HEELONYS
Conseil Digital & IA Santé

Registre des activités de traitement
(RGPD Art 30)

Document d'accompagnement pour le Responsable de Traitement

Éditeur : HEELONYS | Logiciel : HeelonGed

Nom	HeelonGed_Registre_activités-traitement_Heelonys_2026	Référence	GED-RAT-HEELONYS-V1.0
Date création	05/05/2026	Date dernière révision	05/05/2026
Version	1.0	Responsable	PPA
Diffusion	Publique	Approuvé par	PPA

À savoir :

- Ce document est une **maquette générique** pour les clients utilisant **HeelonGed** comme GED interne.
- **À personnaliser** : Complétez les sections entre crochets [ ] et adaptez les exemples à votre contexte.
- **Pour les laboratoires de biologie médicale** : Intégrez ce registre dans votre **Système de Management de la Qualité (SMQ)** et alignez-le avec les exigences **ISO 15189** (Section 4.1 - Management de la qualité).

Introduction

Contexte

Le **Règlement Général sur la Protection des Données (RGPD)** impose aux **responsables de traitement** (votre organisation) de tenir un **registre des activités de traitement** (Article 30). Ce registre permet de :

Documenter les traitements de données personnels effectués via **HeelonGed**.
Prouver la conformité en cas de contrôle par la **CNIL** ou d'audit (ex: COFRAC pour les laboratoires).
Faciliter la transparence envers les personnes concernées (ex: employés, patients).

Périmètre

Ce registre couvre les **traitements de données** liés à l'utilisation de **HeelonGed** pour :

- La **gestion électronique de documents** (ex: procédures qualité, résultats de laboratoire, contrats).
- La **traçabilité des actions** (logs d'audit).
- La **collaboration interne** (partage de documents entre services).

Exclusions :

- Ce registre **ne couvre pas** les traitements externes à HeelonGed (ex: logiciels RH, LIMS).
- Si vous utilisez d'autres outils en lien avec HeelonGed, **ajoutez-les dans un registre séparé**.

Rôles et Responsabilités

Rôle	Responsable	Description
Responsable de traitement	[Nom de votre organisation]	Détermine les **finalités** et les **moyens** du traitement (ex: utiliser HeelonGed pour gérer des documents qualité).
DPO	[Nom du DPO]	Supervise la conformité RGPD. Obligatoire si votre organisation traite des données sensibles à grande échelle.
Administrateur GED	[Nom de l'admin]	Gère les **accès**, les **sauvegardes** et la **sécurité** de HeelonGed.
Utilisateurs	[Liste des services concernés]	Utilisent HeelonGed pour **stocker, modifier ou consulter** des documents.

1. Description Générale des Traitements

1.1 Finalités du Traitement

HeelonGed est utilisé par votre organisation pour :

1. **Gérer des documents** :
    - Stockage, versionnage, archivage et suppression de documents (ex: procédures qualité, résultats de laboratoire, contrats).
2. **Assurer la traçabilité** :
    - Enregistrement des actions (création, modification, suppression) via des **logs d'audit**.
3. **Collaborer en interne** :
    - Partage de documents entre utilisateurs autorisés (avec gestion fine des droits).
4. **Se conformer aux normes** :
    - Répondre aux exigences **ISO 15189** (laboratoires), **ISO 27001** (sécurité), ou autres.

1.2 Catégories de Données Traitées

Important :

- Si vous stockez des **données de santé** (ex: résultats de laboratoire), assurez-vous qu'elles sont **anonymisées, pseudonymisées** ou que votre hébergement est **certifié HDS**.
- Les **données personnelles** (ex: noms, emails) doivent être traitées conformément au RGPD.

Catégorie	Exemples	Base Légale (RGPD)	Sensibilité
Données d'identification	Noms/prénoms des utilisateurs, adresses email, postes.	**Art. 6(1)(b)** (exécution d'un contrat)	Moyenne
Données techniques	Logs d'audit (IP, timestamp, actions), métadonnées des fichiers (nom, taille, hash).	**Art. 6(1)(f)** (intérêt légitime)	Faible
Données de connexion	Identifiants, mots de passe (chiffrés), clés API.	**Art. 6(1)(b)**	Élevée
Données de santé	Résultats de laboratoire, dossiers patients (si stockés **non anonymisés**).	**Art. 9(2)(h)** (santé publique) + **HDS**	**Très élevée**
Données professionnelles	Service, rôle dans l'organisation, documents métiers (ex: procédures, contrats).	**Art. 6(1)(b)** ou **Art. 6(1)(f)**	Moyenne

1.3 Catégories de Personnes Concernées

Catégorie	Description
Employés	Personnels internes utilisant HeelonGed (ex: biologistes, techniciens, administratifs).
Administrateurs	Personnes gérant HeelonGed (ex: admin IT, responsable qualité).
Patients	*Uniquement si vous stockez des données de santé **non anonymisées** dans HeelonGed.*

Prestataires externes	Sous-traitants ayant accès à HeelonGed (ex: prestataire de maintenance, hébergeur).

1.4 Destinataires des Données

Destinataire	Description	Localisation	Base Légale
Utilisateurs autorisés	Personnes ayant un compte HeelonGed avec les droits appropriés.	UE (par défaut)	Art. 6(1)(b) ou (f) RGPD
Hébergeur	Fournisseur d'hébergement (ex: OVH, Scaleway). *Doit être certifié HDS si données de santé.*	UE (recommandé)	Contrat de sous-traitance
Autorités compétentes	CNIL, COFRAC (en cas d'audit ou de contrôle).	France/UE	Obligation légale

2. Registre Détail des Traitements

Méthodologie :
Chaque traitement est décrit selon les **exigences de l'Article 30 du RGPD** :

- Finalité.
- Catégories de données/personnes concernées.
- Durée de conservation.
- Mesures de sécurité.
- Sous-traitants éventuels.

Traitement 1 : Gestion des Comptes Utilisateurs

Champ	Détails
Nom du traitement	Gestion des comptes utilisateurs dans HeelonGed.
Finalité	Créer, modifier et supprimer des comptes pour accéder à HeelonGed.

Base légale	**Art. 6(1)(b)** (exécution d’un contrat) + **Art. 6(1)(f)** (intérêt légitime pour la sécurité).
Catégories de données	Noms, prénoms, adresses email, rôles, mots de passe (chiffrés), clés API.
Catégories de personnes	Employés, administrateurs.
Durée de conservation	**3 ans** après la fin du contrat de travail (ou suppression immédiate à la demande).
Sous-traitants	Aucun (les données sont gérées en interne).
Mesures de sécurité	- Chiffrement des mots de passe (bcrypt). - **2FA** recommandé. - **Logs d’accès** (IP, timestamp).
Transfert hors UE	Non (sauf si l’hébergeur est hors UE, à déclarer à la CNIL).
Analyse d’impact (PIA)	Non requis (faible risque pour les données techniques).

Traitement 2 : Stockage et Gestion des Documents

Champ	**Détails**
Nom du traitement	Stockage, versionnage et archivage des documents dans HeelonGed.
Finalité	Centraliser et sécuriser les documents (ex: procédures qualité, résultats, contrats).
Base légale	**Art. 6(1)(b)** (exécution d’un contrat) + **Art. 6(1)(f)** (intérêt légitime pour l’archivage).
Catégories de données	- **Métadonnées** : Nom du fichier, date, version, hash (SHA-256), tags. - **Contenu des fichiers** : Texte, PDF, images (peut inclure des données personnelles ou de santé).
Catégories de personnes	Employés, administrateurs. *Patients si données de santé non anonymisées.*
Durée de conservation	- **Documents administratifs** : 5 ans (ou selon la réglementation sectorielle). - **Données de santé** : 20 ans (ou selon la loi locale).

	- **Logs d’audit** : 6 ans (recommandation CNIL).
Sous-traitants	- **Hébergeur** (ex: OVH, Scaleway) : Stocke les fichiers et la base de données. - *Autres sous-traitants éventuels (à compléter).*
Mesures de sécurité	- **Chiffrement au repos** (AES-256 pour les fichiers sensibles). - **Chiffrement en transit** (TLS 1.3). - **Sauvegardes automatiques** (quotidiennes). - **Accès restreint** (rôles : lecteur/éditeur/admin). - **Journalisation** (audit_logs).
Transfert hors UE	Non (sauf si l’hébergeur est hors UE, à déclarer à la CNIL).
Analyse d’impact (PIA)	**Requis si données de santé** : Voir Annexe A.

Traitement 3 : Journalisation et Audit

Champ	**Détails**
Nom du traitement	Enregistrement des actions dans les **logs d’audit** (`audit_logs`).
Finalité	Traçabilité des actions (création, modification, suppression) pour la conformité (ISO 15189, RGPD).
Base légale	**Art. 6(1)(f)** (intérêt légitime pour la sécurité et la conformité).
Catégories de données	- **Actions** : `CREATE`, `UPDATE`, `DELETE`, `ACCESS`. - **Métadonnées** : User ID, document ID, timestamp, IP.
Catégories de personnes	Employés, administrateurs.
Durée de conservation	**6 ans** (recommandation CNIL pour les logs de sécurité).
Sous-traitants	Aucun (les logs sont gérés en interne).
Mesures de sécurité	- **Accès restreint** aux logs (uniquement les administrateurs). - **Intégrité** : Les logs ne peuvent pas être modifiés (base SQLite en mode WAL). - **Export sécurisé** : Les logs peuvent être exportés en CSV pour analyse.

Transfert hors UE	Non.
Analyse d’impact (PIA)	Non requis.

Traitement 4 : Support et Maintenance Interne

Champ	Détails
Nom du traitement	Accès aux données pour le **support et la maintenance** de HeelonGed.
Finalité	Résoudre les problèmes techniques (ex: bugs, restaurations).
Base légale	**Art. 6(1)(f)** (intérêt légitime pour la maintenance).
Catégories de données	- **Métadonnées** : Structure des documents, logs techniques. - **Données de configuration** : Fichiers `.env`.
Catégories de personnes	Administrateurs internes.
Durée de conservation	**1 an** (ou jusqu’à résolution du problème).
Sous-traitants	*À compléter si vous externalisez le support (ex: prestataire IT).*
Mesures de sécurité	- **Accès temporaire** (via SSH ou API avec clés limitées dans le temps). - **Journalisation** de toutes les actions du support. - **Contrat de confidentialité** (NDA) signé avec les prestataires.
Transfert hors UE	Non (sauf si le support est assuré depuis un pays hors UE, à déclarer).
Analyse d’impact (PIA)	Non requis.

3. Mesures de Sécurité Mises en Œuvre

3.1 Mesures Techniques

Mesure	Description	Responsable
Chiffrement	- **Au repos** : AES-256 pour les fichiers sensibles (à activer).	Admin IT

	- **En transit** : TLS 1.3 pour toutes les communications.	
Authentification	- **Mots de passe robustes** (12 caractères minimum, complexité élevée). - **2FA** (recommandé pour les administrateurs).	Admin GED
Gestion des accès	- **Principe du moindre privilège** (rôles : lecteur, éditeur, admin). - **Clés API** : Rotation tous les 90 jours.	Admin GED
Sauvegardes	- **Automatiques** (quotidiennes) et **testées** (restauration mensuelle). - **Stockage externe** (ex: AWS S3, NAS).	Admin IT
Journalisation	- **Logs d'audit** (`audit_logs`) pour toutes les actions. - **Logs techniques** (accès, erreurs).	HeelonGed (automatique)
Protection contre les intrusions	- **Pare-feu** (ex: UFW sur le VPS). - **Mises à jour régulières** (OS, conteneurs Podman).	Admin IT
Validation du système	- **Tests de pénétration** (annuels). - **Validation ISO 15189** (pour les laboratoires).	Admin Qualité / IT

3.2 Mesures Organisationnelles

Mesure	Description	Responsable
Politique de sécurité	Document formalisant les règles d'utilisation de HeelonGed (ex: interdiction de partager les clés API).	DPO / Admin Qualité
Formation des utilisateurs	- **Formation initiale** à l'utilisation de HeelonGed. - **Sensibilisation RGPD** (annuelle).	RH / Admin Qualité
Gestion des incidents	- **Processus de signalement** (ex: formulaire dédié). - **Plan de réponse** (ex: isolation du système).	DPO / Admin Sécurité
Revues de sécurité	- **Audit trimestriel** des logs et des accès. - **Revue annuelle** avec le DPO.	DPO / Admin Sécurité
Contrats avec les sous-traitants	- **Clauses RGPD** dans les contrats avec les hébergeurs. - **Vérification de la conformité HDS** (si données de	Juridique / DPO

santé).

4. Sous-Traitants

Définition :
Un **sous-traitant** est une entité qui traite des données **pour le compte du responsable de traitement** (votre organisation).

4.1 Liste des Sous-Traitants

À compléter : Listez ici tous les sous-traitants ayant accès à des données traitées via HeelonGed.

Sous-Traitant	Rôle	Localisation	Conformité	Contact	Contrat RGPD
[Nom de l'hébergeur]	Hébergement du serveur HeelonGed (ex: OVH, Scaleway).	[Pays]	**Certifié HDS** (si données de santé), ISO 27001, SOC 2.	[Site web]	/
[Autre prestataire]	[Ex: Maintenance IT, support technique].	[Pays]	[Ex: RGPD, NDA signé].	[Contact]	/

Conseils :

- Vérifiez que vos sous-traitants ont signé un **contrat de sous-traitance RGPD**.
- Pour les **données de santé**, exigez une **certification HDS** (obligatoire en France).
- Conservez une **copie des contrats** dans `/SMQ/Contrats/`.

4.2 Exemple de Contrat de Sous-Traitance

À adapter pour chaque sous-traitant.

Clauses obligatoires :

1. **Objet** : Décrire précisément les services (ex: "Hébergement de HeelonGed").
2. **Durée** : Date de début et de fin.
3. **Obligations du sous-traitant** :

- Traiter les données **uniquement sur instruction** du responsable.
- **Ne pas sous-traiter** sans autorisation écrite.
- **Notifier les violations de données** dans les **72h**.
- **Supprimer ou restituer les données** à la fin du contrat.

4. **Sécurité** : Mesures techniques et organisationnelles (ex: chiffrement, sauvegardes).
5. **Audit** : Droit pour le responsable de traitement de **contrôler** la conformité.

5. Durées de Conservation

Type de Donnée	Durée de Conservation	Base Légale
Comptes utilisateurs	3 ans après la fin du contrat de travail (ou suppression à la demande).	Art. 6(1)(b) RGPD
Documents administratifs	5 ans (ou selon la réglementation sectorielle, ex: 10 ans pour les contrats).	Obligation légale
Données de santé	20 ans (ou selon la loi locale, ex: article R. 1111-2 du Code de la santé publique).	Art. 9(2)(h) RGPD + HDS
Logs d'audit	6 ans (recommandation CNIL).	Intérêt légitime (Art. 6(1)(f))
Logs techniques	1 an.	Intérêt légitime
Sauvegardes	30 jours (ou jusqu'à validation de la restauration).	Obligation de sécurité

6. Droits des Personnes Concernées

HeelonGed permet de respecter les **droits des personnes concernées** (Art. 12-22 RGPD) :

6.1 Droits et Modalités d'Exercice

Droit	Description	Modalités dans HeelonGed
Droit d'accès (Art. 15)	Accès aux données personnelles.	Export des données via l'API ou l'interface admin (par le responsable de

		traitement).
Droit de rectification (Art. 16)	Correction des données inexactes.	Modification possible via l’interface ou l’API (avec logs d’audit).
Droit à l’effacement (Art. 17)	Suppression des données ("droit à l’oubli").	Suppression du compte et des données associées (via l’API ou l’interface admin).
Droit à la limitation (Art. 18)	Limitation du traitement (ex: désactivation temporaire du compte).	Désactivation du compte (sans suppression des données).
Droit à la portabilité (Art. 20)	Récupération des données dans un format structuré (ex: JSON, CSV).	Export des données via l’API (format JSON).
Droit d’opposition (Art. 21)	Opposition au traitement (ex: désabonnement aux notifications).	Désactivation des notifications dans les paramètres utilisateur.

6.2 Procédure de Réponse aux Demandes

1. **Réception de la demande** :
    - Recevoir la demande via un **formulaire dédié** (ex: sur votre site web) ou par email (ex: dpo@[votre-organisation].fr).
2. **Vérification de l’identité** :
    - Demander une **pièce d’identité** pour éviter les usurpations.
3. **Traitement de la demande** :
    - **Délai** : Répondre dans **1 mois** (extensible à 2 mois pour les demandes complexes).
    - **Gratuité** : Les demandes sont gratuites, sauf si **répétitives ou excessives** (Art. 12(5) RGPD).
4. **Preuves** :
    - **Journaliser** la demande et la réponse dans HeelonGed (ex: `/SMQ/Demandes_RGPD/`).

Modèle de réponse à une demande d’accès :

```
Objet : Réponse à votre demande d’accès (RGPD - Art. 15)

Cher [Nom],

Suite à votre demande du [date], voici les données personnelles vous
concernant que nous traitons dans HeelonGed :

- Nom/Prénom : [Nom]

- Email : [email]

- Rôle : [rôle]

- Dernière connexion : [date]

- Documents associés : [liste des documents, si applicable]

Vous pouvez demander la rectification ou la suppression de ces données
en répondant à cet email.

Cordialement,

[Nom du DPO]

[Coordonnées]
```

7. Violations de Données (Data Breach)

7.1 Procédure en Cas de Violation

1. **Détection** :
    - Surveillance des **logs d’audit** et des **alertes de sécurité** (ex: accès suspect).
2. **Évaluation** :
    - Déterminer si la violation concerne des **données personnelles** et son **niveau de risque** (faible/élevé).
3. **Notification** :
    - **À la CNIL** : Dans les **72h** si risque élevé pour les droits et libertés des personnes (Art. 33 RGPD).
        - Utiliser le **formulaire en ligne** : https://www.cnil.fr/fr/notification-dune-violation-de-donnees-personnelles.

- **Aux personnes concernées** : Sans délai si risque élevé (Art. 34 RGPD).

4. **Documentation** :

   - Consigner l’incident dans un **registre des violations** (ex: `/SMQ/Incidents/`).

7.2 Exemples de Violations et Réponses

Scénario	Risque	Actions
Accès non autorisé à un document	Élevé (données de santé)	- Révoquer les accès. - Notifier la CNIL et les personnes concernées. - Renforcer l’authentification (2FA).
Perte de données (panne serveur)	Moyen	- Restaurer depuis les sauvegardes. - Vérifier l’intégrité des données. - Notifier la CNIL si données personnelles perdues.
Fuite de logs d’audit	Faible	- Corriger la vulnérabilité. - Notifier la CNIL si les logs contiennent des données personnelles.

8. Annexes

Annexe A : Modèle d’Analyse d’Impact (PIA)

À utiliser si vous traitez des données sensibles (ex: santé) ou si le traitement est à haut risque.

```
# **Analyse d’Impact (PIA) - Utilisation de HeelonGed pour les Données de Santé**

*Conforme à l’Article 35 du RGPD*

---

## 1. **Description du Traitement**

- **Nom** : Stockage de données de santé dans HeelonGed.

- **Finalité** : Gestion des résultats de laboratoire et traçabilité.

- **Responsable** : [Nom de votre organisation].

- **Sous-traitants** : [Hébergeur (ex: OVH HDS)].

---

## 2. **Évaluation de la Nécessité et de la Proportionnalité**

- **Nécessité** : Le traitement est nécessaire pour assurer la **traçabilité des résultats** et la **conformité ISO 15189**.

- **Proportionnalité** : Les données collectées sont limitées à :

  - Nom du patient (pseudonymisé si possible).

  - Type d’analyse.

  - Résultat (anonymisé ou chiffré).

  - Date de l’analyse.

---

## 3. **Évaluation des Risques**

| **Risque**               | **Probabilité (1-5)** | **Impact (1-5)** | **Niveau** | **Mesures de Réduction**                          |

|--------------------------|-----------------------|------------------|------------|---------------------------------------------------|
```

| Accès non autorisé | 3 | 5 | Élevé
| 2FA, chiffrement, audit des accès. |

| Perte de données | 2 | 5 | Moyen
| Sauvegardes automatiques, tests de restauration. |

| Fuite de données | 2 | 5 | Moyen
| Chiffrement, accès restreint, HDS. |

| Non-conformité ISO 15189 | 2 | 4 | Moyen
| Validation du système, audits internes. |

---

4. **Mesures Envisagées**

- **Techniques** :

  - Chiffrement AES-256 pour les fichiers sensibles.

  - Sauvegardes quotidiennes + tests de restauration.

  - Hébergement **certifié HDS**.

- **Organisationnelles** :

  - Formation des utilisateurs à la **gestion des données de santé**.

  - Revues de sécurité **trimestrielles**.

- **Juridiques** :

  - Contrat avec l’hébergeur incluant des **clauses RGPD + HDS**.

---

5. **Conclusion**

- **Risque résiduel** : Faible (après mise en œuvre des mesures).

- **Validation** : Le traitement peut être mis en œuvre avec les mesures proposées.

- **Date** : [JJ/MM/AAAA].

- **Signataire** : [Nom du DPO].

Annexe B : Modèle de Registre des Violations de Données

```
# **Registre des Violations de Données**

*Conforme à l’Article 33 du RGPD*

| **Date**       | **Type de Violation**       | **Données Concernées** |
**Nombre de Personnes** | **Risque** | **Mesures Prises**
| **Notification CNIL** | **Notification Personnes** |

|----------------|-----------------------------|-------------------------|------
--------------------|------------|-------------------------------------------|
------------------------|-----------------------------|

| [JJ/MM/AAAA]   | Accès non autorisé          | Données de santé        | 10
| Élevé      | Révocation des accès, renforcement 2FA.      |    (72h)
|                              |

| [JJ/MM/AAAA]   | Perte de données            | Logs d’audit            | 0
| Faible     | Restauration depuis sauvegarde.             |
|                              |
```

Annexe C : Checklist de Conformité RGPD pour HeelonGed

Exigence RGPD	Statut	Preuve	Responsable
Registre des activités		Ce document.	DPO
Base légale des traitements		Documenté dans le RAT.	DPO
Droits des personnes		Fonctionnalités API/interface.	Admin GED
Sécurité des données		Chiffrement, sauvegardes, logs.	Admin IT
Notification des violations		Procédure documentée.	DPO
Sous-traitants conformes		À compléter (contrats RGPD).	Juridique
Analyse d’impact (PIA)		À compléter si données sensibles.	DPO

Annexe D : Glossaire

Terme	Définition
RGPD	Règlement Général sur la Protection des Données (UE 2016/679).
CNIL	Commission Nationale de l'Informatique et des Libertés (autorité française).
HDS	Hébergement de Données de Santé (certification française pour les hébergeurs de données de santé).
Responsable de traitement	Votre organisation (détermine les finalités et moyens du traitement).
Sous-traitant	Entité qui traite des données pour votre compte (ex: hébergeur).
DPO	Délégué à la Protection des Données.
PIA	Privacy Impact Assessment (Analyse d'Impact relative à la Protection des Données).
Logs d'audit	Journaux enregistrant les actions des utilisateurs (création, modification, suppression).
Chiffrement	Technique de protection des données rendant leur lecture impossible sans clé.
ISO 15189	Norme internationale pour les laboratoires de biologie médicale.
COFRAC	Comité Français d'Accréditation (organisme certificateur pour les laboratoires).

9. Conclusion

Ce **Registre des Activités de Traitement (RAT)** vous permet de :
Documenter vos traitements de données via HeelonGed **conformément au RGPD**.
Prouver votre conformité en cas de contrôle par la **CNIL** ou d'audit (ex: COFRAC).
Faciliter la transparence envers les personnes concernées (employés, patients).

Prochaines Étapes

1. **Complétez ce document** avec vos **spécificités** (ex: sous-traitants, durées de conservation).
2. **Nommez un DPO** (si ce n'est pas déjà fait) pour superviser la conformité.
3. **Mettez en place les mesures techniques** (chiffrement, sauvegardes, 2FA).
4. **Formez vos utilisateurs** aux bonnes pratiques RGPD et HeelonGed.
5. **Intégrez ce registre** dans votre **SMQ** (pour les laboratoires) ou votre **politique de confidentialité**.
6. **Mettez à jour ce document au moins une fois par an** ou en cas de changement significatif (ex: nouveau traitement, sous-traitant).