

DigiLernFlow

Management-Zusammenfassung für Schulträger, Schulleiter und Schulen (Datenschutz & Datensicherheit)

Stand: 22.02.2026

Version: Dashboard 1.0 (RC / Demo)

Einsatz: Schulische Lernplattform

Betriebsprinzip: lokal / privat (nicht öffentlich)

1. Kurzbewertung (Executive Summary)

DigiLernFlow ist als schulische Lernplattform auf einen datensparsamen Einsatz mit pseudonymisierten Nutzerkennungen ausgerichtet. Der aktuelle Entwicklungsstand zeigt im Dashboard-Kontext bereits wesentliche Sicherheits- und Betriebsmaßnahmen (u. a. HTTPS-Betrieb, Guard-geschützte Admin-Aktionen, Datenhygiene-Checks, lokale Assets, automatisierte Smoke-Tests).

Empfehlung: DigiLernFlow kann als **Pilot- bzw. Produktivkandidat** betrachtet werden, sofern die schul-/trägerspezifischen Freigabeschritte (insbesondere AVV/TOM/VVT/Informationspflichten, Backup-/Restore-Nachweise und organisatorische Nutzungsregeln) vollständig abgeschlossen werden.

2. Datenschutzprofil (fachliche Einordnung)

- **Keine besonders schützenswerten personenbezogenen Daten** für den vorgesehenen Betrieb erforderlich.
- **Pseudonyme Nutzerkennungen** sind konzeptionell vorgesehen (keine Klarnamenpflicht).
- In Freitexten/Prompts/Bildern/Notizen/Anhängen sollen **keine sensiblen personenbezogenen Inhalte** verarbeitet werden.
- Der Einsatz erfordert ergänzend eine **Nutzungsordnung** und Datenschutzhinweise im Schulkontext.

3. Technischer Sicherheits- und Betriebsstatus (aktueller Stand)

Bereich	Bewertung	Status
Transportverschlüsselung (HTTPS)	Produktivbetrieb mit HTTPS-Zwang vorgesehen/aktiv.	Erfüllt
Kritische Admin-Aktionen	Zusätzlicher Passwortschutz (Guard) für sensible Schreib-/Wartungsaktionen.	Erfüllt
Datenhygiene / Konsistenzkontrolle	Guard-geschützter Hygiene-Scan/Bereinigung im Admin-Dashboard.	Erfüllt
Legacy-Routing / Verwaltungsaltscode	Wesentliche Legacy-Pfade stillgelegt oder umgeleitet.	Erfüllt
DSGVO-Hardening im Dashboard-Kontext	Lokale CSS/JS-Bundles, reduzierte externe Abhängigkeiten.	Erfüllt
Automatisierte Funktionsprüfung	Smoke-Test inkl. Hygiene-Check erfolgreich (24/24).	Erfüllt
Audit-Logging kritischer Aktionen	Empfohlen zur weiteren Nachweis- und Betriebssicherheit.	Offen
Backup-/Restore-Nachweis (formal)	Betrieblich erforderlich; dokumentierte Restore-Tests ergänzen.	Teilweise

4. Freigaberelevante Voraussetzungen (Träger/Schule/DSB)

Datenschutz / Recht

- Rechtsgrundlage im konkreten Schul-/Landeskontext prüfen
- VVT-Eintrag erstellen/ergänzen
- Informationspflichten (Art. 13/14 DSGVO) vorbereiten
- AVV + TOM prüfen (falls externe Betriebs-/Supportkonstellation)

Technik / Betrieb

- Backup- und Restore-Prozess dokumentieren und testen
- Rollen-/Berechtigungskonzept lokal abnehmen
- Monitoring/Fehlerreaktion festlegen
- Upload-/Attachment-Regeln (inkl. ZIP) verbindlich definieren

5. Empfohlener Freigabeweg (praxisnah)

- **Vorprüfung:** Selbstauskunft + technische Unterlagen sichten.
- **Datenschutzprüfung:** DSB/Träger prüft Rechtsgrundlage, AVV/TOM/VVT, Informationshinweise.
- **Pilotbetrieb:** kleine Nutzergruppe, Rollen- und Betriebsabläufe testen.
- **Produktivfreigabe:** Zuständigkeiten, Review-Zyklen und Betriebsroutine schriftlich festlegen.

6. Beizulegende Unterlagen (Kurzliste)

- Detailliertes Qualifizierungsdokument / Whitelist-Prüfkatalog
- Datenschutz-Kurzkonzept (inkl. Pseudonymisierung und Inhaltsregeln)
- TOM-Dokumentation
- VVT-Baustein / Informationshinweise
- Backup-/Restore-Konzept
- Prüfprotokolle (Smoke-Test, Abnahme)

7. Lokaler Prüfvermerk (Management / Träger)

Stelle/Funktion	Name	Datum	Ergebnis / Auflagen
Schulträger / IT			
Datenschutzbeauftragte/r			
Schulleitung			

Ort, Datum

Unterschrift / Freigabevermerk