

Vertrag zur Auftragsverarbeitung

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

Auftragsverarbeiter	Nils Rabe, handelnd unter „Schulbuchhelden“ Bromersfeld 19, 45472 Mülheim an der Ruhr
Verantwortlicher	Die im Schulkonto bezeichnete Schule
Vertragsschluss	Elektronisch im Onboarding der Schulbuchhelden-Plattform
Version / Stand	Version 1.0 02.10.2026

Vertragsparteien und Geltungsbereich

Dieser Vertrag zur Auftragsverarbeitung („AVV“) wird geschlossen zwischen der im jeweiligen Schulkonto bezeichneten Schule als datenschutzrechtlich Verantwortlichem („Verantwortlicher“) und

Nils Rabe, handelnd unter „Schulbuchhelden“, Bromersfeld 19, 45472 Mülheim an der Ruhr („Auftragsverarbeiter“).

Soweit nach dem für die Schule geltenden Recht ausnahmsweise ein anderer Rechtsträger datenschutzrechtlich Verantwortlicher ist und dieser das Schulkonto in eigenem Namen einrichtet, tritt dieser an die Stelle der Schule als Verantwortlicher.

Der AVV gilt für alle personenbezogenen Daten, die der Auftragsverarbeiter bei der Bereitstellung und Nutzung der Schulbuchhelden-Plattform im Auftrag des Verantwortlichen verarbeitet. Er gilt nicht für Verarbeitungsvorgänge, bei denen Schulbuchhelden selbst über Zwecke und Mittel der Verarbeitung entscheidet, insbesondere für eigene Vertrags-, Abrechnungs- oder Förderauszahlungsprozesse.

§ 1 Gegenstand und Dauer der Verarbeitung

Gegenstand der Auftragsverarbeitung ist die technische Bereitstellung der webbasierten Plattform Schulbuchhelden einschließlich Benutzerverwaltung, Authentifizierung, SSO-Anbindung, Systemkommunikation, Speicherung und Verwaltung der für die Plattformnutzung erforderlichen Daten sowie Support, Wartung und Fehlerbehebung.

Art, Zweck und Umfang der Verarbeitung sowie die Kategorien personenbezogener Daten und betroffener Personen ergeben sich ergänzend aus Anhang 1.

Die Verarbeitung beginnt mit dem Abschluss dieses AVV und dauert für die Dauer der Nutzung der Schulbuchhelden-Plattform durch den Verantwortlichen. Verpflichtungen, die ihrer Natur nach über die Vertragsbeendigung hinaus gelten, bleiben unberührt.

Dieser Vertrag gilt ausschließlich für Verarbeitungen personenbezogener Daten, die Schulbuchhelden im Auftrag der Schule durchführt. Verarbeitungen, bei denen Schulbuchhelden selbst Verantwortlicher im Sinne der DSGVO ist, sind nicht Gegenstand dieses Vertrags.

§ 2 Weisungsgebundene Verarbeitung

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen und nur soweit dies zur Erbringung der vereinbarten Leistungen erforderlich ist. Die Nutzung der Plattform und die in diesem AVV beschriebenen Verarbeitungsvorgänge gelten als dokumentierte Weisung.

Eine Verarbeitung für eigene Zwecke ist im Rahmen dieses AVV ausgeschlossen. Hiervon unberührt bleiben Verarbeitungsvorgänge, für die Schulbuchhelden selbst Verantwortlicher ist.

Hält der Auftragsverarbeiter eine Weisung für datenschutzrechtlich unzulässig, weist er den Verantwortlichen hierauf unverzüglich hin. Die Ausführung kann bis zur Bestätigung oder Änderung der Weisung ausgesetzt werden.

Ist der Auftragsverarbeiter unions- oder mitgliedstaatlich gesetzlich zu einer Verarbeitung verpflichtet, informiert er den Verantwortlichen vorab, soweit eine solche Information rechtlich zulässig ist.

§ 3 Vertraulichkeit und Zugriffsberechtigung

Der Auftragsverarbeiter stellt sicher, dass personenbezogene Daten nur solchen Personen zugänglich sind, die den Zugriff zur Bereitstellung, Entwicklung, Wartung, Administration oder Unterstützung der Plattform benötigen.

Zugriffsberechtigte Personen sind zur Vertraulichkeit verpflichtet oder unterliegen einer entsprechenden gesetzlichen Verschwiegenheitspflicht. Die Berechtigungen werden auf das erforderliche Maß beschränkt.

Schulbuchhelden besitzt technisch die Möglichkeit, auf Schulkonten und deren Inhalte zuzugreifen. Tatsächliche Zugriffe erfolgen jedoch nur, soweit dies für Betrieb, Support, Wartung, Fehleranalyse, Sicherheit oder auf Weisung der Schule erforderlich ist.

§ 4 Technische und organisatorische Maßnahmen

Der Auftragsverarbeiter trifft angemessene technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO. Die aktuell eingesetzten Maßnahmen sind in Anhang 3 beschrieben.

Die Maßnahmen dürfen im Rahmen des technischen Fortschritts weiterentwickelt und angepasst werden, sofern das vereinbarte Schutzniveau dadurch nicht unterschritten wird.

Die Plattform verarbeitet planmäßig keine besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO und keine personenbezogenen Schüler- oder Elterndaten. Der Verantwortliche stellt sicher, dass solche Daten nicht ohne vorherige Abstimmung in dafür nicht vorgesehenen Feldern verarbeitet werden.

§ 5 Unterstützung des Verantwortlichen

Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der verfügbaren Informationen in angemessenem Umfang bei der Erfüllung seiner datenschutzrechtlichen Pflichten.

Dies umfasst insbesondere die Unterstützung bei Betroffenenrechten, der Sicherheit der Verarbeitung, der Bewertung und Meldung von Datenschutzverletzungen sowie - soweit erforderlich - bei Datenschutz-Folgenabschätzungen und Konsultationen von Aufsichtsbehörden.

Gehen beim Auftragsverarbeiter Anfragen betroffener Personen ein, die Verarbeitungen im Auftrag des Verantwortlichen betreffen, leitet er diese ohne unangemessene Verzögerung an den Verantwortlichen weiter, sofern er nicht selbst zur Beantwortung berechtigt oder verpflichtet ist.

§ 6 Unterauftragsverarbeiter

Der Verantwortliche erteilt dem Auftragsverarbeiter eine allgemeine Genehmigung zum Einsatz weiterer Auftragsverarbeiter. Die bei Vertragsschluss eingesetzten Unterauftragsverarbeiter sind in Anhang 2 aufgeführt.

Der Auftragsverarbeiter stellt sicher, dass mit Unterauftragsverarbeitern vertragliche Datenschutzpflichten vereinbart werden, die ein angemessenes und mit diesem AVV vergleichbares Schutzniveau gewährleisten.

Beabsichtigt der Auftragsverarbeiter, einen neuen Unterauftragsverarbeiter einzusetzen oder einen bestehenden zu ersetzen, informiert er den Verantwortlichen vor dessen Einbindung in geeigneter Weise. Der Verantwortliche kann aus nachvollziehbaren datenschutzrechtlichen Gründen widersprechen. Können die Parteien keine zumutbare Lösung finden, kann der Verantwortliche die betroffene Leistung beenden.

Soweit Unterauftragsverarbeiter oder deren weitere Dienstleister personenbezogene Daten in Drittländern verarbeiten, stellt der Auftragsverarbeiter sicher, dass die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, insbesondere durch einen Angemessenheitsbeschluss oder geeignete Garantien wie die Standardvertragsklauseln der Europäischen Kommission.

§ 7 Datenschutzverletzungen und Sicherheitsvorfälle

Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, nachdem ihm eine Verletzung des Schutzes personenbezogener Daten bekannt geworden ist, soweit Daten betroffen sind, die im Auftrag des Verantwortlichen verarbeitet werden.

Die Mitteilung enthält, soweit zu diesem Zeitpunkt verfügbar, eine Beschreibung der Art des Vorfalls, betroffene Datenkategorien und Personengruppen, mögliche Folgen, bereits ergriffene oder vorgeschlagene Abhilfemaßnahmen sowie eine Kontaktmöglichkeit für Rückfragen.

Fehlende Informationen werden ohne unangemessene Verzögerung nachgereicht. Der Auftragsverarbeiter dokumentiert den Vorfall und unterstützt den Verantwortlichen bei der Erfüllung etwaiger Melde- und Benachrichtigungspflichten.

§ 8 Nachweise und Kontrollrechte

Der Auftragsverarbeiter stellt dem Verantwortlichen auf angemessene Anfrage die Informationen zur Verfügung, die zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO erforderlich sind.

Der Verantwortliche kann nach angemessener Vorankündigung und unter Wahrung von Betriebs- und Geschäftsgeheimnissen Prüfungen durchführen oder durch einen zur Vertraulichkeit verpflichteten Prüfer durchführen lassen. Soweit aussagekräftige Zertifizierungen, Prüfberichte oder Dokumentationen vorliegen, können diese vorrangig als Nachweis herangezogen werden.

Prüfungen sind so zu gestalten, dass der laufende Betrieb möglichst nicht beeinträchtigt wird. Bei konkreten Anhaltspunkten für einen Datenschutzverstoß bleibt eine weitergehende Prüfung unberührt.

§ 9 Löschung und Rückgabe von Daten

Auf Verlangen des Verantwortlichen oder bei Beendigung der Auftragsverarbeitung löscht der Auftragsverarbeiter die dem Schulkonto zugeordneten personenbezogenen Daten aus dem Produktivsystem unverzüglich, soweit keine gesetzliche Aufbewahrungspflicht entgegensteht.

Die Löschung umfasst insbesondere Nutzerkonten, Zuordnungen, gespeicherte Bücherlisten und sonstige dem Schulkonto zugeordnete Inhalte, soweit diese personenbezogene Daten enthalten.

In technisch erforderlichen Sicherungskopien können Daten bis zum turnusmäßigen Überschreiben oder Löschen des jeweiligen Backups vorübergehend fortbestehen. Eine gesonderte Langzeitarchivierung dieser Auftragsdaten erfolgt nicht. Während der Backup-Aufbewahrungszeit werden die Daten nicht für andere Zwecke verwendet.

§ 10 Verarbeitung innerhalb EU/EWR und Drittlandtransfers

Die primären Anwendungs- und Datenbankressourcen werden in europäischen Regionen betrieben. Die Datenbank und Backups werden bei Supabase in der Projektregion Dublin, Irland, betrieben. Die Anwendung wird über Vercel mit europäischer Primärregion bereitgestellt.

Einige eingesetzte Dienstleister sind Unternehmen mit Sitz außerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums oder nutzen ihrerseits internationale Unterauftragsverarbeiter. Soweit dadurch eine Drittlandübermittlung stattfindet, erfolgt diese nur unter Beachtung der Art. 44 ff. DSGVO und der einschlägigen vertraglichen Garantien der jeweiligen Dienstleister.

§ 11 Datenschutzbeauftragter und Kontakt

Der Auftragsverarbeiter hat derzeit keinen Datenschutzbeauftragten bestellt. Ansprechpartner für Datenschutzfragen ist Nils Rabe.

Kontakt: info@schulbuchhelden.de | Anschrift: Bromersfeld 19, 45472 Mülheim an der Ruhr.

Der Verantwortliche teilt dem Auftragsverarbeiter auf Anfrage die Kontaktdaten seines Datenschutzbeauftragten oder sonstigen Datenschutzansprechpartners mit.

§ 12 Vertragsschluss, Änderungen und Schlussbestimmungen

Dieser AVV wird elektronisch im Rahmen des Onboardings der Schulbuchhelden-Plattform geschlossen. Der Verantwortliche bestätigt dabei, dass die handelnde Person zur Einrichtung des Schulkontos und zum Abschluss der hierfür erforderlichen Vereinbarungen berechtigt ist.

Schulbuchhelden protokolliert den Zeitpunkt der Annahme, das zugehörige Schulkonto und die jeweils akzeptierte Vertragsversion.

Änderungen dieses AVV können in Textform, einschließlich elektronischer Form, vereinbart werden. Bei Änderungen, die die Rechte oder Pflichten des Verantwortlichen wesentlich berühren, wird der Verantwortliche in geeigneter Weise informiert.

Bei Widersprüchen zwischen diesem AVV und sonstigen Vereinbarungen der Parteien gehen die Regelungen dieses AVV hinsichtlich der Verarbeitung personenbezogener Daten im Auftrag vor.

Sollten einzelne Bestimmungen dieses AVV unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Elektronischer Abschluss

Der Vertrag gilt mit der elektronischen Annahme im Registrierungs-/Onboardingprozess als geschlossen. Eine zusätzliche handschriftliche Unterschrift ist für den vorgesehenen elektronischen Abschluss nicht erforderlich.

Anhang 1 – Beschreibung der Auftragsverarbeitung

Dieser Anhang konkretisiert Gegenstand, Art und Zweck der Verarbeitung sowie die betroffenen Daten und Personen.

Gegenstand	Bereitstellung und Nutzung der webbasierten Plattform Schulbuchhelden einschließlich Schulkonto, Nutzerverwaltung, Authentifizierung, eduplaces-SSO, System-E-Mails, Listenverwaltung, Support, Wartung und Fehlerbehebung.
Art und Zweck	Erhebung, Speicherung, Organisation, Abruf, Übermittlung und Löschung der für die Nutzung notwendigen personenbezogenen Daten; Authentifizierung der Nutzer; Zuordnung zu Schule und Berechtigungen; Bereitstellung der SaaS-Funktionen; Versand transaktionaler System-E-Mails; Gewährleistung von Betrieb, Sicherheit und Support.
Betroffene Personen	Hauptnutzer und weitere berechnigte Nutzer der jeweiligen Schule, insbesondere Schulleitung, Lehrkräfte, Verwaltungs- oder sonstige Schulbeschäftigte, soweit diese einen Plattformzugang erhalten.
Personenbezogene Daten	Name, E-Mail-Adresse, Zuordnung zur Schule, Funktion/Rolle und Berechtigungen, interne Benutzer- und Accountkennungen, Authentifizierungsdaten, eduplaces-Nutzer-ID, eduplaces-Schul-ID sowie technische Betriebs-, Protokoll- und Nutzungsdaten. Zusätzlich vom Nutzer eingegebene Inhalte, soweit diese ausnahmsweise personenbezogene Daten enthalten.
Nicht vorgesehene Daten	Keine planmäßige Verarbeitung von Schüler- oder Elterndaten sowie keine Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 DSGVO.
Bücherlisten	Bücherlisten werden in der Plattform verwaltet. Bestehende Listen werden nicht über eine Upload-Funktion der Plattform übernommen. Eine etwaige Übermittlung bestehender Listen per E-Mail ist ein gesonderter Kommunikationsvorgang und nicht Bestandteil einer automatisierten Upload-Verarbeitung der Plattform.
eduplaces-SSO	Nutzer müssen bereits bei Schulbuchhelden registriert sein. Beim SSO werden nach aktueller Implementierung die eduplaces-Nutzer-ID und die eduplaces-Schul-ID verarbeitet und in Schulbuchhelden gespeichert. Passwörter werden nicht von eduplaces an Schulbuchhelden übermittelt.
Dauer	Für die Dauer der Nutzung des Schulkontos. Auf Löschanforderungen werden die Daten im Produktivsystem unverzüglich gelöscht; Sicherungskopien folgen dem regulären Backup-Zyklus des eingesetzten Hosting-/Datenbankdienstes.
Weisungsberechtigte	Die für das Schulkonto vertretungsberechnigten bzw. administrativ berechnigten Personen der Schule.
Eigene Verantwortlichkeit von Schulbuchhelden	Nicht von diesem AVV umfasst sind Verarbeitungsvorgänge, die Schulbuchhelden zu eigenen Zwecken durchführt, z. B. eigene Vertragsverwaltung, Abrechnung sowie Prozesse zur Berechnung und Auszahlung von Förderbeträgen an Fördervereine.

Anhang 2 – Unterauftragsverarbeiter

Der Verantwortliche genehmigt die nachfolgend aufgeführten Unterauftragsverarbeiter. Maßgeblich sind die jeweils geltenden Datenschutzvereinbarungen (DPA/AVV) und Unterauftragsverarbeiter-Regelungen der Anbieter.

Dienstleister	Primärer Standort	Leistung / Datenbezug	Hinweise
Supabase Pte. Ltd.	Dublin, Irland (Projektregion)	Datenbank, Authentifizierung, Dateispeicher (z. B. Schullogos), Backups; Verarbeitung von Nutzer-, Account- und Inhaltsdaten.	Anbieter mit Sitz in Singapur; primäre Speicherung/Verarbeitung in der gewählten EU-Region. Etwaige Drittlandverarbeitungen nach Anbieter-DPA und Art. 44 ff. DSGVO.
Vercel Inc.	Europäische Primärregion (Frankfurt am Main)	Hosting der gesamten Next.js-Anwendung einschließlich Frontend, API-Routen/Functions und technischer System-Logs.	US-Unternehmen; Pro-Tarif mit DPA. Internationale Support-/Unterauftragsverarbeitung kann nach DPA des Anbieters erfolgen.
Sinch Email / Mailjet	EU: Frankfurt (DE) und Saint-Ghislain (BE)	Versand transaktionaler System-E-Mails; Verarbeitung insbesondere von E-Mail-Adressen und Zustell-/Metadaten.	Konkrete vertragsschließende Sinch-Email-/Mailjet-Gesellschaft richtet sich nach dem Schulbuchhelden-Kundenkonto. DPA ist Bestandteil der Anbieterbedingungen.
STRATO GmbH	Deutschland	Bereitstellung der E-Mail-Infrastruktur; Verarbeitung von E-Mail-Adressen, Nachrichteninhalten und Anhängen	Verarbeitung im Rahmen der E-Mail-Kommunikation mit Schulen; bestehende Bücherlisten können per E-Mail übermittelt werden

Hinweis zu eduplaces: eduplaces wird nach der aktuellen technischen Einbindung nicht als von Schulbuchhelden beauftragter Unterauftragsverarbeiter eingesetzt, sondern als vorgelagerter SSO-/Identitätsdienst. Schulbuchhelden erhält beim SSO lediglich die eduplaces-Nutzer-ID und die eduplaces-Schul-ID.

Anhang 3 – Technische und organisatorische Maßnahmen (TOM)

Die folgenden Maßnahmen beschreiben den aktuellen technischen und organisatorischen Schutz der im Rahmen der Schulbuchhelden-Plattform verarbeiteten personenbezogenen Daten. Die Maßnahmen werden bei wesentlichen technischen Änderungen und mindestens in angemessenen regelmäßigen Abständen überprüft und bei Bedarf angepasst.

1. Transport- und Kommunikationssicherheit

- Die Plattform wird ausschließlich über HTTPS bereitgestellt; die Übertragung zwischen Browser, Anwendung und angebundenen Diensten erfolgt TLS-verschlüsselt.
- Zugriffe auf produktive Systeme erfolgen über die von Supabase und Vercel bereitgestellten gesicherten Administrations- und Deploymentwege.

2. Speicherung und Verschlüsselung

- Datenbank und Dateispeicher werden über Supabase betrieben.
- Die bei Supabase gespeicherten Daten werden im Ruhezustand („at rest“) verschlüsselt.
- Passwörter werden über Supabase Auth gehasht (bcrypt) gespeichert; Schulbuchhelden kann keine Klartext-Passwörter einsehen.

3. Identitäts- und Berechtigungsmanagement

- Es besteht ein Rollen- und Rechtekonzept mit Administratoren und weiteren Nutzern mit unterschiedlichen Berechtigungen.
- Nur Administratoren des jeweiligen Schulkontos können weitere Zugänge verwalten.
- Der interne Zugriff auf produktive Daten ist auf einen kleinen, für Entwicklung, Betrieb und Support erforderlichen Personenkreis beschränkt und erfolgt zweckgebunden.
- Eine verpflichtende Zwei-Faktor-Authentifizierung ist derzeit nicht Bestandteil der Plattform.

4. Mandantentrennung und Zugriff auf Schuldaten

- Nutzer und Inhalte werden technisch dem jeweiligen Schulkonto zugeordnet. Die Anwendung stellt sicher, dass Nutzer nur auf die ihnen zugeordneten bzw. freigegebenen Schulkonten und Funktionen zugreifen können.
- Schulbuchhelden besitzt technisch administrativen Zugriff. Tatsächliche Zugriffe erfolgen nur für Betrieb, Support, Wartung, Fehleranalyse, Sicherheit oder auf Weisung des Verantwortlichen.

5. Protokollierung und Nachvollziehbarkeit

- Technische Zugriffe, Fehler und Betriebsereignisse werden über die System-Logs der eingesetzten Infrastruktur von Supabase und Vercel protokolliert.
- Eine zusätzliche eigenständige, anwendungsinterne Vollprotokollierung sämtlicher Nutzeränderungen besteht derzeit nicht.

6. Verfügbarkeit, Backup und Wiederherstellung

- Für die Datenbank werden automatische Backups über Supabase erstellt.
- Die Wiederherstellung erfolgt über die von Supabase bereitgestellten Backup- und Restore-Funktionen.
- Ein separates Langzeitarchiv wird nicht geführt. Die Aufbewahrung der Sicherungen richtet sich nach dem jeweils aktiven Supabase-Standard-Backup-Zyklus.

7. Infrastruktur- und Updatesicherheit

- Netzwerk-, Plattform- und Rechenzentrums-Schutzmaßnahmen werden im Wesentlichen durch Supabase und Vercel als Infrastrukturbetreiber bereitgestellt.
- Sicherheitsupdates der zugrunde liegenden Hosting-Infrastruktur werden durch die Anbieter eingespielt.

- Software-Abhängigkeiten der Schulbuchhelden-Anwendung werden durch die Entwicklung manuell gepflegt und aktualisiert.

8. Datenschutzverletzungen / Incident Response

- Bei einem erkannten oder vermuteten Sicherheitsvorfall wird der Vorfall unverzüglich intern an Nils Rabe eskaliert.
- Soweit möglich werden betroffene Systeme und Daten identifiziert, der weitere Schaden begrenzt und erforderliche Sicherungsmaßnahmen eingeleitet.
- Ist ein Schulkonto betroffen, wird die betroffene Schule ohne unangemessene Verzögerung informiert. Verfügbare Informationen zu Art, Umfang, Folgen und Gegenmaßnahmen werden übermittelt und bei Bedarf ergänzt.
- Der Vorfall, die Bewertung und die ergriffenen Maßnahmen werden dokumentiert.

9. Löschung und Datenminimierung

- Es werden nur die für Onboarding, Nutzung, Authentifizierung und Betrieb der Plattform erforderlichen personenbezogenen Daten verarbeitet.
- Auf Löschverlangen werden das Schulkonto, zugehörige Nutzerkonten, Bücherlisten und sonstige zugeordnete Daten unverzüglich aus dem Produktivsystem entfernt.
- In Backups können Daten bis zur turnusmäßigen Löschung oder Überschreibung technisch fortbestehen; währenddessen werden sie nicht erneut produktiv genutzt, sofern keine Wiederherstellung erforderlich ist.

10. Überprüfung der Maßnahmen

- Die technischen und organisatorischen Maßnahmen werden bei wesentlichen Änderungen der Plattform oder Dienstleister und mindestens jährlich auf Aktualität und Angemessenheit überprüft.
- Derzeit finden keine gesonderten regelmäßigen externen Penetrationstests statt. Sicherheitsrelevante Anpassungen werden im Rahmen der Entwicklung und Infrastrukturpflege umgesetzt.