

Auftragsverarbeitungsvertrag (AVV) nach Art. 28 DSGVO

Geltungsbereich: Dieser AVV betrifft **ausschließlich den Signatur-Vermittlungsdienst** („Relay“) nach § 10 Abs. 3 AGB. Nur dort verarbeitet der Anbieter personenbezogene Daten **im Auftrag** des Kunden.

Nicht Gegenstand dieses AVV sind die Daten der Lizenzschlüsselverifizierung, der Vertrags- und Rechnungsabwicklung sowie die Server-Logfiles: Diese verarbeitet der Anbieter nach § 10 Abs. 2 AGB als **eigener Verantwortlicher** (Art. 4 Nr. 7 DSGVO), nicht im Auftrag. Ebenfalls nicht Gegenstand sind die lokal beim Kunden verarbeiteten Daten der Schülerinnen und Schüler, Lehrkräfte und Erziehungsberechtigten — auf diese hat der Anbieter keinen Zugriff.

Abschluss: Standard-Vereinbarung für alle Kunden — ohne Ausfüllen und ohne Unterschrift (Textform, Art. 28 Abs. 9 DSGVO). Sie gilt mit der ersten Nutzung des Vermittlungsdienstes als angenommen; eine unterschriebene Fassung wird auf Wunsch erstellt (Feld am Dokumentende).

Präambel und Vertragsschluss

Verantwortlicher (Auftraggeber) ist der Kunde des zwischen den Parteien geschlossenen Software-Mietvertrags über die Software LeihPilot — die Schule bzw. der Schulträger als Vertragspartner des Hauptvertrags (nachfolgend „Verantwortlicher“).

Auftragsverarbeiter (Anbieter):

Feuerstein & Holtheide GmbH

Im Heidewinkel 5, 49594 Alfhausen

Amtsgericht Osnabrück, HRB 210162

vertreten durch die Geschäftsführer Norbert Holtheide und Michael Feuerstein

— nachfolgend „Auftragsverarbeiter“ —

Die Parteien schließen die folgende Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 DSGVO. Die Vereinbarung wird **in Textform** geschlossen (Art. 28 Abs. 9 DSGVO); einer Unterschrift bedarf es nicht. Sie gilt als angenommen, sobald der Verantwortliche den Signatur-Vermittlungsdienst **erstmalig nutzt**, spätestens mit einer Annahmeerklärung in Textform. Das Dokument wird dem Verantwortlichen dauerhaft zum Abruf bereitgestellt; auf Wunsch fertigen die Parteien eine gegengezeichnete Fassung (Unterschriftsfeld am Ende dieses Dokuments).

§ 1 Gegenstand, Umfang und Dauer

(1) Grundlage dieser Vereinbarung ist der zwischen den Parteien über die Software **LeihPilot** geschlossene Software-Mietvertrag unter Einbeziehung der Allgemeinen Geschäftsbedingungen des Auftragsverarbeiters (nachfolgend „Hauptvertrag“).

(2) Gegenstand dieser Vereinbarung ist ausschließlich die Verarbeitung personenbezogener Daten im Rahmen des **Signatur-Vermittlungsdienstes** nach § 10 Abs. 3 AGB. Der Vermittlungsdienst ermöglicht es dem Verantwortlichen, eine handschriftliche Unterschrift zwischen zwei seiner Endgeräte zu übertragen, wenn diese sich in getrennten Netzen befinden.

(3) Der Auftragsverarbeiter verarbeitet die übertragenen Daten ausschließlich in Form eines **Ende-zu-Ende-verschlüsselten Chiffrats**. Der zur Entschlüsselung erforderliche private Schlüssel wird lokal in der IT-Umgebung des Verantwortlichen erzeugt und dem Auftragsverarbeiter zu keinem Zeitpunkt übermittelt. Der Auftragsverarbeiter kann die übertragenen Daten technisch **nicht** entschlüsseln und nimmt keine inhaltliche Kenntnis.

(4) Die Nutzung des Vermittlungsdienstes ist für den Verantwortlichen **freiwillig**. Findet keine Nutzung statt, findet keine Verarbeitung im Auftrag statt.

(5) Diese Vereinbarung gilt für die Laufzeit des Hauptvertrags und endet automatisch mit dessen Beendigung.

§ 2 Art und Zweck der Verarbeitung

(1) **Zweck:** Technische Vermittlung („toter Briefkasten“) einer verschlüsselt übertragenen Unterschrift zwischen dem Verwaltungsrechner und dem zur Unterschrift genutzten Endgerät des Verantwortlichen.

(2) **Art der Verarbeitung:** Entgegennahme, kurzzeitige Speicherung und Herausgabe eines verschlüsselten Datenpakets sowie dessen Löschung. Eine inhaltliche Auswertung, Zusammenführung oder sonstige Nutzung findet nicht statt.

(3) **Dauer der Speicherung:**

a) Bei unmittelbarer (zeitgleicher) Übertragung wird das Chifftrat ausschließlich im Arbeitsspeicher gehalten und nach dem Abruf sofort gelöscht (Einmal-Abruf); es wird nicht auf einen dauerhaften Datenträger geschrieben.

b) Bei zeitversetzter Unterschrift (Zugangslink per E-Mail) wird das Chifftrat für **höchstens sieben Kalendertage** verschlüsselt gespeichert und nach dem Abruf durch den Verantwortlichen unverzüglich gelöscht. Nicht abgerufene Datensätze sind nach Ablauf der sieben Kalendertage nicht mehr abrufbar und werden durch einen automatisierten, mindestens täglich laufenden Löschlauf endgültig entfernt.

(4) Der Versand des Zugangslinks an die unterzeichnende Person nimmt der Verantwortliche selbst vor. Die Empfängeradresse wird dem Auftragsverarbeiter nicht bekannt und nicht übermittelt.

§ 3 Art der Daten und Kategorien betroffener Personen

(1) **Verarbeitete Datenarten:**

- das Ende-zu-Ende-verschlüsselte Chifftrat, das die Unterschrift enthält,

- ein zufällig erzeugtes Sitzungs-Token ohne Personenbezug,
- die auf die Schule bezogene Lizenz-Kennung,
- der Ablaufzeitpunkt der Sitzung,
- die IP-Adresse der aufrufenden Geräte, ausschließlich transient zur Missbrauchsabwehr (Rate-Limiting); eine Speicherung dieser IP-Adressen zu den Sitzungen findet nicht statt.

(2) **Kategorien betroffener Personen:** Personen, die im Rahmen der Geräteausleihe eine Unterschrift leisten — insbesondere Schülerinnen und Schüler, Erziehungsberechtigte, Lehrkräfte sowie Vertreterinnen und Vertreter des Verantwortlichen.

(3) **Nicht übermittelt und nicht verarbeitet werden insbesondere:** Namen, Anschriften, E-Mail-Adressen, Klassen- oder Rollenbezeichnungen, ein Bezug zu einem bestimmten Leihvertrag sowie Geräte-, Vertrags-, Schadens- und Fotodaten. Aus den beim Auftragsverarbeiter vorhandenen Daten ist nicht ableitbar, **wer** unterschrieben hat, sondern lediglich, **dass** eine Lizenz eine Signatur-Sitzung geführt hat.

§ 4 Weisungsrecht des Verantwortlichen (Art. 28 Abs. 3 lit. a DSGVO)

(1) Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen. Diese Vereinbarung nebst Hauptvertrag stellt die vollständige Weisung dar; die Nutzung des Vermittlungsdienstes durch den Verantwortlichen gilt als Einzelweisung zur Durchführung der jeweiligen Übertragung.

(2) Weitergehende Weisungen bedürfen der Textform. Weisungsberechtigt und weisungsempfangend sind die in § 12 Abs. 5 benannten Ansprechpartner.

(3) Eine Verarbeitung zu eigenen Zwecken des Auftragsverarbeiters findet im Rahmen dieser Vereinbarung nicht statt.

(4) Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, teilt er dies dem Verantwortlichen unverzüglich mit. Er ist berechtigt, die Durchführung der betreffenden Weisung bis zu deren Bestätigung oder Änderung auszusetzen (Art. 28 Abs. 3 Satz 3 DSGVO).

(5) Eine Übermittlung der Daten in ein Drittland findet nicht statt. Die Verarbeitung erfolgt ausschließlich in der Bundesrepublik Deutschland.

§ 5 Pflichten des Auftragsverarbeiters

(1) **Vertraulichkeit (Art. 28 Abs. 3 lit. b, Art. 29, Art. 32 Abs. 4 DSGVO):** Der Auftragsverarbeiter stellt sicher, dass alle zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet sind und personenbezogene Daten ausschließlich auf Weisung verarbeiten.

(2) **Datenschutzbeauftragter:** Der Auftragsverarbeiter benennt einen Datenschutzbeauftragten, soweit er hierzu gesetzlich verpflichtet ist. Eine Benennungspflicht nach Art. 37 DSGVO, § 38 BDSG besteht derzeit nicht; der Auftragsverarbeiter zeigt dem Verantwortlichen eine spätere Benennung unaufgefordert an.

(3) **Unterstützung bei Betroffenenrechten (Art. 28 Abs. 3 lit. e DSGVO):** Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen des ihm Möglichen bei der Beantwortung von Anträgen betroffener Personen nach Art. 12–22 DSGVO. Aufgrund der Ende-zu-Ende-Verschlüsselung und der fehlenden Identitätsmerkmale kann der Auftragsverarbeiter einzelne betroffene Personen in den verarbeiteten Daten nicht identifizieren (Art. 11 DSGVO).

(4) **Unterstützung bei weiteren Pflichten (Art. 28 Abs. 3 lit. f DSGVO):** Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO.

(5) **Weiterleitung von Anfragen:** Wenden sich betroffene Personen oder eine Aufsichtsbehörde unmittelbar an den Auftragsverarbeiter, leitet er die Anfrage unverzüglich an den Verantwortlichen weiter und beantwortet sie nicht eigenständig, soweit er nicht gesetzlich dazu verpflichtet ist.

(6) **Nachweispflicht (Art. 28 Abs. 3 lit. h DSGVO):** Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO zur Verfügung.

§ 6 Technische und organisatorische Maßnahmen (Art. 28 Abs. 3 lit. c, Art. 32 DSGVO)

(1) Der Auftragsverarbeiter trifft die in **Anlage 1** beschriebenen technischen und organisatorischen Maßnahmen; die für den Vermittlungsdienst maßgeblichen Maßnahmen sind dort in **Ziffer 6** dargestellt. Anlage 1 ist Bestandteil dieser Vereinbarung.

(2) Der Auftragsverarbeiter ist berechtigt, die Maßnahmen fortzuentwickeln, sofern das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen dokumentiert er und weist sie dem Verantwortlichen auf Verlangen nach.

§ 7 Unterauftragsverhältnisse (Art. 28 Abs. 2, Abs. 4 DSGVO)

(1) Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine Genehmigung, folgende Unterauftragnehmer einzusetzen:

Unterauftragnehmer	Sitz	Leistung
Hetzner Online GmbH	Gunzenhausen, Deutschland (Rechenzentrum Falkenstein/Nürnberg)	Bereitstellung der Server-Infrastruktur einschließlich Speicher (Hosting)

(2) Der Auftragsverarbeiter schließt mit jedem Unterauftragnehmer einen Vertrag, der diesem im Wesentlichen dieselben Datenschutzpflichten auferlegt, die in dieser Vereinbarung festgelegt sind.

(3) Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens **30 Kalendertage** vor der beabsichtigten Hinzuziehung oder Ersetzung eines Unterauftragnehmers in Textform. Der Verantwortliche kann innerhalb von 30 Kalendertagen ab Zugang der Mitteilung aus einem datenschutzrechtlich begründeten Anlass in Textform widersprechen. Widerspricht der

Verantwortliche, sind beide Parteien berechtigt, diese Vereinbarung sowie den Hauptvertrag mit einer Frist von einem Monat zu kündigen; für bereits bezahlte, nach Wirksamwerden der Kündigung liegende Leistungszeiträume erstattet der Auftragsverarbeiter die Vergütung anteilig.

(4) Nicht als Unterauftragsverhältnis gelten Nebenleistungen, die der Auftragsverarbeiter bei Dritten in Anspruch nimmt, ohne dass diese Zugang zu den Daten nach § 3 erhalten (z. B. Telekommunikationsleistungen).

§ 8 Kontrollrechte des Verantwortlichen (Art. 28 Abs. 3 lit. h DSGVO)

(1) Der Verantwortliche ist berechtigt, die Einhaltung dieser Vereinbarung zu überprüfen.

(2) Der Nachweis erfolgt im Regelfall durch Vorlage der jeweils aktuellen Fassung der Anlage 1 sowie durch Vorlage der Zertifizierung des Unterauftragnehmers nach ISO/IEC 27001.

(3) Genügen diese Nachweise im Einzelfall nicht, kann der Verantwortliche nach Voranmeldung mit einer Frist von **30 Kalendertagen** zu üblichen Geschäftszeiten eine Überprüfung vor Ort durchführen oder durch einen zur Verschwiegenheit verpflichteten, nicht mit dem Auftragsverarbeiter im Wettbewerb stehenden Prüfer durchführen lassen. Die Überprüfung darf den Betriebsablauf nicht unangemessen beeinträchtigen. Die Kosten trägt der Verantwortliche, es sei denn, es werden erhebliche Verstöße festgestellt.

§ 9 Meldung von Verletzungen des Schutzes personenbezogener Daten (Art. 33 DSGVO)

(1) Der Auftragsverarbeiter meldet dem Verantwortlichen jede Verletzung des Schutzes personenbezogener Daten in seinem Verantwortungsbereich unverzüglich nach Bekanntwerden, spätestens jedoch innerhalb von **48 Stunden**.

(2) Die Meldung enthält die dem Auftragsverarbeiter verfügbaren Angaben entsprechend Art. 33 Abs. 3 DSGVO, insbesondere Art des Vorfalls, betroffene Datenkategorien, wahrscheinliche Folgen sowie ergriffene und vorgeschlagene Maßnahmen.

(3) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei dessen Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO.

(4) Die Meldung erfolgt an die in § 12 Abs. 5 benannte Kontaktstelle des Verantwortlichen.

§ 10 Löschung und Rückgabe (Art. 28 Abs. 3 lit. g DSGVO)

(1) Die im Rahmen des Vermittlungsdienstes verarbeiteten Daten werden nach Maßgabe von § 2 Abs. 3 laufend gelöscht.

(2) Nach Beendigung dieser Vereinbarung löscht der Auftragsverarbeiter sämtliche noch vorhandenen Daten nach § 3 unverzüglich, spätestens innerhalb von **30 Kalendertagen**. Eine

Rückgabe erfolgt nicht, da die Daten für den Verantwortlichen ohne den bei ihm verbliebenen privaten Schlüssel ohnehin nicht lesbar sind und nach § 2 Abs. 3 bereits gelöscht wurden.

(3) Gesetzliche Aufbewahrungspflichten bleiben unberührt; sie bestehen für die Daten nach § 3 nicht.

(4) Auf Verlangen bestätigt der Auftragsverarbeiter die Löschung in Textform.

§ 11 Haftung

(1) Für die Haftung der Parteien gelten die Regelungen des Hauptvertrags (§ 8 AGB) entsprechend.

(2) Art. 82 DSGVO sowie die Verantwortlichkeit der Parteien nach Art. 82 Abs. 2 DSGVO bleiben unberührt.

§ 12 Schlussbestimmungen

(1) Diese Vereinbarung ist Bestandteil des Hauptvertrags und kann nur gemeinsam mit diesem gekündigt werden; § 7 Abs. 3 bleibt unberührt.

(2) Bei Widersprüchen zwischen dieser Vereinbarung und dem Hauptvertrag gehen in datenschutzrechtlichen Fragen die Regelungen dieser Vereinbarung vor.

(3) Änderungen und Ergänzungen bedürfen der Textform. Dies gilt auch für die Abbedingung dieses Formerfordernisses.

(4) Sollte eine Bestimmung dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

(5) **Ansprechpartner für Weisungen und Meldungen nach dieser Vereinbarung.** Beim Verantwortlichen ist dies die im Bestellprozess hinterlegte Kontaktperson, sofern nicht in Textform eine andere Stelle benannt wird; beim Auftragsverarbeiter die E-Mail-Adresse leihpilot@feuerholt.de. Vertragsparteien bleiben die in der Präambel bezeichneten Organisationen; die Ansprechpartner sind lediglich deren Kontaktstellen.

(6) Es gilt das Recht der Bundesrepublik Deutschland. Ausschließlicher Gerichtsstand ist der Sitz des Auftragsverarbeiters, soweit der Verantwortliche Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist.

Optionale Unterschriftsfassung

Der Wirksamkeit dieser Vereinbarung bedarf es keiner Unterschrift (Abschluss in Textform, siehe Präambel). Wünscht der Verantwortliche eine gegengezeichnete Fassung, unterzeichnen die Parteien hier:

Ort, Datum

Verantwortlicher (Kunde)

Ort, Datum

Auftragsverarbeiter (Anbieter)

Anlagen

- **Anlage 1:** Technische und organisatorische Maßnahmen (TOM)

Anlage 1 – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Anlage 1 zum Auftragsverarbeitungsvertrag. Beschreibung der technischen und organisatorischen Maßnahmen des Anbieters gemäß **Art. 32 DSGVO**.

Der AVV ist auf den **Signatur-Vermittlungsdienst** zugeschnitten; die dafür maßgeblichen Maßnahmen stehen in **Ziffer 6**. Die Ziffern 1–4 beschreiben darüber hinaus die allgemeinen Maßnahmen des Anbieters für den Lizenzserver, Ziffer 5 die Produktmerkmale für die lokal beim Kunden verbleibenden Daten. Die Kundenbeziehung regeln im Übrigen die AGB.

Herausgeber dieser Anlage: Feuerstein & Holtheide GmbH, Im Heidewinkel 5, 49594 Alfhausen — im AVV der **Auftragsverarbeiter Stand:** 12. August 2026 **Geltungsbereich:** Lizenzserver der Software LeihPilot und unterstützende Dienste. Lokale Daten beim Lizenznehmer liegen außerhalb des Einflussbereichs des Anbieters; insoweit werden die in den Funktionen der Software vorgesehenen Schutzmaßnahmen beschrieben (Ziffer 5).

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

1.1 Zutrittskontrolle

- Hosting des Lizenzservers ausschließlich bei der **Hetzner Online GmbH** im Rechenzentrum Falkenstein bzw. Nürnberg, Deutschland.
- Die Rechenzentren der Hetzner Online GmbH sind nach **ISO/IEC 27001** zertifiziert (Zertifikat öffentlich abrufbar).
- Physischer Zutritt ist mehrstufig gesichert (Zaun, Vereinzelungsanlage, Videoüberwachung, dokumentierte Zugangsprotokollierung).
- Mitarbeitende des Anbieters haben keinen physischen Zugriff auf die Server-Hardware.

1.2 Zugangskontrolle

- SSH-Zugang zum Lizenzserver ausschließlich über öffentlichen Schlüssel (ed25519); Passwort-Authentifizierung ist deaktiviert.
- Administrative Zugänge zum Lizenzserver und zum Hetzner-Cloud-Panel sind ausschließlich auf namentlich benannte Personen des Anbieters beschränkt.
- **Zweiter Faktor (TOTP) ist im Admin-Bereich des Lizenzservers verpflichtend**; ohne erfolgreiche Bestätigung des zweiten Faktors ist kein Zugriff auf das Verwaltungs-Panel möglich.
- Passwörter der Verwaltungs-Accounts werden mit bcrypt (zwölf Runden) gehasht; TOTP-Geheimnisse und Wiederherstellungs-Codes werden mit dem `APP_KEY` der Anwendung verschlüsselt.
- Inaktive Sitzungen werden automatisch beendet.
- Es werden keine Sammel- oder Shared-Accounts verwendet.

1.3 Zugriffskontrolle

- Rollenkonzept innerhalb des Administrations-Panels (Berechtigungs- und Funktionstrennung).
- Datenbankzugriff ausschließlich über authentifizierte Verbindungen mit eigenem Benutzer und Passwort; verschlüsselte Übertragung über TLS bei Remote-Zugriff.
- Prinzip der minimalen Rechte (Least Privilege).
- Aktivitäten relevanter Verwaltungsvorgänge (Anlage und Änderung von Lizenzen, Rechnungen, Bank-Importen, organisationsbezogene Änderungen, Authentifizierungsereignisse) werden über ein Audit-Log auf Anwendungsebene protokolliert (Spatie ActivityLog).

1.4 Trennungskontrolle

- Produktiv- und Entwicklungsumgebung sind strikt getrennt; in Test- und Entwicklungsumgebungen werden keine Produktivdaten verwendet.
- Daten verschiedener Lizenznehmer sind in der Datenbank logisch über `organization_id` und `license_id` getrennt; jeder Lizenz-Refresh wird über den schulindividuellen Lizenzkey authentifiziert.

1.5 Pseudonymisierung und Verschlüsselung

- **TLS 1.3** für alle Verbindungen zum Lizenzserver, HSTS aktiv.
- **Lokale Datenbank der Software:** AES-256-Verschlüsselung über SQLCipher. Der Datenbankschlüssel wird im OS-Schlüsselspeicher des Arbeitsplatz-Rechners (macOS Keychain, Windows Credential Manager) abgelegt; er wird zu keinem Zeitpunkt an den Anbieter übertragen.
- **Lizenz-Token (JWT):** ed25519-Signatur; der öffentliche Schlüssel ist in der Software eingebettet, der private Schlüssel ausschließlich auf dem Lizenzserver vorhanden.

- **Geräte-Fingerprint:** kryptografischer Hash (SHA-256) über Geräte-Merkmale; nicht reversibel.
-

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

2.1 Weitergabekontrolle

- Sämtliche Übertragungen erfolgen ausschließlich verschlüsselt (TLS 1.3).
- Zertifikate werden über Let's Encrypt automatisch erneuert.
- Es gibt keine unverschlüsselten API-Endpunkte.
- SSH-Schlüssel werden bei Personalwechsel rotiert.

2.2 Eingabekontrolle

- Audit-Log auf Anwendungsebene erfasst alle relevanten Datenänderungen (Lizenzen, Rechnungen, Bank-Transaktionen, Organisationen, Authentifizierungsereignisse).
 - Versionskontrolle (Git) für sämtliche Code-Änderungen.
 - Signierte Git-Commits.
-

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

3.1 Verfügbarkeit

- Verfügbarkeits-Monitoring des Lizenzservers mit Alarmierung per E-Mail bei Ausfall.
- Angestrebte monatliche Durchschnitts-Verfügbarkeit: **mindestens 99,5 %** (vertraglich zugesichert in AGB § 4 Abs. 3).
- DDoS-Schutz auf Netzwerkebene durch Hetzner.

3.2 Wiederherstellbarkeit

- **Tägliche automatische Sicherungen des Lizenzservers** über die Backup-Funktion des Hosters (Hetzner Online GmbH). Gesichert wird der vollständige Server einschließlich der Datenbank.
- **Aufbewahrung:** sieben Sicherungsstände im rollierenden Verfahren — der jeweils älteste wird überschrieben. Die Rückreichweite beträgt damit sieben Tage.
- **Ergänzende Sicherung der Datenbank:** täglich, verschlüsselt und räumlich getrennt vom Lizenzserver gespeichert. Aufbewahrung gestaffelt bis zu sechs Monate.
- **Wiederherstellungs-Test:** anlassbezogen, insbesondere nach Änderungen an der Backup-Infrastruktur.
- **Wiederanlauf-Zielwerte:** RTO (Recovery Time Objective) vier Stunden, RPO (Recovery Point Objective) 24 Stunden.

3.3 Belastbarkeit

- Anwendungsseitiges Rate-Limiting (Lizenz-API: 20 Anfragen je Minute und IP).
 - Skalierbare Cloud-Infrastruktur, vertikale Skalierung bei Bedarf.
-

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

4.1 Datenschutz-Management

- Alle zur Verarbeitung personenbezogener Daten befugten Personen werden vor Aufnahme ihrer Tätigkeit schriftlich zur Vertraulichkeit und zur Einhaltung der datenschutzrechtlichen Anforderungen verpflichtet (Verpflichtungserklärung Datengeheimnis).
- Datenschutz-relevante Verfahrensänderungen werden vor Inbetriebnahme bewertet.
- Die mit der Verarbeitung befassten Personen setzen sich im Rahmen ihrer Aufgaben- und Produktverantwortung laufend mit Datenschutz- und Informationssicherheitsthemen auseinander.

4.2 Incident Response

- Verletzungen des Schutzes personenbezogener Daten werden im eigenen Verantwortungsbereich gemäß Art. 33 und 34 DSGVO an die zuständige Aufsichtsbehörde bzw. an betroffene Personen gemeldet; Kunden als Verantwortliche unterrichtet der Anbieter nach Maßgabe des AVV (spätestens 48 Stunden nach Bekanntwerden).

4.3 Überprüfung der TOM

- Die Wirksamkeit der Maßnahmen wird release-begleitend überprüft: sicherheitsrelevante Abhängigkeits-Audits und archivierte Software-Stücklisten je Release (siehe 4.5) machen den Prüfstand nachvollziehbar.
- Anlassbezogene Überprüfung und Anpassung bei neuen Risiken, Sicherheitsvorfällen oder veränderter Technologielage.

4.4 Auftragskontrolle gegenüber Unterauftragnehmern

- Abschluss von Auftragsverarbeitungsverträgen mit allen Unterauftragnehmern (insbesondere Hetzner Online GmbH).
- Prüfung der Zertifikate der Unterauftragnehmer (insbesondere ISO/IEC 27001) bei Vertragsschluss und bei wesentlichen Änderungen.

4.5 Software-Sicherheitsmanagement

- **Composer-Audit** und **npm audit** (Audit-Level „high“) vor jedem Release; verbleibende Hinweise werden dokumentiert.

- **Plattformspezifische Software-Stücklisten (SBOM)** im Format CycloneDX werden pro Release archiviert (Vorbereitung auf den EU Cyber Resilience Act, anwendbar ab September 2026).
-

5. Besonderheit: Datenhaltung beim Lizenznehmer

Der weit überwiegende Teil der durch die Software verarbeiteten Daten — insbesondere **alle Schüler- und Lehrkräftedaten** — liegt **ausschließlich lokal beim Lizenznehmer**. Der Anbieter hat auf diese Daten **keinen Zugriff** und kann technisch-organisatorische Maßnahmen für sie nur in Form von **Produktmerkmalen** bereitstellen:

5.1 Sicherheit der lokalen Software-Datenbank

- AES-256-Verschlüsselung der lokalen Datenbank über SQLCipher.
- Der Datenbankschlüssel wird über das Betriebssystem-Schlüsselspeicher-API gesichert und nie an den Anbieter übertragen.
- Passwort-Richtlinie der Software: mindestens zehn Zeichen, Groß- und Kleinbuchstabe, Ziffer.
- Passwörter werden mit bcrypt (Konfiguration: zwölf Runden) gehasht.
- Login-Rate-Limiting: nach fünf fehlgeschlagenen Versuchen innerhalb 15 Minuten Sperrung.
- Wiederherstellungs-Code für vergessene Administratoren-Passwörter, einmalig nutzbar.
- Automatischer Logout nach acht Stunden absoluter Sitzungsdauer.
- Rollenkonzept innerhalb der Software (Administrator, Sachbearbeitung, Nur-Lesen).

5.2 Funktionen für den Lizenznehmer

- Integriertes Audit-Log, einsehbar nur durch die Rolle Administrator.
- Backup- und Wiederherstellungsfunktion mit Pfad- und Dateiendung-Prüfung.
- Schutz gegen Selbst-Deaktivierung oder Selbst-Herabstufung des einzigen Administrators.
- Eigenes Protokoll `photo://` mit Pfad-Validierung für die Anzeige hochgeladener Fotos.
- Foto-Upload über das lokale WLAN durch einen ausschließlich während aktiver Modal-Sitzungen geöffneten HTTP-Server mit Einmal-Token (30 Minuten Gültigkeit).
- Whitelist erlaubter Konfigurationsschlüssel zur Vermeidung unzulässiger Einstellungsänderungen.
- Automatische und manuelle Datenbank-Sicherung (Intervall und Aufbewahrung konfigurierbar).

5.3 Empfehlungen an den Lizenznehmer

Der Lizenznehmer ist für die Umsetzung folgender Maßnahmen auf seinen Arbeitsplatz-Rechnern (den schulischen PCs und Notebooks, auf denen die Software installiert ist) selbst verantwortlich:

- Passwortschutz aller Arbeitsplätze und Aktivierung der Bildschirmsperre bei Inaktivität.

- Festplattenverschlüsselung (BitLocker, FileVault).
 - Aktuelle Sicherheits-Updates des Betriebssystems und der eingesetzten Anwendungen.
 - Aktueller Schadcode-Schutz.
 - Separate Benutzerkonten je Mitarbeiterin und Mitarbeiter.
 - Sichere Aufbewahrung der Backup-Dateien.
 - Regelmäßige Datensicherung über die in der Software vorgesehene Funktion.
-

6. Signatur-Vermittlungsdienst (Gegenstand des AVV)

Maßgebliche Maßnahmen für die Verarbeitung im Auftrag nach § 10 Abs. 3 AGB. Der Dienst ist ein reiner, verschlüsselter Durchleiter („toter Briefkasten“).

6.1 Verschlüsselung und Schlüsselhoheit

- **Ende-zu-Ende-Verschlüsselung** der Unterschrift: hybrides Verfahren (AES-256-GCM für den Inhalt, RSA-OAEP/SHA-256 für den Inhaltsschlüssel).
- Das Schlüsselpaar wird **lokal auf dem Verwaltungsrechner des Kunden** erzeugt. Der **private Schlüssel verlässt die IT-Umgebung des Kunden nicht** und wird dem Anbieter zu keinem Zeitpunkt übermittelt.
- Der öffentliche Schlüssel wird ausschließlich im **URL-Fragment** übergeben. Fragmente werden von Browsern technisch nicht an den Server gesendet und erreichen den Anbieter daher nicht.
- **Folge:** Der Anbieter kann das Chifftrat technisch nicht entschlüsseln. Er validiert ausschließlich dessen Größe und Vorhandensein und nimmt keine inhaltliche Kenntnis.
- Transportverschlüsselung: TLS für alle Verbindungen.

6.2 Datenminimierung

- Gespeichert werden ausschließlich: Sitzungs-Token (Zufallswert), Lizenz-Kennung der Schule, Chifftrat, Ablaufzeitpunkt.
- **Nicht übermittelt und nicht gespeichert:** Namen, Anschriften, E-Mail-Adressen, Rollen- oder Klassenbezeichnungen, Bezug zu einem bestimmten Leihvertrag.
- Die Signaturseite zeigt der unterschreibenden Person bewusst nur eine generische Aufforderung ohne personenbezogene Angaben.
- Anzahl und Bezeichnung der zu leistenden Unterschriften stehen ausschließlich im URL-Fragment und sind dem Anbieter nicht bekannt.
- Der Versand des Zugangslinks erfolgt durch den Kunden selbst; die Empfängeradresse wird dem Anbieter nicht bekannt.

6.3 Zugriffsschutz

- Das Sitzungs-Token ist ein kryptografisch zufälliger 128-Bit-Wert und dient als Zugriffsberechtigung für die Sitzung.

- Die Herausgabe des Chiffrats erfolgt ausschließlich an die Lizenz, die die Sitzung angelegt hat; Anfragen fremder Lizenzen erhalten keine Auskunft über die Existenz der Sitzung.
- Rate-Limiting auf Anwendungsebene zur Missbrauchsabwehr; die dabei genutzte IP-Adresse wird transient verarbeitet und nicht zu den Sitzungen gespeichert.

6.4 Speicherbegrenzung und Löschung

Übertragungsweg	Ablage	Höchstdauer	Löschung
Unmittelbar (zeitgleich)	ausschließlich Arbeitsspeicher	Minuten	sofort nach Abruf (Einmal-Abruf)
Zeitversetzt (Zugangslink)	verschlüsselt, dauerhafter Speicher	7 Kalendertage	nach Abruf unverzüglich; zusätzlich automatisierter täglicher Löschlauf für nicht abgerufene Sitzungen

- Für den unmittelbaren Weg erzwingt eine technische Prüfung beim Start der Anwendung einen Arbeitsspeicher-Cache als Ablageort; der Cache wird ohne Datenträger-Persistenz betrieben, sodass das Chifftrat nicht auf einen dauerhaften Datenträger geschrieben wird.

6.5 Ort der Verarbeitung

- Ausschließlich Rechenzentren in der Bundesrepublik Deutschland (Unterauftragnehmer Hetzner Online GmbH); keine Drittlandübermittlung.

Anhang: Unterauftragnehmer

Unternehmen	Sitz	Zweck	Zertifizierungen	Unterauftragnehmer im Sinne des AVV?
Hetzner Online GmbH	Gunzenhausen, DE; Rechenzentrum Falkenstein/Nürnberg	Hosting Lizenzserver, Server- Sicherungen	ISO/IEC 27001	ja (§ 7 AVV)
Heinlein Hosting GmbH (mailbox.org)	Berlin, DE	Versand transaktionaler E-Mails (Rechnung, Lizenzkey)	—	nein — am Vermittlungsdienst nicht beteiligt; betrifft nur die Verarbeitung, die der Anbieter als eigener Verantwortlicher vornimmt (§ 10 Abs. 2 AGB)