

Accordo sul trattamento dei dati (DPA)

Versione 1.0, in vigore dal 7 ottobre 2026

1. Parti e oggetto

Il responsabile del trattamento è Ing. Jiří Psota, numero di identificazione dell'impresa (IČO) 76072266, con sede in Zborovská 1200/6, 150 00 Praha 5 - Smíchov, Repubblica Ceca (il «responsabile del trattamento»). Il titolare del trattamento è l'organizzazione che utilizza il servizio Vaultiqo ai sensi dei [Termini e Condizioni](#) (il «cliente»).

Il presente accordo disciplina il trattamento dei dati personali che il cliente inserisce nel servizio, in conformità all'articolo 28 del regolamento (UE) 2016/679 (GDPR). Costituisce parte integrante dei Termini e Condizioni e il cliente lo accetta accettando questi ultimi. Non è richiesta alcuna firma autografa (articolo 28, paragrafo 9, del GDPR). In materia di protezione dei dati personali, il presente accordo prevale sui Termini e Condizioni.

2. Ambito

L'oggetto, la natura e la finalità del trattamento, nonché le categorie di dati e di interessati, sono descritti nell'Allegato 1. Il trattamento dura per tutto il tempo in cui il servizio è utilizzato e fino alla cancellazione ai sensi della sezione 9.

3. Istruzioni

Il responsabile del trattamento tratta i dati personali soltanto su istruzione documentata del cliente. Tali istruzioni sono costituite dai Termini e Condizioni, dal presente accordo e dalla configurazione e dall'uso del servizio da parte del cliente. Diversamente, solo se lo richiede il diritto dell'Unione o il diritto ceco; in tal caso il responsabile del trattamento informa preventivamente il cliente di tale obbligo, salvo che il diritto lo vieti. Qualora ritenga che un'istruzione sia illecita, il responsabile del trattamento ne informa senza ritardo il cliente.

4. Riservatezza

Le persone che hanno accesso ai dati personali sono vincolate alla riservatezza, per contratto o per legge, anche dopo la cessazione della collaborazione.

5. Sicurezza

Il responsabile del trattamento adotta le misure di cui all'articolo 32 del GDPR elencate nell'Allegato 2. Può modificarle a condizione che il livello di protezione non diminuisca.

6. Sub-responsabili del trattamento

Il cliente concede un'autorizzazione generale al ricorso ai sub-responsabili del trattamento elencati alla pagina www.vaultiqo.app/subprocessors. Il responsabile del trattamento pubblica in anticipo su tale pagina le modifiche previste. Il cliente può opporsi scrivendo a hello@vaultiqo.app e, se le parti non raggiungono un accordo, può recedere dal servizio. Il responsabile del trattamento impone ai propri sub-responsabili gli stessi obblighi in materia di protezione dei dati e rimane responsabile del loro adempimento.

7. Trasferimenti al di fuori del SEE

I dati personali sono conservati nell'UE (Google Cloud, regione europe-west1, Belgio). Sono trasferiti al di fuori del SEE solo nella misura indicata nell'elenco dei sub-responsabili del trattamento e solo in presenza di una garanzia ai sensi del capo V del GDPR: una decisione di adeguatezza (compreso il quadro UE-USA per la protezione dei dati, EU-US Data Privacy Framework) o clausole contrattuali tipo.

8. Assistenza

Il responsabile del trattamento assiste ragionevolmente il cliente nel dare seguito alle richieste degli interessati e nell'adempimento dei suoi obblighi di cui agli articoli da 32 a 36 del GDPR. Il cliente modifica, esporta e cancella i dati autonomamente mediante le funzioni del servizio. Il responsabile del trattamento notifica al cliente una violazione dei dati personali senza ingiustificato ritardo dopo esserne venuto a conoscenza.

9. Cessazione e cancellazione

Fino alla cessazione del servizio il cliente può esportare i propri dati. Dopo la cessazione del servizio, il responsabile del trattamento cancella i dati personali, salvo che la legge ne richieda la conservazione (ad esempio le scritture contabili). Le copie contenute nei backup scadono con la rotazione dei backup.

10. Informazioni e audit

Su richiesta, il responsabile del trattamento fornisce le informazioni necessarie per dimostrare il rispetto del presente accordo e consente audit in misura ragionevole, previo accordo e a spese del cliente. Per i sub-responsabili del trattamento, le loro certificazioni e relazioni pubbliche sostituiscono l'audit.

11. Disposizioni finali

La responsabilità è disciplinata dall'articolo 82 del GDPR e dai Termini e Condizioni. Il presente accordo è regolato dal diritto della Repubblica Ceca. La versione vigente è sempre disponibile all'indirizzo www.vaultiqo.app/dpa; una modifica non può ridurre il livello di protezione dei dati personali. In caso di discrepanze tra le versioni linguistiche, prevale la versione ceca.

Contatto per la protezione dei dati: hello@vaultiqo.app.

Allegato 1: Descrizione del trattamento

Finalità	Conservazione e condivisione delle password e di altri dati sensibili del team del cliente, gestione degli accessi per utenti e gruppi provenienti da Google Workspace e tenuta di un registro di audit dell'utilizzo.
Natura del trattamento	Conservazione, cifratura, visualizzazione agli utenti autorizzati, condivisione, sincronizzazione di utenti e gruppi da Google Workspace (avviata da un amministratore), backup, esportazione e cancellazione.
Interessati	Gli utenti del cliente (dipendenti e collaboratori) e le persone i cui dati il cliente conserva nel vault.
Categorie di dati	• Identità dell'utente fornita da Google: nome, e-mail, foto del profilo; ruoli e appartenenza ai gruppi. • Contenuto del vault: password, note, altri campi sensibili e allegati (cifrati), oltre a nome dell'elemento, nome utente, indirizzo del sito web, tag e data di scadenza (metadati non cifrati). • Registro di audit: chi ha fatto cosa e quando (e-mail dell'utente, azione, elemento). Gli indirizzi IP non vengono conservati. • Sessioni di accesso e, se un amministratore attiva la sincronizzazione della directory, token OAuth di Google cifrati.

Accesso del responsabile del trattamento al contenuto	I campi sensibili sono cifrati nel browser con la chiave dell'organizzazione e nuovamente sul server con una chiave master. Le chiavi sono gestite, pertanto il vault del team non è zero-knowledge: il responsabile del trattamento è tecnicamente in grado di decifrare il contenuto, ma l'accesso alle chiavi è rigorosamente limitato e il contenuto non viene letto. Solo i link di condivisione pubblici sono completamente zero-knowledge.
Categorie particolari di dati	Non trattate intenzionalmente. Se il cliente le conserva nel vault, sono protette come ogni altro contenuto.
Durata	Per tutto il tempo in cui il servizio è utilizzato, quindi cancellazione ai sensi della sezione 9.

Allegato 2: Misure tecniche e organizzative

- **Cifratura:** campi sensibili cifrati con AES-256-GCM nel browser mediante la chiave dell'organizzazione, un secondo livello di cifratura sul server, trasmissione esclusivamente tramite TLS. I token OAuth di Google sono cifrati a riposo.
- **Chiavi:** la chiave master e gli altri segreti in Google Secret Manager con accesso limitato, rotazione delle chiavi senza interruzioni del servizio, nessuna chiave nel codice o nel database.
- **Accesso:** accesso con Google, inclusa la verifica in due passaggi dell'organizzazione, token di accesso di breve durata (15 minuti) con rotazione dei token di aggiornamento, sessioni terminate immediatamente quando Google segnala un account compromesso o disattivato, ruoli e gruppi, rigoroso isolamento dei tenant a ogni richiesta.
- **Visibilità:** un registro di audit di visualizzazioni, compilazioni automatiche, modifiche e condivisioni per gli amministratori; i log operativi sono conservati per 30 giorni.
- **Infrastruttura:** hosting, database e backup nell'UE (Google Cloud, europe-west1), backup giornalieri del database conservati per 7 giorni, account di servizio con privilegi minimi, una Content Security Policy restrittiva e intestazioni di sicurezza, limitazione della frequenza delle richieste (rate limiting).
- **Verifica delle password violate:** tramite Have I Been Pwned con k-anonimato. Il browser invia solo i primi 5 caratteri dell'hash di una password e nessun dato personale, pertanto HIBP non è un sub-responsabile del trattamento.
- **Misure organizzative:** riservatezza delle persone che hanno accesso.