

LehrHub

Technisch-Organisatorische Maßnahmen

(TOM nach Art. 32 DSGVO)

Version 1.7 — Stand August 2026

LehrHub UG (haftungsbeschränkt)

Frank Uhlenbrock — hallo@lehrhub.de

Anlage zum Auftragsverarbeitungsvertrag (Art. 28 DSGVO)

Spiegelt: AGB (Fassung 2026-06), AVV und Datenschutzerklärung (Fassung 2026-08)

Kurzcheck für Schulleitungen

Diese Schnellübersicht beantwortet die häufigsten Fragen, die Schulleitungen und Schulträger zu LehrHub stellen. Detaillierte Erläuterungen finden sich in den folgenden Kapiteln.

Wo werden die Daten gespeichert?	Produktive Schüler- und Anwendungsdaten werden in Frankfurt am Main (AWS eu-central-1, Anbieter Neon, LLC) gespeichert. Schülerfotos liegen im Vercel Blob Storage, ebenfalls in der Region Frankfurt. Lehrkraft- und Zahlungsdaten werden über europäische Dienstleister abgewickelt (Stripe Payments Europe Limited, Dublin; Sendinblue SAS, Paris).
Drittlandsbezug?	Die produktive Datenverarbeitung erfolgt innerhalb Deutschlands bzw. der Europäischen Union. Bei einzelnen Anbietern besteht ein konzernbezogener Drittlandsbezug zu den Vereinigten Staaten (Vercel Inc., Neon LLC / Databricks Inc., Stripe Inc.). Die Absicherung erfolgt über Standardvertragsklauseln nach Durchführungsbeschluss (EU) 2021/914 und über die Zertifizierung nach dem EU-US-Datenschutzrahmen (Data Privacy Framework).
Wer ist Auftragsverarbeiter?	LehrHub UG (haftungsbeschränkt) ist Auftragsverarbeiter im Sinne von Art. 28 DSGVO für die in der Anwendung verarbeiteten Schülerdaten. Verantwortlich ist die jeweilige Schule, der Schulträger oder die sonst zuständige Stelle.
Wie wird der AVV-Beitritt vollzogen?	Über das Online-Formular unter lehrhub.de/avv . Die Anmeldung kann durch die Schulleitung, den Schulträger oder eine sonst beauftragte Person erfolgen; eine Weiterleitung an die zuständige Stelle ist möglich.
Was passiert, wenn eine Lehrkraft LehrHub nutzt, bevor die Schule AVV-beigetreten ist?	Die Lehrkraft kann mit qualifizierter Bestätigung der schulischen Freigabe sofort starten. Parallel wird der AVV-Beitritt der Schule angestoßen. Nach 30 und 60 Tagen ohne Beitritt erfolgen Erinnerungen; nach 90 Tagen wird die Anlage neuer Schüler eingeschränkt — bestehende Schülerakten bleiben in vollem Umfang nutzbar.
Werden Schülerfotos öffentlich ausgeliefert?	Nein. Schülerfotos werden seit der Anpassung vom 14.05.2026 nicht mehr über öffentlich zugängliche URLs der LehrHub-Anwendung bereitgestellt, sondern ausschließlich über einen authentifizierten und nach Klassenzugehörigkeit autorisierten Abrufmechanismus.
Werden Schülerdaten an Stripe oder Brevo übermittelt?	Nein. Diese Dienstleister erhalten ausschließlich Lehrkraft-, Vertrags- oder Zahlungsdaten — keine produktiven Schülerdaten aus der Anwendung.

1. Einleitung

1.1 Zweck dieses Dokuments

Dieses Dokument beschreibt die technischen und organisatorischen Maßnahmen (TOM), die die LehrHub UG (haftungsbeschränkt) zur Erfüllung der Anforderungen aus Art. 32 DSGVO sowie aus dem Auftragsverarbeitungsvertrag (AVV) gemäß Art. 28 DSGVO trifft. Es ist als Anlage zum AVV gegenüber Schulen, Schulträgern und sonst zuständigen Stellen vorgesehen, die LehrHub als Auftragsverarbeiter mit der Verarbeitung personenbezogener Schülerdaten beauftragen.

Das Dokument spiegelt den Stand der Rechtstexte (AGB Fassung 2026-06; AVV einschließlich Anlagen und Datenschutzerklärung Fassung 2026-08) sowie die im internen Konzept Onboarding & AVV-Handling vom 14.05.2026 getroffenen Beschlüsse wider.

1.2 Verantwortliche Stelle bei LehrHub

LehrHub UG (haftungsbeschränkt), vertreten durch Geschäftsführer Frank Uhlenbrock.

Geschäftliche E-Mail: hallo@lehrhub.de.

Verantwortlich für Datenschutz: Frank Uhlenbrock (interne Wahrnehmung; ein externer Datenschutzbeauftragter ist nach § 38 BDSG derzeit nicht erforderlich).

Die Gesellschaft ist im Handelsregister des Amtsgerichts Tostedt unter HRB 212318 eingetragen.

1.3 Dual-Rolle

LehrHub nimmt im Datenschutzrecht eine doppelte Rolle ein, die für das Verständnis der einzelnen TOM-Maßnahmen wichtig ist:

- **Auftragsverarbeiter** im Sinne von Art. 28 DSGVO für alle Schülerdaten, die Lehrkräfte in die Anwendung eingeben. Verantwortlich für diese Daten ist die jeweilige Schule, der Schulträger oder die sonst zuständige Stelle.
- **Verantwortlicher** im Sinne von Art. 4 Nr. 7 DSGVO für Lehrkraft-Daten (Login, Profil, Zahlungs- und Vertragsdaten, geschäftliche Kommunikation).

1.4 Risikoeinschätzung

Vor der Festlegung der einzelnen TOM wurde eine grobe Risikoeinschätzung durchgeführt. Die wesentlichen Risikobereiche und die jeweils getroffenen Maßnahmen sind:

Vertraulichkeit der Schülerdaten	Hoch. Maßnahmen: Verschlüsselung in Transit und in Ruhe; Authentifizierung mit Verifikations-E-Mail; rollenbasierte Trennung der Daten je Lehrkraft und Klasse; Schülerfoto-Auslieferung ausschließlich über authentifizierten Proxy mit Klassenzugehörigkeits-Prüfung.
---	---

Konzernbezogener Drittlandsbezug	Mittel bis hoch. Maßnahmen: Produktive Datenverarbeitung in Frankfurt am Main bzw. innerhalb der EU; Absicherung über Standardvertragsklauseln (EU) 2021/914 und Zertifizierung nach EU-US-Datenschutzrahmen (Data Privacy Framework); transparente Auflistung der betroffenen Anbieter in Anlage 2 des AVV.
Sensible Datenkategorien	Hoch. Maßnahmen: Qualifizierte Lehrkraft-Bestätigung im Freigabeschritt mit ausdrücklichem Bezug auf besonders sensible Kategorien (Schülerfotos, Förderschwerpunkte, Inklusionsstatus); ausschließlich authentifizierter Foto-Abruf über klassenbezogene Autorisierung.
Verfügbarkeit	Mittel. Maßnahmen: Cloud-Infrastruktur mit Standard-Verfügbarkeitsmechanismen der eingesetzten Anbieter; regelmäßige Datenbank-Snapshots; getrennte Umgebungen für Entwicklung, Beta-Test und Produktion.
Integrität	Mittel. Maßnahmen: Transaktionale Datenbankoperationen; Audit-Trail bei sicherheitsrelevanten Schreibvorgängen (Freigabeschritt, AVV-Beitritt); strenge Eingabevalidierung; getrennte Audit-Felder für Lehrkraft-Eingaben und durch Schule autoritativ gesetzte Werte.

2. Maßnahmen zur Vertraulichkeit

2.1 Zugangskontrolle

Der Zugang zur LehrHub-Anwendung erfolgt ausschließlich über authentifizierte Benutzerkonten. Folgende Mechanismen sind im Einsatz:

- Anmeldung über Benutzername (E-Mail-Adresse) und individuelles Passwort gemäß NextAuth.js v5.
- Passwörter werden ausschließlich als kryptografische Hashes gespeichert (bcrypt mit angemessenem Kosten-Parameter).
- Verifikation der E-Mail-Adresse vor erster Nutzung; ohne verifizierte E-Mail-Adresse können keine sicherheitsrelevanten Aktionen wie das Anstoßen eines AVV-Beitritts ausgelöst werden.
- Session-Management mit Server-seitig validierten Tokens; automatische Sitzungsablaufzeiten.

2.2 Zugriffskontrolle

Der Zugriff auf Schülerdaten ist innerhalb der Anwendung eng begrenzt:

- Jede Lehrkraft sieht ausschließlich Schülerdaten ihrer eigenen Klassen. Eine Zuordnung zu fremden Klassen ist technisch ausgeschlossen.
- Schul-Zuordnung über eine eigenständige School-Entität; Lehrkräfte einer Schule sind über die User.schoolId an die gemeinsame Schule angebunden.
- Schülerfotos werden nicht über öffentlich zugängliche URLs der LehrHub-Anwendung bereitgestellt. Der Abruf erfolgt ausschließlich über einen authentifzierten Proxy-Endpoint, der die Klassenzugehörigkeit der anfragenden Lehrkraft serverseitig prüft. Diese Maßnahme wurde mit PR #25 (Commit f612ed1c, 14.05.2026) umgesetzt.
- Auf Datenbankebene ist der Schreib- und Lesezugriff auf das Anwendungs-Servicekonto beschränkt. Administrative Datenbankzugriffe erfolgen über separate, individuell authentifizierte Neon-Konten.

2.3 Trennungskontrolle

- Logische Trennung der Daten je Mandant (Schule) über die Schul-Entität und die zugehörigen Fremdschlüsselbeziehungen.
- Trennung der Verarbeitungszwecke: Schülerdaten ausschließlich in der Hauptanwendung; Zahlungsdaten getrennt bei Stripe Payments Europe; E-Mail-Kommunikation getrennt bei Sendinblue SAS (Brevo).

- Trennung der Umgebungen Entwicklung, Beta-Test und Produktion; produktive Daten sind von Test-Daten separiert.

2.4 Verschlüsselung

- Verschlüsselung in Transit: Alle Verbindungen zur LehrHub-Anwendung erfolgen ausschließlich über HTTPS (TLS 1.2 oder höher). HTTP-Aufrufe werden serverseitig auf HTTPS umgeleitet.
- Verschlüsselung in Ruhe: Die Produktiv-Datenbank bei Neon, LLC wird verschlüsselt gespeichert (AWS-eu-central-1-Standard, AES-256). Der Vercel Blob Storage verschlüsselt Inhalte ebenfalls verschlüsselt im Ruhezustand.
- E-Mail-Versand erfolgt verschlüsselt (TLS) über den Dienstleister Sendinblue SAS.

2.5 Mitarbeiter- und Vertraulichkeitsverpflichtung

LehrHub wird im Berichtszeitraum von Frank Uhlenbrock allein betrieben. Eine schriftliche Verpflichtung auf das Datengeheimnis nach § 53 BDSG ist für den Geschäftsführer in dessen Eigenschaft als gesetzlicher Vertreter und Verantwortlicher gegenstandslos; sie wird sofort eingeführt, sobald weitere Mitarbeiter (auch Werkstudierende oder freie Mitarbeiter) Tätigkeiten aufnehmen, bei denen sie Zugang zu personenbezogenen Daten erhalten könnten.

3. Maßnahmen zur Integrität

3.1 Eingabekontrolle

Lehrkräfte tragen Schülerdaten ausschließlich über die Anwendungsoberfläche der LehrHub-Anwendung ein. Folgende Mechanismen unterstützen die Eingabekontrolle:

- Strenge serverseitige Validierung aller Eingaben (Längenprüfung, Typprüfung, Wertebereichsprüfung).
- Transaktionale Datenbankoperationen auf Basis von Prisma ORM. Schreibvorgänge auf zusammenhängende Datensätze (z. B. Schüler plus Noten) werden in Transaktionen gekapselt.
- Audit-Trail bei sicherheitsrelevanten Schreibvorgängen: Bei jedem Freigabeschritt (TeacherClearance) und bei jedem AVV-Beitritt (SchoolAvvAcceptance) werden Zeitstempel, IP-Hash, User-Agent und Versions-Kennzeichnung der akzeptierten Rechtstexte gespeichert.

3.2 Trennung von Eingabe-Audit und autoritativen Daten

Eine wichtige Detailmaßnahme aus dem Konzept Onboarding & AVV-Handling: Im TeacherClearance werden die Eingabewerte der Lehrkraft (schoolNameInput, schoolCityInput etc.) getrennt vom autoritativen School-Datensatz gespeichert. Eine spätere Korrektur des Schulnamens durch die Schulleitung im AVV-Beitritts-Formular ändert nur den School-Datensatz; die Eingabe-Audit-Felder bleiben unverändert. So bleibt im Streitfall nachvollziehbar, was die Lehrkraft im Freigabeschritt tatsächlich getippt hat.

3.3 Übertragungs- und Speicherintegrität

- Sämtliche Datenübertragungen zwischen Browser und Server erfolgen verschlüsselt (TLS); die Integrität der Übertragung wird durch TLS-Protokoll-Mechanismen sichergestellt.
- Die Produktiv-Datenbank (Neon, LLC, Frankfurt) führt automatisch Schreibprotokolle (Write-Ahead Logs); konsistente Snapshots werden vor schemarelevanten Änderungen erstellt.
- Vor Datenbank-Migrationen wird ein Neon-Snapshot mit konsistenter Naming-Konvention erstellt (pre_<feature>_<DATUM>). Beim Free-Plan ist nur ein Snapshot gleichzeitig zulässig; ältere Snapshots werden vor neuen gelöscht.

3.4 Schutz vor unautorisierten Schreibvorgängen

- API-Endpoints prüfen serverseitig die Identität und Autorisierung des aufrufenden Users gegen die jeweilige Ressource (z. B. nur eigene Klassen schreibbar).
- Cross-Site Request Forgery (CSRF) wird durch NextAuth.js v5 sowie durch SameSite-Cookies und CSRF-Tokens auf zustandsverändernden Endpoints abgewehrt.

- Im Mai 2026 wurde der Konfigurations-Parameter `allowDangerousEmailAccountLinking` aus NextAuth.js v5 entfernt (PR [security/remove-dangerous-email-linking](#), Commit [f47ae167](#)). Dadurch kann ein Account nicht mehr unbeabsichtigt mit einer fremden E-Mail-Identität verknüpft werden.

4. Maßnahmen zur Verfügbarkeit und Belastbarkeit

4.1 Eingesetzte technische Dienstleister und Verarbeitungsorte

Die folgenden technischen Dienstleister werden von LehrHub für den produktiven Betrieb der Anwendung eingesetzt. Eine vollständige Auflistung mit datenschutzrechtlicher Einordnung findet sich in Anlage 2 des AVV; die hier dargestellte Übersicht ist auf die TOM-relevanten Aspekte fokussiert.

Anwendungs-Hosting	Vercel Inc., San Francisco, USA. Produktive Auslieferung der Anwendung über die Region Frankfurt am Main. Standard-Verfügbarkeitsmechanismen des Anbieters (Multi-Region-Failover, automatische Skalierung).
Datenbank	Neon, LLC (Konzerngesellschaft der Databricks, Inc.), San Francisco, USA. Verarbeitung produktiver Anwendungsdaten in der Region Frankfurt am Main (AWS eu-central-1). Anbieter-Verfügbarkeitszusagen, regelmäßige automatische Snapshots.
Objektspeicher (Schülerfotos)	Vercel Blob Storage, Region Frankfurt am Main. Speicherung optional hochgeladener Schülerfotos. Auslieferung ausschließlich über authentifizierten Proxy mit Klassen-Berechtigungsprüfung.
E-Mail-Versand	Sendinblue SAS (Marke Brevo), Paris, Frankreich. Versand transaktionaler E-Mails (Verifikation, AVV-Anstoß, Eskalationen, Bestätigungen) sowie Verwaltung der Warteliste.
Zahlungsabwicklung	Stripe Payments Europe, Limited, Dublin, Irland. Abwicklung kostenpflichtiger Nutzungen (LehrHub Pro, geplante Schul-Lizenzen).
Domain und Geschäfts-E-Mail	IONOS SE, Montabaur, Deutschland. Registrierung und Verwaltung der Domain lehrhub.de und der geschäftlichen E-Mail-Adresse hallo@lehrhub.de. Verarbeitung in Deutschland; keine Schülerdaten aus der Anwendung.

4.2 Sicherungskonzept

- Neon bietet automatische Point-in-Time-Recovery innerhalb der Aufbewahrungsfrist des gewählten Tarifs. Beim Free-Plan beträgt diese 7 Tage; sobald der produktive Tarif (Neon Pro) aktiviert ist, verlängert sich der Wiederherstellungs-Zeitraum entsprechend.
- Vor jedem geplanten Schema-Update wird zusätzlich ein expliziter Snapshot mit Naming-Konvention pre_<feature>_<DATUM> erstellt.
- Schülerfotos im Vercel Blob Storage werden durch die Verfügbarkeitsmechanismen des Anbieters geschützt.

4.3 Wiederherstellung

Bei Datenverlust oder Korruption der Produktiv-Datenbank wird die Wiederherstellung über die Neon-Point-in-Time-Recovery oder durch Einspielen eines aktuellen Snapshots vorgenommen. Die Wiederherstellungs-Schritte sind:

1. Identifikation des Wiederherstellungs-Zeitpunkts (Zeitstempel vor dem Ereignis).
2. Erstellung einer Recovery-Datenbank-Branch in Neon.
3. Verifikation der Datenkonsistenz und der Datenstände kritischer Tabellen (TeacherClearance, SchoolAvvAcceptance, Klassen- und Schülerdaten).
4. Umschaltung der Anwendungs-Connection-String auf die wiederhergestellte Datenbank.
5. Nachträgliche Information betroffener Schulen und Lehrkräfte über das Ereignis und etwaige Datenstands-Lücken.

4.4 Schutz vor Schadprogrammen

- Eingehende Dateien werden ausschließlich als Bilder im Vercel Blob Storage abgelegt; die Anwendung verarbeitet Bilder nicht als ausführbaren Code. Eingaben werden im Hinblick auf MIME-Typ und Größe geprüft.
- Abhängigkeiten werden über die Standard-Mechanismen npm und Vercel-Build-Pipelines auf bekannte Sicherheitslücken hin überwacht; Updates erfolgen zeitnah.

5. Auftragsverarbeitung und Subunternehmer

5.1 Auftragsverarbeitungsvertrag

Der Auftragsverarbeitungsvertrag zwischen LehrHub und der jeweiligen Schule oder zuständigen Stelle wird online über lehrhub.de/avv abgeschlossen. Die Vertragsdokumente (AGB, AVV einschließlich Anlagen, Datenschutzerklärung) sind unter lehrhub.de/recht einsehbar und werden im Beitrittsprozess als PDF angeboten und nach Beitritt als E-Mail-Anhang an die akzeptierende Person übermittelt.

Der Beitrittsprozess folgt dem im Konzept Onboarding & AVV-Handling (Kapitel 5) beschriebenen Ablauf: Zugang über tokenbasiert Link, Direktklick aus der Anwendung oder manuellen Aufruf; Klärungsschritt zur Beitrittsberechtigung; Beitrittsformular mit den nach AVV §3 erforderlichen Feldern; Vorschau und rechtsverbindlicher Abschluss durch drei separate Checkboxen für AGB, AVV und Datenschutzerklärung. Nach Abschluss wird der Status der Schule auf ACCEPTED gesetzt; der bisherige Eskalations-Cronjob wird gestoppt.

5.2 Übergangslösung vor institutionellem AVV-Beitritt

Bis zum Vollzug des institutionellen AVV-Beitritts dürfen Lehrkräfte LehrHub auf Grundlage einer qualifizierten Bestätigung nutzen (Übergangslösung gemäß AVV §3 Abs. 5 in Verbindung mit AGB §4). Die Bestätigung umfasst vier Aussagen, die in einer einzigen Bestätigungs-Checkbox zusammengefasst sind: dienstliche Nutzung und Berechtigung zur Verarbeitung; Vorliegen der schulischen Freigabe einschließlich der Nutzung externer technischer Dienstleister; Kenntnis der Sperre ohne Freigabe; Vorliegen qualifizierter Freigabe und Eltern-Einwilligungen für besonders sensible Datenkategorien (Schülerfotos, Förderschwerpunkte und Inklusionsstatus, die Rückschlüsse auf Gesundheitsdaten zulassen können).

Der Wortlaut der Bestätigung ist im Konzept Onboarding & AVV-Handling (Kapitel 8.1) dokumentiert.

5.3 Eskalation

Ohne institutionellen AVV-Beitritt erfolgt nach DSE §4 Abs. 4 eine zeitlich gestaffelte Eskalation. Die operative Umsetzung ist im Konzept Onboarding & AVV-Handling (Kapitel 6) beschrieben:

- Nach 30 Tagen: Erinnerungs-Mail an Schulleitung und Lehrkraft.
- Nach 60 Tagen: erneute Erinnerung mit eindringlicherem Wortlaut und Hinweis auf bevorstehende Einschränkung.
- Nach 90 Tagen: weiche Sperre — die Anlage neuer Schüler und der Import neuer Schülerlisten werden blockiert. Notenerfassung, Foto-Upload und Förderschwerpunkts-Zuweisung für bereits angelegte Schüler sowie Export, Lesen und Löschen bleiben unverändert möglich.

5.4 Subunternehmer

LehrHub setzt für den technischen Betrieb der Anwendung sowie für den geschäftlichen E-Mail-Verkehr Unterauftragsverarbeiter und sonstige technische Dienstleister ein. Die vollständige Liste mit datenschutzrechtlicher Einordnung, Sitz, verarbeiteten Datenkategorien und Schutzmechanismen findet sich in Anlage 2 des AVV in der Fassung vom 14.05.2026. Stand der Aufzählung:

1. IONOS SE	Montabaur, Deutschland. Domain-Registrierung und geschäftliche E-Mail-Adresse (hallo@lehrhub.de). Sonstiger technischer Dienstleister; keine produktiven Schülerdaten.
2. Neon, LLC	San Francisco, USA (Konzerngesellschaft der Databricks, Inc.). Verarbeitung produktiver Anwendungsdaten in der Region Frankfurt am Main (AWS eu-central-1).
3. Vercel Inc.	San Francisco, USA. Anwendungs-Hosting und Vercel Blob Storage (Schülerfotos). Verarbeitung nach derzeitiger Konfiguration in der Region Frankfurt am Main.
4. Stripe Payments Europe, Limited	Dublin, Irland (Konzerngesellschaft der Stripe, Inc., USA). Zahlungsabwicklung; keine Schülerdaten.
5. Sendinblue SAS (Marke Brevo)	Paris, Frankreich. Transaktionaler E-Mail-Versand; keine Schülerdaten.

Die Absicherung erfolgt jeweils über die mit dem Anbieter bestehende Datenverarbeitungsvereinbarung (Bestandteil der jeweiligen Allgemeinen Geschäftsbedingungen, Nutzungsbedingungen oder gesondert zugänglichen Vertragsdokumente) sowie über Standardvertragsklauseln nach Durchführungsbeschluss (EU) 2021/914 und die Zertifizierung nach dem EU-US-Datenschutzrahmen (Data Privacy Framework), soweit ein Drittlandsbezug besteht und einschlägig.

6. Betroffenenrechte

LehrHub unterstützt die Schule als Verantwortliche im Sinne von Art. 28 Abs. 3 lit. e DSGVO bei der Wahrnehmung der Betroffenenrechte. Die im Folgenden beschriebenen Prozesse decken die zentralen Rechte ab.

6.1 Auskunftsrecht (Art. 15 DSGVO)

- Lehrkräfte können jederzeit alle Schülerdaten ihrer eigenen Klassen einsehen und exportieren (Notenexport, Klassenexport).
- Bei Anfragen Betroffener (Schüler/innen oder Erziehungsberechtigte) an die Schule kann die Schule sich an LehrHub wenden; die Identifikation des betroffenen Schülers erfolgt über die zuständige Lehrkraft oder Schulleitung. Eine technische Suche im Datenbestand ist innerhalb der gesetzlichen Frist möglich.
- Förderschwerpunkts-Zuordnungen sind beim Schüler-Export technisch ein eigenes Datenfeld.

6.2 Berichtigungsrecht (Art. 16 DSGVO)

- Lehrkräfte können Schülerdaten direkt in der Anwendung berichtigen.
- Bei Anfragen Betroffener leitet die Schule die Berichtigung über die zuständige Lehrkraft ein.

6.3 Löschungsrecht (Art. 17 DSGVO)

- Lehrkräfte können einzelne Schüler löschen; dabei werden die zugehörigen Daten einschließlich Noten und Förderschwerpunkts-Zuordnungen entfernt.
- Bei der Löschung eines Schülers werden auch im Vercel Blob Storage abgelegte Schülerfotos entfernt.
- Bei Anfragen Betroffener auf vollständige Löschung erfolgt die Bearbeitung über die Schule. Audit-Trail-Datensätze (TeacherClearance, SchoolAvvAcceptance) werden bei User-Löschung pseudonymisiert; die Bezugfelder zur User-Identität werden anonymisiert, die Bestätigungs-Metadaten bleiben für die Nachweis-Pflichten erhalten.

6.4 Einschränkung der Verarbeitung (Art. 18 DSGVO)

Eine technische Einschränkung der Verarbeitung einzelner Schülerdatensätze erfolgt über die Markierung als gesperrt im Schüler-Datensatz.

6.5 Datenübertragbarkeit (Art. 20 DSGVO)

Lehrkräfte können Klassen- und Schülerdaten im strukturierten Format (CSV) exportieren. Damit ist die Datenübertragbarkeit grundsätzlich gewährleistet.

6.6 Widerspruchsrecht (Art. 21 DSGVO)

Anfragen Betroffener werden über die Schule abgewickelt. LehrHub setzt die Entscheidungen der Schule technisch um.

7. Meldung von Datenschutzvorfällen

Im Falle einer Verletzung des Schutzes personenbezogener Schülerdaten (Datenschutzvorfall) handelt LehrHub im Sinne von Art. 33 DSGVO unverzüglich und unterstützt die Schule als Verantwortliche bei deren Meldepflichten.

7.1 Meldekette

6. Erkennung des Vorfalls (durch Monitoring, durch Hinweis von Nutzer/innen oder durch externe Meldung).
7. Sofortige Bewertung von Art, Umfang und Risiko (innerhalb von 24 Stunden).
8. Eindämmung des Vorfalls; bei Bedarf Sperrung betroffener Konten oder Funktionen.
9. Information der betroffenen Schule(n) als Verantwortliche unverzüglich nach Bewertung, spätestens innerhalb von 72 Stunden nach Erkenntnis (Art. 33 Abs. 1 DSGVO).
10. Unterstützung der Schule bei einer etwaigen Meldung an die zuständige Aufsichtsbehörde.
11. Information der von einem hohen Risiko betroffenen Personen, soweit nach Art. 34 DSGVO erforderlich.

7.2 Aufsichtsbehörde

Die zuständige Aufsichtsbehörde für LehrHub als in Niedersachsen ansässige Stelle ist der Landesbeauftragte für den Datenschutz Niedersachsen, Prinzenstraße 5, 30159 Hannover.

Für Schulen ist die Aufsichtsbehörde des jeweiligen Bundeslandes zuständig.

7.3 Dokumentationspflicht

Jeder Datenschutzvorfall — auch ein nicht meldepflichtiger — wird intern dokumentiert mit Datum, Beschreibung, Auswirkungen, ergriffenen Maßnahmen und betroffenen Schulen.

8. Organisatorische Maßnahmen

8.1 Datenschutz-Beauftragter

Ein externer Datenschutzbeauftragter ist für die LehrHub UG (haftungsbeschränkt) nach § 38 BDSG derzeit nicht erforderlich, weil die Schwellenwerte (in der Regel: 20 Personen, die ständig mit personenbezogener Datenverarbeitung beschäftigt sind) nicht erreicht werden. Bei Erreichen der Schwelle wird unverzüglich ein DSB benannt und der Aufsichtsbehörde gemeldet.

8.2 Vertragsdokumente und Versionspflege

- Die zentralen Rechtsdokumente (AGB, AVV einschließlich Anlagen, Datenschutzerklärung) werden mit Versions-Kennzeichnung gepflegt.
- Bei wesentlichen Änderungen werden Lehrkräfte und beigetretene Schulen rechtzeitig informiert; gegebenenfalls erfolgt eine erneute Bestätigung der relevanten Texte (Re-Confirmation beim nächsten Login).
- Die Pflege der Rechtsdokumente erfolgt seit dem 14.05.2026 intern; eine erneute anwaltliche Iteration ist für ordentliche Aktualisierungen nicht vorgesehen.

8.3 Schulungspflicht

Im Berichtszeitraum ist nur der Inhaber operativ tätig. Schulungs- und Sensibilisierungsmaßnahmen werden eingeführt, sobald weitere Personen Tätigkeiten mit Datenzugang aufnehmen — vor erstem Datenzugang.

8.4 Auskunfts- und Kontaktstellen

Anfragen werden über die geschäftliche E-Mail-Adresse hallo@lehrhub.de bearbeitet. Die Reaktionszeit für datenschutzrelevante Anfragen liegt regulär innerhalb von zwei Werktagen, bei dringlichen Vorfällen innerhalb von 24 Stunden.

8.5 Trennung Geschäfts- und Anwendungs-Mail

Die geschäftliche E-Mail-Adresse hallo@lehrhub.de (gehostet bei IONOS SE in Montabaur) wird ausschließlich für externe Kommunikation eingesetzt. Sie ist von der innerhalb der Anwendung versendeten transaktionalen Kommunikation (über Sendinblue SAS / Brevo) technisch und vertraglich getrennt. Lehrkräfte und Eltern werden gebeten, schülerbezogene Daten ausschließlich innerhalb der Anwendung zu verarbeiten und nicht per E-Mail an die geschäftliche Adresse zu schicken.

9. Besonderheiten Inklusion und sensible Datenkategorien

LehrHub positioniert sich als Verwaltungslösung für inklusiv arbeitende Schulen. Förderschwerpunkte und Inklusionsstatus sind daher Kernfunktionalitäten der Anwendung. Diese Datenkategorien können nach Art. 9 DSGVO als besondere Kategorien personenbezogener Daten einzuordnen sein, weil aus ihnen Rückschlüsse auf Gesundheitsdaten oder eine Behinderung möglich sind.

9.1 Liste der Förderschwerpunkts-Kategorien

Die Anwendung stellt eine Liste von Standard-Förderschwerpunkten bereit; Lehrkräfte und Schulen können eigene Schwerpunkte ergänzen oder Standard-Einträge für die eigene Schule deaktivieren. Standard-Kategorien (Auswahl):

- Lernen, Geistige Entwicklung, Emotional/Sozial, Körperliche/motorische Entwicklung, Hören und Kommunikation, Sehen, Autismus-Spektrum, Deutsch als Zweitsprache.

Die ersten sieben dieser Kategorien sind nach datenschutzrechtlicher Einordnung Art. 9-relevant. Deutsch als Zweitsprache ist als sprachliche Förderkategorie nicht Art. 9-relevant.

9.2 Qualifizierte Bestätigung

Die Lehrkraft bestätigt im Freigabeschritt im Rahmen der Hauptbestätigung ausdrücklich, dass für die Verarbeitung dieser besonders sensiblen Datenkategorien sowohl eine qualifizierte Freigabe der Schule als auch die Einwilligungen der Erziehungsberechtigten bzw. der volljährigen Schülerinnen und Schüler vorliegen. Der entsprechende Bestätigungs-Wortlaut ist Teil der einen Hauptbestätigungs-Checkbox (Design X gemäß Konzept Onboarding & AVV-Handling, Kapitel 8.4).

Ein zusätzliches Just-in-time-Modal vor erstem Foto-Upload oder erster Förderschwerpunkts-Zuweisung wird nicht eingesetzt. Begründung: Die Aussagen gehören aus Lehrkraft-Sicht zu einem zusammenhängenden Compliance-Moment beim Onboarding; eine Aufspaltung in mehrere zeitlich versetzte Modals würde die UX zerstückeln, ohne datenschutzrechtlich einen Mehrwert zu bieten.

9.3 Auslieferung der Schülerfotos

Wie in Kapitel 2.2 dargestellt: Schülerfotos werden seit 14.05.2026 nicht mehr über öffentlich zugängliche URLs der LehrHub-Anwendung bereitgestellt. Der Abruf erfolgt ausschließlich über einen authentifizierten Proxy-Endpoint, der die Klassenzugehörigkeit der anfragenden Lehrkraft serverseitig prüft.

Versionshinweise

Version 1.7 (August 2026)	Entfernung aller Google-Nennungen nach Abschaltung der Anmeldung über ein Google-Konto zum 30.05.2026 (Kurzcheck, Drittlands-Übersicht, Zugangskontrolle, Trennungsgebot, Dienstleister-Übersicht, Unterauftragsverarbeiter-Liste); Spiegelungs-Verweise auf AVV und Datenschutzerklärung Fassung 2026-08 aktualisiert.
Version 1.6 (Juni 2026)	Spiegelung der finalen Rechtstexte vom 12.05.2026 (AGB, AVV, DSE) und Übernahme der Beschlüsse aus dem internen Konzept Onboarding & AVV-Handling vom 14.05.2026. Korrektur der Anbieter-Bezeichnungen (Neon, LLC als Konzerngesellschaft der Databricks, Inc.; Sendinblue SAS als Marke Brevo; Stripe Payments Europe, Limited; Aufnahme der IONOS SE). Präzisierung des Drittlandsbezugs (produktive Verarbeitung in der EU, konzernbezogene Drittlandsbezüge bei einzelnen Anbietern, abgesichert über SCCs und EU-US-Datenschutzrahmen). Aufnahme der Schülerfoto-Auslieferung über authentifizierten Proxy. Aufnahme der Übergangslösung mit qualifizierter Lehrkraft-Bestätigung und 30/60/90-Eskalation einschließlich weicher Sperre. Aufnahme der Förderschwerpunkts-Sensibilität (Art. 9-Einordnung).
Version 1.4 (April 2026)	Vorgängerstand; siehe interne Dokumentenhistorie.

— Ende des Dokuments —