

Auftragsverarbeitungsvertrag (AVV)

Version 1.0, gültig ab 7. Oktober 2026

1. Parteien und Gegenstand

Auftragsverarbeiter ist Ing. Jiří Psota, Identifikationsnummer (IČO) 76072266, mit Sitz in Zborovská 1200/6, 150 00 Praha 5 - Smíchov, Tschechische Republik (der „Auftragsverarbeiter“). Verantwortlicher ist die Organisation, die den Dienst Vaultiqo gemäß den [AGB](#) nutzt (der „Kunde“).

Dieser Vertrag regelt die Verarbeitung personenbezogener Daten, die der Kunde in den Dienst einbringt, gemäß Artikel 28 der Verordnung (EU) 2016/679 (DSGVO). Er ist fester Bestandteil der AGB, und der Kunde nimmt ihn mit der Annahme der AGB an. Eine handschriftliche Unterschrift ist nicht erforderlich (Artikel 28 Absatz 9 DSGVO). In Fragen des Schutzes personenbezogener Daten hat dieser Vertrag Vorrang vor den AGB.

2. Umfang

Gegenstand, Art und Zweck der Verarbeitung sowie die Kategorien von Daten und betroffenen Personen sind in Anlage 1 beschrieben. Die Verarbeitung dauert so lange, wie der Dienst genutzt wird, und bis zur Löschung nach Abschnitt 9.

3. Weisungen

Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Kunden. Diese sind die AGB, dieser Vertrag sowie die Konfiguration und Nutzung des Dienstes durch den Kunden. Im Übrigen nur, soweit das Recht der EU oder der Tschechischen Republik dies verlangt; der Auftragsverarbeiter teilt dem Kunden eine solche Verpflichtung vorab mit, sofern das Recht dies nicht verbietet. Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung rechtswidrig ist, informiert er den Kunden unverzüglich.

4. Vertraulichkeit

Personen mit Zugang zu personenbezogenen Daten sind vertraglich oder gesetzlich zur Vertraulichkeit verpflichtet, auch nach Ende der Zusammenarbeit.

5. Sicherheit

Der Auftragsverarbeiter trifft die in Anlage 2 aufgeführten Maßnahmen nach Artikel 32 DSGVO. Er darf sie ändern, sofern das Schutzniveau nicht sinkt.

6. Unterauftragsverarbeiter

Der Kunde erteilt eine allgemeine Genehmigung zur Inanspruchnahme der unter www.vaultiqo.app/subprocessors aufgeführten Unterauftragsverarbeiter. Der Auftragsverarbeiter veröffentlicht beabsichtigte Änderungen vorab auf dieser Seite. Der Kunde kann unter hello@vaultiqo.app Einspruch erheben und, falls sich die Parteien nicht einigen, den Dienst kündigen. Der Auftragsverarbeiter erlegt seinen Unterauftragsverarbeitern dieselben Datenschutzpflichten auf und haftet weiterhin für deren Erfüllung.

7. Übermittlungen außerhalb des EWR

Personenbezogene Daten werden in der EU gespeichert (Google Cloud, Region europe-west1, Belgien). Sie werden nur in dem in der Liste der Unterauftragsverarbeiter angegebenen Umfang und nur mit einer Garantie nach Kapitel V DSGVO außerhalb des EWR übermittelt: einem Angemessenheitsbeschluss (einschließlich des EU-US Data Privacy Framework) oder Standardvertragsklauseln.

8. Unterstützung

Der Auftragsverarbeiter unterstützt den Kunden in angemessenem Umfang bei der Bearbeitung von Anträgen betroffener Personen und bei der Erfüllung seiner Pflichten nach den Artikeln 32 bis 36 DSGVO. Der Kunde bearbeitet, exportiert und löscht Daten selbst mit den Funktionen des Dienstes. Der Auftragsverarbeiter meldet dem Kunden eine Verletzung des Schutzes personenbezogener Daten unverzüglich, nachdem sie ihm bekannt geworden ist.

9. Beendigung und Löschung

Bis zum Ende des Dienstes kann der Kunde seine Daten exportieren. Nach Ende des Dienstes löscht der Auftragsverarbeiter die personenbezogenen Daten, sofern nicht eine gesetzliche Pflicht zur Aufbewahrung besteht (zum Beispiel Buchhaltungsunterlagen). Kopien in Backups verfallen mit der Rotation der Backups.

10. Informationen und Audits

Auf Anfrage stellt der Auftragsverarbeiter die Informationen bereit, die zum Nachweis der Einhaltung dieses Vertrags erforderlich sind, und ermöglicht Audits in angemessenem Umfang, nach vorheriger Absprache und auf Kosten des Kunden. Bei Unterauftragsverarbeitern ersetzen deren öffentliche Zertifizierungen und Berichte ein Audit.

11. Schlussbestimmungen

Die Haftung richtet sich nach Artikel 82 DSGVO und den AGB. Dieser Vertrag unterliegt dem Recht der Tschechischen Republik. Die aktuelle Fassung ist stets unter www.vaultiqo.app/dpa abrufbar; eine Änderung darf das Schutzniveau personenbezogener Daten nicht senken. Bei Abweichungen zwischen den Sprachfassungen ist die tschechische Fassung maßgeblich.

Kontakt für Datenschutz: hello@vaultiqo.app.

Anlage 1: Beschreibung der Verarbeitung

Zweck	Speichern und Teilen der Passwörter und anderer sensibler Daten des Teams des Kunden, Verwaltung des Zugriffs nach Benutzern und Gruppen aus Google Workspace sowie Führen eines Audit-Protokolls über die Nutzung.
Art der Verarbeitung	Speicherung, Verschlüsselung, Anzeige für berechtigte Benutzer, Teilen, Synchronisierung von Benutzern und Gruppen aus Google Workspace (von einem Administrator gestartet), Sicherung, Export und Löschung.
Betroffene Personen	Die Benutzer des Kunden (Beschäftigte und Mitarbeitende) sowie Personen, deren Daten der Kunde im Tresor speichert.
Kategorien von Daten	- Benutzeridentität von Google: Name, E-Mail, Profilfoto; Rollen und Gruppenmitgliedschaften. - Tresorinhalt: Passwörter, Notizen, andere sensible Felder und Anhänge (verschlüsselt) sowie Name des Eintrags, Benutzername, Website-Adresse, Tags und Ablaufdatum (unverschlüsselte Metadaten). - Audit-Protokoll: wer was wann getan hat (E-Mail des Benutzers, Aktion, Eintrag). IP-Adressen werden nicht gespeichert. - Anmeldesitzungen und, wenn ein Administrator die Verzeichnissynchronisierung aktiviert, verschlüsselte Google-OAuth-Tokens.

Zugriff des Auftragsverarbeiters auf Inhalte	Sensible Felder werden im Browser mit dem Schlüssel der Organisation und auf dem Server erneut mit einem Hauptschlüssel verschlüsselt. Die Schlüssel werden verwaltet, daher ist der Team-Tresor nicht Zero-Knowledge: Der Auftragsverarbeiter ist technisch in der Lage, die Inhalte zu entschlüsseln, der Zugang zu den Schlüsseln ist jedoch streng beschränkt und die Inhalte werden nicht gelesen. Nur öffentliche Freigabelinks sind vollständig Zero-Knowledge.
Besondere Kategorien von Daten	Werden nicht gezielt verarbeitet. Speichert der Kunde sie im Tresor, sind sie wie alle anderen Inhalte geschützt.
Dauer	So lange, wie der Dienst genutzt wird, danach Löschung nach Abschnitt 9.

Anlage 2: Technische und organisatorische Maßnahmen

- **Verschlüsselung:** sensible Felder werden im Browser mit AES-256-GCM unter Verwendung des Schlüssels der Organisation verschlüsselt, eine zweite Verschlüsselungsebene auf dem Server, Übertragung ausschließlich über TLS. Google-OAuth-Tokens werden im Ruhezustand verschlüsselt.
- **Schlüssel:** Hauptschlüssel und andere Geheimnisse in Google Secret Manager mit beschränktem Zugriff, Schlüsselrotation ohne Ausfallzeit, keine Schlüssel im Code oder in der Datenbank.
- **Zugriff:** Anmeldung mit Google einschließlich der Bestätigung in zwei Schritten der Organisation, kurzlebige Zugriffstokens (15 Minuten) mit Rotation der Aktualisierungstokens, sofortige Beendigung von Sitzungen, wenn Google ein kompromittiertes oder deaktiviertes Konto meldet, Rollen und Gruppen, strikte Mandantentrennung bei jeder Anfrage.
- **Nachvollziehbarkeit:** ein Audit-Protokoll über Anzeigen, automatisches Ausfüllen, Änderungen und Freigaben für Administratoren; Betriebsprotokolle werden 30 Tage aufbewahrt.
- **Infrastruktur:** Hosting, Datenbank und Backups in der EU (Google Cloud, europe-west1), tägliche Datenbank-Backups mit einer Aufbewahrung von 7 Tagen, Dienstkonten nach dem Prinzip der minimalen Rechte, eine restriktive Content Security Policy und Sicherheits-Header, Ratenbegrenzung.
- **Prüfung auf kompromittierte Passwörter:** über Have I Been Pwned mit k-Anonymität. Der Browser sendet nur die ersten 5 Zeichen eines Passwort-Hashes und keine personenbezogenen Daten, daher ist HIBP kein Unterauftragsverarbeiter.
- **Organisatorische Maßnahmen:** Vertraulichkeit der Personen mit Zugang.