HEELONYS
Conseil Digital & IA Santé

# Registre des activités de traitement
(RGPD Art 30)

Document d'accompagnement pour le Responsable de Traitement

**Éditeur : HEELONYS | Logiciel : HeelonVault**

---

| | | | |
|---|---|---|---|
| Nom | HeelonVault_Registre_activités-traitement_Heelonys_2026 | Référence | RGP-HEELONYS-V1.0 |
| Date création | 07/04/2026 | Date dernière révision | 07/04/2026 |
| Version | 1.0 | Responsable | PPA |
| Diffusion | Publique | Approuvé par | PPA |

Cette fiche technique détaille les éléments nécessaires à l'inscription de l'outil HeelonVault dans votre registre interne des activités de traitement.

### 1. Identification du Traitement

- **Nom du traitement :** Gestion des accès et sécurisation des secrets d'authentification.
- **Finalité principale :** Centraliser, chiffrer et contrôler l'accès aux identifiants, mots de passe et clés techniques de l'organisation.
- **Base légale :** Intérêt légitime de l'organisme (assurer la sécurité du système d'information et la confidentialité des accès).

### 2. Catégories de Données Personnelles

- **Données d'identification :** Nom, prénom et adresse e-mail professionnelle des utilisateurs du logiciel.
- **Données de connexion (Logs) :** Adresses IP, horodatage des tentatives de connexion et journal d'audit des actions sensibles.
- **Contenu chiffré :** Secrets stockés par les utilisateurs (mots de passe, document, token API, clé SSH), protégés par un chiffrement fort.

### 3. Destinataires et Transferts

- **Destinataires internes :** Seuls les utilisateurs habilités par le Responsable de Traitement ont accès à leurs propres coffres ou aux coffres partagés.
- **Destinataires externes :** Aucun.
- **Transfert hors UE :** Néant. Le stockage est réalisé exclusivement sur l'infrastructure du Client (On-Premise par défaut).

### 4. Mesures de Sécurité Techniques (Art. 32)

Le logiciel HeelonVault intègre nativement les mesures suivantes pour garantir l'intégrité et la confidentialité :

- **Chiffrement au repos :** Utilisation de l'algorithme AES-256-GCM.
- **Hachage des secrets :** Utilisation de Argon2id pour la protection des mots de passe maîtres contre les attaques par force brute.
- **Authentification :** Support natif du MFA/TOTP (Double authentification).
- **Architecture :** Principe du "Zero-Knowledge" ; l'éditeur (HEELONYS) n'a jamais accès aux clés de déchiffrement.

## 5. Durées de Conservation

- **Données d'utilisation :** Durée de présence du collaborateur dans l'organisation ou jusqu'à la suppression du compte par l'administrateur.
- **Logs techniques :** Durée recommandée de 1 an (selon les politiques internes de sécurité du Client), gérée via la rotation des logs du système hôte.

## 6. Exercice des Droits

- **Droit d'accès et de portabilité :** Fonctions d'exportation natives aux formats .hvb ou CSV.
- **Droit à l'effacement :** Fonction de suppression définitive des secrets et des comptes utilisateurs.

Pour plus de détails sur les engagements contractuels, veuillez vous référer au DPA-HEELONYS-V1.0