

Auftragsverarbeitungsvertrag (AVV)

Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag (AVV)

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

“  Word-Version zum Unterzeichnen: [AVV_Schulfunk_v1.docx](#) ”

Zwischen

Verantwortlicher {{Name des Schulträgers bzw. OGS-Trägers}} {{Straße, Hausnummer}}
{{PLZ Ort}} vertreten durch {{Name, Funktion}}

— im Folgenden »Verantwortlicher« genannt —

und

— im Folgenden »Auftragsverarbeiter« genannt —

— gemeinsam die »Parteien« —

§ 1 Gegenstand und Dauer des Auftrags

(1) Gegenstand des Auftrags ist die Erbringung der in Anlage 1 näher beschriebenen Leistungen durch den Auftragsverarbeiter (Bereitstellung und Betrieb der Kommunikationsplattform »Schulfunk«).

(2) Die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter erfolgt ausschließlich auf Grundlage dieses Vertrags und nach Weisung des Verantwortlichen.

(3) Diese Vereinbarung tritt mit Unterzeichnung in Kraft und gilt für die Dauer des zugrundeliegenden Hauptvertrags bzw. der Nutzung von Schulfunk durch den Verantwortlichen. Eine ordentliche Kündigung dieser AVV ohne gleichzeitige Beendigung des Hauptvertrags ist ausgeschlossen.

§ 2 Konkretisierung des Auftragsinhalts

(1) **Art und Zweck der Verarbeitung:** Bereitstellung einer Plattform für die interne und externe Kommunikation einer Schule und/oder OGS, insbesondere:

- Strukturierte Mitteilungen zwischen Mitarbeitenden (Personal-Personal-Kommunikation)
- Mitteilungen zwischen Personal und Sorgeberechtigten (z. B. Termine, allgemeine Hinweise, Krankmeldungen, Abholregelungen)
- Verwaltung von Gruppen, Klassen, Verteilern und Rollen

(2) **Art der personenbezogenen Daten:**

- Stammdaten Mitarbeitende: Vor- und Nachname, dienstliche E-Mail-Adresse, Rolle, Zuordnung zu Klassen/Gruppen

- Stammdaten Sorgeberechtigte: Vor- und Nachname, E-Mail-Adresse, ggf. Telefonnummer
- Stammdaten Kinder: Vor- und Nachname, Klasse/Gruppe, Anwesenheits-/Abwesenheitsstatus
- Inhalte der Kommunikation (Texte, Anhänge), die durch Nutzende eingegeben werden
- Metadaten der Nutzung (Zeitstempel, Lesebestätigungen, Login-Daten)

(3) **Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO)** können in eng begrenztem Umfang anfallen, soweit Eltern in Krankmeldungen freiwillig Angaben zu Gesundheitsdaten ihres Kindes machen. Der Verantwortliche stellt sicher, dass für diese Verarbeitung eine geeignete Rechtsgrundlage besteht.

(4) **Kategorien betroffener Personen:**

- Mitarbeitende des Verantwortlichen (OGS, Schule)
- Sorgeberechtigte
- Schülerinnen und Schüler / OGS-Kinder
- Externe Dienstleister, soweit eingebunden (z. B. AG-Leitungen)

§ 3 Technisch-organisatorische Maßnahmen (TOM)

(1) Der Auftragsverarbeiter trifft die in **Anlage 1 (TOM)** beschriebenen technischen und organisatorischen Maßnahmen zum Schutz der Daten nach Art. 32 DSGVO.

(2) Der Stand der TOM kann während der Vertragslaufzeit fortgeschrieben werden. Wesentliche Änderungen werden dem Verantwortlichen unverzüglich mitgeteilt. Die TOM dürfen das Schutzniveau nicht unterschreiten.

§ 4 Berichtigung, Einschränkung und Löschung

(1) Daten dürfen ausschließlich auf Weisung des Verantwortlichen berichtigt, gelöscht oder in der Verarbeitung eingeschränkt werden.

(2) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung von Betroffenenrechten (Art. 12–22 DSGVO) durch geeignete technische und organisatorische Maßnahmen.

§ 5 Qualitätssicherung und sonstige Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter verpflichtet sich insbesondere zu:

- Bestellung eines Datenschutzbeauftragten, soweit nach Art. 37 DSGVO erforderlich. Aktuell ist keine Bestellung erforderlich; Kontakt für Datenschutzangelegenheiten: **{{kontakt@empennage.de}}**.
- Schriftlicher Verpflichtung sämtlicher mit der Verarbeitung betrauten Personen auf das Datengeheimnis (Vertraulichkeit, Art. 28 Abs. 3 lit. b, Art. 29 DSGVO).
- Unverzüglicher Information des Verantwortlichen über Kontrollhandlungen einer Aufsichtsbehörde gegenüber dem Auftragsverarbeiter, soweit diese sich auf den Auftrag beziehen.
- Sicherstellung, dass eingesetzte Personen über den Inhalt dieses Vertrags geschult sind.
- Unterstützung des Verantwortlichen bei der Durchführung von Datenschutz-Folgenabschätzungen (Art. 35 DSGVO) und ggf. der vorherigen Konsultation (Art. 36 DSGVO).

§ 6 Unterauftragsverhältnisse

(1) Der Auftragsverarbeiter darf weitere Auftragsverarbeiter (Subunternehmen) nur mit vorheriger schriftlicher Genehmigung des Verantwortlichen einsetzen. Eine allgemeine Genehmigung für die in **Anlage 2** genannten Unterauftragsverarbeiter wird hiermit erteilt.

(2) Der Auftragsverarbeiter unterrichtet den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung anderer Auftragsverarbeiter. Der Verantwortliche kann gegen derartige Änderungen Einspruch erheben.

(3) Der Auftragsverarbeiter stellt sicher, dass Unterauftragsverarbeiter denselben Datenschutzpflichten unterliegen wie er selbst.

(4) Nicht als Unterauftragsverhältnis gelten Nebenleistungen wie Telekommunikationsleistungen, Post-/Transportdienstleistungen sowie Wartung und Pflege, soweit diese nicht den vertraglichen Hauptzweck betreffen.

§ 7 Kontrollrechte des Verantwortlichen

(1) Der Verantwortliche hat das Recht, sich vor Beginn der Verarbeitung und während der Vertragslaufzeit von der Einhaltung der getroffenen TOM zu überzeugen.

(2) Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anforderung alle erforderlichen Informationen zum Nachweis der Einhaltung seiner Pflichten zur Verfügung. Hierzu zählen insbesondere aktuelle Testate, Zertifikate oder Berichte von Sachverständigen.

(3) Bei Vor-Ort-Kontrollen sind die Belange des Auftragsverarbeiters angemessen zu berücksichtigen. Kontrollen sind mit angemessener Vorlaufzeit (mindestens 14 Tage) anzukündigen.

§ 8 Meldung bei Verstößen des Auftragsverarbeiters

(1) Der Auftragsverarbeiter meldet dem Verantwortlichen jede Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 48 Stunden nach Kenntnisnahme.

(2) Die Meldung enthält mindestens die in Art. 33 Abs. 3 DSGVO genannten Angaben.

(3) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei Meldepflichten nach Art. 33, 34 DSGVO.

§ 9 Weisungsbefugnis des Verantwortlichen

(1) Die Verarbeitung der Daten erfolgt ausschließlich auf dokumentierte Weisung des Verantwortlichen. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

(2) Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung des Verantwortlichen gegen datenschutzrechtliche Vorschriften verstößt, so hat er den Verantwortlichen unverzüglich darauf

hinzuweisen.

(3) Weisungsberechtigte Personen des Verantwortlichen: {{Name, Funktion, E-Mail}}
Weisungsempfänger beim Auftragsverarbeiter: Philipp Wolters, Winzerstr. 117, 53129 Bonn,
{{kontakt@empennage.de}}

§ 10 Löschung und Rückgabe nach Vertragsende

(1) Nach Beendigung des Auftrags hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten personenbezogenen Daten nach Wahl des Verantwortlichen zurückzugeben oder zu löschen. Bestehende gesetzliche Aufbewahrungspflichten bleiben unberührt.

(2) Die Löschung wird auf Anforderung schriftlich bestätigt.

§ 11 Haftung

Es gelten die gesetzlichen Regelungen zur Haftung nach Art. 82 DSGVO. Im Innenverhältnis haftet jede Partei für die Verstöße, die in ihrem Verantwortungsbereich liegen.

§ 12 Schlussbestimmungen

(1) Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein, berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

(2) Änderungen und Ergänzungen bedürfen der Schriftform.

(3) Es gilt deutsches Recht. Gerichtsstand ist – soweit zulässig – der Sitz des Verantwortlichen.

Unterschriften

Verantwortlicher Ort, Datum: _____

{{Name, Funktion}}

Anlage 1 – Technisch-organisatorische Maßnahmen (TOM)

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle

- Serverstandort: Hetzner Online GmbH, Rechenzentren in Deutschland (Falkenstein / Nürnberg)
- Zertifizierungen des Rechenzentrums (ISO 27001, ...) liegen vor (Nachweise auf Anfrage)
- Physischer Zugang nur für autorisiertes Personal des Rechenzentrumsbetreibers

Zugangskontrolle

- Authentifizierung über E-Mail + Passwort, Passwort-Mindestlänge ≥ 12 Zeichen
- Optional Zwei-Faktor-Authentifizierung
- Automatische Sperrung nach mehreren Fehlversuchen
- Administrative Zugänge über separate Accounts mit Zwei-Faktor-Authentifizierung
- SSH-Zugriffe nur via Public-Key-Authentifizierung, keine Passwort-Logins

Zugriffskontrolle

- Rollenbasiertes Berechtigungskonzept innerhalb der Anwendung (Rollen z. B. Schulleitung, OGS-Leitung, Gruppenleitung, Eltern)
- Trennung administrativer und fachlicher Zugriffe
- Protokollierung administrativer Zugriffe (Audit-Log)

Trennungskontrolle

- Logische Trennung der Daten je Einrichtung (Mandantenfähigkeit)

- Trennung von Test-, Entwicklungs- und Produktivumgebung

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle

- Verschlüsselte Übertragung (TLS 1.2 oder höher) zwischen Endgeräten und Server
- Verschlüsselte Backups
- Keine Datenübermittlung in Drittstaaten ohne ausdrückliche Weisung

Eingabekontrolle

- Protokollierung relevanter Verarbeitungsvorgänge (Wer hat was wann geändert?)
- Aufbewahrung der Protokolle für mindestens 90 Tage

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

- Tägliche automatisierte Backups, Aufbewahrung mindestens 30 Tage
- Backups verschlüsselt und an separatem Standort innerhalb der EU
- Regelmäßige Test-Wiederherstellungen
- Monitoring der Systemverfügbarkeit
- Schutz gegen Schadsoftware durch aktuelle Systempflege (regelmäßige Sicherheitsupdates)

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

- Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DSGVO wird geführt
- Datenschutzvorfälle werden protokolliert und ausgewertet
- TOM werden mindestens jährlich überprüft

5. Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a

DSGVO)

- Passwörter werden ausschließlich als Hash (bcrypt o. ä.) gespeichert
 - Datenbank-Backups verschlüsselt
 - Verschlüsselung at-rest auf Festplatten-Ebene (LUKS / vergleichbar)
-

Anlage 2 – Genehmigte Unterauftragsverarbeiter

Name	Anschrift	Leistung	Standort
Hetzner Online GmbH	Industriestr. 25, 91710 Gunzenhausen	Hosting / Rechenzentrum	Deutschland
{{ggf. weitere}}			

Etwaige weitere Unterauftragsverarbeiter werden dem Verantwortlichen vor Einsatz mitgeteilt; der Verantwortliche hat ein Widerspruchsrecht.

Dokumentversion: v1 · Stand: {{Datum}}

Revision #3
Created 2026-05-12 00:18:22 UTC by philipp
Updated 2026-05-12 07:56:49 UTC by philipp