ACCORD SUR LE TRAITEMENT DES DONNÉES PERSONNELLES (DPA)

Éditeur : HEELONYS | Logiciel : HeelonGed

Entre : Le Client (ci-après le "Responsable de Traitement")

Et : L'Éditeur de la solution Heelonys (ci-après le "Sous-traitant")

Nom	HeelonGed_DPA_Heelonys_2026	Référence	DPA-HEELONYS-V1.0
Date création	05/05/2026	Date dernière révision	05/05/2026
Version	1.0	Responsable	PPA
Diffusion	Publique	Approuvé par	PPA

RÉSUMÉ DE CONFORMITÉ (À L'ATTENTION DU DPO)

Ce résumé facilite l'inscription de **HeelonGed** dans votre registre des activités de traitement (Art. 30 du RGPD).

Information	Détails pour votre Registre
Finalité principale	Gestion sécurisée, cycle de validation (workflow) et diffusion de la documentation légale et technique pour laboratoires de biologie médicale.
Type de données	Documents PDF (santé/légaux), adresses emails des contributeurs/DPO, hash d'intégrité SHA-256, logs d'audit (actions, horodatage, ID de requête).
Localisation des données	**Infrastructure du Client** (ou VPS dédié sous contrôle Client). Stockage localisé sur disque (/app/data/files) et base de données SQLite (ged.db)
Accès de l'Éditeur	Contrôlé par clé API : HEELONYS n'a accès qu'en cas de support technique. L'accès est protégé par des clés d'API hachées en SHA-256 (non stockées en clair).
Sécurité (Art. 32)	TLS via Caddy, authentification par header sécurisé, isolation par conteneur Podman, validation des fichiers PDF (magic bytes), protection contre le path traversal via UUID.
Droits des personnes	Fonction native de suppression définitive (DELETE) effaçant fichiers et versions. Traçabilité complète des modifications via la table.
Conformité NIS2	MFA obligatoire (via couche BFF), expiration automatique des clés d'API, journalisation exhaustive pour l'analyse d'incidents (X-Request-ID).

Note technique :
HeelonGed est conçu selon le principe de Data Protection by Design. Le système garantit l'immuabilité des documents publiés : une fois une version approuvée par le DPO, son hash SHA-256 est scellé, permettant de prouver l'intégrité du document à tout moment. La séparation des rôles (Contributeur vs DPO) assure qu'aucune modification ne peut être rendue publique sans une validation explicite et tracée.

1. Objet et Description du Traitement

Le Sous-traitant fournit une solution de Gestion Électronique de Documents (GED) nommée `heelonged-backend` version `1.0.3`.

- **Nature du traitement** : Stockage, horodatage et mise à disposition de documents légaux et de santé (notices RGPD, rapports d'audit, politiques NIS2).
- **Données traitées** : PDF de santé, identifiants des contributeurs (emails), logs d'audit (actions, timestamps, identité de l'acteur via le label de clé API).

2. Obligations du Sous-traitant

Le Sous-traitant s'engage à :

1. **Instruction** : Ne traiter les données que sur instruction documentée du Laboratoire.
2. **Confidentialité** : Garantir que le personnel autorisé à traiter les données est soumis à une obligation de confidentialité.
3. **Sécurité** : Mettre en œuvre les mesures techniques décrites à l'Article 3.

3. Mesures de Sécurité Techniques (Spécifications Heelonged)

Conformément à la documentation technique, la sécurité repose sur les piliers suivants :

- **Authentification Robuste** : Utilisation de clés d'API uniques transmises via le header `X-DPO-API-Key`. Les clés brutes ne sont jamais stockées ; seul leur condensat SHA-256 est conservé en base de données.
- **Chiffrement des Flux** : Utilisation obligatoire du protocole HTTPS avec terminaison TLS assurée par le serveur Caddy.
- **Isolation des Données** : Les fichiers PDF sont stockés sur le serveur avec des noms de fichiers générés (UUID), empêchant toute attaque par traversée de chemin (*path traversal*).
- **Intégrité** : Chaque version de document fait l'objet d'un calcul de hachage SHA-256 pour garantir l'intégrité des documents de santé déposés.
- **Disponibilité** : Procédures de sauvegarde régulières de la base SQLite (`ged.db`) et des fichiers PDF dans `/srv/heelonged-backend/backups/`.

4. Traçabilité et Audit (Accountability)

Le logiciel maintient un journal d'audit immuable (table `audit_logs`).

- Toute action (upload, soumission, approbation, suppression) est enregistrée avec l'identifiant de l'acteur (`owner`) et un `X-Request-ID` pour assurer la corrélation des logs.
- Le Responsable de Traitement peut exiger un rapport de conformité généré par le script `heelonged-backend-audit` pour vérifier l'état de sécurité du serveur.

5. Droits des Personnes Concernées

- **Droit à l'effacement** : Le Sous-traitant permet la suppression irréversible d'un document et de toutes ses versions via l'endpoint `DELETE /api/v1/dpo/docs/{slug}`.
- **Accès et Rectification** : Les versions successives (DRAFT, PENDING, PUBLISHED) permettent de maintenir une trace historique exacte des documents diffusés aux patients et praticiens.

6. LOCALISATION DES DONNÉES ET HÉBERGEMENT

Le Responsable de Traitement choisit le mode de déploiement de la solution **HeelonGed** parmi les options suivantes :

6.1. Option par défaut : Déploiement On-Premise (Local)

Par défaut, la solution est installée sur l'infrastructure propre du Laboratoire (serveurs internes).

- **Maîtrise totale** : Le Responsable de Traitement assure la maîtrise physique et logique du stockage. Les données (base SQLite ged.db et fichiers PDF dans /app/data/files) ne quittent jamais le réseau local du Laboratoire.
- **Responsabilité** : La maintenance de la machine hôte (Fedora/Podman) et la stratégie de sauvegarde incombent au Laboratoire, conformément au Runbook opérationnel fourni.

6.2. Option 2 : Hébergement Standard (Cloud Privé)

En cas d'externalisation sur un serveur dédié (VPS) :

- **Localisation** : Le Sous-traitant s'engage à ce que les données soient hébergées exclusivement sur le territoire de l'Union Européenne.
- **Isolation** : L'utilisation de Podman rootful garantit une isolation stricte de l'application vis-à-vis des autres services éventuels de l'hébergeur.

6.3. Option 3 : Hébergement de Données de Santé (HDS)

Si les documents déposés dans la GED contiennent des données de santé à caractère personnel (comptes-rendus d'examens, prescriptions nominatives) et sont hébergés par un tiers :

- **Certification** : L'hébergement doit impérativement être confié à un prestataire certifié **HDS** (Hébergeur de Données de Santé) conformément à l'article L.1111-8 du Code de la santé publique.
- **Conformité technique** : Le Sous-traitant garantit que les mécanismes de sécurité de **HeelonGed** (chiffrement TLS, hachage des clés API, logs d'audit) répondent aux exigences techniques du référentiel de certification HDS.

6.4. Flux de données

Quel que soit le mode d'hébergement, aucun transfert de données n'est réalisé vers des pays tiers hors UE ou vers des organisations internationales. Les seuls flux sortants sont les logs techniques et les téléchargements de documents initiés exclusivement par des utilisateurs autorisés.

7. Obligations du Laboratoire (Responsable de Traitement)

Le Laboratoire s'engage à :

1. Implémenter la couche **BFF (Backend For Frontend)** pour ne jamais exposer les clés d'API au navigateur.
2. Activer l'**Authentification à deux facteurs (MFA)** pour tous les accès DPO et contributeurs, conformément à l'Article 21 de la directive NIS2.
3. Définir une durée de vie limitée pour les clés d'API via le paramètre `expires_at`.

Points de vigilance pour votre secteur (Biologie Médicale) :

- **HDS (Hébergeur de Données de Santé)** : Si vous hébergez vous-même le VPS, assurez-vous que votre infrastructure est certifiée HDS, car les documents de votre GED pourraient contenir des données de santé à caractère personnel.
- **Journalisation** : Votre système enregistre l'email des contributeurs dans le champ `created_by`. Pensez à mentionner ce traitement dans votre registre de l'Article 30.

Contact Sécurité & RGPD : `securite@heelonys.fr`