

Informationssicherheitsrichtlinie (IS-Policy)

Dieses Dokument ist die oberste Richtlinie der Informationssicherheits- und Datenschutz-Governance der Empennage GmbH. Alle nachgeordneten Richtlinien, Konzepte und Verfahren leiten sich hieraus ab.

1. Geltungsbereich

Diese Richtlinie gilt für:

- **Organisation:** Empennage GmbH und alle zukünftigen Mitarbeitenden, Auftragnehmer und Dienstleister
- **Produkte:** Schulfunk (schulfunk.app) und alle weiteren Empennage-Produkte
- **Systeme:** Alle IT-Systeme, Cloud-Dienste und Infrastruktur (netcup VPS, Hetzner, SaaS-Dienste)
- **Daten:** Alle verarbeiteten personenbezogenen und geschäftlichen Daten

2. Schutzziele

Ziel	Definition	Bedeutung für Schulfunk
Vertraulichkeit	Daten nur für Befugte zugänglich	Schüler-, Eltern- und Lehrerdaten dürfen nicht unbefugt eingesehen werden
Integrität	Daten korrekt und unverändert	Sendungsinhalte und Nutzerprofile dürfen nicht manipuliert werden
Verfügbarkeit	Systeme zugänglich wenn gebraucht	Schulfunk-Plattform muss während Schulzeiten erreichbar sein
Transparenz	Verarbeitung nachvollziehbar	Schulen und Eltern müssen verstehen was mit Daten passiert

3. Rechtlicher Rahmen

Die Informationssicherheits-Governance von Empennage orientiert sich an folgenden Regelwerken (vollständige Übersicht: [Regulatorischer Rahmen](#)):

Regelwerk	Relevanz
DSGVO / BDSG / TTDSG	Verpflichtend — Datenschutz-Grundlage
DSG NRW / SchulG NRW § 120	Verpflichtend — für Pilotbetrieb in NRW
EU AI Act (Hochrisiko Bildung)	Verpflichtend — sobald KI-Features für Schüler
JMStV / UrhG	Verpflichtend — Medienproduktion mit Minderjährigen
BSI IT-Grundschutz	Angestrebt — für Vertrauen bei öffentlichen Auftraggebern
ISO/IEC 27001	Langfristiges Ziel — ab erster Ausschreibung relevant

4. Verantwortlichkeiten

Rolle	Person	Aufgaben
Geschäftsführung / CIO	Philipp Wolters	Gesamtverantwortung, Budgets, strategische Entscheidungen, Unterzeichnung dieser Richtlinie
Datenschutz (ohne formalen DSB-Titel)	Philipp Wolters	VVT, AVV, DPIA, Einwilligungen, Meldepflichten. Kein formaler DSB nötig (<20 MA, Art. 37 DSGVO)
Security Officer	Philipp Wolters	Technische Schutzmaßnahmen, Incident Response, Schwachstellenmanagement
Compliance-Monitoring	n8n-Agent (automatisiert)	Monatlicher Compliance-Report in BookStack — siehe Compliance-Status

Vollständige Rollenübersicht: [IT-Rollen](#)

5. Grundsätze

- Privacy by Design:** Datenschutz wird von Anfang an in Produkte und Prozesse eingebaut, nicht nachträglich ergänzt.
- Minimalprinzip:** Es werden nur die Daten erhoben, die für den jeweiligen Zweck zwingend erforderlich sind.
- Menschliche Aufsicht bei KI:** Kein KI-System trifft autonom Entscheidungen über Minderjährige. Jede KI-Funktion erfordert menschliche Kontrollmöglichkeit (EU AI Act).

4. **Need-to-know:** Zugriff auf Daten nur für Personen/Systeme die ihn für ihre Aufgabe benötigen.
5. **Dokumentationspflicht:** Alle Verarbeitungstätigkeiten, Sicherheitsvorfälle und Änderungen werden dokumentiert.
6. **Kontinuierliche Verbesserung:** Monatliches Monitoring, jährliche Überprüfung dieser Richtlinie.

6. Nachgeordnete Dokumente

Dokument	Zweck	Status
Regulatorischer Rahmen	Welche Gesetze und Normen gelten	☐ Vorhanden
Datenklassifizierung	Kategorisierung und Schutzmaßnahmen nach Datensensitivität	☐ Vorhanden
Verarbeitungsverzeichnis (VVT)	Art. 30 DSGVO — alle Verarbeitungstätigkeiten	☐ Entwurf
AVV	Art. 28 DSGVO — Verträge mit Auftragsverarbeitern	☐ Entwurf
Eltern-Info (Art. 13)	Informationspflicht gegenüber Erziehungsberechtigten	☐ Entwurf
Governance-Dokumente Übersicht	Alle noch fehlenden Dokumente mit Priorität	☐ Vorhanden
Datenschutz-Folgenabschätzung (DPIA)	Art. 35 DSGVO — Pflicht vor Schülerdaten-Verarbeitung	⚠ Fehlt
Incident Response Plan	Vorgehen bei Datenpannen — 72h-Meldefrist	⚠ Fehlt
Security Governance	Zugangskontrolle, Passwortrichtlinie, Netzwerkkonzept	⚠ Fehlt
Backup-Konzept	Datensicherung VPS und Dienste	⚠ Fehlt
Dokumentenrichtlinie	Wie Dokumente in BookStack erstellt und gepflegt werden	⚠ Fehlt

7. Verpflichtung der Geschäftsführung

Ich, Philipp Wolters, Geschäftsführer der Empennage GmbH, verpflichte mich zur Umsetzung und kontinuierlichen Verbesserung dieser Informationssicherheits- und Datenschutz-Governance. Informationssicherheit und Datenschutz sind strategische Unternehmensziele und Grundlage des Vertrauens unserer Kunden — insbesondere der Schulen und Erziehungsberechtigten.

Datum:	12. Mai 2026
Version:	1.0
Nächste Überprüfung:	Mai 2027 (jährlich)
Unterzeichnet:	Philipp Wolters, Geschäftsführer

Revision #1
Created 2026-05-12 08:47:29 UTC by philipp
Updated 2026-05-12 08:47:29 UTC by philipp