Analyse d'impact relative à la protection des données

Au sens de l'article 22 de la Loi fédérale sur la protection des données (nLPD, RS 235.1)

1. IDENTIFICATION DU RESPONSABLE DU TRAITEMENT

Raison sociale	***[Nom de l'étude / du cabinet]***
Adresse	***[Adresse]***
Représentant	***[Nom du décideur en matière de protection des données]***
Date de l'AIPD	***[Date]***

2. SOUS-TRAITANT

Sous-traitant principal	Souverain IA — Youness Zangui · Lausanne
Sous-traitant ultérieur	Infomaniak Network SA · Genève (hébergement)
DPA signé le	***[Date]***

3. DESCRIPTION SYSTÉMATIQUE DU TRAITEMENT

3.1 Finalités

Automatisation de tâches répétitives au sein de l'étude (saisie des temps facturables, suivi des délais procéduraux, tri intelligent du courrier, génération de courriers types) à partir des données documentaires propres au cabinet.

3.2 Catégories de données traitées

- Données d'identification (clients, parties adverses, témoins, collaborateurs)
- Données de correspondance (courriers, emails, pièces de procédure)
- Données relatives aux dossiers (numéros, types de procédure, montants)

- Données financières associées (honoraires, avances de frais, ventilation des temps)
- Le cas échéant : données sensibles au sens de l'art. 5 let. c nLPD (données médicales, pénales, opinions politiques, etc.)

3.3 Personnes concernées

Clients du cabinet, parties adverses, témoins, tiers identifiés dans les dossiers, collaborateurs.

3.4 Durée du traitement

Liée à la durée du contrat de prestation. À l'issue, restitution ou suppression certifiée selon le choix du responsable.

4. ÉVALUATION DE LA NÉCESSITÉ ET DE LA PROPORTIONNALITÉ

Le traitement est nécessaire à la prestation contractuelle convenue et proportionné aux finalités poursuivies :

- **Nécessité** : les automatisations ne peuvent fonctionner qu'en ayant accès aux documents internes du cabinet ; tout autre approche (modèle ouvert, données génériques) produirait des résultats inexacts.
- **Proportionnalité** : seules les données strictement nécessaires aux automatisations contractuelles sont traitées ; aucun usage secondaire n'est autorisé ; les données ne quittent pas le territoire suisse.
- **Minimisation** : la base vectorielle est isolée par tenant et purgée à la fin du contrat.

5. ÉVALUATION DES RISQUES POUR LES PERSONNES CONCERNÉES

RISQUE	SOURCE	GRAVITÉ	PROBABILITÉ	MESURE DE MITIGATION
Accès non autorisé	Compromission d'un compte	Élevée	Faible	MFA, isolation tenant, journal d'accès
Fuite de données	Faille technique	Élevée	Faible	Chiffrement AES-256, TLS 1.3, mises à jour de sécurité
Hallucination de l'IA	Génération erronée	Moyenne	Moyenne	RAG fermé sur les données du cabinet, citation des sources, validation humaine obligatoire
Transfert hors CH	Sous-traitance non maîtrisée	Élevée	Nulle	Engagement contractuel d'hébergement exclusif en Suisse
Usage secondaire	Réutilisation pour entraînement	Élevée	Nulle	Interdiction contractuelle ; pas d'entraînement de modèle tiers
Perte de disponibilité	Panne d'infrastructure	Faible	Faible	Sauvegardes quotidiennes ; plan de continuité documenté

6. MESURES TECHNIQUES ET ORGANISATIONNELLES MISES EN ŒUVRE

6.1 Mesures techniques

- Hébergement exclusivement chez Infomaniak Network SA (Genève)
- Chiffrement AES-256 au repos, TLS 1.3 en transit
- Authentification forte (MFA) pour tout accès administrateur
- Isolation logique des données par tenant — pas de mutualisation entre clients
- Journal d'accès horodaté et signé
- Sauvegardes chiffrées quotidiennes, rotation 14 jours
- RAG fermé : les modèles d'IA n'utilisent que les documents du cabinet, jamais une base externe
- Méthode « bac à sable » : tout nouveau traitement testé en environnement isolé avec données fictives ou anonymisées avant production
- Validation humaine obligatoire pour toute action engageante (rédaction, envoi, signature)

6.2 Mesures organisationnelles

- DPA signé conformément à l'art. 9 nLPD
- Engagement de confidentialité du Prestataire, sans limitation de durée
- Documentation des incidents et procédure de notification en 24 heures
- Audit possible par le cabinet sur préavis raisonnable
- Restitution ou suppression certifiée à la fin du contrat

7. ÉVALUATION DU RISQUE RÉSIDUEL

Après mise en œuvre des mesures décrites au point 6, le risque résiduel pour les personnes concernées est évalué comme **faible**. Les principaux risques persistants relèvent :

- de l'erreur humaine d'un collaborateur du cabinet (mauvaise validation d'une sortie) : ce risque relève du fonctionnement habituel d'une étude et n'est pas spécifique à l'automatisation
- d'évolutions réglementaires futures : revue annuelle de l'AIPD prévue

Le risque résiduel est considéré comme acceptable au regard des bénéfices opérationnels et organisationnels apportés par l'automatisation.

8. CONSULTATION DU PFPDT (ART. 23 NLPD)

Une consultation du Préposé fédéral à la protection des données et à la transparence n'est requise que si l'AIPD démontre que le traitement, malgré les mesures, présente encore un risque élevé pour la personnalité ou les droits fondamentaux. **L'évaluation ci-dessus permet de conclure qu'une consultation préalable n'est pas requise dans le présent cas.**

9. VALIDATION ET RÉVISION

La présente AIPD est validée par le responsable du traitement à la date indiquée ci-dessous. Elle fera l'objet d'une révision en cas de modification substantielle du traitement, et au minimum une fois par an.

RESPONSABLE DU TRAITEMENT	SOUS-TRAITANT (À TITRE D'INFORMATION)
Nom, fonction, lieu, date	Youness Zangui · Souverain IA · Lausanne