Émetteur : Équipe Retr'aide **Objet :** Garanties relatives au respect du cadre légal de la protection des données (nLPD) **Version :** 1.0 — 24 août 2026

---

1. Préambule

Ce document s'adresse à toute autorité, institution ou partenaire amené à évaluer le projet Retr'aide sous l'angle de la protection des données. Nous comprenons que, en particulier pour un service étatique ou une institution publique, il soit essentiel de pouvoir s'assurer que **tous les éléments relatifs à la protection des données sont réunis et respectent le cadre légal** avant tout soutien ou partenariat.

Le présent document a précisément pour but de **fournir cette garantie** : il rassemble, de manière structurée et vérifiable, les éléments de conformité de Retr'aide à la **nouvelle loi fédérale sur la protection des données (nLPD)**, en vigueur depuis le 1er septembre 2023, ainsi qu'à son ordonnance d'exécution (OPDo) et, par alignement volontaire, au RGPD européen.

Notre conviction : la conformité n'est pas un obstacle à documenter *a posteriori*, mais un **principe de conception** (*privacy by design*) intégré dès l'origine du projet. C'est ce que nous détaillons ci-après.

Le dispositif décrit ici repose sur trois choix d'architecture retenus dès la conception : un hébergement entièrement suisse, l'absence de tout prestataire étranger dans la chaîne d'authentification et de messagerie, et un assistant volontairement dépourvu d'intelligence artificielle générative.

> **En une phrase :** les données des utilisateurs de Retr'aide sont hébergées et traitées **exclusivement en Suisse** (Infomaniak, Genève), chiffrées en transit, sauvegardées de manière chiffrée en Suisse, limitées au strict nécessaire ; l'assistant **ne recourt à aucune intelligence artificielle générative** ; et l'utilisateur garde à tout moment le contrôle (consultation, export, suppression).

---

2. Nature du projet et périmètre des données

Retr'aide est une **plateforme de coordination de l'entraide** autour d'une personne aidée. Elle permet à un proche aidant d'organiser un « cercle » de personnes de confiance (famille, voisins, bénévoles) et de répartir des tâches du quotidien (courses, transport, accompagnement, démarches administratives, etc.). Un assistant d'information complète le dispositif pour orienter les proches aidants vers les bonnes ressources.

Choix structurant — pas de dossier médical : Retr'aide se situe **hors du périmètre des soins**. L'application **ne constitue, ne stocke et ne gère aucun dossier médical** : ni diagnostic, ni traitement, ni prescription, ni donnée transmise par un professionnel de santé.

Ce que nous traitons néanmoins, et que nous ne minimisons pas. À la création d'un cercle, le proche aidant peut cocher les besoins de la personne aidée dans une liste fermée : repas, **médicaments**, **hygiène**, **déplacements**, rendez-vous, courses, compagnie, administratif. Rattachées à une personne nommée,

dont l'année de naissance et le NPA sont connus, ces indications permettent des déductions sur son état de santé. Nous les traitons donc comme des **données sensibles au sens de l'art. 5 let. c nLPD**, sur la base d'un **consentement explicite** (art. 6 al. 7 let. a), et elles font l'objet d'une analyse d'impact dédiée (§ 8).

Nous préférons l'écrire ainsi plutôt que d'affirmer « aucune donnée de santé » : c'est ce que dit déjà notre déclaration de confidentialité publique, et une note qui la contredirait ne servirait ni votre examen, ni notre crédibilité.

2.1 Catégories de données effectivement traitées

Catégorie	Données concernées	Finalité
Identité / contact	Prénom, nom, **adresse e-mail** (identifiant de connexion, obligatoire), numéro de téléphone (facultatif), photo de profil (facultative)	Création du compte, identification dans le cercle
Données de compte	Rôle (aidant / aidé), langue, **mot de passe haché (bcrypt)**, codes e-mail à usage unique (vérification et 2FA), jetons de session, jetons de notification	Fonctionnement du service, authentification
Données d'organisation	Cercles, membres, tâches, messages internes au cercle	Cœur fonctionnel de coordination
Données d'usage de l'assistant	Requêtes adressées à l'assistant de navigation guidée, historique de consultation	Orientation vers les fiches d'information pertinentes
Données techniques	Version d'app, plateforme, horodatage de connexion, logs de sécurité	Sécurité, support, lutte contre les abus
Personne aidée (tiers)	Prénom, nom, photo (facultative), NPA, année de naissance, lien de parenté, **besoins d'aide indiqués** — saisis par le proche aidant, pour une personne qui n'a pas de compte	Adapter les tâches proposées et identifier le cercle
Mesure d'usage	Type d'action, horodatage, identifiant de l'utilisateur et du cercle, canal d'acquisition. **Aucun contenu**	Piloter le service et démontrer son effet
Baseline et consentement de recontact	Minutes par semaine déclarées, charge perçue (1-5), canal auto-déclaré, consentement horodaté	Mesurer l'effet du service ; entretiens de bêta
Signalements et blocages	Auteur, cible, motif, précisions, copie du message signalé, statut	Sécurité du contenu généré par les utilisateurs
Prospects (formulaire « soignants »)	Nom, prénom, e-mail, type d'intérêt, remarques libres — saisis volontairement via le formulaire de contact professionnel	Recontact des professionnels et partenaires intéressés

2.2 Point de vigilance assumé : les champs de texte libre

Au-delà des besoins évoqués au § 2, certains champs libres (intitulé d'une tâche, message dans le cercle, requête à l'assistant) peuvent **incidemment** contenir des éléments relevant de la sphère privée, voire de

données sensibles au sens de l'art. 5 let. c nLPD (p. ex. mention d'une pathologie).

Nous traitons ce point de manière explicite plutôt que de l'ignorer :

- ces champs ne sont **jamais sollicités** pour des informations de santé ;
- ils bénéficient des **mêmes mesures de sécurité** que l'ensemble des données (chiffrement en transit, cloisonnement par cercle, accès restreint) ;
- ils sont **exclus de tout usage analytique** ;
- ils ne sont **jamais transmis à un tiers**, ni à un service d'intelligence artificielle (voir §7.1) ;
- la déclaration de confidentialité informe l'utilisateur de ne pas y inscrire d'informations médicales sensibles.

2.3 Recommandations de protection affichées dans l'application

La protection des données ne repose pas uniquement sur des mesures techniques invisibles : elle est aussi **rappelée à l'utilisateur, de manière contextuelle, aux endroits clés de l'application**. Ces rappels sont intégrés à l'application et affichés au plus près des moments sensibles :

- à la **saisie de champs de texte libre** (tâche, message, requête à l'assistant) : rappel de ne pas y inscrire d'informations médicales ou sensibles ;
- lors de l'**invitation de membres dans un cercle** : rappel de n'inviter que des personnes de confiance ;
- lors de la **saisie des données de la personne aidée** : rappel qu'il s'agit d'un tiers, qu'il convient de l'informer et de lui rappeler son droit à l'effacement (art. 19 nLPD, voir § 6.2) ;
- au moment du **partage d'informations** ou de l'usage de l'**assistant d'information** : rappel des bonnes pratiques de confidentialité.

Cette **sensibilisation intégrée** (*privacy by design*, art. 7 nLPD) responsabilise l'utilisateur et réduit le risque à la source, en complément des garanties techniques.

---

3. Conformité aux principes de la nLPD

Principe (nLPD)	Mise en œuvre dans Retr'aide
Licéité & bonne foi (art. 6 al. 1-2)	Traitement fondé sur l'exécution du service demandé par l'utilisateur et sur son consentement éclairé à l'inscription.
Proportionnalité & minimisation (art. 6 al. 2-3)	Seules les données strictement nécessaires sont collectées. Téléphone, photo et écran des besoins restent **facultatifs**. Aucun dossier médical, et une liste de besoins volontairement grossière (« médicaments », non « quels médicaments »).
Finalité (art. 6 al. 3)	Données utilisées uniquement pour la coordination de l'entraide. Pas de revente, pas de publicité, pas de profilage commercial.
Exactitude (art. 6 al. 5)	L'utilisateur peut corriger ses données à tout moment depuis l'application.

Principe (nLPD)	Mise en œuvre dans Retr'aide
Sécurité (art. 8 + OPDo)	Voir section 5 (chiffrement, contrôle d'accès, hébergement CH).
Transparence (art. 19)	Déclaration de confidentialité claire, accessible avant l'inscription et dans les paramètres.
Privacy by design / by default (art. 7)	Conformité intégrée dès l'architecture : minimisation, soft-delete automatique, cloisonnement, hébergement souverain, **absence d'IA générative dans le produit**.

---

4. Hébergement et souveraineté des données

C'est l'un des points où Retr'aide offre la **garantie la plus forte** : l'ensemble de l'infrastructure est situé en Suisse.

Élément	Choix retenu
Hébergeur	**Infomaniak** (Genève, Suisse) — serveur privé virtuel, Ubuntu 24.04
Localisation des données	**Exclusivement en Suisse** — datacenters certifiés **ISO 27001**
DNS	Serveurs de noms **Infomaniak** (`ns11` / `ns12.infomaniak.ch`)
Chemin des requêtes (app et API)	**Aucun proxy ni CDN étranger** : les domaines pointent directement sur le serveur suisse
Base de données	PostgreSQL 16, auto-hébergé sur le serveur suisse, **non exposé publiquement** (accès réseau restreint)
Stockage fichiers	Volume sur le serveur suisse (photos de profil uniquement)
Sauvegarde locale	Dump PostgreSQL quotidien (03h15), conservé sur le serveur suisse
Sauvegarde externalisée	Quotidienne (03h30) vers **Infomaniak Swiss Backup** (Suisse), **chiffrée côté client** (restic, AES-256) — rétention 14 jours / 8 semaines / 12 mois
E-mail transactionnel	**SMTP Infomaniak** (Suisse)

4.1 Aucune dépendance étrangère dans la chaîne technique

Deux dépendances que l'on rencontre couramment dans ce type d'architecture sont **délibérément absentes** du dispositif :

1. **Hébergement hors de Suisse** : le serveur applicatif est hébergé par **Infomaniak à Genève**. Aucun serveur applicatif ni aucune base de données ne se trouve à l'étranger, y compris au sein de l'Union européenne.
2. **Proxy / CDN étranger** : les domaines ne transitent par aucun proxy de type Cloudflare — un tel service terminerait les connexions TLS et verrait donc le trafic en clair. Les serveurs de noms sont ceux

d'Infomaniak et les requêtes atteignent directement le serveur suisse.

Aucune donnée personnelle des utilisateurs n'est stockée ni acheminée hors de Suisse. Le choix d'Infomaniak — hébergeur suisse soumis au droit suisse — écarte la problématique des transferts vers des juridictions à protection inadéquate.

---

5. Mesures techniques et organisationnelles de sécurité

Conformément à l'art. 8 nLPD et à l'OPDo, la sécurité repose sur des mesures concrètes et auditables :

Domaine	Mesure
Chiffrement en transit	**TLS 1.2 minimum, TLS 1.3 privilégié** sur l'ensemble des communications (app, admin, API), certificats automatiques (Let's Encrypt), HSTS avec `preload`
Chiffrement des sauvegardes	Sauvegardes externalisées **chiffrées côté client** (restic, AES-256) : le prestataire de stockage ne peut pas lire leur contenu. La clé de chiffrement est détenue par la seule équipe Retr'aide
Chiffrement au repos (base & volumes)	Assuré au niveau de l'infrastructure Infomaniak
Authentification	E-mail + mot de passe **haché avec bcrypt**. **Code e-mail à usage unique** (expiration 5 minutes) pour la vérification d'adresse et la double authentification (2FA)
Gestion des sessions	Jeton d'accès JWT (24 h) ; jeton de rafraîchissement (30 jours) **stocké haché en SHA-256**, **renouvelé à chaque usage**, avec **révocation de toute la famille de jetons en cas de réutilisation détectée** (défense contre le vol de jeton)
Contrôle d'accès	Cloisonnement strict par cercle : un utilisateur ne voit que les données des cercles dont il est membre
Protection applicative	Limitation de débit (60 requêtes/min/IP), validation systématique des entrées, en-têtes de sécurité (Helmet/HSTS), politique CORS restrictive, protection injection SQL et XSS
Journalisation	Table d'audit (`audit_events`) des actions sensibles : suppression, export, accès administrateur (acteur, cible, contexte, IP)
Gestion des secrets	Variables d'environnement en fichiers à permissions restreintes (600). Les valeurs secrètes de la table de configuration applicative — dont le mot de passe SMTP — sont **chiffrées au repos en AES-256-GCM** : un dump de la base ne livre aucun identifiant exploitable
Supervision des sauvegardes	Alerte e-mail automatique en cas d'**échec** d'une sauvegarde externalisée ; restauration **testée avec succès** (vérification d'intégrité restic + restauration + contrôle du dump)
Notifications	**Entièrement paramétrables** par l'utilisateur. Le message transporté hors de Suisse est une **phrase générique choisie par nous** (« Une nouvelle tâche vous a été attribuée »), accompagnée d'identifiants techniques passés par une liste blanche. Ni le titre d'une tâche, ni le texte d'un message, ni le nom d'une personne ne quittent nos serveurs : l'application va les chercher elle-même, derrière authentification, à l'ouverture de la notification

Domaine	Mesure
Monitoring d'erreurs	Instance **GlitchTip auto-hébergée** sur le même serveur suisse — aucun prestataire de suivi d'erreurs, aucune trace d'exécution hors de Suisse. Seules les erreurs serveur sont rapportées, avec filtrage des paramètres d'URL sensibles
Disponibilité	Objectif 99,5 %, sauvegardes quotidiennes, monitoring

---

6. Droits des personnes concernées

Les droits prévus aux art. 25 à 28 nLPD sont **implémentés dans le produit**, et non seulement promis :

Droit	Mise en œuvre
Information (art. 19)	Déclaration de confidentialité présentée avant inscription
Accès (art. 25)	Données consultables dans l'application ; demande d'accès complète possible
Rectification (art. 6 al. 5 / 32)	Modification directe du profil et des contenus par l'utilisateur
Effacement / droit à l'oubli	Bouton « Supprimer mon compte » dans les réglages de l'application, puis **effacement définitif automatique** sous 30 jours par tâche planifiée quotidienne (voir § 6.1)
Portabilité / export	Export complet des données personnelles déclenchable par l'utilisateur depuis l'application, format standard lisible
Opposition	L'utilisateur peut désactiver notifications et traitements optionnels

6.1 Politique de conservation

- **Compte actif :** données conservées tant que le compte existe.
- **Suppression de compte :** désactivation immédiate, puis **suppression définitive automatique sous 30 jours** par une tâche planifiée quotidienne (04h15). La purge efface les contenus rédigés par la personne, ses sessions, sa baseline et ses blocages ; un **cercle qui se retrouve sans aucun membre est supprimé avec la fiche de la personne aidée** qu'il contenait. Le journal d'audit conserve la preuve que l'effacement a eu lieu, jamais une copie de ce qui a été effacé.
- **Mesure d'usage :** conservée **24 mois**, puis purge automatique. À la suppression d'un compte, les enregistrements sont immédiatement **privés de tout identifiant** : il ne reste qu'un type d'action et une date, qui ne désignent plus personne (donnée anonyme au sens de l'art. 5 let. a).
- **Signalements :** supprimés avec le compte du signalant. Un signalement encore en attente survit sans sa copie de contenu, le temps que la modération puisse l'examiner.
- **Sauvegardes :** les sauvegardes externalisées suivent leur propre cycle de rotation (14 jours / 8 semaines / 12 mois) ; les données supprimées disparaissent des sauvegardes à l'expiration de ce cycle.

- **Prospects (formulaire « soignants ») :** conservés **12 mois** à compter de leur envoi, puis **supprimés automatiquement** par une tâche planifiée quotidienne. Le délai court depuis la soumission, indépendamment du suivi : un contact jamais traité est purgé lui aussi. Ces personnes peuvent en outre demander leur radiation à tout moment auprès du point de contact.
- **Aucune conservation au-delà** de la finalité ni à des fins commerciales.

6.2 La personne aidée — un tiers qui n'a pas consenti

C'est le point le plus délicat du dispositif, et nous préférons l'exposer que l'enfouir. La personne aidée est décrite dans l'application **par quelqu'un d'autre**. Elle n'a pas de compte, ne se connecte pas, ne voit pas ce qui est écrit à son sujet.

Ce que nous faisons :

- **Rappel contextuel** affiché au moment précis où le formulaire commence à collecter ses données, demandant au coordinateur de l'informer et de lui rappeler qu'elle peut demander la suppression de ces données (art. 19 nLPD) ;
- **Traitement direct de ses demandes** : une demande adressée à privacy@retraide.ch est traitée comme toute autre demande d'accès ou d'effacement, sans exiger qu'elle dispose d'un compte ;
- **Effacement automatique en cascade** : elle n'a rien à faire pour que ses données disparaissent lorsque le cercle cesse d'exister ;
- **Minimisation** : rien n'est demandé au-delà de ce qui sert à l'organisation, et la photo reste facultative.

Limite que nous reconnaissons : le rappel s'adresse au coordinateur et nous ne pouvons pas vérifier qu'il informe effectivement la personne aidée. C'est une mesure de responsabilisation, non une garantie. La seule alternative technique — exiger que la personne aidée crée un compte — exclurait précisément les personnes les moins autonomes, c'est-à-dire celles que le service vise. Nous sommes ouverts à toute recommandation de votre service sur ce point.

---

7. Sous-traitants et communication des données

Conformément à l'art. 9 nLPD (sous-traitance) et aux art. 16-17 nLPD (communication transfrontière), voici l'inventaire **transparent** des tiers impliqués.

Sous-traitant	Rôle	Localisation	Données concernées	Cadre
Infomaniak	Hébergement, base de données, stockage, sauvegardes, DNS, SMTP	**Suisse**	L'ensemble des données	Contrat de sous-traitance, ISO 27001, droit suisse

Sous-traitant	Rôle	Localisation	Données concernées	Cadre
Expo Application Services (push)	Relais des notifications avant Apple/Google	**États-Unis**	Jeton de notification technique, **phrase générique** et identifiants. Aucun contenu, aucun nom (voir §5)	Conditions du prestataire ; flux minimisé par conception, désactivable par l'utilisateur
Apple / Google (push)	Acheminement final de la notification jusqu'à l'appareil	International	Idem	Selon plateforme ; usage limité, désactivable
Sanity.io (CMS éditorial)	Rédaction et diffusion des **fiches d'information publiques** (articles, FAQ)	International	**Aucune donnée d'utilisateur** : uniquement du contenu éditorial public rédigé par l'équipe	Contenu public ; aucun traitement de données personnelles

Sous-traitants volontairement écartés : le recours à un prestataire SMS (type Twilio), à un prestataire d'e-mail transactionnel étranger (type Resend), à la connexion sociale Google/Apple et à un proxy Cloudflare est **délibérément exclu** : aucune de ces dépendances ne figure dans le produit ni dans le code.

7.1 Assistant d'information — aucune intelligence artificielle générative

Ce point mérite d'être énoncé sans ambiguïté, car il est fréquemment source de malentendu.

L'assistant de Retr'aide ne repose sur aucun modèle de langage ni sur aucune intelligence artificielle générative. Il s'agit d'un **assistant de navigation guidée** : il effectue une recherche par mots-clés au sein des **fiches d'information rédigées et validées par l'équipe éditoriale** dans le back-office (articles et foire aux questions), puis oriente l'utilisateur vers ces fiches internes.

Il en découle, sur le plan de la protection des données :

1. **Aucun traitement par IA :** aucune requête d'utilisateur n'est soumise à un modèle de langage, qu'il soit suisse ou étranger. La question du traitement automatisé par IA (et des risques associés) **ne se pose donc pas** pour ce produit.
2. **Aucun transfert transfrontière :** les requêtes sont traitées **exclusivement en Suisse**, sur la même infrastructure que le reste de la plateforme. Aucune donnée n'est transmise à un service d'IA tiers, ni à une API de modèle de langage étrangère.
3. **Aucune invention de contenu :** l'assistant ne peut restituer que des fiches existantes, validées par des humains. Chaque réponse est accompagnée d'un avertissement rappelant qu'elle ne constitue pas un avis médical ou juridique.
4. **Pas d'entraînement sur les données :** les données des utilisateurs ne servent à entraîner aucun modèle.
5. **Information de l'utilisateur :** la déclaration de confidentialité décrit le fonctionnement de l'assistant et invite à ne pas y saisir de données sensibles.

Perspective de recherche (hors production). Un assistant génératif fait l'objet d'un **projet de recherche mené avec la HEIG-VD** (Haute École d'Ingénierie et de Gestion du Canton de Vaud, HES-SO), dans un cadre Innosuisse. Ce travail est **délibérément tenu hors du produit en production** : il ne traite aucune donnée d'utilisateur réel. **Aucune mise en production d'un assistant génératif n'interviendra sans analyse d'impact préalable (art. 22 nLPD), information des utilisateurs et, le cas échéant, consultation du PFPDT.**

> En résumé, l'IA — souvent le point de friction des projets numériques — **n'est pas un risque pour Retr'aide, parce qu'elle n'y est pas utilisée**. Le projet académique avec la HEIG-VD garantit que, si elle l'est un jour, ce sera avec un partenaire public suisse et sous encadrement documenté.

7.2 Authentification et e-mails transactionnels — intégralement suisses

L'envoi des codes d'authentification et des e-mails transactionnels est un point où beaucoup de services conservent une dépendance étrangère. Ce n'est pas le cas de Retr'aide :

- l'authentification **ne recourt à aucun SMS** : les codes de vérification et de double authentification sont transmis par **e-mail** ;
- les **e-mails transactionnels** sont envoyés via le **serveur SMTP d'Infomaniak**, en Suisse.

Le seul flux subsistant vers l'étranger est celui des notifications *push*, qui transitent par Expo (États-Unis) puis par Apple ou Google. Ce qui y circule se limite à un **jeton technique, une phrase générique choisie par nous et des identifiants** : ni le titre d'une tâche, ni le texte d'un message, ni le nom d'une personne. Ce flux est désactivable par l'utilisateur depuis les réglages.

Le CMS éditorial Sanity.io héberge quant à lui du **contenu public**, sans aucune donnée d'utilisateur. Ses images sont servies directement au navigateur des visiteurs du site vitrine ; l'application mobile et l'API n'y font aucun appel.

7.3 Mesure d'usage — sans outil tiers

Le service enregistre **le fait qu'une action a eu lieu** (compte créé, cercle créé, invitation envoyée ou acceptée, tâche créée ou terminée, message envoyé, fiche consultée, question posée à l'assistant). Sans ces chiffres, il est impossible de démontrer à un partenaire public que le service produit un effet.

Trois choix structurent ce traitement :

1. **Émission côté serveur**, dérivée des appels API existants — **aucun SDK d'analyse, aucune donnée hors de Suisse**, aucune bannière de consentement à rouvrir ;
2. **Aucun contenu enregistré** : ni titre de tâche, ni texte de message, ni question à l'assistant. Seulement le type d'action, un horodatage et des identifiants ;
3. **Ni profilage, ni décision individuelle automatisée** (art. 21 nLPD) : les agrégats sont des compteurs et des taux, jamais un score attaché à une personne.

Conservation : 24 mois, puis purge. À la suppression d'un compte, les enregistrements sont privés de tout identifiant.

7.4 Tableau de bord de pilotage (indicateurs agrégés)

Un point d'accès en lecture seule expose des **indicateurs strictement agrégés et anonymes** (nombres de comptes, d'invitations, etc.) à destination d'un tableau de bord de pilotage interne. Il est protégé par un jeton d'authentification dédié, distinct de celui des utilisateurs, et soumis à la limitation de débit. **Aucune donnée personnelle, aucun identifiant et aucun contenu ne transitent par ce point d'accès.**

---

8. Gouvernance et documentation de conformité

Obligation nLPD	État
Registre des activités de traitement (art. 12)	**Rédigé et à jour** — 13 traitements décrits, vérifiés contre le code. Joint sur demande
Déclaration de confidentialité (art. 19)	Rédigée, présentée à l'inscription, publiée en ligne (FR/DE) ; décrit l'assistant, le formulaire professionnel et les durées de conservation
Analyse d'impact (AIPD) (art. 22)	**Réalisée** sur les deux traitements à risque accru : indications de besoins relevant de l'art. 5 let. c, et données d'un tiers non consentant. Joint sur demande. À refaire avant toute mise en production d'un assistant génératif
Annonce des violations (art. 24)	Procédure définie : notification au PFPDT et aux personnes concernées en cas de risque élevé
Contrats de sous-traitance (art. 9)	En place avec Infomaniak
Point de contact protection des données	Identifié au sein de l'équipe Retr'aide — privacy@retraide.ch
Sécurité du contenu généré par les utilisateurs	Signalement et blocage en place ; file de modération dans la console d'administration ; examen sous 24 h ouvrables, engagement publié dans les conditions d'utilisation

---

9. Synthèse : ce que nous garantissons

Pour répondre directement à votre préoccupation — *« pouvoir assurer que tous les éléments sont réunis et respectent le cadre légal »* :

✅ **Hébergement 100 % suisse** (Infomaniak Genève, ISO 27001) — aucune donnée stockée hors de Suisse. ✅ **Aucun proxy ni CDN étranger** dans le chemin des requêtes ; DNS suisse. ✅ **Chiffrement** en transit (TLS 1.3) et **sauvegardes chiffrées côté client** (AES-256), clé détenue par Retr'aide seule. ✅ **Aucune intelligence artificielle générative** dans le produit : l'assistant ne fait que restituer des fiches validées par des humains. ✅ **Aucun prestataire étranger** dans l'authentification ni la messagerie : ni SMS, ni service d'e-mail hors de Suisse. ✅ **Minimisation** : aucun dossier médical, aucune donnée

transmise par un professionnel de santé ; téléphone, photo et écran des besoins facultatifs ; ni profilage, ni décision individuelle automatisée. ✅ **Droits des personnes** implémentés dans le produit (accès, rectification, export, suppression). ✅ **Suppression automatique** sous 30 jours après fermeture de compte. ✅ **Sessions robustes** : jetons de rafraîchissement hachés, rotatifs, révocation de famille en cas de réutilisation. ✅ **Sauvegardes supervisées** (alerte en cas d'échec) et **restauration testée**. ✅ **Notifications paramétrables** : seule une phrase générique quitte la Suisse, jamais le contenu. ✅ **Mesure d'usage sans outil tiers** : émise par notre serveur, sans aucun contenu, conservée 24 mois. ✅ **Monitoring d'erreurs auto-hébergé** en Suisse — aucun prestataire de suivi d'erreurs. ✅ **Signalement et blocage** en place, modération sous 24 h ouvrables. ✅ **Sous-traitants identifiés** et réduits à un seul acteur principal, suisse.

✅ **Durées de conservation définies et appliquées** : 30 jours après fermeture de compte, 12 mois pour les prospects du formulaire « soignants ».

⚠️ **Une limite que nous reconnaissons** (voir §6.2) : nous ne pouvons pas vérifier que le proche aidant informe effectivement la personne aidée, malgré le rappel affiché dans l'application.

Autrement dit, **aucun contenu et aucune identité ne quittent la Suisse**. Le seul flux vers l'étranger est celui des notifications *push* (Expo, puis Apple/Google) : un jeton technique, une phrase générique et des identifiants.

---

10. Vérification des affirmations de cette note

Chaque affirmation technique de ce document est **vérifiable contre le code et sur le serveur**, et a été contrôlée lors de la rédaction du registre des traitements et de l'analyse d'impact. Nous ne décrivons pas des intentions : les mesures énoncées aux § 4 à 7 sont implémentées et contrôlées. En particulier, le chiffrement au repos des secrets applicatifs a été vérifié en base — la valeur du mot de passe SMTP y figure sous forme chiffrée (préfixe `enc:v1:`) et jamais en clair. Nous pouvons produire ces vérifications sur demande.

---

11. Proposition pour la suite

Nous nous tenons à la disposition de toute autorité ou institution partenaire pour :

1. **Transmettre les pièces complémentaires**, disponibles immédiatement : registre des activités de traitement, analyse d'impact, déclaration de confidentialité complète, contrat de sous-traitance et attestations Infomaniak.
2. **Organiser un échange** avec le ou la référent·e protection des données compétent·e (ou l'autorité de protection des données concernée) pour valider conjointement l'approche.
3. **Adapter le dispositif** à toute exigence spécifique jugée nécessaire dans le cadre de la proche aidance.

Nous restons à disposition pour toute information complémentaire.

Avec nos meilleures salutations, **L'équipe Retr'aide**