AVV Kovetto

Anlage zu den Allgemeinen Geschäftsbedingungen von Kovetto

Vertrag zur Auftragsverarbeitung (AVV) nach Art. 28 DSGVO

zwischen

[Firma des Kunden], [Anschrift] – nachfolgend „Verantwortlicher" –

und

Coperte GmbH, Kopernikusstraße 14, 30167 Hannover – nachfolgend „Auftragsverarbeiter" –

– gemeinsam die „Parteien" –

1. Gegenstand, Rangfolge, Dauer

1.1 Dieser Vertrag konkretisiert die datenschutzrechtlichen Pflichten der Parteien für die Verarbeitung personenbezogener Daten, die der Auftragsverarbeiter im Rahmen der Bereitstellung der Plattform „Kovetto" im Auftrag des Verantwortlichen vornimmt (Hauptvertrag = AGB).

1.2 Bei Widersprüchen zwischen diesem AVV und dem Hauptvertrag gehen in datenschutzrechtlichen Fragen die Regelungen dieses AVV vor.

1.3 Die Laufzeit dieses AVV entspricht der Laufzeit des Hauptvertrags. Solange der Auftragsverarbeiter Daten des Verantwortlichen verarbeitet, gelten die Pflichten dieses AVV fort.

2. Art und Zweck der Verarbeitung, Datenarten, Betroffene

Gegenstand, Art und Zweck der Verarbeitung, die Arten personenbezogener Daten und die Kategorien betroffener Personen ergeben sich aus **Anlage 1**.

3. Weisungsrecht des Verantwortlichen

3.1 Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist gesetzlich zur Verarbeitung verpflichtet (Art. 28 Abs. 3 lit. a DSGVO); in diesem Fall teilt er dem Verantwortlichen die rechtliche Anforderung vor der Verarbeitung mit, soweit das Gesetz dies nicht verbietet.

3.2 Weisungen erfolgen in der Regel über die Funktionen und Konfigurationen der Plattform sowie in Textform. Mündliche Weisungen werden unverzüglich in Textform bestätigt.

3.3 Hält der Auftragsverarbeiter eine Weisung für datenschutzrechtlich unzulässig, informiert er den Verantwortlichen unverzüglich; er ist berechtigt, die Durchführung bis zur Bestätigung oder Änderung auszusetzen.

4. Vertraulichkeit

Der Auftragsverarbeiter setzt zur Verarbeitung nur Personen ein, die zur Vertraulichkeit verpflichtet oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b, Art. 29, Art. 32 Abs. 4 DSGVO), und stellt sicher, dass sie personenbezogene Daten nur weisungsgemäß verarbeiten.

5. Technische und organisatorische Maßnahmen (TOM)

5.1 Der Auftragsverarbeiter trifft die zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus erforderlichen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO. Der aktuelle Stand ist in **Anlage 2** beschrieben.

5.2 Die TOM unterliegen dem technischen Fortschritt. Der Auftragsverarbeiter darf sie weiterentwickeln, solange das vereinbarte Schutzniveau nicht unterschritten wird.

6. Unterauftragsverarbeiter

6.1 Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine Genehmigung zur Hinzuziehung der in **Anlage 3** genannten Unterauftragsverarbeiter (Art. 28 Abs. 2 S. 1 DSGVO).

6.2 Der Auftragsverarbeiter informiert den Verantwortlichen über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern mit angemessener Frist (mindestens 14 Tage) vorab in Textform. Der Verantwortliche kann einer Änderung aus wichtigem, datenschutzrechtlich begründetem Grund innerhalb dieser Frist widersprechen. Bei berechtigtem Widerspruch, der eine Leistungserbringung verhindert, steht beiden Parteien ein Sonderkündigungsrecht zu.

6.3 Der Auftragsverarbeiter verpflichtet jeden Unterauftragsverarbeiter durch Vertrag auf datenschutzrechtliche Pflichten, die denen dieses AVV im Wesentlichen entsprechen (Art. 28 Abs. 4 DSGVO).

7. Unterstützung des Verantwortlichen

7.1 Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen des Zumutbaren bei der Beantwortung von Anträgen betroffener Personen (Art. 12–23 DSGVO) durch geeignete technische und organisatorische Maßnahmen. Richtet sich ein Betroffener direkt an den Auftragsverarbeiter, leitet dieser den Antrag unverzüglich an den Verantwortlichen weiter.

7.2 Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der Pflichten aus Art. 32–36 DSGVO (Datensicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation) unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen.

8. Meldung von Verletzungen des Schutzes personenbezogener Daten

Der Auftragsverarbeiter meldet dem Verantwortlichen jede ihm bekannt gewordene Verletzung des Schutzes personenbezogener Daten ohne unangemessene Verzögerung, in der Regel innerhalb von 48 Stunden, in Textform. Die Meldung enthält die nach Art. 33 Abs. 3 DSGVO verfügbaren Angaben.

9. Löschung und Rückgabe

Nach Abschluss der Erbringung der Verarbeitungsleistungen löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle personenbezogenen Daten oder gibt sie zurück und löscht vorhandene Kopien, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht (Art. 28 Abs. 3 lit. g DSGVO). Der Verantwortliche kann seine Daten innerhalb von 30 Tagen nach Vertragsende über die Exportfunktionen der Plattform selbst abrufen.

10. Nachweise und Kontrollen

10.1 Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO zur Verfügung (Art. 28 Abs. 3 lit. h DSGVO), vorrangig durch aktuelle Dokumentation der TOM, Testate oder anerkannte Zertifizierungen.

10.2 Der Verantwortliche ist berechtigt, sich von der Einhaltung zu überzeugen, einschließlich Inspektionen. Vor-Ort-Prüfungen sind mit angemessener Vorankündigung, während der Geschäftszeiten und ohne Störung des Betriebsablaufs durchzuführen.

11. Drittlandtransfer

Eine Verarbeitung personenbezogener Daten in einem Drittland erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (Angemessenheitsbeschluss, Standardvertragsklauseln nebst ergänzenden Maßnahmen oder eine sonstige zulässige Garantie). Die je Unterauftragsverarbeiter maßgeblichen Mechanismen sind in **Anlage 3** ausgewiesen.

12. Haftung

Für die Haftung gelten Art. 82 DSGVO sowie die Haftungsregelungen des Hauptvertrags (AGB Ziff. 11), soweit Art. 82 DSGVO dem nicht entgegensteht.

13. Schlussbestimmungen

13.1 Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist – soweit zulässig – der Sitz des Auftragsverarbeiters.

13.2 Änderungen dieses AVV bedürfen der Textform. Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen unberührt.

Anlage 1 — Gegenstand und Einzelheiten der Verarbeitung

Gegenstand: Bereitstellung der SaaS-Feedback-Plattform Kovetto (Erfassung, Speicherung, Transkription und KI-Auswertung von visuellem Feedback).

Art der Verarbeitung: Erheben, Erfassen, Speichern, Organisieren, Auslesen, Verwenden (KI-Transkription/-Analyse), Übermitteln an Unterauftragsverarbeiter, Löschen.

Zweck: Durchführung der Feedback-Sessions, Audio-Transkription, KI-gestützte Strukturierung und Zusammenfassung, interne Verwaltung des Feedbacks durch den Verantwortlichen.

Dauer: Für die Laufzeit des Hauptvertrags zzgl. der Lösch-/Rückgabefristen nach Ziff. 9.

Kategorien betroffener Personen:

- Nutzer/Mitarbeiter des Verantwortlichen (Kontoinhaber-Seite)
- Feedback-Geber/Tester, die über öffentliche Feedback-Links teilnehmen
- ggf. Dritte, deren Daten in hochgeladenen Assets (Screenshots) oder in Audio-/Textfeedback enthalten sind

Arten personenbezogener Daten:

- Stammdaten/Kontaktdaten (Name, E-Mail-Adresse, sofern erhoben)
- Inhaltsdaten: hochgeladene Screenshots/Assets (können personenbezogene Daten enthalten), Text-Feedback, Audioaufnahmen, Transkripte, Marker-/Positionsdaten
- Nutzungs- und Metadaten (z. B. Session-Token, Zeitstempel, technische Logdaten, IP-Adresse)
- Zahlungsbezogene Daten werden durch den Zahlungsdienstleister eigenverantwortlich verarbeitet (siehe Anlage 3)

Besondere Kategorien (Art. 9 DSGVO): nicht vorgesehen. Der Verantwortliche stellt durch geeignete Auswahl der geteilten Inhalte sicher, dass keine besonderen Kategorien personenbezogener Daten ohne Rechtsgrundlage verarbeitet werden.

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

Vertraulichkeit

- Zutrittskontrolle: Hosting in EU-Rechenzentren der eingesetzten Anbieter; kein physischer Serverbetrieb beim Auftragsverarbeiter.
- Zugangskontrolle: individuelle Benutzerkonten, Authentifizierung über Supabase Auth, Passwort-/Session-Sicherheit, Rollen-/Rechtekonzept.
- Zugriffskontrolle: rollenbasierte Berechtigungen; strikte Trennung interner Ansichten und öffentlicher, ausschließlich tokenbasierter Session-Zugriffe; Row-Level-Security in der Datenbank.
- Trennungskontrolle: mandantenbezogene Trennung der Daten je Konto/Projekt.

Integrität

- Weitergabekontrolle: Transportverschlüsselung (TLS/HTTPS) bei allen Übertragungen.
- Eingabekontrolle: Protokollierung relevanter Aktionen (Activity-Logs).

Verfügbarkeit und Belastbarkeit

- Verschlüsselung gespeicherter Daten (Encryption at Rest beim Hosting-/Storage-Anbieter).
- Regelmäßige Backups; Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO).

Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)

- Validierung von Datei-Uploads (MIME-Typ, Dateigröße); Eingangsvalidierung (Schema-Prüfung).
- Datenschutz durch Technikgestaltung: Minimierung der an externe Clients ausgelieferten Felder; keine sensiblen internen Metadaten an öffentliche Clients.

Anlage 3 — Genehmigte Unterauftragsverarbeiter

Anbieter	Zweck	Sitz / Region	Drittland-Mechanismus
Railway (auf Google Cloud Platform)	Hosting/Infrastruktur	EU – Frankfurt	EU-Verarbeitung; GCP als Unterauftragsverarbeiter
Supabase	Datenbank, Auth, Storage	EU – eu-central-1 Frankfurt	EU-Verarbeitung
OpenAI	Audio-Transkription, KI-Analyse	USA (EU Data Residency verfügbar)	EU Data Residency + Zero Data Retention; sonst SCC + DPF
Resend	Transaktions-E-Mails	EU-Versandregion; Account-/Metadaten teils USA	SCC / DPF
PostHog	Produktanalyse	EU Cloud – Frankfurt	EU-Verarbeitung
Cloudflare	Website-Screenshots/Captures	EU/global	SCC / DPF
Stripe	Zahlungsabwicklung	EU-Entität Irland	Eigenverantwortliche Verarbeitung; SCC bei US-Bezug

Optionale, vom Verantwortlichen selbst verbundene Integrationen (nur bei aktiver Verbindung; eigene Rechtsgrundlage/Verantwortlichkeit des Verantwortlichen): Meta/WhatsApp, ClickUp, Jira, Linear.

Unterschriften

Ort, Datum: _____

Verantwortlicher

Name: _____

Funktion: _____

Unterschrift: _____

Auftragsverarbeiter — Coperte GmbH

Name: _____

Funktion: _____

Unterschrift: _____