**Anlage zum Verarbeitungsverzeichnis der paedML®:**
**Katalog der technischen und organisatorischen Maßnahmen der Schule zur pädagogischen Musterlösung paedML®**

Die grün eingefärbten Maßnahmen sind bereits in der paedML realisiert. Alle anderen Maßnahmen obliegen der Schule. Bitte Prüfen Sie, welche Maßnahmen aus dem Katalog Sie im Rahmen Ihrer Möglichkeiten umsetzen können. Die Liste ist als Hilfestellung gedacht.

## Beschreibung der technischen und organisatorischen Maßnahmen zum Datenschutz gemäß Art. 32 DS-GVO

### A) Vertraulichkeit:

**Zutrittskontrolle:**
Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden zu verwehren, z.B. Maßnahmen zur Gebäude- und Raumsicherung.

- ✓ Separate Räumlichkeit, die nur Befugten zugänglich ist.
- ✓ Abschließbare Räumlichkeit
- ✓ Abschließbare Schränke
- ✓ Manuelles Schließsystem, Zugang nur für Mitarbeiter
- ✓ Sicherheitsschlösser
- ✓ Absicherung der Gebäudeschächte durch verschlossene Gitter
- ✓ Organisatorische Maßnahmen:
    - Schlüsselregelung / Liste
    - Besucher in Begleitung durch Mitarbeiter

**Zugangskontrolle:**
Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

- ✓ Identifizierung und Authentifizierung durch Benutzername/Passwort
    - Keine Weitergabe von Passwörtern
- ✓ Arbeitsanweisung „Sperren des Bildschirms“ bzw. „Abmelden vom System“ -> (Um Unbefugten keinen Zugriff auf sensitive Daten an einem „offenen“ Rechner zu ermöglichen)
- ✓ Protokollierung der Anmeldung
- ✓ Firewall und Antivirensoftware auf Clients und Servern
- ✓ Einsatz IPsec und SSL basierte VPN bei Remote-Zugriffen
- ✓ Automatische Desktopsperre

- ✓ Organisatorische Maßnahmen:
    - Verwalten von Benutzerberechtigungen
    - Erstellen von Benutzerprofilen
    - Zentrale Passwortvergabe, Passwort ist nur dem Nutzer bekannt
    - Richtlinie „Sicheres Passwort“

- Richtlinie Datenschutz und / oder Sicherheit

**Zugriffskontrolle:**
Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können

- ✓ Berechtigungskonzept mit Rollen und unterschiedlichen Berechtigungsstufen
- ✓ Nur wenige Administratoren
- ✓ Vernichtung von Papier durch Aktenvernichter.

**Trennungskontrolle:**
Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können

- ✓ Mehrere voneinander getrennte Systeme zum Verarbeiten von Daten - Umsetzung laut Netzbrief des Kultusministeriums Baden-Württemberg (z.B. Verwaltungsnetz, päd. Netz, Lehrernetz)

**B) Integrität:**

**Weitergabekontrolle:**
Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- ✓ Es erfolgt keine Weitergabe von Datenträgern an Dritte (schriftliche Fixierung durch die Schule und Lehrer notwendig)
- ✓ Einsatz von VPN-Technologie
- ✓ Bereitstellung über verschlüsselte Verbindungen (HTTPS)
- ✓ Sichere Aufbewahrung von Datenträgern in abschließbaren Serverräumen bzw. Schränken

**Eingabekontrolle:**
Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystem eingegeben, verändert oder entfernt worden sind.

- ✓ Protokollierung der Eingabe, Änderung und Löschung von Daten
- ✓ Nachvollziehbarkeit von Eingabe, Änderung und Löschen von Daten durch individuelle Zugangsdaten
- ✓ Rechtevergabe Lesen, Eingeben, Änderung und Löschung im Rahmen des Berechtigungskonzeptes

**C) Verfügbarkeit und Belastbarkeit**

**Verfügbarkeitskontrolle:**

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Es geht hier um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.

Technische Maßnahmen:

- ✓ Feuer- und Rauchmeldeanlagen
- ✓ Feuerlöscher im Serverraum
- ✓ Serverraumüberwachung bzgl. Temperatur und Feuchtigkeit
- ✓ Serverraum klimatisiert
- ✓ USV
- ✓ Schutzsteckdosenleisten im Serverraum
- ✓ RAID System / Festplattenspiegelung
- ✓ Redundante Server-Infrastruktur

Organisatorische Maßnahmen:

- ✓ Backup & Recovery-Konzept (LMZ Vorlage kann verwendet werden)
- ✓ Kontrolle des Sicherungsvorgangs
- ✓ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
- ✓ Bei einem Wartungsvertrag mit einem Dienstleister die obige Punkten extra vermerken.
- ✓ Getrennte Partitionen für Betriebssysteme und Daten

## D) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

**Datenschutzmanagement:**

- ✓ Dokumentation, Verfahren, Verarbeitungsverzeichnisse sind vorhanden, vollständig und aktuell
- ✓ Fachkundenachweise des Datenschutzbeauftragten liegen vor
- ✓ Einhaltung Datengeheimnis, sämtliche Mitarbeiter sind auf das Datengeheimnis verpflichtet
- ✓ Regelmäßige Datenschutzmerkblätter für die Mitarbeiter, Datenschutzschulung durch den Datenschutzbeauftragten
- ✓ jährliche Audits durch den Datenschutzbeauftragten

**Incident-Response-Management:**

- ✓ Etwaige Vorfälle werden unverzüglich dem Datenschutzbeauftragten gemeldet
- ✓ Bearbeitung etwaiger Fälle durch den Datenschutzbeauftragten

Technische Maßnahmen:

- ✓ Einsatz von Firewall und regelmäßige Aktualisierung (Das Firewall-Update ist manuell anzustoßen)
- ✓ Einsatz von Spamfilter und regelmäßige Aktualisierung
- ✓ Einsatz von Virenscanner und regelmäßige Aktualisierung

Organisatorische Maßnahmen:

- ✓ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen/ Daten- Pannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
- ✓ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
- ✓ Einbindung des Datenschutzbeauftragten in Sicherheitsvorfälle und Datenpannen
- ✓ Dokumentation von Sicherheitsvorfällen und Datenpannen z. B. mittes eines Ticketsystems
- ✓ Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

**Datenschutzfreundliche Voreinstellungen**

Technische Maßnahmen:

- ✓ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind *(privacy by design, privacy by default)*