



DIE BÜCHEREI

Technisch-organisatorische Maßnahmen (TOM)

Technischer Datenschutz nach § 26 KDG

Erstellt am: 28.6.2018

1. Rechtsträger

Katholische Kirchengemeinde St. Nikolaus und St. Bruno
Nikolausplatz 17
50937 Köln

2. Name und Kontaktdaten des Verantwortlichen

Hildegard Mogge
Lotharstr., im Jugendheim, Rückseite der Kirche
Postanschrift: Nikolausplatz 17, 50937 Köln
0221/416034, E-Mail: koeb.nikolaus@kirche-sk.de

2. Name und Kontaktdaten des Datenschutzbeauftragten

Erzbistum Köln (KdöR)
Marzellenstraße 32
50668 Köln

Telefon: 0049 (0)221 1642 0
Fax: 0049 (0)221 1642 1700
E-Mail: info@erzbistum-koeln.de

Kontaktdaten des Datenschutzbeauftragten:
betrieblicher-datenschutz@erzbistum-koeln.de

3. Aufsichtsbehörde

Verantwortliche im Sinne gemäß Art. 4 Nr. 7 DS-GVO bzw. § 4 Nr. 9 KDG
sowie sonstiger datenschutzrechtlicher Bestimmungen ist
Erzbistum Köln (KdöR)
Marzellenstraße 32
50668 Köln
Telefon: 0049 (0)221 1642 0
Fax: 0049 (0)221 1642 1700
E-Mail: info@erzbistum-koeln.de

Kontaktdaten des Datenschutzbeauftragten:
betrieblicher-datenschutz@erzbistum-koeln.de



DIE BÜCHEREI

ENTDECKE

4. Maßnahmen

1. Pseudonymisierung und Verschlüsselung

Zur Identifizierung eines Nutzers/in wird eine Lesernummer oder Barcode verwendet.

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

Alle Mitarbeiter/innen haben ein eigenes Login in BVS mit unterschiedlichen Rechten. Das wird in BVS nachgehalten. Es gibt kein allgemeingültiges Login. Alle Mitarbeiter haben einen Schlüssel.

Wer seinen Arbeitsplatz verlässt, muss sich in BVS abmelden. Jeder darf auch nur unter seinem eigenen Login arbeiten.

Regelmäßige Backups, sowohl lokal als auch auf einem externen Speichermedium sichern eine hohe Verfügbarkeit der Daten. Das externe Speichermedium wird von der Büchereileitung extern aufbewahrt.

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.

3. Kontrollvorgaben

Zutrittskontrolle

Die Schlüsselvergabe an Mitarbeiter/innen wird dokumentiert, ebenso auch ein Schlüsselumlauf von Mitarbeiterin zu Mitarbeiterin von einem Öffnungstag auf den anderen. Zugang zu den Räumen haben alle Mitarbeiter*innen der KÖB, Hauptamtliche der Pfarrei, Mitarbeiter der örtlichen Caritas (Seniorenberatung) Sollten die Räume für Aktivitäten der Gemeinde genutzt werden(, Kommunion- oder Firmunterricht, u.a.), geschieht das nur in Absprache mit den Hauptamtlichen der Pfarrei und der Büchereileitung.

Zugangskontrolle

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

Zugriffskontrolle

Die PCs der Bücherei sind mit verschiedenen Benutzerkonten (Admin, User) 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

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

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

