Analyse d'Impact (PIA) - Utilisation de HeelonGed

Conforme au RGPD (Article 35), aux recommandations de la CNIL et aux normes ISO 15189/HDS
Version : 1.0
Date : [DD/MM/AAAA]
Rédigé par : [Nom du DPO ou du Responsable Qualité]
Organisation : [Nom du Laboratoire/Entreprise]

À savoir :

- Ce document est une **maquette générique** pour les clients utilisant **HeelonGed**.
- **À personnaliser** : Complétez les sections entre crochets [ ] et adaptez les exemples à votre contexte.
- **Pour les laboratoires de biologie médicale** : Ce PIA doit être intégré dans votre **Système de Management de la Qualité (SMQ)** et aligné avec les exigences **ISO 15189** (Section 4.1 - Management de la qualité) et **HDS** (si données de santé).

Introduction

Contexte et Objectifs

L'**Analyse d'Impact (PIA)** est un outil obligatoire (RGPD, Article 35) pour évaluer les **risques liés au traitement de données personnelles**, en particulier lorsque ces traitements sont **susceptibles d'engendrer un risque élevé** pour les droits et libertés des personnes concernées.

HeelonGed, en tant que **Gestion Électronique de Documents (GED)**, peut traiter des données sensibles, notamment :

- **Données personnelles** (ex: noms, emails des utilisateurs).
- **Données de santé** (ex: résultats de laboratoire, dossiers patients).
- **Données techniques** (ex: logs d'audit, métadonnées).

Ce PIA a pour objectif d'**identifier, évaluer et mitiger les risques** liés à l'utilisation de HeelonGed, en conformité avec :

- Le **RGPD** (règlement européen).
- Les **recommandations de la CNIL** (notamment le Guide PIA).
- Les **normes ISO 15189** (pour les laboratoires de biologie médicale).
- Les **exigences HDS** (Hébergement de Données de Santé, si applicable).

Périmètre

Ce PIA couvre :

L'utilisation de HeelonGed pour la gestion de documents (ex: procédures qualité, résultats de laboratoire).

Les traitements de données associés (ex: stockage, versionnage, audit).

Les risques spécifiques aux laboratoires de biologie médicale (ex: conformité ISO 15189, gestion des données de santé).

Exclusions :

- Les traitements externes à HeelonGed (ex: logiciels RH, LIMS).
- Les risques liés à l'infrastructure réseau (ex: pare-feu, VPN).

Méthodologie

Ce PIA suit la **méthodologie recommandée par la CNIL** :

1. **Description du traitement** (finalités, données, acteurs).
2. **Évaluation de la nécessité et de la proportionnalité**.
3. **Identification et évaluation des risques**.
4. **Mesures de mitigation**.
5. **Validation et suivi**.

---

1. Description du Traitement

1.1 Finalités du Traitement

Finalité	Description	Base Légale (RGPD)
Gestion documentaire	Stockage, versionnage, archivage et suppression de documents (ex: procédures, résultats).	Art. 6(1)(b) (exécution d'un contrat)
Traçabilité et audit	Enregistrement des actions (création, modification, suppression) pour la conformité.	Art. 6(1)(f) (intérêt légitime)

Collaboration interne	Partage de documents entre utilisateurs autorisés.	Art. 6(1)(b) ou (f)
Conformité réglementaire	Répondre aux exigences ISO 15189, HDS, ou autres normes sectorielles.	Obligation légale

---

1.2 Catégories de Données Traitées

Attention :

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

Catégorie	Exemples	Sensibilité	Volume Estimé
Données d'identification	Noms, prénoms, adresses email, postes des utilisateurs.	Moyenne	[Ex: 50-100 utilisateurs]
Données de connexion	Identifiants, mots de passe (chiffrés), clés API, IP.	Élevée	[Ex: 100 comptes]
Données techniques	Logs d'audit (actions, timestamp, document ID), métadonnées des fichiers (nom, taille, hash).	Faible	[Ex: 10 000 logs/mois]
Données de santé	Résultats de laboratoire, dossiers patients (si stockés **non anonymisés**).	**Très élevée**	[Ex: 1 000 dossiers/an]
Documents métiers	Procédures qualité, contrats, rapports d'audit.	Moyenne	[Ex: 500 documents]

1.3 Catégories de Personnes Concernées

Catégorie	Description	Nombre Estimé
Employés	Personnels internes utilisant HeelonGed (ex: biologistes, techniciens, administratifs).	[Ex: 50]
Administrateurs	Personnes gérant HeelonGed (ex: admin IT, responsable qualité).	[Ex: 5]
Patients	*Uniquement si vous stockez des données de santé **non anonymisées** dans HeelonGed.*	[Ex: 1 000]
Prestataires	Sous-traitants ayant accès à HeelonGed (ex: hébergeur,	[Ex: 2]

externes	support technique).

1.4 Acteurs du Traitement

Rôle	Acteur	Responsabilités
Responsable de traitement	[Nom de votre organisation]	Détermine les finalités et les moyens du traitement.
DPO	[Nom du DPO]	Supervise la conformité RGPD et valide le PIA.
Administrateur GED	[Nom de l'admin]	Gère les accès, les sauvegardes et la sécurité de HeelonGed.
Hébergeur	[Nom de l'hébergeur (ex: OVH)]	Fournit l'infrastructure (VPS) et garantit la sécurité physique/logique.
Utilisateurs	[Liste des services concernés]	Utilisent HeelonGed pour stocker, modifier ou consulter des documents.

1.5 Contexte du Traitement

- **Environnement technique** :
  - HeelonGed est déployé sur un **VPS** (ex: Fedora + Podman rootful) ou en local.
  - **Base de données** : SQLite (`ged.db`).
  - **Stockage des fichiers** : `/srv/heelonged-backend/files/`.
  - **Logs** : `audit_logs` (actions des utilisateurs) et logs techniques.
- **Flux de données** :
  - L'utilisateur **upload** un document via l'interface ou l'API.
  - HeelonGed **stocke** le fichier et enregistre l'action dans `audit_logs`.
  - Les **administrateurs** peuvent consulter/modifier les documents et les logs.
  - Les **sauvegardes** sont effectuées quotidiennement.
- **Sous-traitants** :
  - **Hébergeur** (ex: OVH, Scaleway) : Stocke les données.
  - *Autres sous-traitants éventuels (ex: support technique).*

1.6 Évaluation de la Nécessité et de la Proportionnalité

Critère	Évaluation
Nécessité	HeelonGed est **nécessaire** pour : - Centraliser la gestion des documents. - Assurer la traçabilité (ISO 15189). - Collaborer en interne.
Proportionnalité	Les données collectées sont **limitées au strict nécessaire** : - Métadonnées (nom, date, version). - Contenu des documents (si pertinent). - Logs d'audit (pour la conformité).
Alternatives	- **Solutions papier** : Non adaptées (manque de traçabilité, risque de perte). - **Autres GED** : HeelonGed a été choisi pour sa **conformité RGPD/ISO 15189** et son **coût maîtrisé**.

2. Évaluation des Risques

2.1 Méthodologie d'Évaluation

- **Impact** : Échelle de 1 (faible) à 5 (critique).
- **Probabilité** : Échelle de 1 (très improbable) à 5 (très probable).
- **Score de risque** = Impact × Probabilité.
- **Seuils** :
    - **1-5** : Risque faible (acceptable).
    - **6-12** : Risque moyen (à mitiger).
    - **13-25** : Risque élevé (mitigation **obligatoire**).

2.2 Risques Identifiés

Risques Liés à la Confidentialité

ID	Risque	Description	Cause Possible	Impact	Probabilité	Score	Niveau

R1	**Accès non autorisé**	Un utilisateur non autorisé accède à des documents sensibles (ex: résultats patients).	Mauvaises permissions, clés API compromises.	5	3	15	**Élevé**
R2	**Fuite de données**	Fuites de documents via des vulnérabilités (ex: injection SQL, mauvaise configuration CORS).	Failles de sécurité dans l'API.	5	2	10	Moyen
R3	**Chiffrement insuffisant**	Données sensibles non chiffrées (au repos ou en transit).	Configuration incorrecte.	4	3	12	Moyen

Risques Liés à l'Intégrité

ID	Risque	Description	Cause Possible	Impact	Probabilité	Score	Niveau
R4	**Modification non autorisée**	Un document est modifié sans validation (ex: procédure qualité).	Absence de workflow d'approbation.	4	3	12	Moyen
R5	**Corruption de données**	La base SQLite (`ged.db`) ou les fichiers sont corrompus.	Panne matérielle, arrêt brutal.	5	2	10	Moyen
R6	**Falsification de logs**	Les logs d'audit (`audit_logs`) sont altérés.	Accès root non contrôlé.	5	1	5	Faible

Risques Liés à la Disponibilité

ID	Risque	Description	Cause Possible	Impact	Probabilité	Score	Niveau
R7	**Indisponibilité du service**	HeelonGed inaccessible (ex: panne serveur, attaque DDoS).	Problème réseau, saturation du serveur.	4	2	8	Moyen
R8	**Perte de**	Suppression	Erreur	5	2	10	Moyen

	données	accidentelle ou corruption de documents (ex: base SQLite, fichiers).	humaine, panne matérielle.				

Risques Liés à la Conformité

ID	Risque	Description	Cause Possible	Impact	Probabilité	Score	Niveau
R9	**Non-conformité RGPD**	Données personnelles (ex: noms, emails) non protégées.	Absence de chiffrement ou de pseudonymisation.	5	2	10	Moyen
R10	**Non-conformité ISO 15189**	HeelonGed ne répond pas aux exigences de traçabilité ou de validation.	Validation incomplète du système.	5	2	10	Moyen
R11	**Non-conformité HDS**	Hébergement de données de santé sans certification HDS.	Hébergement non conforme en France.	5	1	5	Faible

Risques Spécifiques aux Laboratoires (ISO 15189)

ID	Risque	Description	Cause Possible	Impact	Probabilité	Score	Niveau
R12	**Erreur de traçabilité**	Impossibilité de retracer une action (ex: modification d’un résultat de laboratoire).	Logs d’audit incomplets ou corrompus.	4	2	8	Moyen
R13	**Non-respect des durées de conservation**	Données de santé conservées au-delà de 20 ans.	Absence de politique d’archivage.	4	2	8	Moyen

3. Mesures de Mitigation

3.1 Mesures pour les Risques Élevés (Score ≥ 13)

ID	Risque	Mesures de Mitigation	Responsable	Échéance	Statut
R1	Accès non autorisé	- **Authentification forte** (2FA) pour tous les utilisateurs. - **Rôles stricts** (lecteur/éditeur/admin). - **Clés API sécurisées** (rotation tous les 90 jours). - **Audit des accès** (logs `audit_logs`).	Admin GED	Immédiat	
		- **Chiffrement des données sensibles** (AES-256). - **Sensibilisation des utilisateurs** (formation RGPD).	Admin IT	1 mois	

3.2 Mesures pour les Risques Moyens (Score 6-12)

ID	Risque	Mesures de Mitigation	Responsable	Échéance	Statut
R2	Fuite de données	- **Chiffrement en transit** (TLS 1.3). - **Chiffrement au repos** (AES-256 pour les fichiers sensibles). - **Tests de pénétration** annuels.	Admin Sécurité	2 semaines	
R4	Modification non autorisée	- **Workflow d'approbation** (statut `draft` → `approved`). - **Notifications** pour les modifications.	Admin Qualité	1 mois	
R5	Corruption de données	- **Sauvegardes automatiques** (quotidiennes). - **Tests de restauration** mensuels. - **Stockage redondant** (ex: RAID ou cloud).	Admin IT	1 semaine	
R7	Indisponibilité	- **Redondance du serveur** (cluster Podman/Kubernetes). - **Monitoring** (ex: Prometheus + Grafana).	Admin IT	3 mois	
R8	Perte de données	- **Sauvegardes externes** (ex: AWS S3, NAS).	Admin IT	1 semaine	

		- **Alertes en cas d’échec de sauvegarde**.		
R9	Non-conformité RGPD	- **Anonymisation/pseudonymisation** des données personnelles. - **DPO désigné** pour superviser.	DPO	Immédiat
R10	Non-conformité ISO 15189	- **Validation complète** du système (voir Guide de Conformité ISO 15189). - **Audit interne** annuel.	Admin Qualité	2 mois
R12	Erreur de traçabilité	- **Vérification régulière des logs** (`audit_logs`). - **Export sécurisé** des logs (CSV).	Admin GED	1 mois
R13	Non-respect des durées	- **Politique d’archivage** claire (ex: 20 ans pour les données de santé). - **Automatisation** de la suppression.	Admin Qualité	1 mois

3.3 Mesures pour les Risques Faibles (Score ≤ 5)

ID	Risque	Mesures de Mitigation	Responsable	Échéance	Statut
R6	Falsification de logs	- **Accès restreint** aux logs (uniquement les administrateurs). - **Intégrité** : Base SQLite en mode WAL (non modifiable).	Admin GED	Immédiat	
R11	Non-conformité HDS	- **Vérifier la certification HDS** de l’hébergeur. - **Contrat HDS** signé avec l’hébergeur.	Juridique	Immédiat	

4. Risques Résiduels

Après application des mesures de mitigation, les **risques résiduels** sont les suivants :

ID	Risque	Score Initial	Score Résiduel	Niveau Résiduel	Acceptabilité	Justification
R1	Accès non autorisé	15	5	Faible	Acceptable	Mesures : 2FA + rôles stricts + audit + chiffrement.

R2	Fuite de données	10	4	Moyen	À surveiller	Chiffrement activé, mais risque résiduel lié aux vulnérabilités 0-day.
R4	Modification non autorisée	12	3	Faible	Acceptable	Workflow d’approbation + notifications.
R5	Corruption de données	10	3	Faible	Acceptable	Sauvegardes automatiques + tests de restauration.
R7	Indisponibilité	8	6	Moyen	À surveiller	Redondance partielle (pas de cluster encore).
R8	Perte de données	10	3	Faible	Acceptable	Sauvegardes externes + alertes.
R9	Non-conformité RGPD	10	3	Faible	Acceptable	Anonymisation + DPO + chiffrement.
R10	Non-conformité ISO 15189	10	4	Moyen	À surveiller	Validation en cours, audit interne prévu.

5. Validation et Suivi

5.1 Validation du PIA

- **Date de validation** : [JJ/MM/AAAA].
- **Validé par** : [Nom du DPO ou du Responsable Qualité].
- **Commentaires** :
  [Ex: "Les mesures proposées réduisent les risques à un niveau acceptable. Le PIA sera révisé annuellement ou en cas de changement significatif."]

5.2 Plan de Suivi

Action	Responsable	Échéance	Statut	Indicateur de Suivi
Mettre en place le 2FA	Admin Sécurité	[JJ/MM/AAAA]		% d’utilisateurs avec 2FA activé.
Tester les sauvegardes automatiques	Admin IT	[JJ/MM/AAAA]		Rapport de test de restauration.

Chiffrer les données sensibles	Admin IT	[JJ/MM/AAAA]	% de fichiers chiffrés.
Former les utilisateurs	RH	[JJ/MM/AAAA]	Nombre d’utilisateurs formés.
Valider HeelonGed (ISO 15189)	Admin Qualité	[JJ/MM/AAAA]	Rapport de validation signé.
Mettre en place un monitoring	Admin Sécurité	[JJ/MM/AAAA]	Tableau de bord Grafana opérationnel.
Réviser le PIA	DPO	[JJ/MM/AAAA]	PIA mis à jour.

5.3 Révisions du PIA

Ce PIA doit être **révisé** :

- **Au moins une fois par an**.
- **En cas de changement significatif** :
    - Nouveau traitement de données.
    - Modification de l’architecture technique (ex: changement d’hébergeur).
    - Incident de sécurité majeur.
    - Évolution réglementaire (ex: nouvelle version du RGPD).

6. Annexes

Annexe A : Schéma des Flux de Données

```
graph TD
    A[Utilisateur] -->|Upload document| B[HeelonGed]
    B -->|Stocke fichier| C[/srv/heelonged-backend/files/]
    B -->|Enregistre action| D[Base SQLite: audit_logs]
    C -->|Sauvegarde| E[Stockage Externe: AWS S3/NAS]
    D -->|Export| F[Logs CSV]
    G[Administrateur] -->|Consulte/Modifie| B
    H[Hébergeur] -->|Fournit infrastructure| B
```

Annexe B : Modèle de Registre des Incidents

```
# **Registre des Incidents de Sécurité**
*À remplir en cas d’incident lié à HeelonGed*

| **Date/Heure**       | **Type d’Incident**       | **Données Concernées** | **Impact** | **Mesures Prises**                          | **Responsable** | **Statut** |
|----------------------|---------------------------|------------------------|------------|---------------------------------------------|-----------------|------------|
| [JJ/MM/AAAA HH:MM]   | Accès non autorisé        | Données de santé       | Élevé      | Révocation des accès, notification CNIL.    | Admin Sécurité  | Résolu     |
| [JJ/MM/AAAA HH:MM]   | Perte de données          | Base SQLite            | Moyen      | Restauration depuis sauvegarde.             | Admin IT        | En cours   |
```

Annexe C : Checklist de Conformité RGPD/ISO 15189

Exigence	HeelonGed	Statut	Preuve	Responsable
Chiffrement des données sensibles	AES-256 (optionnel)		Configuration serveur.	Admin IT
Authentification forte (2FA)	Intégré (à activer)		Logs d’authentification.	Admin Sécurité
Sauvegardes automatiques	Script de backup		Rapport de sauvegarde.	Admin IT

	quotidien		
Logs d’audit	Intégré (`audit_logs`)	Exemple de log.	Admin GED
Validation ISO 15189	À réaliser	Rapport de validation.	Admin Qualité
Conformité HDS (si données de santé)	Hébergement certifié HDS	Certificat HDS de l’hébergeur.	Juridique

---

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).
ISO 15189	Norme internationale pour les laboratoires de biologie médicale.
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.
2FA	Double Authentification (ex: mot de passe + code SMS).
DPO	Délégué à la Protection des Données.
COFRAC	Comité Français d’Accréditation (organisme certificateur pour les laboratoires).
Podman	Outil de conteneurisation (alternative à Docker).

7. Conclusion

Ce **PIA** démontre que :

Les risques liés à l'utilisation de HeelonGed ont été **identifiés et évalués**.
Des mesures de mitigation ont été proposées pour réduire les risques à un **niveau acceptable**.
HeelonGed peut être utilisé en conformité avec le **RGPD**, l'**ISO 15189** et les **exigences HDS** (si applicable).

Prochaines Étapes

1. **Mettre en œuvre les mesures prioritaires** (2FA, sauvegardes, chiffrement).
2. **Former les utilisateurs** aux bonnes pratiques de sécurité et de conformité.
3. **Valider HeelonGed** selon les exigences **ISO 15189** (pour les laboratoires).
4. **Intégrer ce PIA** dans votre **Système de Management de la Qualité (SMQ)**.
5. **Réviser ce document annuellement** ou en cas de changement significatif.
