**Datenschutzkonzept**

**(- Muster allgemein -)**

**1. Einleitung**

Der Schutz der personenbezogenen Daten der genießt höchste Priorität. Das vorliegende Konzept beschreibt, wie Datenschutz in d. - nachfolgend als „Dienststelle“ bezeichnetberücksichtigt und umgesetzt wird. Bei d.  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.

**2. Datenschutzrechtliche Rahmenbedingungen**

Das Erheben, Verarbeiten und Nutzen personenbezogener Daten ist in der Anordnung über den kirchlichen Datenschutz (KDO) 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 dieser Dienststelle gelten zusätzlich bereichsspezifische Regelungen wie z.B. die „Anordnung der deutschen Bischöfe über den Sozialdatenschutz in der freien Jugendhilfe und die Kirchliche Archivordnung.

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 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. wegen gesetzlicher 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 diese Dienststelle. Sie wird durch       vertreten. Zum Zeitpunkt der Erstellung dieses Konzeptes ist dies:

*

Die Verantwortung für die Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung liegt bei der vorbezeichneten Person.

**5. Verpflichtung zum Datenschutz**

Die Dienststelle - eingeschlossen ihre 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 die Mitglieder d      . Die Daten betreffen Einzelangaben zu den persönlichen und sachlichen Verhältnissen der Mitglieder, z.B.:

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

Die Daten werden zu folgenden Zwecken eingesetzt:

*
*
*
*

**6.2 Mitarbeiterdaten**

Bei dem betroffenen Personenkreis handelt es sich um die haupt-, neben und ehrenamtlichen Mitarbeiter/-innen der      .

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 dieser Dienststelle Geld- oder Sachspenden zuwenden. Die Daten sind 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.

**6.5** *(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:

* SGB (Sozialgesetzbücher),
* KDO (Anordnung über den kirchlichen Datenschutz),
* KMAO (Anordnung über das kirchliche Meldewesen),
* BayKiBiG (Bayer. Kinderbildungs-, erziehungs- und betreuungsgesetz),
* Bundesdatenschutzgesetz (BDSG)
* Bayerisches Landesdatenschutzgesetz
* BayEUG (Bayer. Erziehungs- und Unterrichtsgesetz).

**7. Verfahrensbeschreibung**

Für automatisierte Verfahren sind nach §31 KDG 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 Verfahrensverzeichnis festzulegen und auf dem neuesten Stand zu halten, sofern bei der verantwortliche Stelle kein betrieblicher Datenschutzbeauftragter bestellt ist.

Das Verfahrensverzeichnis ist dem Diözesandatenschutzbeauftragten zu melden, es liegt diesem Datenschutzkonzept als Anlage 1 bei.

**8. Beschreibung der Gewährleistung von Betroffenenrechten**

*(Hier bitte Angaben zum möglichen Ablauf einer Auskunftserteilung nach § 17 KDG entsprechen der tatsächlichen Gegebenheiten in der Verwaltung aufnehmen)*

**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, IV. Anlage 1 zu § 26 KDG, §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 dieser Dienststelle getroffenen Maßnahmen folgt auf den nächsten Seiten.

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

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

Entsprechend der datenschutzrechtlichen Bestimmungen (z.B. § 26 KDG i.V. mit KDG-DVO, IV. Anlage 1 zu § 26 KDO, §78a SGB X i.V. mit der Anlage zu § 78a SGB X) sind folgende technische und organisatorische Maßnahmen zu treffen:

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)

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

**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 bei.

**12. Ein betriebliche(r) Datenschutzbeauftragte(r) der Dienststelle**

🞏 ist bestellt, nämlich Frau/Herr
 Meldung an die Datenschutzaufsicht ist am \_\_\_\_\_\_\_\_\_\_\_\_ erfolgt.

🞏 ist nicht bestellt, weil

     , den

Für

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