Kovetto DPA

Annex to the General Terms and Conditions of Kovetto

Data Processing Agreement (DPA) pursuant to Art. 28 GDPR

between

the **Customer (account holder)** who accepts the General Terms and Conditions of Coperte GmbH including this DPA upon registration or ordering and who is identified by the account details (company, address, contact data) stored in their user account – hereinafter the "Controller" –

and

Coperte GmbH, Kopernikusstraße 14, 30167 Hannover, Germany – hereinafter the "Processor" –

– together the "Parties" –

Conclusion without signature: This DPA is an annex to and part of the Processor's General Terms and Conditions (GTC). It is concluded uniformly for every customer and without separate signing by the Controller agreeing to the GTC including this DPA upon registration or ordering. The agreement is concluded in electronic form pursuant to **Art. 28(9) GDPR**; a handwritten signature is not required. The Processor documents the time of consent, the user account and the contract version as evidence. On request, the Processor provides a separately signed version.

1. Subject matter, order of precedence, term

1.1 This agreement specifies the data protection obligations of the Parties for the processing of personal data that the Processor carries out on behalf of the Controller in connection with providing the "Kovetto" platform (main contract = GTC).

1.2 In the event of contradictions between this DPA and the main contract, the provisions of this DPA prevail on data protection matters.

1.3 The term of this DPA corresponds to the term of the main contract. As long as the Processor processes the Controller's data, the obligations of this DPA continue to apply.

2. Nature and purpose of processing, data types, data subjects

The subject matter, nature and purpose of the processing, the types of personal data and the categories of data subjects are set out in **Annex 1**.

3. Controller's right to issue instructions

3.1 The Processor processes personal data solely on the documented instructions of the Controller, unless it is legally required to process (Art. 28(3)(a) GDPR); in that case it informs the Controller of the

legal requirement before processing, unless the law prohibits this.

3.2 Instructions are generally given via the functions and configurations of the platform as well as in text form. Verbal instructions are confirmed in text form without undue delay.

3.3 If the Processor considers an instruction to be unlawful under data protection law, it informs the Controller without undue delay; it is entitled to suspend execution until confirmation or amendment.

4. Confidentiality

The Processor only uses persons who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality (Art. 28(3)(b), Art. 29, Art. 32(4) GDPR) and ensures that they process personal data only in accordance with instructions.

5. Technical and organisational measures (TOMs)

5.1 The Processor implements the technical and organisational measures required under Art. 32 GDPR to ensure a level of protection appropriate to the risk. The current status is described in **Annex 2**.

5.2 The TOMs are subject to technical progress. The Processor may develop them further as long as the agreed level of protection is not fallen below.

6. Sub-processors

6.1 The Controller grants the Processor general authorisation to engage the sub-processors listed in **Annex 3** (Art. 28(2) sentence 1 GDPR).

6.2 The Processor informs the Controller of intended changes regarding the engagement or replacement of sub-processors with reasonable notice (at least 14 days) in advance in text form. The Controller may object to a change within this period for an important, data-protection-related reason. In the case of a justified objection that prevents provision of the service, both Parties have a right to extraordinary termination.

6.3 The Processor binds each sub-processor by contract to data protection obligations that substantially correspond to those of this DPA (Art. 28(4) GDPR).

7. Support for the Controller

7.1 The Processor supports the Controller, to the extent reasonable, in responding to requests from data subjects (Art. 12–23 GDPR) through appropriate technical and organisational measures. If a data subject contacts the Processor directly, the Processor forwards the request to the Controller without undue delay.

7.2 The Processor supports the Controller in complying with the obligations under Art. 32–36 GDPR (data security, notification of breaches, data protection impact assessment, prior consultation), taking into account the nature of the processing and the information available to it.

8. Notification of personal data breaches

The Processor notifies the Controller of any personal data breach that becomes known to it without undue delay, generally within 48 hours, in text form. The notification contains the information available pursuant to Art. 33(3) GDPR.

9. Deletion and return

After the end of the provision of the processing services, the Processor deletes or, at the Controller's choice, returns all personal data and deletes existing copies, unless a statutory retention obligation applies (Art. 28(3)(g) GDPR). The Controller may retrieve its data itself within 30 days after the end of the contract using the platform's export functions.

10. Evidence and audits

10.1 The Processor makes available to the Controller all information necessary to demonstrate compliance with the obligations under Art. 28 GDPR (Art. 28(3)(h) GDPR), primarily through up-to-date documentation of the TOMs, attestations or recognised certifications.

10.2 The Controller is entitled to satisfy itself of compliance, including inspections. On-site inspections are to be carried out with reasonable prior notice, during business hours and without disrupting operations.

11. Third-country transfers

Processing of personal data in a third country only takes place where the requirements of Art. 44 et seq. GDPR are met (adequacy decision, standard contractual clauses together with supplementary measures, or another permissible safeguard). The mechanisms relevant to each sub-processor are set out in **Annex 3**.

12. Liability

Liability is governed by Art. 82 GDPR as well as the liability provisions of the main contract (GTC Sec. 11), unless Art. 82 GDPR precludes this.

13. Final provisions

13.1 The law of the Federal Republic of Germany applies. The place of jurisdiction is – to the extent permissible – the registered office of the Processor.

13.2 Amendments to this DPA require text form. Should individual provisions be invalid, the validity of the remaining provisions remains unaffected.

Annex 1 — Subject matter and details of the processing

Subject matter: Provision of the SaaS feedback platform Kovetto (capture, storage, transcription and AI analysis of visual feedback).

Nature of processing: Collecting, recording, storing, organising, retrieving, using (AI transcription/analysis), transmitting to sub-processors, deleting.

Purpose: Conducting feedback sessions, audio transcription, AI-assisted structuring and summarisation, internal management of the feedback by the Controller.

Duration: For the term of the main contract plus the deletion/return periods under Sec. 9.

Categories of data subjects:

- Users/employees of the Controller (account-holder side)
- Feedback providers/testers who participate via public feedback links
- where applicable, third parties whose data is contained in uploaded assets (screenshots) or in audio/text feedback

Types of personal data:

- Master/contact data (name, email address, where collected)
- Content data: uploaded screenshots/assets (may contain personal data), text feedback, audio recordings, transcripts, marker/position data
- Usage and metadata (e.g. session token, timestamps, technical log data, IP address)
- Payment-related data is processed by the payment service provider on its own responsibility (see Annex 3)

Special categories (Art. 9 GDPR): not intended. The Controller ensures, through appropriate selection of the shared content, that no special categories of personal data are processed without a legal basis.

Annex 2 — Technical and organisational measures (Art. 32 GDPR)

Confidentiality

- Physical access control: hosting in EU data centres of the providers used; no physical server operation at the Processor.
- System access control: individual user accounts, authentication via Supabase Auth, password/session security, role/permission concept.
- Data access control: role-based permissions; strict separation of internal views and public, exclusively token-based session access; row-level security in the database.
- Separation control: tenant-based separation of data per account/project.

Integrity

- Transfer control: transport encryption (TLS/HTTPS) for all transmissions.
- Input control: logging of relevant actions (activity logs).

Availability and resilience

- Encryption of stored data (encryption at rest at the hosting/storage provider).
- Regular backups; recoverability (Art. 32(1)(c) GDPR).

Procedures for regular review (Art. 32(1)(d) GDPR)

- Validation of file uploads (MIME type, file size); input validation (schema check).
- Data protection by design: minimisation of the fields delivered to external clients; no sensitive internal metadata to public clients.

Annex 3 — Approved sub-processors

Provider	Purpose	Location / Region	Third-country mechanism
Railway (on Google Cloud Platform)	Hosting/infrastructure	EU – Frankfurt	EU processing; GCP as sub-processor
Supabase	Database, auth, storage	EU – eu-central-1 Frankfurt	EU processing
Mistral AI (Mistral AI SAS)	Audio transcription, AI analysis	EU – France	EU processing; no model training
Plunk (useplunk.com)	Transactional emails	EU/EEA – Hetzner (Germany)	EU processing; Amazon SES as sub-processor (transit only), SCCs Module 2
PostHog	Product analytics	EU Cloud – Frankfurt	EU processing
Cloudflare	Website screenshots/captures	EU/global	SCCs / DPF
Stripe	Payment processing	EU entity Ireland	Independent controllership; SCCs where a US nexus applies

Optional integrations connected by the Controller itself (only when actively connected; separate legal basis/controllership of the Controller): Meta/WhatsApp, ClickUp, Jira, Linear.

Conclusion and evidence

This DPA applies uniformly to all customers of the "Kovetto" platform and becomes effective **without a handwritten signature**. It is concluded in electronic form (Art. 28(9) GDPR) by the Controller agreeing to the Processor's General Terms and Conditions including this DPA upon registration or ordering.

As evidence of conclusion, the Processor documents, per customer, the time of consent, the consenting user account and the version of this DPA accepted in each case. The Processor provides a separately signed copy to a customer on request.

Version date: 2026-08-16