Compliance & DSGVO

- Compliance-Status
- Audit-Log
- Datenklassifizierung
- Governance-Dokumente Übersicht
- Regulatorischer Rahmen (Gesetze & Normen)
- Informationssicherheitsrichtlinie (IS-Policy)

Compliance-Status

Automatisch generiert am 12.05.2026 um 03:07 Uhr · Monatlicher Compliance-Check (Template-basiert) · Audit-Log

DSGVO-Compliance-Checkliste

Rechtsgrundlage	Thema	Status	Wo / Was fehlt
Art. 5 DSGVO	Datenklassifizierung	**OK**	Datenklassifizierung — 4 Klassen dokumentiert
Art. 13/14	Informationspflichten	**Offen**	Erstellen: Eltern-Info-Brief (Art. 13) — Vorlage vorhanden, noch nicht versandt
Art. 25 DSGVO	Privacy by Design	**Offen**	Datenschutz-Folgenabschätzung fehlt — im Kapitel Compliance anlegen
Art. 28 DSGVO	Auftragsverarbeitung	**Teilweise**	AVV-Vorlage vorhanden — mit netcup + Anthropic abschließen
Art. 30 DSGVO	Verarbeitungsverzeichnis	**Teilweise**	VVT-Eintrag Schulfunk — Vorlage vorhanden, vervollständigen
Art. 32 DSGVO	TOMs	**Teilweise**	Datenklassifizierung definiert Maßnahmen — technische Umsetzung prüfen
Art. 37 DSGVO	Datenschutzbeauftragter	**OK**	Kein DSB erforderlich (Startup <20 MA, keine großmaßstäbige Verarbeitung). Datenschutz-Aufgaben: Philipp Wolters (Gründer). GF kann nicht formaler DSB sein (Interessenkonflikt Art. 38 Abs. 6).

Legende

- **OK** Umgesetzt
- **Teilweise** In Bearbeitung
- **Offen** Handlungsbedarf
- **Hinweis** Klärungsbedarf

Wird monatlich am 1. des Monats automatisch aktualisiert (n8n). · Audit-Log ansehen

Audit-Log

Datum	Aktion	Methode	Status
12.05.2026	Monatliches Compliance-Monitoring	Template (ohne KI)	Abgeschlossen

Datenklassifizierung

Datenklassifizierung Empennage

Letzte Aktualisierung: 2026-05-12 | Verantwortlich: Philipp Wolters (DSB)

Klasse 1 — Öffentlich

Keine Einschränkungen, öffentlich zugänglich.

Beispiele: Website-Inhalte, Produktbeschreibungen, Pressemitteilungen

Maßnahme	Status
Kein besonderer Schutz erforderlich	✓ Umgesetzt
Versionskontrolle	✓ Umgesetzt
Markierung als Öffentlich	⚠ Offen

Klasse 2 — Intern

Nur für Mitarbeitende und autorisierte Partner.

Beispiele: Betriebliche Prozesse, Kostendaten, interne Kommunikation

Maßnahme	Status
Zugriffskontrolle (Login)	✓ Umgesetzt
Verschlüsselung in Transit (HTTPS)	✓ Umgesetzt
Markierung als Intern	⚠ Offen
Löschfrist definiert	⚠ Offen

Klasse 3 — Vertraulich (personenbezogen)

DSGVO-relevante personenbezogene Daten.

Beispiele: Schülernamen, Elterndaten, Lehrerdaten, Kommunikationsinhalte

Maßnahme	Status
Verschlüsselung at-rest + in-transit	✓ Umgesetzt
Zugriffs- und Änderungsprotokoll	⚠ Offen
Löschkonzept + Aufbewahrungsfristen	⚠ Offen
Auftragsverarbeitungsvertrag (AVV)	⚠ Offen
Verarbeitungsverzeichnis (VVT)	⚠ Offen
Datenschutz-Folgenabschätzung (DSFA)	⚠ Offen

Klasse 4 — Streng vertraulich

Besondere Kategorien (Art. 9 DSGVO) und Zugangsdaten.

Beispiele: API-Keys, Passwort-Hashes, Vertragsdaten

Maßnahme	Status
Secrets-Manager aktiv	✓ Umgesetzt
Keine Klartextspeicherung	✓ Umgesetzt
Zugriff auf Minimum beschränkt	✓ Umgesetzt
Separates Audit-Log	⚠ Offen
Regelmäßige Credential-Rotation	⚠ Offen

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.

Regulatorischer Rahmen (Gesetze & Normen)

Welche Gesetze, Normen und Regelwerke treffen auf Empennage GmbH / Schulfunk zu? Stand: Mai 2026. **Kein Rechtsrat — bei Unsicherheiten Anwalt konsultieren.**

Regelwerk	Status	Bedeutung für Schulfunk
Datenschutz & Privatsphäre		
DSGVO (EU 2016/679)	**Trifft zu**	Kerngesetz. Verarbeitung von Schüler-, Eltern- und Lehrerdaten. Gilt ab erstem Nutzer.
BDSG (Bundesdatenschutzgesetz)	**Trifft zu**	Deutsche Ausführung der DSGVO. Gilt parallel.
TTDSG (Telekommunikation-Telemed	**Trifft zu**	Gilt für Online-Dienste, Cookies, App-Tracking. Relevant ab Launch schulfunk.app.
Datenschutzrecht NRW (DSG NRW)	**Trifft zu**	OGS Monte Bonn liegt in NRW. Schulen unterliegen DSG NRW + Schulgesetz NRW § 120.
KI & Digitale Dienste		
EU AI Act (VO 2024/1689)	**Achtung**	**Hochrisiko-KI!** Annex III klassifiziert KI-Systeme in Bildungseinrichtungen als Hochrisiko. Betrifft Schulfunk sobald KI-Features für Schüler eingesetzt werden. Anforderungen: Konformitätsbewertung, Transparenz, menschliche Aufsicht, Logging.
EU Digital Services Act (DSA)	**Beobachten**	Ab 17 Mio. Nutzern/Monat in der EU als 'Very Large Platform'. Jetzt nicht relevant, aber Grundanforderungen (Meldepflicht illegaler Inhalte) gelten bereits.
EU Data Act (2023/2854)	**Beobachten**	Regelt Datenzugang und -portabilität. Relevant wenn Schulen ihre Daten aus Schulfunk exportieren wollen.

Regelwerk	Status	Bedeutung für Schulfunk
Informationssicherheit		
NIS2 (EU 2022/2555 / NIS2UmsuCG)	Nicht jetzt	Gilt ab 50 MA oder €10M Umsatz für 'wichtige Einrichtungen'. Bildungssektor nicht direkt gelistet. **Jetzt nicht verpflichtend** — aber öffentliche Auftraggeber fordern NIS2-Konformität oft vertraglich.
BSI IT-Grundschutz	Beobachten	Nicht gesetzlich verpflichtend für Privatunternehmen, aber **de-facto Standard für öffentliche Auftraggeber**. Schulen und Kommunen erwarten BSI-Konformität von IT-Dienstleistern. Relevant für Vertrieb.
ISO/IEC 27001	Beobachten	Internationale Norm für ISMS. Nicht verpflichtend, aber Zertifizierung erhöht Vertrauen bei Schulträgern und Kommunen erheblich. Aufbau auf BSI Grundschutz möglich.
KRITIS (BSI-Gesetz §8a)	Nicht jetzt	Gilt erst ab sehr hohen Schwellenwerten (z.B. 500.000 betroffene Personen). Nicht relevant.
Medien & Urheberrecht		
Jugendmedienschutz-Staatsvertrag (J	Trifft zu	**Relevant!** Schulfunk produziert Medieninhalte für/mit Minderjährigen. Jugendschutzbeauftragter ggf. nötig ab bestimmter Reichweite. Inhalte müssen altersgerecht sein.
Urheberrechtsgesetz (UrhG)	Trifft zu	Schüler erstellen Audioinhalte (Urheber!). Einwilligungen der Eltern nötig. Musiknutzung in Beiträgen (GEMA). Klären wer die Rechte an Sendungen hält.
Rundfunkrecht / MStV	Beobachten	Medienstaatsvertrag könnte greifen wenn Schulfunk als 'Rundfunk' eingestuft wird (Linearität, Breitenwirkung). Bisher eher nicht — aber prüfen lassen.
Sonstige		

Regelwerk	Status	Bedeutung für Schulfunk
GoBD (Grundsätze ordnungsmäßiger	**Trifft zu** **ung)**	Gilt für alle deutschen Unternehmen. Buchführung, Aufbewahrungspflichten.
Schulgesetz NRW (§ 120 SchulG NRW	**Trifft zu**	Regelt Datenverarbeitung durch Schulen und ihre Dienstleister. Schulfunk als Auftragsverarbeiter muss konform sein.
Barrierefreiheitsstärkungsgesetz (B	**Beobachten**	Ab Juni 2025 für digitale Produkte. Öffentliche Schulen erwarten barrierefreie Software. Betrifft schulfunk.app.

Die wichtigsten Sofortmaßnahmen

1. **EU AI Act:** Sobald KI-Features für Schüler → Hochrisiko-Konformität prüfen. Kein AI-Feature ohne menschliche Aufsicht und Logging.
2. **JMStV:** Eltern-Einwilligung für Medienproduktion mit Minderjährigen dokumentieren.
3. **UrhG:** Klären wer Rechte an Schüler-Produktionen hält. Eltern-Einwilligung + Nutzungsrechte.
4. **DSG NRW / SchulG NRW § 120:** AVV mit OGS Monte Bonn abschließen bevor Pilotstart.
5. **TTDSG:** Cookie-Banner und Datenschutzerklärung vor Launch schulfunk.app.

Strategische Hinweise

- **BSI Grundschutz** ist kein Gesetz, aber Kommunen und Schulträger fragen danach. Frühzeitig aufbauen = Vertriebsvorteil.
- **NIS2** trifft Empennage heute nicht direkt — aber Schulen als öffentliche Stellen unterliegen ggf. NIS2 und fordern Konformität von Dienstleistern vertraglich.
- **EU AI Act Hochrisiko** ist der größte strategische Einfluss: KI in Bildung = hochreguliert. Das kann USP sein ("wir sind compliant") oder Bremse.

Stand: Mai 2026 · Quellen: DSGVO, NIS2UmsuCG, EU AI Act, JMStV, SchulG NRW. Kein Rechtsrat.

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

1. **Privacy by Design:** Datenschutz wird von Anfang an in Produkte und Prozesse eingebaut, nicht nachträglich ergänzt.
2. **Minimalprinzip:** Es werden nur die Daten erhoben, die für den jeweiligen Zweck zwingend erforderlich sind.
3. **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