# Einführung

Nach §18 DSO-BUND müssen verantwortliche Stellen, also z. B. Gemeinden, für die Verarbeitung von personenbezogenen Daten geeignete technische und organisatorische Maßnahmen (TOMs) treffen und dokumentieren, um ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten.

Den meisten Vorlagen für solche TOMs ist leider anzumerken, dass bei der Entwicklung der Datenschutzgesetze das Thema hauptsächlich aus rein technischer Perspektive betrachtet wurde. Der Schutz von personenbezogenen Daten in einer Serverfarm ist aber sehr viel „leichter“, als in einer Gemeinde, in der persönliche Beziehungen und Begegnungen im Vordergrund stehen.

Diese Vorlage soll euch erleichtern, bei den technischen und organisatorischen Maßnahmen und dem Umsetzen des „angemessenen Sicherheitsniveaus“, das ihr in der Gemeinde zum Schutz von personenbezogen Daten erfüllen müsst, auf die richtige Spur zu kommen.

Lest euch die Vorlage einmal durch, um ein Gefühl dafür zu entwickeln, worum es in welchem Abschnitt geht. Ihr werdet feststellen, dass sich nicht alles ganz trennscharf voneinander abgrenzen lässt. Aber ihr werdet merken, was die Zielrichtung ist und worauf es bei den TOMs ankommt: **Wenn ihr die Vorlage fertig bearbeitet habt, muss ein unbeteiligter Dritter aus dem Dokument ersehen können, wie ihr personenbezogene Daten schützt.**

Nachdem ihr das Dokument durchgegangen seid, fangt an dieses auszufüllen. Einige Punkte sind blau geschrieben. Hier gilt: Alles ankreuzen, was zutrifft. Die Summe und Kombination der angekreuzten Punkte muss ein angemessenes Schutzniveau ergeben. Was genau das bedeutet, lässt sich pauschal nicht sagen. Es ist immer auch noch Platz für Freitext, wo ihr erklären könnt, wie ihr die einzelnen Sachen umsetzt, wenn sich eure Situation nicht durch die Standardpunkte zum Abhaken darstellen lässt.

Dann gibt es einige Punkte, die orange sind. Hier gilt: Falls euch der Punkt betrifft, muss er zwingend umgesetzt werden.

Wenn ihr die Vorlage bearbeitet, werdet ihr feststellen, dass ihr einige Sachen einfach ankreuzen könnt und bei anderen nur ein Gefühl habt, was „am ehesten auf euch zutrifft“. Dann seid ihr am Kern dessen angekommen, was diese Vorlage bezwecken soll. Diskutiert diese Punkte und haltet schriftlich fest, wie genau ihr sie bei euch umsetzen wollt. Vielleicht ist z. B. allen klar, dass nicht jeder einen Schlüssel für eure Büroräume bekommt. Aber niemand weiß genau, wer alles einen haben darf. Dann besprecht das, dokumentiert das Ergebnis in den TOMs und setzt es entsprechend um. Klärt also, wer alles einen Schlüssel hat/bekommt. Führt eine Liste, wann die Schlüssel aus- und zurückgegeben werden und lasst den Empfang/die Rückgabe darauf unterschreiben. Haltet fest, wer für das Führen dieser Liste verantwortlich ist. Immer, wenn von einem „Berechtigungskonzept“ die Rede ist, solltet ihr dieses Konzept aufschreiben, damit ihr es bei einer Prüfung vorlegen könnt.

Der zweite Schritt bei der Bearbeitung dieser Vorlage ist die Umsetzung. Also, um noch ein weiteres praktisches Beispiel zu nennen: Nicht nur ankreuzen, dass externe Datenträger mit personenbezogenen Daten verschlüsselt werden, sondern auch einen Informationsweg und Workflow einrichten, wie das von den haupt- und ehrenamtlichen Mitarbeitern umgesetzt werden soll und diesen implementieren.

[Stand: 23.11.2023]

TOMS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| Stand |  | Ansprechperson für den Datenschutz in [verantwortliche Stelle] |  | Dezentraler Beauftragter für den Datenschutz |

In [verantwortliche Stelle] werden personenbezogene Daten erhoben, verarbeitet und genutzt. Um diese bestmöglich zu schützen, werden folgende technischen und organisatorischen Maßnahmen getroffen.

# Grundsätzliches

### Verpflichtung auf den Datenschutz

Mitarbeiter, die Zugang zu personenbezogenen Daten haben, werden auf den Datenschutz verpflichtet. (Bei Hauptamtlichen sollte dies bereits im Rahmen der Anstellung geschehen sein.) Alle ehrenamtlichen Mitarbeiter unterzeichnen das „Merkblatt über den Datenschutz für ehrenamtliche Mitarbeiter“, bevor ihnen Zugang zu personenbezogenen Daten gewährt wird. Das unterschriebene Dokument wird von der verantwortlichen Stelle archiviert.

Die Vorlage steht unter folgendem Link zum Download zur Verfügung:
<https://www.befg.de/angebote-fuer/gemeinden/datenschutz/praktische-tipps-und-faq/#c46550>

# **Zutrittskontrolle**

*(Zutritt* = *Wer hat Zugang zu Gebäuden, in denen die Daten verarbeitet werden?)*

*Maßnahmen, die verhindern, dass Unbefugte Zutritt* zu „Anlagen“ bekommen, in/mit denen personenbezogene Daten verarbeitet oder genutzt werden.

Als Maßnahmen zur Zutrittskontrolle können bei der Gebäude- und Raumsicherung beispielsweise eingesetzt werden: manuelle Schließsysteme mit Sicherheitsschlüssel, Einsatz von Chipkarten oder Transpondern, automatische Zutrittskontrollsysteme oder auch Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen.

Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen müssen in verschließbaren (Server-)Schränken untergebracht sein.

Als organisatorische Maßnahme der Zutrittskontrolle, kann z. B. per Dienstanweisung angeordnet werden, die Diensträume bei Abwesenheit zu verschließen.

|  |
| --- |
| Technische Maßnahmen |
| * **Manuelles Schließsystem mit Sicherheitsschlössern am Haus**
 |
| * **Sicherheitsschlösser an den Büros**

Bzw. abschließbare Schränke für personenbezogene Daten, wenn Büros nicht abschließbar sind |
| * Alarmanlage
 |
| * Chipkarten / Transpondersysteme
 |
| * Schließsystem mit Codesperre
 |
| * Biometrische Zugangssperren
 |
| * Türen mit Knauf an der Außenseite
 |
| * Automatisches Zugangskontrollsystem
 |
| * Klingelanlage mit Kamera
 |
| * Videoüberwachung der Eingänge
 |
| * Absicherung der Gebäudeschächte
 |
| * Einbruchssichere Fenster
 |

|  |
| --- |
| Organisatorische Maßnahmen |
| * **Schlüsselregelung / Liste** Es wird eine Liste der dauerhaft ausgegebenen Schlüssel/Schlüsselkarten etc. geführt.
 |
| * Der Letzte schließt das Gebäude ab
* Büros werden bei längerem Verlassen abgeschlossen
 |
| * Empfang / Rezeption / Pförtner
 |
| * Wenn Besucher nicht von einem Mitarbeiter begleitet werden, haben sie nur Zugang zu Räumen ohne personenbezogene Daten.
 |
| * Sorgfalt bei Auswahl des Wachpersonals
 |
| * Sorgfalt bei Auswahl des Reinigungsdienstes
 |

|  |
| --- |
| * Sonstiges (Hier könnt ihr beschreiben, welche weiteren technischen und organisatorischen Maßnahmen der Zutrittskontrolle ihr ergreift):
 |

# Zugangskontrolle

(Zugang = Wer kommt an die Computer/Sonstige Daten?)

Maßnahmen, die verhindern, dass Unbefugte Datenverarbeitungssysteme (z. B. Computer) nutzen können.

Dazu gehören beispielsweise Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung oder der Einsatz von Zwei-Faktor-Authentifizierung.

Es können auch organisatorische Maßnahmen notwendig sein. Beispielweise können die Mitarbeiter regelmäßig bestimmte „Standards“ und Regelungen unterzeichnen, wie es oft auch bei Brandschutzordnungen gehandhabt wird. In diesen Regelungen kann z. B. festgelegt werden, wie die Bildschirme aufzustellen sind, sodass keine Unbefugten Einblick bekommen, (besonders im Home Office oder in Empfangsbereichen) oder wie sichere Passwörter erstellt werden.

|  |
| --- |
| Technische Maßnahmen |
| * Login mit Benutzernamen und sicherem Passwort/biometrischem Zugang für PCs und Smartphones.
 |
| * Bildschirmsperre beim Verlassen des Rechners. (Ggf. automatisch)
 |
| * Verschlüsselung von Datenträgern (interne Festplatten, externe Festplatten, USB-Sticks, etc.) – auch Tablets! Verschlüsselungsstandard: AES 256 Bit mit Hash von HMAC-SHA-512; Bei Windows BitLocker aktivieren; Bei Mac FileVault; Externe Medien mit VeraCrypt oder BitLocker to go verschlüsseln.
 |
| * Anti-Viren-Software Clients / Desktop / Notebooks
 |
| * Anti-Viren-Software Server (wenn Server vorhanden)
 |
| * VPN bei Remotezugriff (IKE V2 Authentifizierung; kein PPTP)
 |
| * Verschlüsselung Smartphones
 |
| * Ggf. Sicherung der Netzwerkzugangs durch MAC-Filter
 |
| * E-Mail-Anmeldung über TLS/SSL, Abruf über IMAP
 |
| * Softwarefirewall (i. d. R. im Betriebssystem integriert)
 |
| * Verschlüsselung und sofortige Löschung von Daten auf internen Festplatten von **Multifunktionsgeräten** (Drucker, Kopierer, etc.) (siehe <https://www.datenschutz.bremen.de/datenschutztipps/orientierungshilfen-und-handlungshilfen/fotokopierer-die-angreifbare-datenstation-3904>)
 |
| * Hardwarefirewall (ggf. FritzBox ausreichend)
 |
| * BIOS Schutz (separates Passwort)
 |
| * SSH-Zugriff auf externe Server nur mittels PGP-Key
 |
| 2-Faktor-Authentifizierung für* Fileserver/NAS
* Lokale Server
* Externe Server
* Serververwaltung (z. B. AWS, netcup, Hetzner)
* Netzwerke
* Datenbanken
* ... ggf. ergänzen
 |
| * Zugang zum internen Netzwerk (auch WLAN, sofern darüber ein Zugriff auf das interne Netzwerk möglich ist) ist nur entsprechend des Berechtigungskonzeptes zu gewähren.
* Gäste nutzen ein Gastnetzwerk
 |
| * Analoge personenbezogene Daten werden sicher verschlossen
 |
|  |

|  |
| --- |
| Organisatorische Maßnahmen |
| * Verwalten von Benutzerberechtigungen
 |
| * Erstellen von Benutzerprofilen
 |
| * Anleitung „Manuelle Desktopsperre“ (Alle wissen, wie man den Computer sperrt, wenn man den Arbeitsplatz verlässt.)
 |
| * Richtlinie „Sicheres Passwort“: (Kombination aus min. 8 Zeichen, Buchstaben und Zahlen, Groß- und Kleinbuchstaben, Sonderzeichen)
 |
| * Richtlinie „Löschen / Vernichten“
 |
| * Richtlinie „Clean desk“ (= aufgeräumter Arbeitsplatz)
 |
| * Jährliche Überprüfung der Verschlüsselungsstandards
 |
| * Passwortmanager
 |
| * Nicht digitale Dokumente mit personenbezogenen Daten (z. B. Personalakten und Elternerklärungen) werden in einem verschlossenen Schrank/Büro aufbewahrt
 |
| * Auf Ausdrucke von Dokumenten mit personenbezogenen Daten wird soweit wie möglich und praktikabel verzichtet
 |
| * Gemeinschaftlich benutze Drucker werden in Räumen aufgestellt, zu denen Unbefugte ohne Begleitung von Mitarbeitern keinen Zugang haben
 |
| * Mitarbeiter sind angehalten, Dokumente mit pb Daten unmittelbar nach dem Ausdrucken aus der Druckablage zu entfernen
 |
| * Deaktivierung der Passwortauthentifizierung für den Zugriff auf externe Server
 |
| * Mitarbeiter werden jährlich auf die Umsetzung der technischen Maßnahmen hingewiesen
 |

|  |
| --- |
| * Sonstiges (Hier könnt ihr beschreiben, welche weiteren technischen und organisatorischen Maßnahmen der Zugangskontrolle ihr ergreift):
 |

# Zugriffskontrolle

|  |
| --- |
| Technische Maßnahmen |
| Vernichtung von Daten* **Akten und Unterlagen** mit personenbezogenen Daten werden grundsätzlich mit einem cross-cut-Schredder vernichtet
 |
| * **Datenträger** werden entweder sicher vernichtet oder durch mehrfaches Überschreiben des gesamten Datenträgers gelöscht. (CD-ROMs werden durch Cross-Cut Aktenschredder zerstört)
 |
| * **Zugriffe auf Datenbanken (z. B. ChurchTools)** werden bei Eingabe, Änderung und Löschung von Daten durch die Datenbank protokolliert
 |

|  |
| --- |
| Organisatorische Maßnahmen |
| * Verantwortliche Person für Verwaltung der Berechtigungskonzepte bestimmt
* Halbjährliche Überprüfung der Berechtigungskonzepte und der Berechtigungen
* Mitarbeiter werden jährlich auf die Berechtigungskonzepte hingewiesen, mit besonderem Hinweis auf das Verbot des Accountsharings

**Berechtigungskonzepte für** (Wenn ihr die diese Dinge nutzt, braucht ihr dafür ein Berechtigungskonzept)* Lokale Computer
* Fileserver/NAS
* Externe Server
* Serververwaltung (z. B. AWS, netcup, Hetzner)
* Lokale Server
* Netzwerke
* Typo3
* Datenbanken
* E-Mails
* Social-Media Accounts
* ... ggf. ergänzen:
 |

|  |
| --- |
| * Sonstiges (Hier könnt ihr beschreiben, welche weiteren technischen und organisatorischen Maßnahmen der Zugriffskontrolle ihr ergreift):
 |

# Trennungskontrolle

Wie wird gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können?

|  |
| --- |
| Technische Maßnahmen |
| * softwareseitiger Ausschluss (Mandantentrennung)
 |
| * Dateiseparierung (z. B. Trennung von Fotos nach Erhebungsursprung und -zweck)
 |
| * Berechtigungskonzept für Datenbanken
 |
| * Berechtigungskonzept für Webseitenverwaltung (z. B. Joomla, Typo3, Wordpress ...)
 |
| Aus welchen Gründen ist eine Trennung nicht möglich oder nicht notwendig? **Beschreibung der Fälle und Begründung:**  |
|  |

|  |
| --- |
| * Sonstiges (Hier könnt ihr beschreiben, welche weiteren technischen und organisatorischen Maßnahmen der Trennungskontrolle ihr ergreift):
 |

# Verfügbarkeitskontrolle

|  |
| --- |
| Technische Maßnahmen |
| Regelmäßige Backups von * Rechnern/Laptops
* Servern
* Datenbanken
* Webseiten
 |

|  |
| --- |
| Organisatorische Maßnahmen |
| * Backupplan für personenbezogene Daten (manuell oder automatisch)

Bitte hier beschreiben: |

|  |
| --- |
| * Sonstiges (Hier könnt ihr beschreiben, welche weiteren technischen und organisatorischen Maßnahmen der Verfügbarkeitskontrolle ihr ergreift):
 |

# Sicherheitskonzept für Gemeindeevents (Z. B. Jugendfreizeiten)

|  |
| --- |
| Technische Maßnahmen |
| * Wenn Ordner/Dokumente (digital und/oder analog) mit personenbezogenen Daten an Mitarbeiter herausgegeben werden, müssen diese auf dem Event eingeschlossen (in einem Raum, im Kofferraum oder in einer abschließbaren Truhe, etc.) oder am Mann getragen werden.
 |

|  |
| --- |
| Organisatorische Maßnahmen |
| * Welchen Mitarbeitern Zugriff auf welche personenbezogenen Daten gewährt wird, regelt ein Berechtigungskonzept.
 |