

# Auftragsbearbeitungsvertrag (AVV)

gemäss Art. 9 revDSG · Stand April 2026 · Version 1.0

Dieser Auftragsbearbeitungsvertrag (nachfolgend «AVV») regelt die Rechte und Pflichten der Schule (nachfolgend «Verantwortliche») und der Vertretio (nachfolgend «Auftragsbearbeiterin») bei der Bearbeitung von Personendaten im Rahmen der Nutzung der Vertretio-Plattform. Er ergänzt den Hauptvertrag über die Nutzung der Plattform und konkretisiert die Pflichten gemäss Art. 9 des revidierten Schweizer Datenschutzgesetzes (revDSG).

## 1. Vertragsparteien

Verantwortliche ist die jeweilige Schule (Volksschule, Bezirksschule, Kantonsschule oder vergleichbare Bildungsinstitution), welche die Vertretio-Plattform für ihre Lehrpersonen einsetzt und mit Vertretio einen Nutzungsvertrag abgeschlossen hat. Die Verantwortliche bleibt im datenschutzrechtlichen Sinn alleinige Herrin über die in der Plattform bearbeiteten Personendaten.

Auftragsbearbeiterin ist:

### **Vertretio**

Toygar Türkmen

8964 Rudolfstetten, Schweiz

E-Mail: [info@vertretio.ch](mailto:info@vertretio.ch)

## 2. Gegenstand und Dauer

Gegenstand dieses AVV ist die Bearbeitung von Personendaten durch die Auftragsbearbeiterin im Auftrag und nach Weisung der Verantwortlichen, soweit dies für die Bereitstellung und den Betrieb der Vertretio-Plattform erforderlich ist.

Der AVV gilt für die gesamte Laufzeit des Hauptvertrags über die Nutzung der Plattform und endet automatisch mit dessen Beendigung. Pflichten, die ihrer Natur nach über die Vertragsbeendigung hinaus fortbestehen (insbesondere Rückgabe und Löschung), bleiben davon unberührt.

## 3. Art und Zweck der Bearbeitung

Die Auftragsbearbeiterin bearbeitet Personendaten ausschliesslich zu folgenden Zwecken:

- Bereitstellung und Betrieb der Vertretio-Plattform (Web-App, iOS-App, Schnittstellen)
- Authentifizierung und Verwaltung von Lehrpersonen, Schul-Administrationen und weiteren Nutzerrollen
- Verwaltung von Stundenplänen, Verfügbarkeiten und Abwesenheiten
- Automatisierte Vermittlung von Vertretungen (3-Stufen-Matching: Springer, Bereitschaft, reguläre Lehrpersonen)
- Verwaltung von Langzeitabwesenheiten und externen Stellvertretungen

- Versand von Benachrichtigungen (E-Mail, Push) bei Vertretungsanfragen und Statusaktualisierungen
- Speicherung von Dokumenten zu Langzeitabwesenheiten (z.B. Kantonsformulare, Stelleninserate)
- Erstellen statistischer Auswertungen für die Verantwortliche (Excel-Export-Center)
- Sicherstellung der Funktionsfähigkeit, Stabilität und Sicherheit der Plattform
- Erbringung von Support-Leistungen auf Anfrage der Verantwortlichen

Eine über diese Zwecke hinausgehende Bearbeitung, insbesondere zu eigenen Zwecken der Auftragsbearbeiterin, zu Werbezwecken oder zur Weitergabe an Dritte, findet nicht statt.

## 4. Kategorien betroffener Personen und Personendaten

### 4.1 Betroffene Personen

- Lehrpersonen der Schule (reguläre Lehrpersonen, Springer, Assistenzen)
- Externe Stellvertretungen mit zeitlich befristetem Zugang
- Schul-Administrationen (Schulleitung, Sekretariat, Stellvertretungs-Verantwortliche)

### 4.2 Bearbeitete Personendaten

- Account-Daten: E-Mail-Adresse, verschlüsseltes Passwort, Vor- und Nachname, Lehrerkürzel, Telefonnummer (optional)
- Berufliche Daten: Schule, Rolle, unterrichtete Fächer, Klassen, Räume, Stundenplan-Lektionen, Stufen
- Verfügbarkeits- und Bereitschaftsdaten
- Krank- und Abwesenheitsmeldungen (ohne medizinische Diagnose)
- Vertretungs-Zuteilungen mit Status (offen, akzeptiert, abgelehnt, bestätigt)
- Langzeitabwesenheiten (Beginn, Ende, Typ, Pensum, optionale Notizen)
- Hochgeladene Dokumente zu Langzeitabwesenheiten (z.B. Arztzeugnisse, Kantonsformulare)
- Benachrichtigungs-Einstellungen und Push-Token (iOS-App)
- Technische Logdaten (IP-Adresse, Zeitstempel, aufgerufene URLs)

Die Auftragsbearbeiterin bearbeitet keine personenbezogenen Daten von Schülerinnen und Schülern. Klassenbezeichnungen (z.B. «3a», «Bb25») gelten nicht als Personendaten im Sinne des revDSG.

### 4.3 Besondere Personendaten

Hochgeladene Arztzeugnisse können besondere Personendaten im Sinne von Art. 5 lit. c Ziff. 2 revDSG (Daten über die Gesundheit) enthalten. Die Auftragsbearbeiterin trifft hierfür erhöhte Schutzmassnahmen (private Storage-Buckets, signierte URLs mit kurzer Gültigkeit, strikte Zugriffskontrolle nur für Schul-Admins der jeweiligen Schule).

## 5. Pflichten der Auftragsbearbeiterin

Die Auftragsbearbeiterin verpflichtet sich:

- Personendaten ausschliesslich im Rahmen der dokumentierten Weisungen der Verantwortlichen zu bearbeiten
- Die Verantwortliche unverzüglich zu informieren, falls eine Weisung gegen geltendes Datenschutzrecht verstösst
- Alle mit der Bearbeitung befassten Personen zur Vertraulichkeit zu verpflichten
- Die Verantwortliche bei der Erfüllung ihrer Pflichten gegenüber betroffenen Personen zu unterstützen (Auskunft, Berichtigung, Löschung, Datenübertragbarkeit)
- Die Verantwortliche bei der Erfüllung ihrer Meldepflichten bei Datenpannen zu unterstützen
- Die Verantwortliche bei Datenschutz-Folgenabschätzungen und Konsultationen mit Aufsichtsbehörden zu unterstützen
- Auf Verlangen alle für den Nachweis der Einhaltung dieser Pflichten erforderlichen Informationen zur Verfügung zu stellen

## 6. Technische und organisatorische Massnahmen (TOMs)

Die Auftragsbearbeiterin trifft folgende Massnahmen zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus (Art. 8 revDSG):

### 6.1 Vertraulichkeit

- Verschlüsselte Übertragung via HTTPS (TLS 1.2 oder höher)
- Verschlüsselte Speicherung in der Datenbank (Encryption at Rest)
- Sicheres Hashing von Passwörtern (bcrypt-basiert, keine Klartext-Speicherung)
- Multi-Tenant-Isolation mittels Row Level Security
- Strikte rollenbasierte Zugriffskontrolle
- Schutz der Arztzeugnis-Dokumente in privaten Storage-Buckets mit signierten URLs

### 6.2 Integrität

- Schutz gegen XSS, SQL-Injection und vergleichbare Angriffe
- Content-Security-Policy (CSP) und HTTP-Sicherheits-Header
- HMAC-signierte Tokens für E-Mail-Aktionslinks
- Input-Validierung auf Server- und Datenbank-Ebene

### 6.3 Verfügbarkeit und Belastbarkeit

- Hosting bei spezialisierten Anbietern mit Redundanz und automatisierten Backups
- Rate-Limiting auf allen API-Endpunkten
- Regelmässige Sicherheits-Updates der eingesetzten Software

### 6.4 Verfahren zur regelmässigen Überprüfung

- Regelmässige interne Sicherheits-Audits (zuletzt: April 2026)
- Pseudonymisierung und Minimierung der Datenbearbeitung
- Dokumentation aller Bearbeitungstätigkeiten

## 7. Unterauftragsbearbeiter

Die Verantwortliche genehmigt mit Abschluss dieses AVV den Einsatz folgender Unterauftragsbearbeiter:

Anbieter	Zweck	Standort
Supabase	Datenbank, Authentifizierung, Storage	Zürich, Schweiz
Vercel Inc.	Hosting der Web-App und Serverless-Funktionen	Frankfurt, Deutschland
Anthropic PBC	Optionale KI-gestützte Texterkennung von PDF-Stundenplänen, soweit von der Verantwortlichen genutzt.	USA
Resend	Versand von Transaktions-E-Mails	USA
Apple Inc.	Push-Benachrichtigungen (APNs) für iOS-App	USA
ImprovMX	E-Mail-Weiterleitung für info@vertretio.ch	Frankreich

Mit allen Unterauftragsbearbeitern bestehen entsprechende Auftragsbearbeitungsvereinbarungen. Die Auftragsbearbeiterin informiert die Verantwortliche über jede beabsichtigte Änderung und gibt ihr die Möglichkeit, Einspruch zu erheben.

## 8. Datenübermittlung ins Ausland

Aus dem Einsatz der oben aufgeführten Unterauftragsbearbeiter ergibt sich, dass Personendaten in bestimmten Fällen ins Ausland übermittelt werden. Der Bundesrat anerkennt die EU/EWR-Staaten als Länder mit angemessenem Datenschutzniveau.

Für Übermittlungen in die USA stützt sich die Auftragsbearbeiterin auf:

- Standardvertragsklauseln (SCCs) mit Schweizer Anpassungen
- Technische Schutzmassnahmen (Verschlüsselung)
- Vertragliche Verpflichtung der Anbieter
- Prüfung der Erforderlichkeit im Einzelfall

Die Hauptdatenbank mit allen Personendaten verbleibt physisch in der Schweiz (Supabase, Zürich).

## 9. Meldung von Datenpannen

Die Auftragsbearbeiterin meldet der Verantwortlichen unverzüglich, spätestens innerhalb von 72 Stunden nach Kenntnis, jede Verletzung der Datensicherheit. Die Meldung enthält mindestens:

- Beschreibung der Art der Datenpanne
- Betroffene Kategorien und ungefähre Anzahl betroffener Personen
- Wahrscheinliche Folgen
- Ergriffene oder vorgeschlagene Massnahmen zur Behebung

Die Auftragsbearbeiterin unterstützt die Verantwortliche bei der Erfüllung ihrer Meldepflichten gegenüber dem EDÖB sowie gegenüber betroffenen Personen.

## 10. Rechte der betroffenen Personen

Wenden sich betroffene Personen direkt an die Auftragsbearbeiterin, leitet diese die Anfragen unverzüglich an die Verantwortliche weiter. Die Auftragsbearbeiterin unterstützt mit geeigneten technischen und organisatorischen Massnahmen.

## 11. Auditrechte

Die Verantwortliche ist berechtigt, die Einhaltung der Pflichten zu überprüfen oder durch einen unabhängigen Prüfer prüfen zu lassen (mindestens 30 Tage Vorankündigung). Die Auftragsbearbeiterin stellt auf Anfrage Berichte über Sicherheits-Audits zur Verfügung.

## 12. Rückgabe und Löschung

Nach Beendigung des Hauptvertrags werden sämtliche Personendaten nach Wahl der Verantwortlichen zurückgegeben (JSON-Export) oder unwiderruflich gelöscht (innert 90 Tagen). Die Löschung wird schriftlich bestätigt. Gesetzliche Aufbewahrungspflichten bleiben vorbehalten.

## 13. Haftung

Die Haftung richtet sich nach dem Hauptvertrag sowie den anwendbaren gesetzlichen Vorschriften. Jede Partei haftet für Schäden durch schuldhafte Verletzung dieses AVV.

## 14. Schlussbestimmungen

Änderungen bedürfen der Schriftform (E-Mail genügt). Bei Widersprüchen zwischen diesem AVV und dem Hauptvertrag gehen die Bestimmungen dieses AVV in datenschutzrechtlichen Belangen vor. Es gilt schweizerisches Recht. Gerichtsstand ist Bremgarten AG, Schweiz.

## 15. Inkrafttreten

Dieser AVV tritt mit der Annahme des Hauptvertrags über die Nutzung der Vertretio-Plattform durch die Verantwortliche in Kraft und gilt für dessen gesamte Laufzeit.