LEGAL

Data Processing Addendum (DPA)

Version 1.0, valid from 7 October 2026

1. Parties and subject matter

The processor is Ing. Jiří Psota, Company ID (IČO) 76072266, registered at Zborovská 1200/6, 150 00 Praha 5 - Smíchov, Czech Republic (the “processor”). The controller is the organization that uses the Vaultiqo service under the Terms (the “customer”).

This addendum governs the processing of personal data the customer puts into the service, in line with Article 28 of Regulation (EU) 2016/679 (GDPR). It forms an integral part of the Terms and the customer accepts it by accepting them. No handwritten signature is required (Article 28(9) GDPR). In matters of personal data protection, this addendum takes precedence over the Terms.

2. Scope

The subject matter, nature and purpose of processing and the categories of data and data subjects are described in Annex 1. Processing lasts for as long as the service is used and until deletion under section 9.

3. Instructions

The processor processes personal data only on the customer’s documented instructions. These are the Terms, this addendum and the customer’s configuration and use of the service. Otherwise only where EU or Czech law requires it; the processor informs the customer of such a requirement in advance unless the law prohibits it. If the processor considers an instruction unlawful, it tells the customer without delay.

4. Confidentiality

Persons with access to personal data are bound by confidentiality, by contract or by law, also after the cooperation ends.

5. Security

The processor takes the measures under Article 32 GDPR listed in Annex 2. It may change them as long as the level of protection does not decrease.

6. Sub-processors

The customer gives general authorization to engage the sub-processors listed at www.vaultiqo.app/subprocessors. The processor publishes planned changes on that page in advance. The customer may object at hello@vaultiqo.app and, if the parties cannot agree, may terminate the service. The processor imposes the same data protection obligations on its sub-processors and remains responsible for their performance.

7. Transfers outside the EEA

Personal data is stored in the EU (Google Cloud, region europe-west1, Belgium). It is transferred outside the EEA only to the extent stated in the sub-processor list and only with a safeguard under Chapter V GDPR: an adequacy decision (including the EU-US Data Privacy Framework) or standard contractual clauses.

8. Assistance

The processor reasonably assists the customer in handling data subject requests and in meeting its obligations under Articles 32 to 36 GDPR. The customer edits, exports and deletes data itself using the service’s functions. The processor notifies the customer of a personal data breach without undue delay after becoming aware of it.

9. Termination and deletion

Until the service ends, the customer can export its data. After the service ends, the processor deletes the personal data unless the law requires it to be kept (for example accounting records). Copies in backups expire as the backups rotate.

10. Information and audits

On request, the processor provides the information needed to demonstrate compliance with this addendum and allows audits to a reasonable extent, by prior arrangement and at the customer's cost. For sub-processors, their public certifications and reports replace an audit.

11. Final provisions

Liability is governed by Article 82 GDPR and the Terms. This addendum is governed by the laws of the Czech Republic. The current version is always at www.vaultiqo.app/dpa; a change must not lower the level of personal data protection. In case of any discrepancy between the language versions, the Czech version prevails.

Data protection contact: hello@vaultiqo.app.

Annex 1: Description of processing

Purpose	Storing and sharing the customer team's passwords and other sensitive data, managing access by users and groups from Google Workspace, and keeping an audit record of use.
Nature of processing	Storage, encryption, display to authorized users, sharing, syncing users and groups from Google Workspace (started by an administrator), backup, export and deletion.
Data subjects	The customer's users (employees and collaborators) and persons whose data the customer stores in the vault.
Categories of data	• User identity from Google: name, email, profile photo; roles and group memberships. • Vault content: passwords, notes, other sensitive fields and attachments (encrypted), plus item name, username, website address, tags and expiry date (unencrypted metadata). • Audit log: who did what and when (user email, action, item). IP addresses are not stored. • Sign-in sessions and, if an administrator turns on directory sync, encrypted Google OAuth tokens.
Processor's access to content	Sensitive fields are encrypted in the browser with the organization's key and again on the server with a master key. Keys are managed, so the team vault is not zero-knowledge: the processor is technically able to decrypt the content, but access to the keys is strictly restricted and the content is not read. Only public share links are fully zero-knowledge.
Special categories of data	Not processed intentionally. If the customer stores them in the vault, they are protected like all other content.
Duration	For as long as the service is used, then deletion under section 9.

Annex 2: Technical and organizational measures

- **Encryption:** sensitive fields encrypted with AES-256-GCM in the browser using the organization's key, a second encryption layer on the server, transport over TLS only. Google OAuth tokens are encrypted at rest.
- **Keys:** the master key and other secrets in Google Secret Manager with restricted access, key rotation without downtime, no keys in code or in the database.
- **Access:** sign-in with Google including the organization's 2-step verification, short-lived access tokens (15 minutes) with refresh token rotation, sessions ended immediately when Google reports a compromised or disabled account, roles and groups, strict tenant isolation on every request.
- **Visibility:** an audit log of views, autofills, edits and shares for administrators; operational logs are kept for 30 days.
- **Infrastructure:** hosting, database and backups in the EU (Google Cloud, europe-west1), daily database backups kept for 7 days, least-privilege service accounts, a restrictive Content Security Policy and security headers, rate limiting.
- **Breached password checks:** through Have I Been Pwned with k-anonymity. The browser sends only the first 5 characters of a password hash and no personal data, so HIBP is not a sub-processor.
- **Organizational measures:** confidentiality of persons with access.