

Acuerdo de tratamiento de datos (DPA)

Versión 1.0, vigente desde el 7 de octubre de 2026

1. Partes y objeto

El encargado del tratamiento es Ing. Jiří Psota, número de identificación de empresa (IČO) 76072266, con domicilio en Zborovská 1200/6, 150 00 Praha 5 - Smíchov, República Checa (el «encargado»). El responsable del tratamiento es la organización que utiliza el servicio Vaultiqo conforme a los [Términos](#) (el «cliente»).

Este acuerdo regula el tratamiento de los datos personales que el cliente introduce en el servicio, de conformidad con el artículo 28 del Reglamento (UE) 2016/679 (RGPD). Forma parte integrante de los Términos y el cliente lo acepta al aceptar estos. No se requiere firma manuscrita (artículo 28, apartado 9, del RGPD). En materia de protección de datos personales, este acuerdo prevalece sobre los Términos.

2. Alcance

El objeto, la naturaleza y la finalidad del tratamiento, así como las categorías de datos y de interesados, se describen en el anexo 1. El tratamiento dura mientras se utilice el servicio y hasta la supresión conforme a la cláusula 9.

3. Instrucciones

El encargado trata los datos personales únicamente siguiendo instrucciones documentadas del cliente. Estas son los Términos, este acuerdo y la configuración y el uso del servicio por parte del cliente. En otros casos, solo cuando lo exija el Derecho de la Unión o el Derecho checo; el encargado informará previamente al cliente de dicha exigencia, salvo que la ley lo prohíba. Si el encargado considera que una instrucción es ilícita, lo comunicará al cliente sin dilación.

4. Confidencialidad

Las personas con acceso a los datos personales están sujetas a una obligación de confidencialidad, contractual o legal, también después de finalizar la colaboración.

5. Seguridad

El encargado aplica las medidas previstas en el artículo 32 del RGPD que se enumeran en el anexo 2. Puede modificarlas siempre que no disminuya el nivel de protección.

6. Subencargados del tratamiento

El cliente otorga una autorización general para recurrir a los subencargados del tratamiento enumerados en www.vaultiqo.app/subprocessors. El encargado publica en dicha página, con antelación, los cambios previstos. El cliente puede oponerse a través de hello@vaultiqo.app y, si las partes no llegan a un acuerdo, puede dar por terminado el servicio. El encargado impone a sus subencargados las mismas obligaciones de protección de datos y sigue siendo responsable de su cumplimiento.

7. Transferencias fuera del EEE

Los datos personales se almacenan en la UE (Google Cloud, región europe-west1, Bélgica). Solo se transfieren fuera del EEE en la medida indicada en la lista de subencargados y únicamente con una garantía conforme al capítulo V del RGPD: una decisión de adecuación (incluido el Marco de Privacidad de Datos UE-EE. UU.) o cláusulas contractuales tipo.

8. Asistencia

El encargado asiste razonablemente al cliente en la atención de las solicitudes de los interesados y en el cumplimiento de sus obligaciones con arreglo a los artículos 32 a 36 del RGPD. El cliente modifica, exporta y suprime los datos por sí mismo mediante las funciones del servicio. El encargado notifica al cliente cualquier violación de la seguridad de los datos personales sin dilación indebida tras tener conocimiento de ella.

9. Terminación y supresión

Hasta que finalice el servicio, el cliente puede exportar sus datos. Una vez finalizado el servicio, el encargado suprime los datos personales, salvo que la ley exija conservarlos (por ejemplo, los registros contables). Las copias en las copias de seguridad caducan a medida que estas se rotan.

10. Información y auditorías

A petición del cliente, el encargado facilita la información necesaria para demostrar el cumplimiento de este acuerdo y permite auditorías en una medida razonable, previo acuerdo y a cargo del cliente. En el caso de los subencargados, sus certificaciones e informes públicos sustituyen a la auditoría.

11. Disposiciones finales

La responsabilidad se rige por el artículo 82 del RGPD y por los Términos. Este acuerdo se rige por el Derecho de la República Checa. La versión vigente está siempre disponible en www.vaultiqo.app/dpa; ninguna modificación podrá reducir el nivel de protección de los datos personales. En caso de discrepancia entre las versiones lingüísticas, prevalecerá la versión checa.

Contacto para la protección de datos: hello@vaultiqo.app.

Anexo 1: Descripción del tratamiento

Finalidad	Almacenar y compartir las contraseñas y otros datos sensibles del equipo del cliente, gestionar el acceso de usuarios y grupos procedentes de Google Workspace y mantener un registro de auditoría del uso.
Naturaleza del tratamiento	Almacenamiento, cifrado, visualización por usuarios autorizados, compartición, sincronización de usuarios y grupos desde Google Workspace (iniciada por un administrador), copia de seguridad, exportación y supresión.
Interesados	Los usuarios del cliente (empleados y colaboradores) y las personas cuyos datos el cliente almacena en la bóveda.
Categorías de datos	- Identidad del usuario procedente de Google: nombre, correo electrónico, foto de perfil; funciones y pertenencia a grupos. - Contenido de la bóveda: contraseñas, notas, otros campos sensibles y archivos adjuntos (cifrados), además del nombre del elemento, el nombre de usuario, la dirección del sitio web, las etiquetas y la fecha de caducidad (metadatos sin cifrar). - Registro de auditoría: quién hizo qué y cuándo (correo electrónico del usuario, acción, elemento). No se almacenan direcciones IP. - Sesiones de inicio de sesión y, si un administrador activa la sincronización del directorio, tokens OAuth de Google cifrados.

Acceso del encargado al contenido	Los campos sensibles se cifran en el navegador con la clave de la organización y de nuevo en el servidor con una clave maestra. Las claves son gestionadas, por lo que la bóveda del equipo no es de conocimiento cero (zero-knowledge): el encargado tiene la capacidad técnica de descifrar el contenido, pero el acceso a las claves está estrictamente restringido y el contenido no se lee. Solo los enlaces públicos para compartir son totalmente de conocimiento cero.
Categorías especiales de datos	No se tratan de forma intencionada. Si el cliente las almacena en la bóveda, se protegen como el resto del contenido.
Duración	Mientras se utilice el servicio y, después, supresión conforme a la cláusula 9.

Anexo 2: Medidas técnicas y organizativas

- **Cifrado:** campos sensibles cifrados con AES-256-GCM en el navegador mediante la clave de la organización, una segunda capa de cifrado en el servidor, transmisión exclusivamente a través de TLS. Los tokens OAuth de Google se cifran en reposo.
- **Claves:** la clave maestra y otros secretos se guardan en Google Secret Manager con acceso restringido, rotación de claves sin interrupción del servicio, sin claves en el código ni en la base de datos.
- **Acceso:** inicio de sesión con Google, incluida la verificación en dos pasos de la organización, tokens de acceso de corta duración (15 minutos) con rotación de los tokens de actualización, cierre inmediato de las sesiones cuando Google notifica una cuenta comprometida o desactivada, funciones y grupos, aislamiento estricto entre clientes (tenants) en cada solicitud.
- **Trazabilidad:** registro de auditoría de visualizaciones, autocompletados, modificaciones y comparticiones para los administradores; los registros operativos se conservan durante 30 días.
- **Infraestructura:** alojamiento, base de datos y copias de seguridad en la UE (Google Cloud, europe-west1), copias de seguridad diarias de la base de datos conservadas durante 7 días, cuentas de servicio con privilegios mínimos, una Content Security Policy restrictiva y cabeceras de seguridad, limitación de la frecuencia de solicitudes.
- **Comprobación de contraseñas filtradas:** a través de Have I Been Pwned con k-anonimato. El navegador envía únicamente los 5 primeros caracteres del hash de una contraseña y ningún dato personal, por lo que HIBP no es un subencargado del tratamiento.
- **Medidas organizativas:** confidencialidad de las personas con acceso.