zumindest mündlich). Ist das im konkreten Fall nicht machbar, so ist bei der Wahl des Motivs (Person und Situation) sowie der Begleittexte Vorsicht geboten. Fotos „prominenter“ Personen bzw. Aufnahmen im öffentlichen Bereich sind

grundsätzlich risikoärmer, aber auch hier gibt es Grenzen. Die rechtliche Abgrenzung ist oftmals schwierig. Im Zweifel sollte daher die Wahl auf ein neutrales Foto fallen.

Kurz-Checkliste bzgl. Foto-Veröffentlichung:

- **Fotos, die identifizierbare Personen zeigen –> Prüfung der Persönlichkeitsrechte der/des Abgebildeten:**
  - Könnte das Foto berechtigte Interessen der/des Abgebildeten verletzen?
  - Benötige ich eine Zustimmung der/des Abgebildeten?
  - Sind Kinder abgebildet? Wenn ja, habe ich die Zustimmung des/der Erziehungsberechtigten?
- **Fotos, die nicht ich erstellt habe –> Prüfung der Nutzungsrechte:**
  - Wer ist Urheber:in des Fotos?
  - Habe ich die Erlaubnis (Lizenz) des Fotografen/der Fotografin zur Verwendung?

IX. GEFAHREN BEI SOCIAL-MEDIA-NUTZUNG

Beachten Sie bitte, dass neben datenschutzrechtlichen Risiken bei der Nutzung von Social-Media-Kanälen weiters eine Verantwortung der Medieninhaberin/des Medieninhabers (z. B. eines offiziellen Facebook-Auftrittes) nicht nur für eigene Inhalte, sondern auch für Kommentare („Postings“) darunter besteht!

§ **Neben dem Verbotsgesetz können Straftatbestände bei Internet-Postings unter anderem durch Cyber-Mobbing (§ 107c StGB), Verhetzung (§ 283 StGB) und Beleidigung (§ 115 StGB) erfüllt sein.**

- Eine **regelmäßige Beobachtung** des eigenen Auftritts im Web ist daher erforderlich!
- Entsprechende Kommentare **löschen** und für Beweiszwecke dokumentieren (Screenshot)
- ***Grundsatz: „Was offline verboten ist, ist auch online verboten!“***

Bei jeglicher Konversation über Social-Media-Kanäle wie etwa WhatsApp ist besonders auf die übermittelten **Inhalte** zu achten – WAS wird gesendet (keine vertraulichen, sensiblen Daten). Dies gilt natürlich besonders für diözesane Mitarbeiter:innen!

Merksatz: „Termine ausmachen & informieren ist okay, das Versenden von Gehaltslisten nicht!“

X. ARCHIVE

Die DSGVO ermöglicht die Verarbeitung von (auch sensiblen) personenbezogenen Daten zu **Archivzwecken** über den Zeitpunkt hinaus, zu dem der ursprüngliche Zweck der (zulässigen) Datenverarbeitung endet. Archivierung bedeutet nicht bloße Aufbewahrung. Es geht um **Aufzeichnungen von bleibendem Wert, die für das allgemeine öffentliche Interesse für immer und ewig erhalten, aufbereitet und verbreitet werden sollen.**

Neben den einschlägigen Rechtsgrundlagen bzgl. der Verarbeitung von personenbezogenen Daten zu Archivzwecken in der DSGVO (Artikel 5 Absatz 1 lit. b und e DSGVO, Artikel 9 Absatz 2 lit. j DSGVO, Artikel 89 Absatz 3 DSGVO) und im nationalen Datenschutzgesetz (§ 7 DSG) sind überdies das **Kanonische Recht** (can. 491, 535 CIC) und die **diözesane Archivordnung**[4] zu beachten! Weiters müssen auch für Archive grundlegende **Datensicherheitsmaßnahmen** gewährleistet sein.

Bzgl. Aufbewahrungsfristen bzw. -pflichten im Zusammenhang mit Archiven beachten Sie bitte die Vorgaben im „Wegweiser zur Führung der Pfarrmatriken“ (zu finden im diözesanen Mitarbeiter:innen-Portal „DiALog“)!

[4] Bei der Frühjahrsvollversammlung der Österreichischen Bischofskonferenz im März 2021 wurde die „Ordnung für die kirchlichen Archive Österreichs (KAO-Ö)“ beschlossen. Diese trat mit Veröffentlichung im Amtsblatt der Österreichischen Bischofskonferenz Nr. 83 vom 1. Juni 2021 in Rechtskraft (das entsprechende Amtsblatt siehe unter https://www.bischofskonferenz.at).

XI. STICHWORTVERZEICHNIS

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

Z

„Die größte Unzulänglichkeit beim Datenschutz ist das Wort ‚Datenschutz'. Der Begriff ist irgendwie blutleer und teilweise negativ besetzt. Er banalisiert das eigentliche Anliegen. Es sollen ja nicht die Daten als solche geschützt werden, sondern die Autonomie des Individuums."

(KARL MICHAEL BETZL, REDE VOR DEM BAYERISCHEN LANDTAG, 14. FEBRUAR 2006)

IMPRESSUM:
Medieninhaberin und Herausgeberin: Diözese Linz, Herrenstraße 19, 4020 Linz
Herstellerin: Druckerei Haider | **Verlagsort:** Linz | **Herstellungsort**: Schönau im Mühlkreis
Für den Inhalt verantwortlich: Mag. Alexander Marktler | Datenschutzreferent der Diözese Linz
Hafnerstraße 18 | 4021 Linz | +43 732 79800-1424 | datenschutz@dioezese-linz.at
Layout/Grafik: Margit Pschorn
Bildnachweise: Umschlagbild – shutterstock.com, Piktogramme – pixabay.com