**Datenschutzkonzept**

**(- Muster -)**

**1. Einleitung**

Der Schutz der personenbezogenen Daten der Gemeindemitglieder der Pfarrei „St.      “, Stiftung des öffentlichen Rechts mit dem Sitz in       */der Kinder und deren Eltern bzw. Personensorgeberechtigten der Kindertagesstätte      ,* in       unterliegt der höchste Priorität. Das vorliegende Konzept beschreibt, wie Datenschutz in der Pfarrei „St. */in der Kindertagesstätte* berücksichtigt und umgesetzt wird. Bei der Pfarrei „St.      “ */ der Kindertagesstätte* wird für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nach folgendem Datenschutzkonzept verfahren:

Die Verarbeitung personenbezogener Daten soll unter Berücksichtigung

* der Integrität (z. B. Schutz vor vorsätzlicher oder fahrlässiger Verfälschung von Programmen oder der Manipulation von Daten),
* der Vertraulichkeit (z. B. Schutz vor unbefugter Kenntnisnahme von Daten) und
* der Verfügbarkeit (z. B. Schutz vor Diebstahl oder Zerstörung)

gewährleistet werden. Die Sicherheitsmaßnahmen werden in dem Datenschutzkonzept in die Bereiche

* Allgemeine Datenverarbeitung
* Automatisierte Datenverarbeitung
* Nutzung der Internetdienste
* Nutzung der Telekommunikationsdienste und
* Zusatzmaßnahmen für sensible personenbezogene Daten (Sozialdaten)

gegliedert und geben damit das Sicherheitsniveau vor. Die festgelegten Sicherheitsmaßnahmen gelten als Mindestanforderungen für die Pfarrei „St.      “ */die Kindertagesstätte*

**2. Datenschutzrechtliche Rahmenbedingungen**

Das Erheben, Verarbeiten und Nutzen personenbezogener Daten ist in dem Gesetz über den kirchlichen Datenschutz (KDG) und im Telemediengesetz (TMG) geregelt. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (so genannter Betroffener).

Im Bereich der Pfarrei „St.      “ */der Kindertagsesstätte* gelten zusätzlich bereichsspezifische Regelungen wie die „Anordnung der deutschen Bischöfe über den Sozialdatenschutz in der freien Jugendhilfe“ sowie weitere Regelungen, die speziell für Pfarreien /*katholische Kindertagesstätten* in der Diözese Augsburg konzipiert wurden.

Generell gilt, dass personenbezogene Daten nur erhoben, verarbeitet und genutzt werden dürfen, wenn gesetzliche Vorschriften dies ausdrücklich zulassen oder der Betroffene ausdrücklich, schriftlich eingewilligt hat. Eine Einwilligung ist nur wirksam, wenn der Betroffene über die Tragweite des Verfahrens informiert wurde, dies heißt, welche Daten zu welchem Zweck in welcher Form gespeichert und verarbeitet werden und die Einwilligung nicht in anderen Erklärungen verborgen ist.

**3. Inhalt und Zweck des Konzeptes**

Grundvoraussetzung für den kirchlichen Datenschutz ist das Prinzip der Datenvermeidung und Datensparsamkeit i. S. des § 7 Abs. 1 KDG. Das bedeutet, dass nicht mehr Daten als benötigt verwendet werden. Als zweiten zentralen Punkt sehen wir die Notwendigkeit, Daten, die nicht mehr benötigt werden, aber noch nicht gelöscht werden können (z.B. wegn gesetzlichher Aufbewahrungsfristen) so früh als möglich zu pseudonymisieren bzw. zu anonymisieren.

**4. Beteiligte, speichernde Stelle im Sinne des Datenschutzes**

Die beteiligte speichernde Stelle im Sinne des Datenschutzes ist die Kath. Pfarrkirchenstiftung „St.       in       . Diese wird durch den jeweiligen Pfarrer als Vorstand der Kirchenverwaltung vertreten. Zum Zeitpunkt der Erstellung dieses Konzeptes ist dies:

* Hochw. Herr

Die Verantwortung für die Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung liegt daher beim Pfarrer.

**5. Verpflichtung zum Datenschutz**

Die Kath. Pfarrkirchenstiftung „St.      “, eingeschlossen ihrer haupt-, neben- und ehrenamtlichen Mitarbeiter /-innen, verpflichtet sich zur Einhaltung von datenschutzrechtlichen Vorschriften. Die betroffenen Personen haben eine entsprechende Verpflichtungserklärung auf das Datengeheimnis nach § 5 KDG unterzeichnet.

**6. Beschreibung der personenbezogenen Daten und Angabe der jeweiligen Zweckbindung (Nutzungszweck)**

**6.1 Mitgliederdaten**

Bei dem betroffenen Personenkreis handelt es sich um Mitglieder der Pfarrei „St.      “, römisch-katholischen Bekenntnisses sowie derer Familienangehöriger in häuslicher Gemeinschaft, soweit diese nicht Mitglieder der katholischen Kirche sind (Familienverband).

Bei den Daten handelt es sich um Einzelangaben zu den persönlichen und sachlichen Verhältnissen der Mitglieder nach § 19 Abs. 1 MRRG (Melderechtsrahmengesetz) sowie Daten derer nicht-katholischer Familienmitglieder nach § 19 Abs. 2 MRRG, z.B.:

* Familiennamen,
* Vornamen,
* Tag der Geburt,
* jetzige und letzte Anschrift,
* Zugehörigkeit zu einer öffentlich-rechtlichen Religionsgesellschaft,
* Übermittlungssperren,

sowie Daten über kirchliche Amtshandlungen (Taufe, Kommunion, Firmung, Trauung, Beerdigung).

Die Daten werden zu Zwecken der

* allgemeinen Seelsorge,
* Pflege des Mitgliederverzeichnisses,
* Durchführung kirchlicher Amtshandlungen,
* Kirchensteuer (Kirchgeld)

eingesetzt, entsprechend der kirchlichen Aufgaben, welche unsere Pfarrei zu erfüllen hat.

***6.1 Kinder- und Elterndaten, Daten von Personensorgeberechtigten***

*Bei dem betroffenen Personenkreis handelt es sich um Kinder, die in der Kindertagesstätte       betreut werden sowie deren Eltern oder Personensorgeberechtigte.*

*Bei den Daten handelt es sich um Einzelangaben zu den persönlichen und sachlichen Verhältnissen der Kinder sowie derer Eltern und Personensorgeberechtigter, z.B.:*

* *Familiennamen*
* *Vornamen,*
* *Tag der Geburt,*
* *Anschrift,*
* *Beruf des Vaters/ Beruf der Mutter,*
* *Arbeitgeber des Vaters/ der Mutter,*
* *Bankverbindung des Vaters/ der Mutter,*

*sowie Daten der persönlichen und erzieherischen Hilfe (z.B. Beobachtungsbögen: PERIK, SISMIK, SELDAK).*

*Die Daten werden eingesetzt zur pädagogischen Förderung und Betreuung der Kinder im Rahmen der Vorgaben des BayKiBiG, des pädagogischen Konzeptes der Kindertagesstätte, zur Information der Eltern / Personensorgeberechtigten sowie zu Prüfungszwecken durch kommunale und staatliche Aufsichtsbehörden. Ferner werden die Daten für Zwecke der Erhebung und Abrechnung von Beiträgen und Gebühren eingesetzt.*

**6.2 Mitarbeiterdaten**

Bei dem betroffenen Personenkreis handelt es sich um die haupt-, neben und ehrenamtlichen Mitarbeiter/-innen der Kath. Pfarrkirchenstiftung „St.      “ in      .

Bei den Daten handelt es sich um Einzelangaben zu den persönlichen und sachlichen Verhältnissen der Mitarbeiter/-innen, z.B:

* Familiennamen,
* Vornamen,
* Tag der Geburt,
* Anschrift,
* Gehaltsabrechnung,
* Arbeitsvertrag,
* Mitarbeitergespräch,
* Fortbildungsmaßnahmen,
* Art und Dauer eines Ehrenamtes.

Die Daten werden eingesetzt zur Mitarbeiterführung und –förderung, zur Lohn- und Gehaltsabrechnung, zur Förderung des Ehrenamtes sowie zur Planung ehrenamtlicher Einsätze.

**6.3 Spenderdaten**

Bei dem betroffenen Personenkreis handelt es sich um natürliche Personen, welche der Kath. Pfarrkirchenstiftung „St.      “ in       Geld- oder Sachspenden zuwenden.

Bei den Daten handelt es sich um Einzelangaben zu den persönlichen und sachlichen Verhältnissen der Zuwender, z.B:

* Familiennamen,
* Vornamen,
* Tag der Geburt,
* Anschrift,
* Bankverbindung,
* Art und Höhe einer Zuwendung,

Die Daten werden eingesetzt zur Ausstellung von steuerlich begünstigten Zuwendungsbestätigungen sowie für Zwecke der Buchführung.

**6.4 Stifterdaten**

Bei dem betroffenen Personenkreis handelt es sich um natürliche Personen, welche bei der Kath. Pfarrkirchenstiftung „St.      “ in       Messintentionen für Verstorbene bestellen oder eine Zustiftung zur Kirchenstiftung leisten.

Bei den Daten handelt es sich um Einzelangaben zu den persönlichen und sachlichen Verhältnissen der Stifter, z.B:

* Familiennamen,
* Vornamen,
* Tag der Geburt,
* Anschrift,
* Bankverbindung,
* Art und Höhe einer Zustiftung,
* Dauer und/oder Anzahl von Messintention,
* Namen des/der Verstorbenen.

Die Daten werden eingesetzt zur Planung der Messintentionen sowie für Zwecke der Buchführung.

**6.5** *(Hier Angaben über ggf, weitere Datenarten aufnehmen)*

…

**6.6 Rechtsgrundlage**

Die Rechtsgrundlage zur Nutzung der erhobenen, von kirchlichen/diözesanen Stellen und von den kommunalen Meldestellen übermittelten personenbezogenen Daten bilden die nachfolgend genannten Gesetze:

* MRRG (Melderechtsrahmengesetz) / *ab 05.2015 BMG (Bundesmeldegesetz)*,
* MeldeG (Gesetz über das Meldewesen im Freistaat Bayern),
* SGB (Sozialgesetzbücher),
* KDG (Gesetz über den kirchlichen Datenschutz),
* KDG-DVO Durchführungsverordnung dazu
* KMAO (Anordnung über das kirchliche Meldewesen),
* BayKiBiG (Bayer. Kinderbildungs-, erziehungs- und betreuungsgesetz),
* BayEUG (Bayer. Erziehungs- und Unterrichtsgesetz).

**7. Verfahrensbeschreibung**

Für EDV- Verfahren sind nach §31 KD1 unter anderem

* der Zweck der Datenerhebung,
* der wesentliche Inhalt,
* eine Beschreibung der betroffenen Personengruppen,
* die Regelfristen für die Löschung,
* die Angaben zur Art der Verarbeitung sowie den Schutzmaßnahmen

in einem Verzeichnis der Verarbeitungstätigkeiten festzulegen und auf dem neuesten Stand zu halten, sofern bei der verantwortliche Stelle kein betrieblicher Datenschutzbeauftragter bestellt ist.

**8. Beschreibung der Gewährleistung von Betroffenenrechten**

*(Hier bitte Angaben zum möglichen Ablauf einer Auskunftserteilung nach § 17 KDG entsprechen der tatsächlichen Gegebenheiten im Pfarrbüro/Büro der Kindertagesstätte aufehmen)*

**9. Verfahren zur Pseudonymisierung und Anonymisierung inklusive Risikoabschätzung**

Die Verfahren zur Pseudonymisierung und Anonymisierung werden nach dem jeweils aktuellen Stand der Technik durchgeführt.

Pseudonymisierung und Anonymisierung sind in der Regel immer dann notwendig, wenn Daten, die nicht mehr zur rechtmäßigen Aufgabenerfüllung benötigt werden aus gesetzlichen oder aus technischen Gründen noch nicht gelöscht werden können.

**10. Beschreibung der technischen und organisatorischen Maßnahmen zum Datenschutz**

Entsprechend der datenschutzrechtlichen Bestimmungen (z.B. § 26 KDG i.V. mit KDG-DVO, §78a SGB X i.V. mit der Anlage zu § 78a SGB X) sind Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass

1. nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit),
2. personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Integrität),
3. personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Verfügbarkeit),
4. jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (Authentizität),
5. festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit),
6. die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (Transparenz).

Die Beschreibung der bei der Pfarrei „St.      “ in       getroffenen Maßnahmen liegt diesem

Datenschutzkonzept als Anlage 2 bei.

------------------------------------------------------------------------------

**Erläuterungen zu Nr. 10:**

1. **Zutrittskontrolle**

*Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff „räumlich“ zu verstehen ist.*

Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:

Beispiele

* Zutrittskontrollsystem, Ausweisleser, Magnetkarte, Chipkarte
* Manuelles Schließsystem
* Schlüssel, Schlüsselvergabe, Schlüsselliste, Schließplan
* Türsicherung (elektrische Türöffner, über Telefonanlage öffnen, usw.)
* Empfang/Pförtner
* Überwachungseinrichtung (Alarmanlage, Video-/Fernsehmonitor)

**2. Zugangskontrolle**

*Das Eindringen Unbefugter in die EDV-Systeme ist zu verhindern.*

Technische (Kennwort-/Passwortschutz) und organisatorische (Benutzerkonto)
Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

Beispiele

* Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)
* Automatische Sperrung (z.B. Bildschirmschoner mit Kennwortreaktivierung oder Pausenschaltung)
* Einrichtung eines Benutzerkontos pro User (Einzelaccount)
* Verschlüsselung von Datenträgern (auch mobilen Datenträgern)
* Virenschutz (aktueller Anti-Virensoftware)
* Hardware-/Softwarefirewall

**3. Zugriffskontrolle**

*Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.*

Bedarfsorientierte Ausgestaltung eines Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

Beispiele

* Differenzierte Berechtigungen (Profile, Rollen, usw.) vergeben
* Auswertungen durchführen (durch EDV-Abteilung des Bistums oder Administrator der Pfarrei selbst)
* Kenntnisnahme (Regelungen treffen, wer darf alles Kenntnis über die Daten erlangen?)
* Veränderung (Regelungen treffen, wer darf Daten verändern?)
* Löschung (Protokollierung der Löschung unter Rücksichtnahme der Kassationsordnung,
Archivordnung des jeweiligen Bistums)

**4. Weitergabekontrolle**

*Aspekte der Weitergabe personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, Übermittlungskontrolle, usw.*

Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

Beispiele

* Verschlüsselung/Tunnelverbindung (VPN = Virtual Private Network)
* Elektronische Signatur (Email-Signatur)
* Protokollierung (Listen, Begleitpapiere, usw.)
* Transportsicherung (abschließbare Behältnisse, Plomben, usw.)
* Speicherung auf verschlüsselten Medien (eigener Server, externe Festplatte, USB-Stick, DVD, usw.)
* Emailverschlüsselung, Dateiverschlüsselung

**5. Eingabekontrolle**

*Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.*

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

Beispiel

* Protokollierungs- und Protokollauswertungssysteme (durch Vergabe von einzelnen
Benutzerkontos bereits möglich)
* Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen (Software) welche Daten eingegeben, geändert und gelöscht werden können
* Erstellen einer Übersicht, aus der sich ergibt, welche Personen Daten eingeben, ändern oder Löschen dürfen

**6.** **Verfügbarkeitskontrolle**

*Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.*

Maßnahmen zur Datensicherung (physikalisch/logisch):

Beispiele

* Backup-Verfahren (Sicherung und Wiederherstellung der Daten mittels diverser Sicherungsmedien: Magnetband, zweite Festplatte, externe Festplatte, USB-Stick, usw.)
* Spiegeln von Festplatten (z.B. RAID-Verfahren)
* Unterbrechungsfreie Stromversorgung (USV) oder Schutzsteckdosenleisten
* Getrennte Aufbewahrung (Magnetband, externe Festplatte oder USB-Stick in einem andern abgesperrten Raum lagern)
* Erstellung eines Notfallplans
* Feuerlöschgeräte vorhanden (Gebäude, Raum)

**7. Trennungskontrolle**

*Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.*

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

Beispiele

* physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
* bei pseudonymisierten Daten erfolgt eine Trennung der Zuordnungsdatei und die Aufbewahrung auf einem getrennten, abgesicherten IT-System (eigener Server) oder Medium (Magnetband, DVD, USB-Stick, externe Festplatte)

**8. Einteilung der Datenverarbeitungssysteme in Datenschutzklassen**

Die eingesetzten Datenverarbeitungssysteme müssen bei der Verarbeitung von personenbezogenen Daten durch den Dienstellenleiter in eine von drei sog. Datenschutzklassen eingeteilt werden.

**Datenschutzklasse I**

Zur Datenschutzklasse I gehören personenbezogene Daten, deren Missbrauch keine besonders schwer wiegende Beeinträchtigung des Betroffenen erwarten lässt. Hierzu gehören insbesondere Adressangaben ohne Sperrvermerke, z. B. Berufs-, Branchen- oder Geschäftsbezeichnungen.

**Datenschutzklasse II**

Zur Datenschutzklasse II gehören personenbezogene Daten, deren Missbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann. Hierzu gehören z.B. Daten über Mietverhältnisse, Geschäftsbeziehungen sowie Geburts- und
Jubiläumsdaten, usw.

**Datenschutzklasse III**

Zur Datenschutzklasse III gehören personenbezogene Daten, deren Missbrauch die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen erheblich beeinträchtigen kann. Hierzu gehören z.B. Daten über kirchliche Amtshandlungen, gesundheitliche Verhältnisse, strafbare Handlungen, religiöse oder politische Anschauungen, die Mitgliedschaft in einer Religionsgesellschaft, arbeitsrechtliche Rechtsverhältnisse, Disziplinarentscheidungen, usw. sowie Adressangaben mit Sperrvermerken.

**Hilfestellung für die Einteilung in Datenschutzklassen:**

Sämtliche Datenverarbeitungssysteme, welche bei der Verarbeitung von personenbezogenen Daten „**Meldewesen Plus**“ oder „**Adebis Kita**“ als Software nutzen sind in **Datenschutzklasse III** einzuteilen. Die übrigen in einer Kirchenstiftung verwendeten Systeme können i. d. R. der Datenschutzklasse II zugeordnet werden.

------------------------------------------------------------------------------

**11. Datenzugriff**

Zugriff auf personenbezogene Daten nach Ziffer 6. haben nur Mitarbeiter/-innen im Rahmen des Berechtigungskonzeptes zur Erfüllung ihrer rechtmäßigen Aufgaben. Das Berechtigungskonzept liegt diesem Datenschutzkonzept als Anlage 3 bei.

     , den

Für die Kat. Pfarrkirchenstiftung „St.      “

------------------------------------- ( S )

Pfarrer und Kirchenverwaltungsvorstand (Siegel des Kath. Pfarramtes)