

Accord de traitement des données (DPA)

Version 1.0, en vigueur à compter du 7 octobre 2026

1. Parties et objet

Le sous-traitant est Ing. Jiří Psota, numéro d'identification (IČO) 76072266, domicilié Zborovská 1200/6, 150 00 Praha 5 - Smíchov, République tchèque (le « sous-traitant »). Le responsable du traitement est l'organisation qui utilise le service Vaultiqo conformément aux [Conditions Générales](#) (le « client »).

Le présent accord régit le traitement des données à caractère personnel que le client introduit dans le service, conformément à l'article 28 du règlement (UE) 2016/679 (RGPD). Il fait partie intégrante des Conditions Générales et le client l'accepte en acceptant celles-ci. Aucune signature manuscrite n'est requise (article 28, paragraphe 9, du RGPD). En matière de protection des données à caractère personnel, le présent accord prévaut sur les Conditions Générales.

2. Champ d'application

L'objet, la nature et la finalité du traitement ainsi que les catégories de données et de personnes concernées sont décrits à l'annexe 1. Le traitement dure aussi longtemps que le service est utilisé et jusqu'à la suppression prévue à la section 9.

3. Instructions

Le sous-traitant ne traite les données à caractère personnel que sur instruction documentée du client. Ces instructions sont les Conditions Générales, le présent accord ainsi que la configuration et l'utilisation du service par le client. Autrement, uniquement si le droit de l'Union ou le droit tchèque l'exige ; le sous-traitant informe le client de cette obligation au préalable, sauf si la loi l'interdit. Si le sous-traitant considère qu'une instruction est illicite, il en informe le client sans délai.

4. Confidentialité

Les personnes ayant accès aux données à caractère personnel sont tenues à la confidentialité, par contrat ou en vertu de la loi, y compris après la fin de la collaboration.

5. Sécurité

Le sous-traitant prend les mesures prévues à l'article 32 du RGPD, énumérées à l'annexe 2. Il peut les modifier à condition que le niveau de protection ne diminue pas.

6. Sous-traitants ultérieurs

Le client donne une autorisation générale pour le recours aux sous-traitants ultérieurs figurant sur la page www.vaultiqo.app/subprocessors. Le sous-traitant publie à l'avance sur cette page les changements prévus. Le client peut formuler une objection à l'adresse hello@vaultiqo.app et, si les parties ne parviennent pas à un accord, peut résilier le service. Le sous-traitant impose les mêmes obligations en matière de protection des données à ses sous-traitants ultérieurs et demeure responsable de l'exécution de leurs obligations.

7. Transferts hors de l'EEE

Les données à caractère personnel sont stockées dans l'UE (Google Cloud, région europe-west1, Belgique). Elles ne sont transférées hors de l'EEE que dans la mesure indiquée dans la liste des sous-traitants ultérieurs et uniquement moyennant une garantie prévue au chapitre V du RGPD : une décision d'adéquation (y compris le cadre de protection des données UE-États-Unis, EU-US Data Privacy Framework) ou des clauses contractuelles types.

8. Assistance

Le sous-traitant aide raisonnablement le client à traiter les demandes des personnes concernées et à respecter ses obligations au titre des articles 32 à 36 du RGPD. Le client modifie, exporte et supprime lui-même les données au moyen des fonctions du service. Le sous-traitant notifie au client toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.

9. Fin du service et suppression

Jusqu'à la fin du service, le client peut exporter ses données. Après la fin du service, le sous-traitant supprime les données à caractère personnel, sauf si la loi impose leur conservation (par exemple les pièces comptables). Les copies contenues dans les sauvegardes expirent au fil de la rotation des sauvegardes.

10. Informations et audits

Sur demande, le sous-traitant fournit les informations nécessaires pour démontrer le respect du présent accord et permet la réalisation d'audits dans une mesure raisonnable, après accord préalable et aux frais du client. Pour les sous-traitants ultérieurs, leurs certifications et rapports publics remplacent un audit.

11. Dispositions finales

La responsabilité est régie par l'article 82 du RGPD et par les Conditions Générales. Le présent accord est régi par le droit de la République tchèque. La version en vigueur est toujours disponible à l'adresse www.vaultiqo.app/dpa ; une modification ne doit pas réduire le niveau de protection des données à caractère personnel. En cas de divergence entre les versions linguistiques, la version tchèque prévaut.

Contact pour la protection des données : hello@vaultiqo.app.

Annexe 1 : Description du traitement

Finalité	Stockage et partage des mots de passe et autres données sensibles de l'équipe du client, gestion des accès par utilisateurs et groupes issus de Google Workspace, et tenue d'un journal d'audit de l'utilisation.
Nature du traitement	Stockage, chiffrement, affichage aux utilisateurs autorisés, partage, synchronisation des utilisateurs et des groupes depuis Google Workspace (lancée par un administrateur), sauvegarde, export et suppression.
Personnes concernées	Les utilisateurs du client (salariés et collaborateurs) et les personnes dont le client stocke les données dans le coffre-fort.
Catégories de données	• Identité de l'utilisateur provenant de Google : nom, adresse e-mail, photo de profil ; rôles et appartenance à des groupes. • Contenu du coffre-fort : mots de passe, notes, autres champs sensibles et pièces jointes (chiffrés), ainsi que nom de l'élément, nom d'utilisateur, adresse du site web, étiquettes et date d'expiration (métadonnées non chiffrées). • Journal d'audit : qui a fait quoi et quand (adresse e-mail de l'utilisateur, action, élément). Les adresses IP ne sont pas conservées. • Sessions de connexion et, si un administrateur active la synchronisation de l'annuaire, jetons OAuth Google chiffrés.

Accès du sous-traitant au contenu	Les champs sensibles sont chiffrés dans le navigateur avec la clé de l'organisation, puis à nouveau sur le serveur avec une clé maîtresse. Les clés sont gérées par le service, le coffre-fort de l'équipe n'est donc pas à divulgation nulle de connaissance (zero-knowledge) : le sous-traitant est techniquement en mesure de déchiffrer le contenu, mais l'accès aux clés est strictement restreint et le contenu n'est pas consulté. Seuls les liens de partage publics sont entièrement zero-knowledge.
Catégories particulières de données	Non traitées intentionnellement. Si le client les stocke dans le coffre-fort, elles sont protégées comme tout autre contenu.
Durée	Aussi longtemps que le service est utilisé, puis suppression conformément à la section 9.

Annexe 2 : Mesures techniques et organisationnelles

- **Chiffrement** : champs sensibles chiffrés en AES-256-GCM dans le navigateur avec la clé de l'organisation, seconde couche de chiffrement sur le serveur, transport exclusivement via TLS. Les jetons OAuth Google sont chiffrés au repos.
- **Clés** : clé maîtresse et autres secrets dans Google Secret Manager avec accès restreint, rotation des clés sans interruption de service, aucune clé dans le code ni dans la base de données.
- **Accès** : connexion avec Google, y compris la validation en deux étapes de l'organisation, jetons d'accès de courte durée (15 minutes) avec rotation des jetons d'actualisation, fin immédiate des sessions lorsque Google signale un compte compromis ou désactivé, rôles et groupes, isolation stricte des clients (tenants) à chaque requête.
- **Visibilité** : journal d'audit des consultations, remplissages automatiques, modifications et partages pour les administrateurs ; les journaux d'exploitation sont conservés 30 jours.
- **Infrastructure** : hébergement, base de données et sauvegardes dans l'UE (Google Cloud, europe-west1), sauvegardes quotidiennes de la base de données conservées 7 jours, comptes de service selon le principe du moindre privilège, politique de sécurité du contenu (Content Security Policy) restrictive et en-têtes de sécurité, limitation du débit des requêtes.
- **Vérification des mots de passe compromis** : via Have I Been Pwned avec k-anonymat. Le navigateur n'envoie que les 5 premiers caractères de l'empreinte (hash) d'un mot de passe et aucune donnée à caractère personnel ; HIBP n'est donc pas un sous-traitant ultérieur.
- **Mesures organisationnelles** : confidentialité des personnes ayant accès.