

Governance-Dokumente

Übersicht

Welche Governance-Dokumente brauchen wir — und was ist schon vorhanden? Priorisierung: DSGVO-Pflichtdokumente zuerst, dann Sicherheit, dann Betrieb.

Dokument	Status	Wo / Was fehlt
DSGVO / Datenschutz		
Datenklassifizierung	Vorhanden	Datenklassifizierung
Verarbeitungsverzeichnis (VVT)	Entwurf	VVT-Eintrag Schulfunk — vervollständigen
AVV (Auftragsverarbeitung)	Entwurf	AVV-Vorlage — mit netcup + Anthropic abschließen
Eltern-Info (Art. 13 DSGVO)	Entwurf	Eltern-Info-Brief — Vorlage vorhanden, noch nicht versandt
Datenschutz-Folgenabschätzung (DPIA)	Fehlt	Pflicht bei Verarbeitung von Schülerdaten — anlegen
Datenschutzerklärung (Website)	Fehlt	Für schulfunk.app und empennage.de erstellen
Informationssicherheit		
Informationssicherheitsrichtlinie (ISR)	Fehlt	Übergeordnetes Dokument — Schutzziele, Scope, Verantwortlichkeiten
Security Governance	Fehlt	Rollen, Eskalation, Incident-Klassifikation
Passwortrichtlinie	Fehlt	Mindestanforderungen, MFA-Pflicht, Rotation
Zugangskontrollkonzept	Fehlt	Wer darf was — Rollen, Rechte, Onboarding/Offboarding
Netzwerkkonzept	Fehlt	Infrastruktur-Übersicht, Segmentierung, Firewall-Regeln
Backup-Konzept	Fehlt	Backup-Strategie für VPS, BookStack, n8n

Dokument	Status	Wo / Was fehlt
Incident Response Plan	Fehlt	Was tun bei Datenpanne — Meldefrist 72h (Art. 33 DSGVO)
Betrieb & Organisation		
Dokumentenrichtlinie	Fehlt	Wie werden Dokumente in BookStack erstellt, versioniert, archiviert
Change Management	Fehlt	Wie werden Änderungen an Produkt/Infra freigegeben
Business Continuity / Notfallplan	Fehlt	Was passiert bei Serverausfall, Krankheit des Gründers
IT-Rollen & Verantwortlichkeiten	Vorhanden	IT-Rollen — aktuell
Compliance-Status	Vorhanden	Compliance-Status — monatlich aktualisiert

Prioritäten

1. **DPIA** (Datenschutz-Folgenabschätzung) — vor Produktivbetrieb mit Schülerdaten Pflicht
2. **Incident Response Plan** — 72h-Meldefrist bei Datenpanne ist knapp
3. **Datenschutzerklärung** — vor Launch auf schulfunk.app
4. **Backup-Konzept** — VPS-Daten aktuell ungesichert
5. **Dokumentenrichtlinie** — wie BookStack genutzt wird, für CIO-Demos relevant

Stand: Mai 2026 · wird manuell gepflegt.