

Zpracovatelský dodatek (DPA)

Verze 1.0, platná od 7. října 2026

1. Strany a předmět

Zpracovatelem je Ing. Jiří Psota, IČO 76072266, se sídlem Zborovská 1200/6, 150 00 Praha 5 - Smíchov („zpracovatel“). Správcem je organizace, která službu Vaultiqo používá na základě [Obchodních podmínek](#) („zákazník“).

Dodatek upravuje zpracování osobních údajů, které zákazník do služby vloží, podle čl. 28 nařízení (EU) 2016/679 (GDPR). Je nedílnou součástí Obchodních podmínek a zákazník jej přijímá jejich přijetím. Vlastnoruční podpis se nevyžaduje (čl. 28 odst. 9 GDPR). V otázkách ochrany osobních údajů má dodatek přednost před Obchodními podmínkami.

2. Rozsah

Předmět, povaha a účel zpracování, kategorie údajů a subjektů údajů jsou popsány v Příloze 1. Zpracování trvá po dobu užívání služby a do výmazu podle článku 9.

3. Pokyny

Zpracovatel zpracovává osobní údaje jen podle doložených pokynů zákazníka. Těmi jsou Obchodní podmínky, tento dodatek a nastavení a používání služby zákazníkem. Jinak jen tehdy, ukládá-li to právo EU nebo České republiky. O takové povinnosti zákazníka předem informuje, pokud mu v tom nebrání zákon. Považuje-li pokyn za protiprávní, neprodleně na to zákazníka upozorní.

4. Mlčenlivost

Osoby s přístupem k osobním údajům jsou vázány mlčenlivostí smluvně nebo ze zákona, a to i po skončení spolupráce.

5. Zabezpečení

Zpracovatel přijímá opatření podle čl. 32 GDPR uvedená v Příloze 2. Může je měnit, pokud se úroveň ochrany nesníží.

6. Subzpracovatelé

Zákazník uděluje obecné povolení k zapojení subzpracovatelů uvedených na www.vaultiqo.app/subprocessors. Plánované změny zpracovatel zveřejní na této stránce předem. Zákazník proti nim může vznést námitku na hello@vaultiqo.app, a pokud se strany nedohodnou, může službu ukončit. Zpracovatel uloží subzpracovatelům stejné povinnosti ochrany údajů a odpovídá za jejich plnění.

7. Předání mimo EHP

Osobní údaje jsou uloženy v EU (Google Cloud, region europe-west1, Belgie). Mimo EHP se předávají jen v rozsahu uvedeném v seznamu subzpracovatelů a jen se zárukou podle kapitoly V GDPR, tedy na základě rozhodnutí o odpovídající ochraně (včetně EU-US Data Privacy Framework) nebo standardních smluvních doložek.

8. Součinnost

Zpracovatel zákazníkovi v přiměřeném rozsahu pomáhá vyřizovat žádosti subjektů údajů a plnit povinnosti podle čl. 32 až 36 GDPR. Úpravu, export a výmaz údajů zákazník provádí sám funkcemi služby. Porušení zabezpečení osobních údajů zpracovatel zákazníkovi ohlásí bez zbytečného odkladu poté, co se o něm dozví.

9. Ukončení a výmaz

Do ukončení služby si zákazník může data exportovat. Po ukončení služby zpracovatel osobní údaje vymaže, ledaže jejich uchování ukládá právo (například účetní doklady). Kopie v zálohách zanikají jejich běžnou rotací.

10. Informace a audit

Zpracovatel poskytne na vyžádání informace potřebné k doložení plnění tohoto dodatku a umožní audit v přiměřeném rozsahu, po předchozí domluvě a na náklady zákazníka. U subzpracovatelů audit nahrazují jejich veřejné certifikace a zprávy.

11. Závěrečná ustanovení

Odpovědnost se řídí čl. 82 GDPR a Obchodními podmínkami. Dodatek se řídí právem České republiky. Aktuální znění je vždy na www.vaultiqo.app/dpa; změna nesmí snížit úroveň ochrany osobních údajů. Při rozporu mezi jazykovými verzemi má přednost česká verze.

Kontakt pro ochranu osobních údajů: hello@vaultiqo.app.

Příloha 1: Popis zpracování

Účel	Ukládání a sdílení hesel a dalších citlivých údajů týmu zákazníka, správa přístupu podle uživatelů a skupin z Google Workspace a auditní záznam použití.
Povaha zpracování	Uložení, šifrování, zobrazení oprávněným uživatelům, sdílení, synchronizace uživatelů a skupin z Google Workspace (spouští administrátor), záloha, export a výmaz.
Subjekty údajů	Uživatelé zákazníka (zaměstnanci a spolupracovníci) a osoby, jejichž údaje zákazník do trezoru uloží.
Kategorie údajů	- Identita uživatele z Google: jméno, e-mail, profilová fotka; role a členství ve skupinách. - Obsah trezoru: hesla, poznámky, další citlivá pole a přílohy (šifrované), a dále název položky, uživatelské jméno, adresa webu, štítky a datum expirace (nešifrovaná metadata). - Auditní log: kdo, co a kdy (e-mail uživatele, akce, položka). IP adresy se neukládají. - Přihlašovací relace a, pokud administrátor zapne synchronizaci, šifrované tokeny Google OAuth.
Přístup zpracovatele k obsahu	Citlivá pole se šifrují už v prohlížeči klíčem organizace a na serveru podruhé hlavním klíčem. Klíče jsou spravované, týmový trezor tedy není zero-knowledge: zpracovatel je technicky schopen obsah dešifrovat, přístup ke klíčům je však přísně omezen a obsah nečte. Plně zero-knowledge jsou jen veřejné sdílené odkazy.
Zvláštní kategorie údajů	Nezpracovávají se záměrně. Pokud je zákazník do trezoru vloží, jsou chráněny stejně jako ostatní obsah.
Doba zpracování	Po dobu užívání služby, poté výmaz podle článku 9.

Příloha 2: Technická a organizační opatření

- **Šifrování:** citlivá pole AES-256-GCM v prohlížeči klíčem organizace, druhá vrstva šifrování na serveru, přenos výhradně přes TLS. Tokeny Google OAuth jsou šifrované i při uložení.
- **Klíče:** hlavní klíč a další tajemství v Google Secret Manager s omezeným přístupem, rotace klíčů bez výpadku, klíče nejsou v kódu ani v databázi.
- **Přístup:** přihlášení přes Google včetně dvoufázového ověření organizace, krátkodobé přístupové tokeny (15 minut) s rotací obnovovacích tokenů, okamžité ukončení relací při signálu Googlu o napadení nebo deaktivaci účtu, role a skupiny, striktní oddělení organizací při každém požadavku.
- **Přehled:** auditní log zobrazení, vyplnění, úprav a sdílení dostupný administrátorům; provozní logy se uchovávají 30 dní.
- **Infrastruktura:** hosting, databáze a zálohy v EU (Google Cloud, europe-west1), denní zálohy databáze s uchováním 7 dní, služební účty s minimálními oprávněními, restriktivní Content Security Policy a bezpečnostní hlavičky, omezení počtu požadavků.
- **Kontrola úniků hesel:** přes Have I Been Pwned s k-anonymitou. Prohlížeč odešle jen prvních 5 znaků otisku hesla, žádné osobní údaje, proto HIBP není subzpracovatel.
- **Organizační opatření:** mlčenlivost osob s přístupem.