

Vertrag über die Verarbeitung von Daten im Auftrag (AVV)

Zwischen

Invario UG

Am Sportplatz 10 83052 Bruckmühl

— **Auftragnehmer** —

und

[Name der Schule / des Schulträgers]

[Straße, Hausnummer] [PLZ, Ort]

— **Auftraggeber** —

1. Allgemeines

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers gemäß Art. 4 Nr. 8 und Art. 28 DS-GVO. Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Bereitstellung der Software.
- (2) Es wird die Definition der „Verarbeitung“ gemäß Art. 4 Nr. 2 DS-GVO zugrunde gelegt.
- (3) Im Falle von Widersprüchen zwischen diesem Vertrag und sonstigen vertraglichen Regelungen gehen die Regelungen dieses AVV für datenschutzrechtliche Sachverhalte vor.

2. Gegenstand des Auftrags

- (1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Rahmen des Hostings, des Betriebs, der Wartung und der Verwaltung der Software „**Invario Modul Suite**“ als Software-as-a-Service (SaaS). Die genauen technischen und funktionalen Leistungsbeschreibungen ergeben sich aus dem Hauptvertrag.
- (2) Dies umfasst die Bereitstellung der Webanwendung sowie zugehöriger optionaler Module. Sofern nach Vertragsschluss weitere Module oder funktionale Erweiterungen vereinbart werden, welche die Verarbeitung personenbezogener Daten betreffen, werden die Parteien die

Invario UG
Am Sportplatz
83052 Bruckmühl
Tel.: 08061/3497799
Fax.: 08061/3497798

USt-IdNr.: De 000000000
Steuernummer: 000/000/00000
Amtsgericht Traunstein HRB 35441
Geschäftsführer: Simon V. Brieger

Invario UG
Commerzbank AG
IBAN: DE27 7114 0041 0183 3136 00
BIC: COBADEFFXXX

Beschreibung der Verarbeitung (insb. Datenkategorien und Kreis der Betroffenen) in **Anlage 1** dieses Vertrages entsprechend anpassen oder ergänzen.

3. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist der Verantwortliche im Sinne des Art. 4 Nr. 7 DS-GVO für die Verarbeitung von personenbezogenen Daten im Rahmen dieses Vertrages. Ihm obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung sowie die Wahrung der Rechte der betroffenen Personen.

(2) Der Auftraggeber ist für die Erfüllung der Betroffenenrechte (insb. nach Art. 12 bis 22 DS-GVO) verantwortlich. Unter Berücksichtigung der Natur der Verarbeitung unterstützt der Auftragnehmer den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflicht zur Beantwortung von Anträgen auf Wahrung der in Kapitel III der DS-GVO genannten Rechte der betroffenen Personen (gemäß Art. 28 Abs. 3 Satz 2 lit. e DS-GVO).

(3) Der Auftragnehmer verarbeitet die personenbezogenen Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierten Weisungen des Auftraggebers. Weisungen werden grundsätzlich in Textform (z. B. per E-Mail) erteilt. Mündlich oder fernmündlich erteilte Weisungen hat der Auftraggeber unverzüglich in Textform zu bestätigen. Der Auftragnehmer ist berechtigt, die Durchführung der Weisung bis zu dieser Bestätigung auszusetzen.

4. Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet die personenbezogenen Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierten Weisungen des Auftraggebers (gemäß Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).

(2) Die Speicherung und Verarbeitung der Daten erfolgt ausschließlich in Rechenzentren innerhalb der Bundesrepublik Deutschland. Der Einsatz von Subunternehmern (weiteren Auftragsverarbeitern) ist nur auf den in Anlage 2 definierten Servern und Systemen zulässig.

(3) Der Auftragnehmer verpflichtet sich, alle Personen, die mit der Verarbeitung der Daten betraut sind, auf die Vertraulichkeit zu verpflichten (Datengeheimnis gemäß Art. 28 Abs. 3 Satz 2 lit. b DS-GVO), sofern sie nicht bereits einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(4) Der Auftragnehmer setzt die erforderlichen technischen und organisatorischen Maßnahmen (TOM) gemäß Art. 32 DS-GVO um, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die konkreten Maßnahmen sind in **Anlage 3** zu diesem Vertrag festgelegt und werden vom Auftragnehmer während der Vertragslaufzeit auf dem aktuellen Stand der Technik gehalten.

(5) Der Auftragnehmer gewährleistet, dass die Daten des Auftraggebers strikt von den Daten anderer Kunden und von den eigenen Daten des Auftragnehmers getrennt verarbeitet werden (logische Mandantentrennung).

(6) Der Auftragnehmer wird den Auftraggeber unverzüglich benachrichtigen, wenn ihm Verletzungen des Schutzes personenbezogener Daten (Datenpannen) im Sinne des Art. 33 DS-GVO im Bereich seiner datenschutzrechtlichen Verantwortung bekannt werden.

5. Datenschutz beim Auftragnehmer

(1) Der Auftragnehmer stellt sicher, dass alle mit der Verarbeitung der personenbezogenen Daten betrauten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet (Datengeheimnis) und über die Pflichten des Datenschutzes angemessen unterwiesen wurden. Diese Pflicht zur Verschwiegenheit besteht auch nach Beendigung ihrer Tätigkeit und des Auftragsverhältnisses fort.

(2) Die Parteien sind sich einig, dass die Verarbeitung von besonderen Kategorien personenbezogener Daten gemäß Art. 9 DS-GVO (z. B. Gesundheitsdaten, Religionszugehörigkeit, ethnische Herkunft) **nicht** Gegenstand dieses Vertrages ist. Dem Auftraggeber ist es untersagt, solche Daten in der Software zu erfassen oder zu verarbeiten. Erlangt der Auftragnehmer Kenntnis von einer solchen vertragswidrigen Verarbeitung, informiert er den Auftraggeber unverzüglich und unterstützt nach dokumentierter Weisung bei Sperrung, Löschung oder Bereinigung der betroffenen Daten.

(3) Der Auftragnehmer benennt dem Auftraggeber die folgende Person als direkten Ansprechpartner für alle datenschutzrechtlichen Fragestellungen im Rahmen dieses Vertrages:

- **Ansprechpartner:** Simon V. Brieger
- **E-Mail-Adresse:** info@invario-software.de

6. Meldepflichten des Auftragnehmers

(1) Der Auftragnehmer meldet dem Auftraggeber jede Verletzung des Schutzes personenbezogener Daten (Datenpanne) unverzüglich nach Bekanntwerden.

(2) Die Meldung hat mindestens folgende Informationen zu enthalten oder unverzüglich nachzuliefern:

- eine Beschreibung der Art der Verletzung (z. B. unbefugter Zugriff, Datenverlust);
- soweit möglich, die Kategorien und die ungefähre Anzahl der betroffenen Personen (z. B. Schüler einer bestimmten Schule) sowie der betroffenen Datensätze;
- den Namen und die Kontaktdaten des zuständigen Ansprechpartners beim Auftragnehmer (gemäß § 5 Abs. 3 dieses Vertrages);
- eine Beschreibung der wahrscheinlichen Folgen der Datenpanne;
- die vom Auftragnehmer bereits ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

7. Unterauftragsverhältnisse

(1) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter (Subunternehmer) hinzuzuziehen. Die zum Zeitpunkt des Vertragsschlusses zugelassenen Subunternehmer sind in **Anlage 2** aufgeführt. Der Auftragnehmer verpflichtet weitere Auftragsverarbeiter vertraglich auf dieselben Datenschutzpflichten, die dem

Auftragnehmer nach diesem Vertrag obliegen. Der Auftragnehmer bleibt gegenüber dem Auftraggeber für die Einhaltung dieser Pflichten durch weitere Auftragsverarbeiter verantwortlich.

(2) Der Auftragnehmer informiert den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung weiterer Auftragsverarbeiter mindestens vier (4) Wochen vor dem geplanten Einsatz in Textform (z. B. per E-Mail).

(3) Der Auftraggeber kann der Änderung innerhalb von zwei (2) Wochen nach Erhalt der Mitteilung aus wichtigem, datenschutzrechtlichem Grund in Textform widersprechen. Erhebt der Auftraggeber innerhalb dieser Frist keinen Widerspruch, gilt die Änderung als genehmigt.

(4) Macht der Auftraggeber von seinem Widerspruchsrecht Gebrauch und ist eine einvernehmliche Lösung zwischen den Parteien nicht möglich, ist der Auftragnehmer berechtigt, den Hauptvertrag sowie diese Vereinbarung mit einer Frist von zwei (2) Wochen außerordentlich zu kündigen, sofern dem Auftragnehmer die Erbringung der geschuldeten Leistung ohne den vorgeschlagenen Subunternehmer wirtschaftlich oder technisch nicht zumutbar ist.

8. Kontrollbefugnisse

(1) Der Auftraggeber hat das Recht, die Einhaltung der datenschutzrechtlichen Vereinbarungen zu überprüfen. Der Auftraggeber erkennt an, dass der Auftragnehmer als rein digital und remote organisiertes Unternehmen **keine öffentlichen Geschäftsräume (Physisches Office)** unterhält und die Datenverarbeitung ausschließlich dezentral und verschlüsselt auf Systemen der STRATO GmbH erfolgt.

(2) Überprüfungen und Inspektionen werden daher **grundsätzlich im Wege von datenschonenden Fernprüfungen (Remoteverfahren)** durchgeführt. Der Auftragnehmer erfüllt seine Nachweispflichten durch das Bereitstellen von:

- aktuellen Zertifikaten (z. B. ISO 27001) des Subunternehmers STRATO GmbH;
- den eigenen dokumentierten TOMs (Anlage 3);
- falls erforderlich, geführten System-Präsentationen via gesicherter Videokonferenz (Screensharing).

(3) Eine physische Vor-Ort-Inspektion in den privaten Wohnräumen der Mitarbeiter/Gesellschafter des Auftragnehmers ist zum Schutz der grundgesetzlich geschützten Privatsphäre (Art. 13 GG) und zur Wahrung von Geschäftsgeheimnissen anderer Kunden dauerhaft ausgeschlossen. Vor-Ort-Prüfungen in privaten Wohnräumen finden grundsätzlich nicht statt. Soweit eine Fernprüfung im Einzelfall zur Erreichung des Prüfungszwecks nicht ausreicht, werden die Parteien ein angemessenes, datenschutz- und vertraulichkeitsschonendes Prüfverfahren vereinbaren, etwa die Prüfung in geeigneten neutralen Räumlichkeiten, durch einen unabhängigen Prüfer oder durch Vorlage zusätzlicher Nachweise. Gesetzliche Befugnisse von Aufsichtsbehörden bleiben unberührt.

(4) Sollte eine Behörde oder der Auftraggeber eine über die Absätze 2 hinausgehende Prüfung fordern, die einen nachweisbaren administrativen Mehraufwand beim Auftragnehmer verursacht, wird dieser Aufwand nach vorheriger Absprache auf Basis eines angemessenen Stundensatzes

vergütet, es sei denn, die Prüfung ist infolge eines vom Auftragnehmer verschuldeten Datenschutzverstoßes erforderlich.

9. Beendigung und Löschung

(1) Nach Beendigung des Hauptvertrages hat der Auftragnehmer nach Wahl des Auftraggebers alle im Auftrag verarbeiteten personenbezogenen Daten entweder vollständig und datenschutzkonform zu löschen oder an den Auftraggeber zurückzugeben, sofern nicht nach dem Unionsrecht oder dem anwendbaren nationalen Recht eine Verpflichtung zur Aufbewahrung der Daten besteht (Art. 28 Abs. 3 Satz 2 lit. g DS-GVO).

(2) Wählt der Auftraggeber die Rückgabe der Daten, erfolgt diese in einem gängigen, maschinenlesbaren Format (z. B. als CSV- oder JSON-Export). Der Auftragnehmer ist berechtigt, für den über den Standardexport hinausgehenden Aufwand der Datenaufbereitung eine angemessene Vergütung zu verlangen.

(3) Die endgültige Löschung der Live-Datenbestände erfolgt innerhalb von vierzehn (14) Tagen nach Vertragsbeendigung bzw. nach erfolgter Datenrückgabe. Die Vernichtung von digitalen Datenträgern oder die Bereinigung der Speicherbereiche erfolgt gemäß DIN 66399 (mindestens Sicherheitsstufe 3).

(4) Der Auftraggeber nimmt zur Kenntnis, dass eine selektive Löschung von Daten aus automatisierten, systemweiten Datensicherungen (Backups) technisch nicht möglich ist. Daten in Backups werden im Rahmen der regulären Backup-Zyklen des Subunternehmers STRATO GmbH nach spätestens dreißig (30) Tagen automatisch überschrieben und damit endgültig gelöscht. Bis zu diesem Zeitpunkt werden diese Daten vom Auftragnehmer für jegliche andere Verarbeitung gesperrt.

(5) Der Auftragnehmer bestätigt dem Auftraggeber die ordnungsgemäße Löschung auf Verlangen in Textform.

Anlage 1 - Gegenstand des Auftrags

- Gegenstand und Zweck der Verarbeitung Der Auftragnehmer unterstützt den Auftraggeber im Rahmen des Hauptvertrages bei der digitalen Organisation, Verwaltung und Ausleihe von Lehrmitteln (wie Büchern, digitalen Medien, Tablets und ähnlichem) über die Software „Invario Modul Suite“. Die Verarbeitung umfasst im Einzelnen die Verwaltung von Schüler-, Eltern-, Erziehungsberechtigten- und Lehrkräftedaten zur Abwicklung des Leihverkehrs, die barcode- und systembasierte Erfassung von Ausleihen, Rückgaben und Inventurbeständen, die Generierung von pseudonymisierten Identifikatoren (Hashes) zur Systemsicherheit sowie die Erstellung und den Export von Mahnungen und Schadenrechnungen bei Fristüberschreitung, Verlust oder Beschädigung von Lehrmitteln.
- Art der personenbezogenen Daten Zu den verarbeiteten Daten gehören Bestandsdaten wie Nachname, Vorname, Klasse oder Kurs, der Status als Schüler, Lehrkraft oder Erziehungsberechtigter sowie die schulische E-Mail-Adresse, sofern diese vom Auftraggeber genutzt wird. Zudem werden Nutzungs-

und Verlaufsdaten verarbeitet, wie zugewiesene Lehrmittel, die Leih-Historie, Verlust- und Beschädigungsprotokolle, offene Gebühren beziehungsweise Mahnstufen sowie sonstige schul- und datenschutzrechtlich relevante Verwaltungsdaten für den Leihbetrieb. Schließlich umfasst die Verarbeitung Zugangs- und Protokolldaten, bestehend aus Benutzernamen, kryptografischen Passwort-Hashes über das Verfahren scrypt, temporären Sitzungsdaten wie Session-JWT und Cookies sowie IP-Adressen und System-Logfiles.

- **Kategorien betroffener Personen** Die von der Verarbeitung betroffenen Personengruppen sind Schülerinnen und Schüler des Auftraggebers, Erziehungsberechtigte und Eltern als Sorgeberechtigte der minderjährigen Schüler, Lehrkräfte und schulisches Personal sowie das Bibliothekspersonal, IT-Beauftragte und Administratoren des Auftraggebers.
- **Löschfristen und Datenbereinigung** Die Löschung von Bestands- und Nutzungsdaten im laufenden Betrieb (beispielsweise bei einem Schulabgang) erfolgt eigenverantwortlich durch den Auftraggeber über die in der Software bereitgestellten Löschfunktionen, wobei der Auftragnehmer diese Löschbefehle unverzüglich im Live-System umsetzt. Nach Beendigung des Hauptvertrages erfolgt die endgültige Löschung aller Datenbestände im Live-System innerhalb von vierzehn Tagen nach den Vorgaben der DIN 66399 (mindestens Sicherheitsstufe 3), sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen. In systemweiten, automatisierten Datensicherungen (Backups) des Subunternehmers STRATO GmbH verbleibende Daten werden im Rahmen der regulären Backup-Zyklen nach maximal dreißig Tagen automatisch überschrieben und damit endgültig vernichtet. System-Logfiles und Transaktionsprotokolle werden rollierend nach acht bis maximal dreißig Tagen, je nach gewählter Systemkonfiguration, automatisch gelöscht, während flüchtige Daten im Arbeitsspeicher (transiente Daten) unmittelbar nach Abschluss des jeweiligen Systemvorgangs bereinigt werden.

Anlage 2 - Unterauftragnehmer

Unternehmen	Anschrift	Leistung	Ort der Verarbeitung
Strato GmbH	Otto-Ostrowski-Straße 7 10249 Berlin	Cloud-Hosting, Datenbank & E-Mail-Relay	Deutschland

Anlage 3 - Technische und organisatorische Maßnahmen

Der Auftragnehmer setzt gemäß Art. 32 DS-GVO die nachfolgenden technischen und organisatorischen Maßnahmen um, um ein dem Risiko angemessenes Schutzniveau für die Daten des Auftraggebers zu gewährleisten:

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- **Verschlüsselung bei Übertragung:** Sämtliche Datenübertragungen zwischen den Endgeräten der Nutzer und der Software „Invario Modul Suite“ erfolgen ausnahmslos verschlüsselt über das Protokoll **TLS 1.3** (bzw. mindestens TLS 1.2 mit Perfect Forward Secrecy).
- **Kryptografischer Schutz von Zugangsdaten:** Benutzerpasswörter werden niemals im Klartext gespeichert. Die Speicherung erfolgt ausschließlich als kryptografischer Hash unter Verwendung des starken, vom BSI empfohlenen Verfahrens **scrypt** mit einem jeweils benutzerspezifischen, zufällig generierten Salt. Dies stellt sicher, dass die Passwörter nach dem aktuellen Stand der Technik gegen unbefugte Entschlüsselung und Brute-Force-Angriffe geschützt sind.
- **Datensparsamkeit / Datenminimierung:** Das Datenmodell der Software ist auf das notwendige Minimum reduziert. Die Erfassung und dauerhafte Speicherung von Geburtsdaten oder privaten E-Mail-Adressen von Schülerinnen und Schülern ist im Datenbankschema standardmäßig nicht vorgesehen.
- **Zugangskontrolle (Administration):** Der administrative Zugriff der beiden Gesellschafter des Auftragnehmers auf die Serverinfrastruktur und die Datenbanken ist durch strikte Zugriffskontrollen, zertifikatsbasierte SSH-Schlüssel und eine verpflichtende Zwei-Faktor-Authentisierung (2FA) geschützt.

2. Integrität und Verfügbarkeit (Art. 32 Abs. 1 lit. b und c DS-GVO)

- **Infrastruktur & Hosting:** Die Software und die zugehörigen Datenbanken werden ausschließlich in den nach **ISO/IEC 27001 zertifizierten Hochsicherheits-Rechenzentren der STRATO GmbH** innerhalb Deutschlands betrieben. Die physische Absicherung (Zutrittskontrolle, Brandschutz, unterbrechungsfreie Stromversorgung) wird vollumfänglich durch die STRATO GmbH gewährleistet.
- **Datensicherung (Backup-Management):** Es erfolgen automatisierte, tägliche Datensicherungen (Backups) der gesamten Anwendungsdatenbank. Die Backups werden verschlüsselt gespeichert und nach einem rollierenden Zyklus von maximal 30 Tagen automatisch überschrieben.

3. Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DS-GVO)

- **Patch-Management:** Die verwendeten Serverkomponenten, Betriebssysteme und Software-Bibliotheken werden durch den Auftragnehmer regelmäßig auf Sicherheitsupdates überprüft und zeitnah aktualisiert.
- **Mandantentrennung:** Die logische Trennung der Datenbestände verschiedener Schulen wird auf Software- und Datenbankebene (Multi-Tenancy-Architektur) strikt sichergestellt, sodass ein unbefugter Datenzugriff zwischen verschiedenen Auftraggebern technisch ausgeschlossen ist.