

Umowa powierzenia przetwarzania danych (DPA)

Wersja 1.0, obowiązuje od 7 października 2026 r.

1. Strony i przedmiot

Podmiotem przetwarzającym jest Ing. Jiří Psota, numer identyfikacyjny przedsiębiorcy (IČO) 76072266, z siedzibą pod adresem Zborovská 1200/6, 150 00 Praha 5 - Smíchov, Republika Czeska („podmiot przetwarzający”). Administratorem jest organizacja, która korzysta z usługi Vaultiqo na podstawie [Regulaminu](#) („klient”).

Niniejsza umowa reguluje przetwarzanie danych osobowych, które klient umieszcza w usłudze, zgodnie z art. 28 rozporządzenia (UE) 2016/679 (RODO). Stanowi integralną część Regulaminu, a klient akceptuje ją poprzez akceptację Regulaminu. Własnoręczny podpis nie jest wymagany (art. 28 ust. 9 RODO). W sprawach ochrony danych osobowych niniejsza umowa ma pierwszeństwo przed Regulaminem.

2. Zakres

Przedmiot, charakter i cel przetwarzania oraz kategorie danych i osób, których dane dotyczą, opisano w Załączniku 1. Przetwarzanie trwa przez okres korzystania z usługi i do usunięcia danych zgodnie z pkt 9.

3. Polecenia

Podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie klienta. Poleceniami tymi są Regulamin, niniejsza umowa oraz konfiguracja usługi i sposób korzystania z niej przez klienta. W pozostałym zakresie wyłącznie wtedy, gdy wymaga tego prawo Unii lub prawo Republiki Czeskiej; o takim obowiązku podmiot przetwarzający informuje klienta z wyprzedzeniem, chyba że prawo tego zabrania. Jeżeli podmiot przetwarzający uzna polecenie za niezgodne z prawem, niezwłocznie informuje o tym klienta.

4. Poufność

Osoby mające dostęp do danych osobowych są zobowiązane do zachowania poufności na mocy umowy lub przepisów prawa, również po zakończeniu współpracy.

5. Bezpieczeństwo

Podmiot przetwarzający stosuje środki, o których mowa w art. 32 RODO, wymienione w Załączniku 2. Może je zmieniać, o ile poziom ochrony nie ulegnie obniżeniu.

6. Dalsze podmioty przetwarzające

Klient udziela ogólnej zgody na korzystanie z usług dalszych podmiotów przetwarzających wymienionych na stronie www.vaultiqo.app/subprocessors. Podmiot przetwarzający z wyprzedzeniem publikuje na tej stronie planowane zmiany. Klient może wnieść sprzeciw pod adresem hello@vaultiqo.app, a jeżeli strony nie dojdą do porozumienia, może wypowiedzieć usługę. Podmiot przetwarzający nakłada na dalsze podmioty przetwarzające te same obowiązki w zakresie ochrony danych i pozostaje odpowiedzialny za wypełnianie przez nie tych obowiązków.

7. Przekazywanie danych poza EOG

Dane osobowe są przechowywane w UE (Google Cloud, region europe-west1, Belgia). Są przekazywane poza EOG wyłącznie w zakresie wskazanym w wykazie dalszych podmiotów przetwarzających i wyłącznie przy zastosowaniu zabezpieczenia przewidzianego w rozdziale V RODO: decyzji stwierdzającej odpowiedni stopień ochrony (w tym ram ochrony danych UE-USA, EU-US Data Privacy Framework) lub standardowych klauzul umownych.

8. Pomoc

Podmiot przetwarzający w rozsądnym zakresie pomaga klientowi w realizacji żądań osób, których dane dotyczą, oraz w wywiązywaniu się z obowiązków określonych w art. 32 do 36 RODO. Klient samodzielnie edytuje, eksportuje i usuwa dane za pomocą funkcji usługi. Podmiot przetwarzający zgłasza klientowi naruszenie ochrony danych osobowych bez zbędnej zwłoki po jego stwierdzeniu.

9. Zakończenie i usunięcie danych

Do czasu zakończenia świadczenia usługi klient może wyeksportować swoje dane. Po zakończeniu świadczenia usługi podmiot przetwarzający usuwa dane osobowe, chyba że przepisy prawa wymagają ich przechowywania (na przykład dokumentacji księgowej). Kopie w kopiach zapasowych wygasają wraz z rotacją kopii zapasowych.

10. Informacje i audyty

Na żądanie podmiot przetwarzający udostępnia informacje niezbędne do wykazania przestrzegania niniejszej umowy i umożliwia przeprowadzanie audytów w rozsądnym zakresie, po uprzednim uzgodnieniu i na koszt klienta. W przypadku dalszych podmiotów przetwarzających audyt zastępują ich publicznie dostępne certyfikaty i raporty.

11. Postanowienia końcowe

Odpowiedzialność reguluje art. 82 RODO oraz Regulamin. Niniejsza umowa podlega prawu Republiki Czeskiej. Aktualna wersja jest zawsze dostępna pod adresem www.vaultiqo.app/dpa; zmiana nie może obniżyć poziomu ochrony danych osobowych. W razie jakichkolwiek rozbieżności między wersjami językowymi rozstrzygająca jest wersja czeska.

Kontakt w sprawach ochrony danych: hello@vaultiqo.app.

Załącznik 1: Opis przetwarzania

Cel	Przechowywanie i udostępnianie haseł oraz innych poufnych danych zespołu klienta, zarządzanie dostępem użytkowników i grup z Google Workspace oraz prowadzenie rejestru audytowego korzystania z usługi.
Charakter przetwarzania	Przechowywanie, szyfrowanie, wyświetlanie uprawnionym użytkownikom, udostępnianie, synchronizacja użytkowników i grup z Google Workspace (uruchamiana przez administratora), tworzenie kopii zapasowych, eksport i usuwanie.
Osoby, których dane dotyczą	Użytkownicy klienta (pracownicy i współpracownicy) oraz osoby, których dane klient przechowuje w sejfie.
Kategorie danych	- Tożsamość użytkownika z Google: imię i nazwisko, adres e-mail, zdjęcie profilowe; role i przynależność do grup. - Zawartość sejfu: hasła, notatki, inne poufne pola i załączniki (zaszyfrowane), a także nazwa elementu, nazwa użytkownika, adres strony internetowej, tagi i data wygaśnięcia (niezaszyfrowane metadane). - Dziennik audytu: kto, co i kiedy zrobił (adres e-mail użytkownika, czynność, element). Adresy IP nie są przechowywane. - Sesje logowania oraz, jeżeli administrator włączy synchronizację katalogu, zaszyfrowane tokeny Google OAuth.

Dostęp podmiotu przetwarzającego do treści	Poufne pola są szyfrowane w przeglądarce kluczem organizacji, a następnie ponownie na serwerze kluczem głównym. Klucze są zarządzane, dlatego sejf zespołowy nie działa w modelu zero-knowledge: podmiot przetwarzający ma techniczną możliwość odszyfrowania treści, jednak dostęp do kluczy jest ściśle ograniczony, a treść nie jest odczytywana. W pełni w modelu zero-knowledge działają wyłącznie publiczne linki udostępniania.
Szczególne kategorie danych	Nie są przetwarzane celowo. Jeżeli klient przechowuje je w sejfie, są chronione tak samo jak wszystkie pozostałe treści.
Czas trwania	Przez okres korzystania z usługi, a następnie usunięcie zgodnie z pkt 9.

Załącznik 2: Środki techniczne i organizacyjne

- **Szyfrowanie:** poufne pola szyfrowane algorytmem AES-256-GCM w przeglądarce kluczem organizacji, druga warstwa szyfrowania na serwerze, transmisja wyłącznie przez TLS. Tokeny Google OAuth są przechowywane w postaci zaszyfrowanej.
- **Klucze:** klucz główny i inne sekrety w Google Secret Manager z ograniczonym dostępem, rotacja kluczy bez przerw w działaniu, brak kluczy w kodzie i w bazie danych.
- **Dostęp:** logowanie przez Google z uwzględnieniem weryfikacji dwuetapowej organizacji, krótkotrwałe tokeny dostępu (15 minut) z rotacją tokenów odświeżania, natychmiastowe zakończenie sesji, gdy Google zgłosi przejęte lub wyłączone konto, role i grupy, ścisła izolacja klientów przy każdym żądaniu.
- **Przejrzystość:** dziennik audytu wyświetleń, autouzupełnień, edycji i udostępnień dla administratorów; logi operacyjne są przechowywane przez 30 dni.
- **Infrastruktura:** hosting, baza danych i kopie zapasowe w UE (Google Cloud, europe-west1), codzienne kopie zapasowe bazy danych przechowywane przez 7 dni, konta usługowe z minimalnymi uprawnieniami, restrykcyjna polityka Content Security Policy i nagłówki bezpieczeństwa, ograniczanie liczby żądań.
- **Sprawdzanie wyciekłych haseł:** za pośrednictwem Have I Been Pwned z zastosowaniem k-anonimowości. Przeglądarka wysyła wyłącznie pierwsze 5 znaków skrótu hasła i żadnych danych osobowych, dlatego HIBP nie jest dalszym podmiotem przetwarzającym.
- **Środki organizacyjne:** zobowiązanie osób mających dostęp do zachowania poufności.