

Auftragsverarbeitungsvertrag (AVV)

Version 2026-08b · Stand: August 2026

Dieser Vertrag wird **digital geschlossen**: Der Administrator des Vereins bestätigt ihn bei der Registrierung per Checkbox (Art. 28 Abs. 9 DSGVO lässt das elektronische Format ausdrücklich zu). Klubklar speichert Zeitpunkt und Version der Zustimmung — keine Zettelwirtschaft.

1. Gegenstand und Parteien

Vertrag zwischen dem registrierenden Verein (**Verantwortlicher**) und Die Technikbude (<https://die-technikbude.de>), Inhaber Lars Hieronymi, Merianstraße 23, 60316 Frankfurt am Main (**Auftragsverarbeiter**) über die Verarbeitung personenbezogener Daten im Rahmen der Nutzung der Software „Klubklar“. Die zustimmende Person sichert zu, zum Abschluss dieses Vertrags für den Verein berechtigt zu sein (bei eingetragenen Vereinen insbesondere nach § 26 BGB).

2. Art, Zweck und Dauer der Verarbeitung

Hosting und Bereitstellung der Vereinsverwaltungs-Software; Speicherung, Anzeige und Verarbeitung der vom Verein eingegebenen Daten. Dauer: Laufzeit des Nutzungsvertrags; danach Rückgabe/Löschung nach Ziffer 8.

3. Art der Daten und Kreis der Betroffenen

- Stammdaten von Personen im Verein (Name, Kontaktdaten, Anschrift)
- Bankverbindungen (IBAN) für Erstattungen und Zahläufe
- Abrechnungs- und Belegdaten (Spesen, Übungsleiterabrechnungen, Rechnungen)
- Struktur- und Funktionsdaten (Ämter, Abteilungen, Rollen)

Betroffene: Mitglieder — darunter regelmäßig auch **Kinder und Jugendliche** —, Übungsleiter, Funktionsträger und Beschäftigte des Vereins sowie Dritte, deren Daten in Belegen erscheinen.

4. Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter verarbeitet die Daten nur auf dokumentierte Weisung des Vereins (Weisungen in Textform, z. B. per E-Mail oder über die Funktionen der Software); alle eingesetzten Personen sind zur Vertraulichkeit verpflichtet. Es gelten die technischen und organisatorischen Maßnahmen der Anlage TOM zu diesem Vertrag; sie werden fortlaufend an den Stand der Technik angepasst, ohne das Schutzniveau abzusenken.

Der Auftragsverarbeiter unterstützt den Verein bei der Beantwortung von Betroffenenanfragen und bei den Pflichten aus Art. 32–36 DSGVO — Anfragen des Vereins werden in der Regel innerhalb von 14 Tagen beantwortet. Eine Verletzung des Schutzes personenbezogener Daten meldet der Auftragsverarbeiter dem Verein unverzüglich, spätestens 48 Stunden nach Kenntniserlangung, mit den nach Art. 33 Abs. 3 DSGVO verfügbaren Informationen.

5. Unterauftragsverarbeiter

- Hosting, Objektspeicher und Backups: Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland (Rechenzentren Falkenstein/Nürnberg)
- E-Mail-Versand (Anmelde-Codes, Benachrichtigungen): Scaleway SAS, 8 rue de la Ville l'Évêque, 75008 Paris, Frankreich — Verarbeitung in der EU (Region Paris)
- Betriebsüberwachung und Fehlerdiagnose (Logs können personenbezogene Daten enthalten): Hetzner Online GmbH, Rechenzentrum Helsinki, Finnland (EU)
- Rechnungsstellung für den Klubklar-Vertrag (Vertrags- und Rechnungsdaten des Vereins, keine Mitgliederdaten): Haufe-Lexware GmbH & Co. KG, Freiburg, Deutschland

Karten- und Adressdienste (keine Auftragsverarbeitung)

Für die Ortssuche, die Zuordnung von Postleitzahlen zu Orten, die Prüfung von Adressen und die Berechnung von Fahrtstrecken ruft Klubklar zwei offene Kartendienste auf:

- Ortssuche, Postleitzahl-Zuordnung und Adressprüfung: Photon, betrieben von der komoot GmbH, Potsdam, Deutschland (Kartendaten aus OpenStreetMap)
- Berechnung von Fahrtstrecken: Demo-Server des offenen OSRM-Projekts, gehostet in der Schweiz

Diese Abrufe erfolgen ausschließlich über die Server von Klubklar, nie aus dem Browser der Nutzerin oder des Nutzers. Übermittelt wird allein der Suchbegriff selbst — eine Ortsbezeichnung, eine Postleitzahl oder ein Koordinatenpaar. **Nicht** übermittelt werden Namen, Mitglieds- oder Vereinskennungen, Vorgangsdaten, Sitzungsmerkmale oder die IP-Adresse der Nutzerin oder des Nutzers; auch Cookies und Referrer werden nicht gesendet. Antworten werden zwischengespeichert, damit dieselbe Anfrage nicht mehrfach hinausgeht.

Die übermittelten Angaben sind für die aufgerufenen Dienste keiner Person zuzuordnen. Klubklar behandelt diese Abrufe daher nicht als Auftragsverarbeitung nach Art. 28 DSGVO; die beiden Dienste sind entsprechend nicht als Unterauftragsverarbeiter aufgeführt. Die Abrufe sind reine Eingabehilfen — Orte und Kilometer können jederzeit von Hand eingetragen werden.

Der Auftragsverarbeiter informiert den Verein vorab in Textform über die Aufnahme oder den Wechsel von Unterauftragsverarbeitern. Der Verein kann aus wichtigem datenschutzrechtlichem Grund innerhalb von 14 Tagen widersprechen; führt der Widerspruch zu keiner einvernehmlichen Lösung, kann jede Partei den Nutzungsvertrag zum Zeitpunkt des Wirksamwerdens der Änderung kündigen. Mit allen Unterauftragsverarbeitern bestehen Verträge nach Art. 28 Abs. 4 DSGVO.

6. Verarbeitungsort

Verarbeitung der Vereinsdaten in Deutschland; Betriebs-Infrastruktur (Überwachung, E-Mail-Versand) ausschließlich in der EU. Keine Übermittlung personenbezogener Vereinsdaten in Drittländer.

Die unter Ziffer 5 genannten Kartendienste werden aus Deutschland beziehungsweise der Schweiz beantwortet. Die Schweiz ist von der Europäischen Kommission als Land mit angemessenem Datenschutzniveau anerkannt (Art. 45 DSGVO); übermittelt werden dorthin ausschließlich Koordinatenpaare ohne Personenbezug.

7. Kontroll- und Nachweisrechte

Der Verein kann Nachweise über die Einhaltung dieses Vertrags verlangen; Audit-Rechte nach Art. 28 Abs. 3 lit. h DSGVO.

8. Rückgabe und Löschung

Nach Vertragsende stellt Klubklar dem Verein einen vollständigen Export bereit und löscht die Daten anschließend **90 Tage nach Vertragsende** endgültig aus den Produktivsystemen; Sicherungskopien werden turnusgemäß überschrieben. Gesetzliche Aufbewahrungspflichten (z. B. § 147 AO) liegen beim Verein und werden durch den Export erfüllt.

9. Haftung

Für die Haftung der Parteien gelten die gesetzlichen Regelungen, insbesondere Art. 82 DSGVO, sowie ergänzend die Haftungsregelung der Nutzungsbedingungen (klubklar.de/nutzungsbedingungen).

Anlage: Technische und organisatorische Maßnahmen (TOM)

Stand: August 2026 — beschreibt die tatsächlich umgesetzten Maßnahmen (Art. 32 DSGVO).

- **Zutrittskontrolle:** Betrieb ausschließlich in ISO-27001-zertifizierten Rechenzentren der Hetzner Online GmbH in Deutschland (Falkenstein/Nürnberg); kein physischer Zugriff Dritter.
- **Zugangskontrolle:** Passwortlose Anmeldung per E-Mail-Einmalcode mit Versuchs- und Ratenbegrenzung (pro Konto und pro IP-Adresse), optional Zwei-Faktor-Authentisierung (TOTP); für Betreiber-Zugänge ist der zweite Faktor verpflichtend. Server-Zugriff nur per SSH-Schlüssel.
- **Zugriffskontrolle:** Rollenmodell je Verein (Administrator, Finanzverwaltung, Verwaltung, Mitglied); Betreiber-Zugriffe laufen über eine getrennte Identität und werden protokolliert.
- **Trennungskontrolle:** Strikte Mandantentrennung, auf Datenbank-Ebene erzwungen (Row-Level Security) — ein Zugriff über Vereinsgrenzen hinweg ist technisch ausgeschlossen.
- **Verschlüsselung:** Transportverschlüsselung (TLS) auf allen Verbindungen; besonders sensible Felder (Bankverbindungen, Geheimnisse der Zwei-Faktor-Anmeldung) zusätzlich feldverschlüsselt (AES-256-GCM) mit getrennt verwahrtem Schlüssel.
- **Integrität und Nachvollziehbarkeit:** Belege sind nach dem Hochladen unveränderbar und per SHA-256-Prüfsumme gesichert (GoBD); Finanz- und Freigabeaktionen werden in einem nicht löschbaren Aktivitätsprotokoll festgehalten; Vier-Augen-Prinzip in den Freigabeprozessen.
- **Verfügbarkeitskontrolle:** Redundanter Objektspeicher für Belege; regelmäßige verschlüsselte Datensicherungen, getrennt vom Produktivsystem aufbewahrt, mit erprobter Wiederherstellung; externe Überwachung der Erreichbarkeit.
- **Auftragskontrolle:** Unterauftragsverarbeiter nur nach Ziffer 5 mit Verträgen nach Art. 28 DSGVO; Entwicklungs-, Test- und Produktivumgebungen sind getrennt, Testumgebungen enthalten keine echten Vereinsdaten.

Stand: August 2026 (Version 2026-08b)