DELIVVO LEGAL DOCUMENT

Data Processing Agreement

Last updated April 23, 2026

This Data Processing Agreement ("DPA") forms part of the agreement between Delivvo and the customer identified below to the extent Delivvo processes personal data on the customer's behalf in connection with Delivvo services.

Customer: Completed by the customer at execution Customer address: Completed by the customer at execution Customer signatory: Completed by the customer at execution Effective date: The date the customer signs this DPA

Processor: Delivvo Processor contact: support@delivvo.io

Purpose and scope

This DPA applies when the customer acts as a controller and Delivvo acts as a processor for personal data that the customer or its authorized users submit to Delivvo in connection with the Delivvo platform. If the parties have a separate written master agreement, order form, or terms of service governing the Delivvo services, that agreement remains in force and this DPA supplements it.

Roles of the parties

For the personal data covered by this DPA, the customer is the controller and Delivvo is the processor. Delivvo will process personal data only on documented instructions from the customer, unless otherwise required by applicable law.

Duration

This DPA begins on the Effective Date and remains in effect for as long as Delivvo processes personal data on behalf of the customer in connection with the services. Upon termination of the underlying services, the data return and deletion section below will apply.

Nature and purpose of processing

Delivvo may process personal data to host and organize project and client records, display files and workflow data to authorized users, authenticate users and portal visitors, send transactional emails and access messages at the customer's direction, generate PDFs and audit records, and maintain backups and security controls necessary to provide the platform.

Categories of data subjects

The categories of data subjects may include:

- the customer's employees, contractors, and authorized users
- the customer's clients, leads, end customers, and project contacts
- signatories, invoice recipients, and client portal users
- other individuals whose personal data the customer intentionally submits to Delivvo through the services

Categories of personal data

The categories of personal data may include contact data, account and profile data, project data, uploaded files and documents, transaction-related data, and technical or security data reasonably necessary to secure and operate the service.

The customer controls the specific personal data it chooses to upload or make available through Delivvo.

Customer obligations

The customer represents, warrants, and agrees that it has a valid legal basis for the processing of personal data and for instructing Delivvo to process that data, will provide any required notices to data subjects, will not instruct Delivvo to process personal data in violation of applicable law, and is responsible for the accuracy, quality, and legality of the personal data it submits to the services.

Delivvo obligations

Delivvo will process personal data only on the customer's documented instructions, ensure that personnel authorized to process personal data are bound by confidentiality obligations, implement appropriate technical and organizational measures to protect personal data, and notify the customer if, in Delivvo's opinion, an instruction infringes applicable data-protection law, unless prohibited from doing so by law.

Confidentiality and access controls

Delivvo will limit access to personal data to personnel and subprocessors who need that access to provide, support, or secure the services.

Security measures

Delivvo will maintain reasonable technical and organizational measures appropriate to the risks of the processing. These measures include:

- encryption of data in transit using HTTPS or similar secure transport
- encryption at rest where supported by Delivvo's infrastructure providers
- access controls, least-privilege practices, and logical separation of environments
- logging, monitoring, and incident-response processes
- backup and recovery procedures designed to support service continuity

The customer understands that no security measure can eliminate all risk. Delivvo may update its security practices from time to time so long as the overall level of protection is not materially reduced.

Subprocessors

The customer authorizes Delivvo to use subprocessors that are reasonably necessary to provide the services. Delivvo's current subprocessors may include:

- Supabase for database hosting, authentication, and file storage

• Vercel for application hosting and delivery, where applicable

• Resend for transactional email delivery

• Lemon Squeezy for subscription billing and payment processing when those features are enabled

Delivvo will require subprocessors to protect personal data under written terms that are materially consistent with Delivvo's processor obligations under this DPA.

International transfers

Because Delivvo and its subprocessors may process personal data in multiple jurisdictions, personal data may be transferred outside the European Economic Area, the UAE, or the country where the customer is established. Where such transfers are subject to transfer restrictions under applicable law, Delivvo will use transfer mechanisms and safeguards that Delivvo reasonably determines are appropriate.

Assistance with data subject requests and assessments

Taking into account the nature of the processing, Delivvo will provide reasonable assistance to the customer to help the customer respond to requests from data subjects and to the customer's obligations relating to security, breach notification, consultation with regulators, or data-protection impact assessments where Delivvo's cooperation is reasonably required.

If Delivvo receives a data subject request relating to personal data processed on the customer's behalf, Delivvo may redirect the requester to the customer unless Delivvo is legally required to respond directly.

Personal data breaches

If Delivvo becomes aware of a confirmed personal data breach affecting personal data processed on behalf of the customer, Delivvo will notify the customer without undue delay and, where feasible, within 72 hours after becoming aware of the breach. The notification may be phased if complete information is not immediately available.

Delivvo's notification will include available information reasonably useful to the customer, such as:

• the nature of the breach

• the categories of data involved

• the likely consequences, if known

• measures taken or proposed to address the breach

Delivvo's notification under this section is not an admission of fault or liability.

Audit rights

Upon reasonable written notice, and no more than once per 12-month period unless required by law or a regulator, Delivvo will make available information reasonably necessary to demonstrate compliance with this DPA. Where that information is insufficient and the customer has a legitimate compliance need, the customer may request an audit by an independent third party bound by confidentiality obligations.

Any audit must be limited in scope to the processing covered by this DPA, be conducted during normal business hours, avoid unreasonable disruption to Delivvo's operations or other customers, and exclude access to information that would compromise the confidentiality, security, or privacy of other Delivvo customers.

The customer will bear the costs of the audit unless applicable law or a regulator requires otherwise.

Return and deletion of personal data

Upon termination or expiration of the services, Delivvo will, at the customer's choice and subject to available product functionality, return or delete personal data processed on the customer's behalf, unless Delivvo is required by law to retain some or all of the data. Delivvo may retain limited backup copies for a reasonable period consistent with backup, security, fraud-prevention, and legal-retention practices.

Liability

The liability of each party under this DPA is subject to the limitations and exclusions of liability in the parties' underlying agreement, except to the extent such limitations are not enforceable under applicable data-protection law.

Governing law

This DPA is governed by the laws of the United Arab Emirates, unless the parties have agreed in writing to a different governing law in the underlying services agreement. The courts of Dubai, UAE will have jurisdiction over disputes arising out of this DPA, subject to any mandatory rights under applicable law.

Execution

This DPA may be executed electronically and in counterparts. Electronic signatures and scanned signatures will be treated as originals to the extent permitted by applicable law.

Accepted and agreed by the customer

Name: _____ Title: _____ Entity: _____ Signature: _____ Date: _____

Accepted and agreed by Delivvo

Name: Mohammed Title: Founder Contact: support@delivvo.io Signature: To be countersigned electronically Date: Date of Delivvo countersignature

How to execute

To request countersignature, email support@delivvo.io with your entity name, signatory details, and a copy of the completed DPA.