Mustervorlage. Auszufüllendes in [], Erläuterungen *kursiv*, bitte vor Veröffentlichung löschen!

*Grundsätzlich* *gilt: Der Aufwand für den Datenschutz muss in einem angemessenen Verhältnis zum Schutz der personenbezogenen Daten stehen und darf eine Bücherei nicht überfordern (§ 26 Abs. 3 KDG). Gleichzeitig darf diese Einschränkung nicht zur Ausrede werden, sich nicht um den Datenschutz zu kümmern!*

# 170101-Logo Buechereiarbeit-jpgTechnisch-organisatorische Maßnahmen (TOM)

## Technischer Datenschutz nach § 26 KDG

Erstellt am: [Datum]

## 1. Rechtsträger

## [Name und Kontaktdaten des Trägers der Bücherei]

## 2. Name und Kontaktdaten des Verantwortlichen

[Name des leitenden Pfarrers bzw. der mit der Geschäftsführung beauftragten Person]

[Anschrift]

[Telefonnummer] | [E-Mail-Adresse]

## 2. Name und Kontaktdaten des Datenschutzbeauftragten

[Name]

[Anschrift]

[Telefonnummer] | [E-Mail-Adresse]

*Nach § 36 Abs. 1 KDG in Verbindung mit § 3 Abs. 1 Buchstabe a müssen Kirchengemeinden/Pfarrgemeinden/Seelsorgeeinheiten oder wie auch immer das Gebilde genannt wird, einen Datenschutzbeauftragten benennen. Erkundigen Sie sich bitte bei Ihrem leitenden Pfarrer oder dem Kirchenvorstand, wer das in Ihrem Falle ist.*

## 3. Aufsichtsbehörde

[Name]

[Anschrift]

[Telefonnummer] | [E-Mail-Adresse]

*Hier geben Sie die entsprechenden Kontaktdaten des Diözesandatenschutzbeauftragten Ihrer Diözese an (die Angaben können Sie z.B. der Datenschutzerklärung der Webseite ihrer Diözese entnehmen).*

## 4. Maßnahmen

1. Pseudonymisierung und Verschlüsselung

*Egal, ob Sie Ihre Bücherei mit Software verwalten oder mit Karteikarten: Im Tagesgeschäft an der Ausleihtheke verwenden Sie selten Name und Vorname des Nutzers (die Sie selbstverständlich mit Namen ansprechen dürfen), sondern die Lesernummer bzw. einen Barcode. D.h. in diesen Abschnitt können alle Büchereien eintragen:*

Zur Identifizierung eines Nutzers/in wird eine Lesernummer/Barcode *(nichtzutreffendes löschen)* verwendet.



*Büchereien, die Software zur Büchereiverwaltung einsetzen, können an dieser Stelle i.d.R. auch notieren:* 

Passwörter der Nutzer/innen (z.B. für das Nutzer/innen-Konto im eOPAC/WebOPAC) werden verschlüsselt gespeichert. D.h. niemand, der in dem Programm oder dessen Datenbank arbeitet, kann das Passwort einsehen.

2. Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit

*Personenbezogene Daten müssen vertraulich behandelt werden. Das können alle Büchereien zum einen durch Schulungen erreichen. Zum anderen sollten Büchereien, die mit einer Nutzer/innen-Kartei arbeiten, diese Kartei außerhalb der Öffnungszeiten wegschließen und hier beschreiben, wie der Zugang geregelt wird. Gibt es einen Schlüssel, der von einer diensthabenden Mitarbeiterin zur anderen wandert? Haben alle Mitarbeiterinnen einen Schlüssel?*

*Wenn Sie Büchereisoftware einsetzen, müssen alle Mitarbeiter/innen ein eigenes Login haben, am besten mit unterschiedlichen Rechten. Auch das wird hier dokumentiert (nicht wer welche Rechte, sondern dass mit abgestuften Rechten und mitarbeiterbezogenen Logins gearbeitet wird). Selbstverständlich sollte auch diese Regeln sein:*

Wer seinen Arbeitsplatz verlässt, muss den Computer mit Windowstaste + Taste L (=lock) sperren.

Regelmäßige Backups, sowohl lokal als auch auf einem externen Server sichern eine hohe Verfügbarkeit der Daten.

Regelmäßige Programmupdates sowohl für das Betriebssystem als auch für die Bibliothekssoftware tragen zur Sicherheit und Verfügbarkeit des gesamten EDV-Systems bei.

E-Mail-Anhänge werden nur umsichtig und nur von vertrauenswürdigen Absendern geöffnet. Eine aktuelle Anti-Virensoftware verringert das Risiko einer Infektion mit Schadsoftware.

Die Mitarbeiter/innen der Bücherei haben eine Verschwiegenheitserklärung unterzeichnet und sind über die Vorschriften zum Datenschutz informiert worden.

3. Kontrollvorgaben

Zutrittskontrolle

*Wer hat Zutritt zu den Räumen bzw. Bereichen der Bücherei, in denen Daten aufbewahrt und verarbeitet werden? Wo immer möglich, sollten nur die Büchereimitarbeiter/innen Zugang zu den Räumen bzw. PCs haben, auf denen die personenbezogenen Daten der Nutzer/innen gespeichert werden.*

*Die Schlüsselvergabe an Mitarbeiter/innen sollte dokumentiert werden, auch ein Schlüsselumlauf von Mitarbeiterin zu Mitarbeiterin von einem Öffnungstag auf den anderen sollte dokumentiert werden.*

*Wird der Raum, in dem sich die Bücherei befindet, auch von anderen Gruppen in der Gemeinde genutzt, sollte der Bücherei-PC nach Möglichkeit in einem abschließbaren Schubladencontainer o.ä. untergebracht werden.*

Zugangskontrolle

*Nur für Büchereien, die Bibliothekssoftware einsetzen: Wer kann die Bibliothekssoftware nutzen?*

Mitarbeiter/innen erhalten ein persönliches, passwortgeschütztes Login zum Büchereisystem.

*Vermeiden Sie unbedingt unsichere allgemeine Zugänge wie Leser/lesen oder St. Nimmerlein / 12345!*

Zugriffskontrolle

*Nur praktikabel für Büchereien, die Bibliothekssoftware einsetzen: Wie wird kontrolliert, wer auf die personenbezogenen Daten der Bücherei zugreifen kann?*

Die PCs der Bücherei sind mit verschiedenen Benutzerkonten ausgestattet; nicht jede/r Mitarbeiter/in hat und benötigt vollen Zugriff auf alle dort gespeicherten Daten.

Die Anmeldungen an die Bibliothekssoftware werden protokolliert, auch die Änderung personenbezogener Daten wird programmintern mit Benutzerkennung, Datum und Uhrzeit dokumentiert. Durch die Zuweisung bestimmter Rechte kann der Zugriff auf personenbezogene Daten eingeschränkt werden.

Weitergabekontrolle

*Wie werden personenbezogene Daten geschützt, wenn sie die Bücherei verlassen müssen?* 

Die Mitarbeiter/innen werden regelmäßig im Umgang mit personenbezogenen Daten geschult.

Die Weitergabe von Daten erfolgt nur in bestimmten Fällen auf verschlüsselte Weise: 

E-Mail-Versand per SSL/TLS,

Datenupload für das Backup nur per SFTP oder FTPS

Übertragung an den eOPAC/WebOPAC/die divibib nur verschlüsselt

Verfügbarkeitskontrolle

*Wie stellt die Bücherei sicher, dass Daten im Schadensfall möglichst schnell wieder verfügbar sind?*

Die Bücherei stellt durch Backups sicher, dass Daten im Schadensfall wiederhergestellt werden können. Dazu wird außerdem regelmäßig getestet, ob sich Backups auch zurückspielen lassen.