Vereinbarung zur Auftragsverarbeitung

gem. Art. 28 Abs. 3 DSGVO — GoodFunds-Plattform

Vorlage — Version 1.1 (Entwurf), Stand: Juli 2026

zwischen

[Name und Anschrift des Auftraggebers]
[Straße, PLZ Ort, Land]
— *nachfolgend „Auftraggeber*" —

und

goodDEV Softwareentwicklung, Tim Schmidt, Seifhennersdorfer Str. 4, 01099 Dresden
Betreiber der Plattform GoodFunds (goodfunds.org)
— *nachfolgend „Auftragnehmer*" —

§ 1 Gegenstand, Dauer, Art und Zweck

(1) Diese Vereinbarung regelt die Rechte und Pflichten der Parteien bei der Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers im Rahmen der Nutzung der Plattform GoodFunds. Sie gilt für alle Tätigkeiten, bei denen der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet.

(2) Die Dauer entspricht der Laufzeit des Hauptvertrags (Nutzungsvertrag GoodFunds). Zweck der Verarbeitung ist die Erbringung der vereinbarten Leistungen, insbesondere Kontakt- und Unterstützerverwaltung, Spendenerhebung und -verwaltung, Zahlungsabwicklung, Petitionen, Veranstaltungsanmeldungen, Kommunikation und zugehörige Analyse- und Reportingfunktionen.

§ 2 Datenkategorien und Betroffene

(1) Im Rahmen der Plattformnutzung können folgende Datenkategorien verarbeitet werden:

- Kontakt- und Adressdaten (Name, Anschrift, E-Mail-Adresse, Telefonnummer)
- Zahlungs- und Bankverbindungsdaten (IBAN, BIC, Kreditkartendaten via Payment Provider, Transaktionsdaten)
- Unterstützerdaten (Spendenhöhe, -datum, -zweck, Spendenverlauf, Zuwendungsbestätigungen, Petitionsunterschriften, Veranstaltungsanmeldungen)
- Kommunikationsdaten (E-Mail-Korrespondenz, Newsletter-Abonnements, Mailing-Verlauf)
- Zugangsdaten (Benutzername, Passwort-Hash, Rolle/Berechtigung)
- Nutzungsdaten der Plattform und eingebetteter Formulare (IP-Adressen, Zeitstempel, Geräteinformationen)
- Mitgliedschaftsdaten (Mitgliedsnummer, Status, Beitragsverlauf)
- Pseudonymisierte Engagement-Daten (Aktivitäten werden zunächst ohne Personenbezug gespeichert und erst bei Registrierung dem Nutzer zugeordnet)
- Sonstige personenbezogene Daten, die der Auftraggeber in der Plattform speichert

(2) Kategorien betroffener Personen:

- Spender*innen und Fördermitglieder
- Petitionsunterzeichner*innen
- Veranstaltungsteilnehmer*innen und Bewerber*innen
- Interessent*innen und Newsletter-Abonnent*innen
- Mitglieder und Unterstützer*innen des Auftraggebers
- Kontaktpersonen und Anfragende
- Mitarbeiter*innen des Auftraggebers (soweit in der Plattform erfasst)

(3) Der konkrete Umfang ergibt sich aus der jeweiligen Nutzung und Konfiguration der Plattform durch den Auftraggeber. Nicht alle genannten Kategorien müssen zutreffen.

§ 3 Sensible Daten

(1) Die Plattform ist nicht für die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO bestimmt (z.B. Gesundheitsdaten, politische Meinungen, religiöse Überzeugungen).

(2) Sollte der Auftraggeber dennoch solche Daten in der Plattform speichern, trägt er die alleinige Verantwortung für die Rechtmäßigkeit dieser Verarbeitung und die Einhaltung der zusätzlichen Anforderungen nach Art. 9 DSGVO. Der Auftragnehmer wendet auf alle gespeicherten Daten die in Anhang 2 beschriebenen Schutzmaßnahmen gleichermaßen an.

§ 4 Weisungen

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, es sei denn, er ist nach EU- oder Mitgliedstaatsrecht zur Verarbeitung verpflichtet. Die anfänglichen Weisungen ergeben sich aus dem Hauptvertrag und der Konfiguration der Plattform durch den Auftraggeber; Änderungen bedürfen der Textform.

(2) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er eine Weisung für rechtswidrig hält, und darf deren Umsetzung bis zur Klärung aussetzen.

(3) Die Datenverarbeitung findet ausschließlich im EWR statt. Soweit Dienste von Drittanbietern (z.B. Payment Provider) eingesetzt werden, die Daten in einem Drittland verarbeiten, erfolgt dies nur auf Grundlage geeigneter Garantien (Angemessenheitsbeschluss, Standardvertragsklauseln) und nach Abstimmung mit dem Auftraggeber.

§ 5 Pflichten des Auftragnehmers

(1) Der Auftragnehmer gewährleistet, dass alle mit der Datenverarbeitung befassten Personen zur Vertraulichkeit verpflichtet sind. Diese Pflicht besteht auch nach Vertragsende fort.

(2) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit bei der Erfüllung von Betroffenenrechten (Kap. III DSGVO), bei der Durchführung von Datenschutz-Folgenabschätzungen (Art. 35 DSGVO) und bei den Pflichten nach Art. 32–36 DSGVO.

(3) Der Auftragnehmer meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich, in der Regel innerhalb von 24 Stunden nach Kenntnisnahme, an den Auftraggeber. Die Meldung umfasst mindestens:

- Art der Verletzung mit Angabe der betroffenen Datenkategorien und geschätzter Anzahl Betroffener
- Kontaktdaten des Ansprechpartners beim Auftragnehmer
- Voraussichtliche Folgen der Verletzung
- Ergriffene oder vorgeschlagene Gegenmaßnahmen

Soweit Informationen nicht gleichzeitig bereitgestellt werden können, werden sie ohne unangemessene Verzögerung nachgereicht.

(4) Der Auftragnehmer führt ein Verzeichnis der Verarbeitungstätigkeiten gem. Art. 30 Abs. 2 DSGVO.

§ 6 Pflichten des Auftraggebers

(1) Der Auftraggeber ist als Verantwortlicher (Art. 4 Nr. 7 DSGVO) für die Rechtmäßigkeit der Datenverarbeitung verantwortlich. Er informiert den Auftragnehmer unverzüglich über Fehler oder Unregelmäßigkeiten und benennt auf Anforderung einen Ansprechpartner für Datenschutzfragen.

(2) Die Plattform bietet die Möglichkeit, Drittdienste über Integrationen anzubinden (z.B. Newsletter-Tools, Payment Provider, Übersetzungsdienste, CRM-Systeme). Diese Anbindung erfolgt eigenständig durch den Auftraggeber (z.B. per API-Key). Für die Rechtmäßigkeit der Datenübermittlung an diese Drittdienste sowie für den Abschluss eigener Auftragsverarbeitungsverträge mit den jeweiligen Anbietern ist ausschließlich der Auftraggeber verantwortlich. Diese Drittdienste sind keine Unterauftragnehmer des Auftragnehmers.

§ 7 KI-gestützte Funktionen

(1) Die Plattform bietet KI-gestützte Funktionen zur Erstellung von Kampagnen, Mailings und Conversion-Elementen an. Diese Funktionen arbeiten ausschließlich mit Platzhaltern und Vorlagen. Personenbezogene Daten (PII) werden zu keinem Zeitpunkt an KI-Modelle übermittelt. Eingaben in KI-gestützte Felder durchlaufen zusätzlich einen PII-Filter, der versehentlich eingegebene personenbezogene Daten (z.B. Namen, E-Mail-Adressen, Anschriften) erkennt und entfernt, bevor Inhalte an ein Sprachmodell übermittelt werden.

(2) Der Auftragnehmer setzt für die KI-Funktionen externe Sprachmodelle ein (z.B. Anthropic Claude, OpenAI). Die jeweiligen Anbieter sind als Unterauftragnehmer in Anhang 1 aufgeführt. Es werden ausschließlich Inhalts- und Strukturdaten (Vorlagentexte, Anweisungen, Platzhalter) an die Modelle gesendet, keine personenbezogenen Daten der Betroffenen.

(3) Der Auftragnehmer gewährleistet, dass mit den eingesetzten KI-Anbietern vertraglich vereinbart ist, dass Kundendaten nicht für das Training von KI-Modellen verwendet werden.

(4) Alternativ kann der Auftraggeber eine eigene KI-Integration mit eigenem API-Key einrichten. In diesem Fall gilt § 6 Abs. 2 entsprechend: Der Auftraggeber ist für die Rechtmäßigkeit der Datenübermittlung und den Abschluss eigener Vereinbarungen mit dem KI-Anbieter selbst verantwortlich.

§ 8 Löschung, Rückgabe und Datenexport

(1) Der Auftraggeber kann seine Daten jederzeit während der Vertragslaufzeit selbstständig über die Exportfunktionen der Plattform exportieren.

(2) Nach Vertragsende kann der Auftraggeber innerhalb von 4 Wochen einen Datenexport beauftragen. Anschließend löscht der Auftragnehmer alle personenbezogenen Daten des Auftraggebers, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht.

(3) Daten der Zahlungsverarbeitung werden gemäß den gesetzlichen Aufbewahrungsfristen gespeichert (in der Regel 10 Jahre gem. HGB/AO).

(4) Vom Auftraggeber in der Plattform gelöschte Datensätze werden nach einer Übergangsfrist von 90 Tagen unwiderruflich gelöscht.

(5) Auf Anfrage bestätigt der Auftragnehmer die Löschung in Textform.

§ 9 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer trifft die in Anhang 2 beschriebenen Maßnahmen gem. Art. 32 DSGVO. Er passt diese dem Stand der Technik an, ohne das Schutzniveau zu unterschreiten.

(2) Änderungen an den technischen und organisatorischen Maßnahmen werden dem Auftraggeber mit einer Frist von 4 Wochen mitgeteilt. Das Datenschutzniveau darf sich durch Änderungen nicht verschlechtern.

(3) Der Auftragnehmer stellt dem Auftraggeber auf Anfrage alle Informationen zum Nachweis der Einhaltung seiner Pflichten zur Verfügung und ermöglicht Überprüfungen nach Anmeldung mit mindestens 14 Tagen Vorlauf.

§ 10 Subunternehmer

(1) Der Auftraggeber genehmigt den Einsatz der unter https://goodfunds.de/legal/subunternehmer genannten Subunternehmer. Über Änderungen informiert der Auftragnehmer mindestens 14 Tage im Voraus per E-Mail. Der Auftraggeber kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund Einspruch erheben.

(2) Der Auftragnehmer überträgt seine datenschutzrechtlichen Pflichten auf jeden weiteren Auftragsverarbeiter und haftet dem Auftraggeber gegenüber für deren Einhaltung.

§ 11 Haftung

Die Haftungsregelungen des Hauptvertrags gelten auch für diese Vereinbarung. Bei Schadensersatzansprüchen Betroffener (Art. 82 DSGVO) unterstützen sich die Parteien gegenseitig bei der Aufklärung.

§ 12 Schlussbestimmungen

(1) Änderungen dieser Vereinbarung bedürfen der Textform und der Zustimmung beider Parteien.

(2) Im Falle eines Widerspruchs zwischen dieser Vereinbarung und dem Hauptvertrag hat diese Vereinbarung Vorrang, soweit der Schutz personenbezogener Daten betroffen ist.

(3) Gerichtsstand ist Dresden, vorbehaltlich zwingender gesetzlicher Gerichtsstände. Es gilt deutsches Recht.

(4) Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

(5) Diese Vereinbarung kann gem. Art. 28 Abs. 9 DSGVO in elektronischer Form geschlossen werden. Sie wird wirksam, sobald der Auftraggeber sie im Rahmen der Registrierung oder Nutzung der Plattform GoodFunds bestätigt. Der Zeitpunkt der Zustimmung wird elektronisch protokolliert.

Auftragnehmer (vorab gezeichnet):

goodDEV Softwareentwicklung
Tim Schmidt
Dresden, [DATUM]

Auftraggeber (elektronische Zustimmung):

Organisation: [Name des Auftraggebers]
Anschrift: [Straße, PLZ Ort]
Bestätigt durch: [Name der Person]
E-Mail: [E-Mail-Adresse]
Zeitpunkt der Zustimmung: [Timestamp]

Diese Vereinbarung wurde elektronisch bei der Registrierung auf goodfunds.org abgeschlossen. Eine handschriftliche Unterschrift ist gem. Art. 28 Abs. 9 DSGVO nicht erforderlich.

Anhang 1 — Subunternehmer

Die aktuelle Liste der eingesetzten Subunternehmer mit Angabe von Name, Sitz und Leistungsbeschreibung ist unter folgender URL einsehbar:

https://goodfunds.de/legal/subunternehmer

Sollten sich Änderungen an den Subunternehmern ergeben, wird der Auftraggeber innerhalb der in § 10 vereinbarten Frist (14 Tage) per E-Mail darüber informiert. Unter der oben genannten URL sind auch frühere Fassungen der Liste abrufbar.

Anhang 2 — Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

goodDEV ist ein Entwicklungsteam aus Dresden und Betreiber der GoodFunds-Plattform. Die serverseitige Infrastruktur wird bei OVH im Rechenzentrum Limburg an der Lahn (Deutschland) betrieben. Die Datenbanken laufen auf einem selbst betriebenen PostgreSQL-Cluster (Patroni) auf dieser Infrastruktur; Dateien liegen in einem S3-kompatiblen OVH-Objektspeicher (Region Frankfurt, Deutschland). Verschlüsselte Backups werden getrennt davon bei Hetzner Online (ISO 27001, Deutschland) aufbewahrt. Das vollständige, versionierte TOM-Dokument ist unter https://goodfunds.de/legal/tom einsehbar.

Vertraulichkeit

- Arbeitsplätze in abschließbaren Räumen; Server in zertifizierten Rechenzentren mit Zutrittskontrolle
- SSH-Zugang nur per Public-Key-Authentifizierung, kein Passwort-Login
- Zwei-Faktor-Authentifizierung für alle Admin-Zugänge (GitLab, Hosting, Datenbank, E-Mail)
- Individuelle Benutzerkonten, kein Teilen von Zugangsdaten, Passwort-Manager
- Festplattenverschlüsselung auf allen Arbeitsgeräten (FileVault / LUKS)
- Berechtigungen nach Least-Privilege-Prinzip; getrennte Umgebungen (Dev/Staging/Prod)
- Staging-Umgebungen können Kopien von Produktivdaten enthalten; Zugriff ist auf das Entwicklungsteam beschränkt und erfolgt ausschließlich über gesicherte Verbindungen
- Mandantenfähige Datenarchitektur: Daten verschiedener Auftraggeber sind logisch voneinander getrennt
- Personenbezogene Daten (Name, E-Mail, Telefon, Adresse, IBAN u.a.) werden auf Feldebene mittels AES-256-GCM (Authenticated Encryption) verschlüsselt in der Datenbank gespeichert
- Passwörter werden mittels BCrypt irreversibel gehasht
- Authentifizierung über RS256-signierte JWT-Tokens in HttpOnly-Cookies

Integrität

- Ausschließlich verschlüsselte Übertragung (TLS 1.2+); SSH/SFTP statt FTP
- Verschlüsselung der Datenbank-Verbindungen (SSL/TLS)
- Zahlungsdaten werden nicht auf eigenen Systemen gespeichert, sondern direkt an zertifizierte Payment Provider übermittelt
- Versionskontrolle (Git) für alle Code- und Konfigurationsänderungen
- Datenbankänderungen über dokumentierte Migrations-Skripte

- Server- und Anwendungszugriffe werden protokolliert

Verfügbarkeit und Wiederherstellung

- Selbst betriebenes PostgreSQL-Cluster mit Patroni: automatisches Failover bei Ausfall eines Datenbank-Knotens
- Redundante Produktions-Webserver mit Load Balancing; vorgelagerter HAProxy mit Floating IP
- Tägliche automatisierte Datenbank-Backups mit verschlüsselter Aufbewahrung
- Monitoring der Plattform-Verfügbarkeit mit automatischer Benachrichtigung
- Getestete Wiederherstellungsprozeduren; Ziel: Wiederherstellung innerhalb von 24 Stunden
- Redundante Infrastruktur (Strom, Netzwerk) durch die eingesetzten Rechenzentrumsbetreiber

Überprüfung

- Zeitnahe Sicherheitsupdates für Betriebssysteme und eingesetzte Software
- Regelmäßige Überprüfung der Wirksamkeit der Maßnahmen
- Verpflichtung aller Mitarbeiter auf Vertraulichkeit und Datenschutz
- Automatisierte CI/CD-Pipeline mit Sicherheitsprüfungen vor Deployment