

Dossier d'aide à l'analyse d'impact (AIPD / EIPD / DPIA) — Phimetra, version 2026-09-29

Destinataires : le responsable du traitement (la clinique utilisatrice de Phimetra) et son juriste ou délégué à la protection des données (DPO). Structure calquée sur la méthode de la CNIL et les lignes directrices du G29 (WP248 rév. 01).

Objet et portée du document. Phimetra intervient comme **sous-traitant** (art. 28 RGPD) de la clinique, qui est **responsable du traitement**. Ce dossier rassemble les informations que Phimetra est en mesure de fournir sur son service pour aider la clinique à conduire sa propre analyse d'impact (art. 35 RGPD). Il ne remplace pas cette analyse : la décision de la mener, son contenu final et sa validation appartiennent au responsable du traitement.

Les rubriques marquées À compléter par le responsable du traitement sont volontairement laissées à la clinique : elles dépendent de son organisation et de ses choix, que Phimetra ne connaît pas.

Transparence. Phimetra ne détient **aucune certification** (ni HDS, ni ISO 27001, ni SOC 2) et n'a fait l'objet d'**aucun audit externe**. Phimetra n'a **pas désigné de DPO** ; le contact dédié est privacy@phimetra.com. Les mesures décrites ci-dessous sont déclarées par l'éditeur et reflètent l'état du service au 29/09/2026.

1. Description du traitement

1.1 Finalité

Pré-consultation esthétique **informative** : à partir d'une photo du visage prise par la patiente, le service produit une analyse et, lorsque le moteur est actif, une simulation visuelle, destinées à préparer l'échange avec la clinique. Phimetra **n'est pas un dispositif médical** et **ne pose aucun diagnostic médical**.

1.2 Personnes concernées

Patientes adultes de la clinique qui utilisent le parcours de pré-consultation.

1.3 Catégories de données

Donnée	Nature	Caractère
Photo du visage et empreinte faciale dérivée	Donnée biométrique et, selon l'usage, donnée concernant la santé — catégorie particulière (art. 9 RGPD)	Nécessaire au service
Nom, adresse e-mail, téléphone	Données d'identification et de contact	Facultatifs
Résultats : analyse, sessions de simulation, devis, rendez-vous, invitations	Données produites par le service ; peuvent révéler des informations relatives à la santé	Produits par le service
Consentement	Preuve du consentement, horodatée	Nécessaire

Donnée	Nature	Caractère
Journal des accès	Identifiant du compte (ou « patiente / anonyme »), date, type de données et identifiants, route, résultat, empreinte d'adresse IP (pas l'IP en clair)	Sécurité et traçabilité

1.4 Flux de données

1. **Navigateur de la patiente.** La détection du visage s'effectue dans le navigateur (MediaPipe) ; les modèles sont servis par phimetra.com, sans appel à Google pendant la capture.
2. **Serveur Phimetra en France** (OVHcloud, serveur situé à Strasbourg) : réception en HTTPS, stockage dans un volume chiffré.
3. **Analyse** par Scaleway SAS, service « Generative APIs », centres de données de **Paris** (modèle Mistral Small 3.2 ; repli Mistral Medium 3.5, même fournisseur, même région).
4. **Simulation visuelle** par IONOS Cloud, AI Model Hub, en **Allemagne** (modèle FLUX.2 [klein] 4B, Black Forest Labs, licence Apache-2.0).
5. **Recomposition sur le serveur en France** : la zone traitée est replacée sur la photo d'origine ; le reste de la photo reste identique au pixel près.
6. **E-mails transactionnels** (confirmation, rendez-vous, devis) par Scaleway Transactional Email (Paris). Aucun e-mail ne contient d'image du visage.

État du moteur de simulation au 29/09/2026 : en cours d'activation. Tant qu'il n'est pas actif, la simulation est indisponible. Il n'existe **aucun moteur de repli hors de l'Union européenne**.

Aucune photo, analyse ou simulation n'est transférée hors de l'Union européenne. Tous les échanges (navigateur ↔ serveur, serveur ↔ sous-traitants) sont chiffrés par TLS (HTTPS).

1.5 Destinataires

- La clinique (responsable du traitement), par ses comptes sur l'application.
- Phimetra (sous-traitant) : une seule personne, l'éditeur, dispose d'un accès administrateur à la production.
- Les sous-traitants ultérieurs listés en section 5, dans la limite de leur rôle.

Correspondance : les messages adressés à contact@phimetra.com et privacy@phimetra.com transitent par Cloudflare Email Routing et sont lus dans une boîte Google (Gmail). Ce canal ne sert pas au traitement des photos ; il ne faut pas y envoyer de photos.

À compléter par le responsable du traitement : personnes habilitées au sein de la clinique, et autres destinataires éventuels côté clinique.

1.6 Durées de conservation (purge automatique chaque nuit, vérifiée)

Données	Durée maximale chez Phimetra
Photos du visage et empreinte faciale dérivée	30 jours après la capture
Fichiers temporaires de simulation	Effacés dès que le résultat est lu, au plus tard 2 heures après

Données	Durée maximale chez Phimetra
Analyses, rendez-vous, sessions de simulation, devis, invitations, journal des accès	12 mois après leur création
Requêtes chez Scaleway (analyse)	Non conservées selon le fournisseur, sauf abus ou erreur serveur : 2 semaines au plus
Entrées chez IONOS (simulation)	Ni journalisées ni stockées selon le fournisseur

À compléter par le responsable du traitement : durée de conservation des données que la clinique extrait ou recopie dans ses propres outils (dossier patient, agenda, messagerie).

2. Base légale

- **Article 9 (données sensibles) :** consentement explicite de la patiente (art. 9-2-a RGPD), recueilli par l'interface **avant la capture** de la photo et horodaté.
- **Article 6 (licéité générale) :** le choix de la base légale relève du responsable du traitement.

À compléter par le responsable du traitement : base légale retenue au titre de l'article 6, et modalités de retrait du consentement proposées par la clinique.

3. Nécessité et proportionnalité

- **Minimisation :** seule la photo du visage est nécessaire ; nom, e-mail et téléphone sont facultatifs. La détection du visage est faite dans le navigateur. Aucune image du visage n'est envoyée par e-mail. Le journal des accès conserve une empreinte d'IP, pas l'IP en clair.
- **Conservation courte :** photos supprimées au plus tard 30 jours après la capture ; fichiers temporaires de simulation au plus tard 2 heures ; autres données 12 mois (section 1.6).
- **Pas d'entraînement :** ni Phimetra ni ses sous-traitants d'IA n'utilisent les photos ou les résultats pour entraîner des modèles (engagement de Phimetra ; déclarations de Scaleway et d'IONOS dans leurs conditions).
- **Pas de publicité sur le parcours patient :** le pixel publicitaire Meta ne se charge jamais sur les pages du parcours patient (et, sur les pages marketing, seulement après consentement).
- **Localisation :** tous les traitements de données de patientes ont lieu dans l'Union européenne (France, Allemagne).
- **Information des personnes :** l'interface informe la patiente avant la capture et recueille son consentement ; elle l'informe qu'il s'agit d'un système d'IA (section 7).
- **Droits des personnes** (accès, rectification, effacement, retrait du consentement...) : ils s'exercent auprès de la clinique ; Phimetra l'assiste sur demande (privacy@phimetra.com).
- **Fin de contrat :** suppression des données et attestation écrite remise à la clinique.

4. Mesures de sécurité

Mesure	Description
Chiffrement en transit	TLS (HTTPS) entre le navigateur et le serveur, et vers chaque sous-traitant.
Chiffrement au repos	Base de données (photos, analyses, rendez-vous, journal) et fichiers temporaires de simulation dans un volume chiffré LUKS2 (AES-256-XTS, dérivation de clé argon2id) . La clé n'est pas stockée sur le serveur : elle est conservée chez Scaleway Secret Manager (Paris) et n'est lue qu'au démarrage, en mémoire.
Sauvegardes	Sauvegardes de la base réalisées dans le volume chiffré ; copies hors serveur chiffrées (AES-256).
Journal des accès	Chaque lecture, liste, export, création, modification, suppression ou partage d'un dossier patient via l'application est enregistré (qui, quand, quoi, route, résultat, empreinte d'IP). Conservé 12 mois, consultable par l'éditeur ; extrait fourni à la clinique sur demande pour ses propres dossiers. Les accès administrateur à la base sont aussi journalisés par la base (journaux de requêtes).
Contrôle des accès	Une seule personne (l'éditeur) a un accès administrateur à la production ; accès au serveur par clé SSH uniquement.
Purges automatiques	Exécutées chaque nuit sur le serveur (durées en section 1.6).
Réduction de l'exposition	Aucune image de visage par e-mail ; pas de pixel Meta sur le parcours patient ; modèles de détection du visage servis par phimetra.com (aucun appel à Google pendant la capture) ; aucun moteur de repli hors UE.
Violations de données	Notification à la clinique sous 48 heures après que Phimetra en a eu connaissance.
Sous-traitants ultérieurs	Préavis de 30 jours avant tout changement ; liste versionnée et datée sur /legal/security.

Limites connues. Il n'y a **pas de chiffrement de bout en bout**. Le chiffrement au repos protège contre l'accès aux disques et aux copies ; il **ne protège pas un serveur compromis en fonctionnement**. L'administration repose sur une seule personne. Aucune certification ni aucun audit externe n'étaye ces mesures.

5. Sous-traitants ultérieurs

Liste en vigueur au 29/09/2026 (générée à partir de la liste officielle publiée sur /legal/security) :

Sous-traitant / entité	Localisation	Rôle	Données traitées	Garanties	Depuis / statut
OVHcloud OVH SAS, 2 rue Kellermann, 59100 Roubaix, France	France (Strasbourg) Hors EEE : non	Hébergement du serveur applicatif et de la base de données (VPS)	Toutes les données du service, stockées dans un volume chiffré (LUKS2, AES-256) Données de patientes : oui	Contrat de sous-traitance OVHcloud (Data Processing Agreement) intégré aux conditions de service Contrat de sous-traitance (lien)	2026-07-17 Actif

Sous-traitant / entité	Localisation	Rôle	Données traitées	Garanties	Depuis / statut
Scaleway — Generative APIs Scaleway SAS, 8 rue de la Ville l'Évêque, 75008 Paris, France	France (Paris) Hors EEE : non	Analyse de la photo par un modèle d'IA (Mistral Small 3.2 ; repli Mistral Medium 3.5, même fournisseur, même région)	Photo du visage et consignes d'analyse, le temps du traitement ; le fournisseur déclare ne pas conserver les requêtes (sauf abus ou erreur serveur, 2 semaines au plus) et ne pas les utiliser pour l'entraînement Données de patientes : oui	Contrat de sous-traitance (DPA) Scaleway intégré au contrat ; pas de conservation des requêtes ni d'entraînement (déclaration du fournisseur) Contrat de sous-traitance (lien)	2026-09-28 Actif
IONOS Cloud — AI Model Hub IONOS Cloud (entité du groupe IONOS désignée au contrat) ; inférence dans les centres de données IONOS Cloud en Allemagne	Allemagne Hors EEE : non	Rendu de la simulation visuelle (modèle FLUX.2 [klein] 4B) ; la zone traitée est ensuite recomposée sur la photo d'origine sur notre serveur en France	Photo du visage, le temps du rendu ; le fournisseur déclare ne pas journaliser ni stocker les entrées et ne pas les utiliser pour l'entraînement Données de patientes : oui	Contrat de sous-traitance IONOS Cloud intégré au contrat ; entrées non journalisées, non stockées, non utilisées pour l'entraînement (déclaration du fournisseur) Contrat de sous-traitance (lien)	2026-09-28 En cours d'activation
Scaleway — Transactional Email Scaleway SAS, 8 rue de la Ville l'Évêque, 75008 Paris, France	France (Paris) Hors EEE : non	Envoi des e-mails transactionnels (confirmation, rendez-vous, devis)	Nom et adresse e-mail du destinataire, contenu du message ; jamais d'image du visage Données de patientes : oui	Contrat de sous-traitance (DPA) Scaleway intégré au contrat Contrat de sous-traitance (lien)	2026-09-28 Actif
Stripe Stripe Payments Europe, Ltd., Dublin, Irlande	Irlande (UE) Hors EEE : non	Paiement de l'abonnement de la clinique	Données de facturation de la clinique uniquement — aucune donnée de patiente Données de patientes : non	Accord de traitement des données Stripe ; ne reçoit aucune donnée de patiente Contrat de sous-traitance (lien)	2026-05-01 Actif

Historique des changements

- 2026-09-29** — Les simulations antérieures stockées chez fal.ai ont été supprimées (478 requêtes, 369 fichiers). Aucun sous-traitant ajouté. Précisions : entité IONOS Cloud désignée au contrat ; lien vers les contrats d'OVHcloud (OVH SAS).
- 2026-09-28** — Tous les traitements de données de patientes passent dans l'Union européenne : l'analyse passe d'OpenRouter (États-Unis) à Scaleway (Paris), la simulation de fal.ai (États-Unis) à IONOS Cloud (Allemagne), les e-mails de Resend (États-Unis) à Scaleway (Paris). Les modèles d'IA gratuits de secours sont supprimés. Le site n'est plus relayé par le proxy Cloudflare.

Anciens sous-traitants retirés les 28-29/09/2026 : OpenRouter (États-Unis, analyse), modèles d'IA gratuits de secours, fal.ai (États-Unis, simulation), Resend (États-Unis, e-mails), proxy Cloudflare (le site n'est plus relayé par Cloudflare). Les simulations antérieures stockées chez fal.ai ont été supprimées (478 requêtes, 369 fichiers).

6. Risques pour les droits et libertés des personnes

Échelles utilisées (méthode CNIL) : *négligeable, limité, important, maximal*. Les niveaux ci-dessous sont une **estimation proposée par Phimetra**, à discuter et à **valider par le responsable du traitement**, qui peut les revoir en fonction de son propre contexte.

Risque	Sources de risque et menaces	Mesures existantes	Risque résiduel proposé
Accès illégitime aux données Impact : divulgation de la photo du visage et d'informations d'ordre esthétique ou de santé ; atteinte à la vie privée, gêne, préjudice moral.	Attaquant externe (application, serveur) ; compromission ou erreur d'un sous-traitant ; utilisation abusive d'un compte de la clinique ou d'un accès administrateur ; vol d'identifiants ; envoi de photos par un canal non prévu (e-mail).	TLS ; volume chiffré LUKS2 avec clé hors serveur ; copies hors serveur chiffrées ; accès SSH par clé uniquement ; un seul administrateur ; journal des accès (y compris requêtes administrateur) ; conservation courte (photos ≤ 30 j) ; pas de conservation ni d'entraînement déclarés par les sous-traitants d'IA ; aucune image par e-mail ; pas de pixel Meta sur le parcours patient ; traitement 100 % UE ; notification sous 48 h.	Gravité : importante (données de l'article 9) Vraisemblance : limitée Points de vigilance : pas de chiffrement de bout en bout ; un serveur compromis en fonctionnement n'est pas protégé par le chiffrement au repos ; pas d'audit externe.
Modification non désirée des données Impact : analyse, rendez-vous ou devis erronés ; information inexacte donnée à la patiente.	Attaquant externe ; erreur logicielle ; erreur de manipulation ; résultat inexact d'un modèle d'IA.	Journal de toute création, modification et suppression ; accès restreints ; TLS ; simulation recomposée sur la photo d'origine (reste de la photo identique au pixel près) ; service présenté comme informatif, non médical, avec information sur l'usage de l'IA.	Gravité : limitée Vraisemblance : limitée
Disparition des données Impact : perte de l'analyse, des rendez-vous ou devis ; nouvelle capture à réaliser.	Panne matérielle ou de l'hébergeur ; erreur d'administration ; logiciel malveillant ; perte d'accès à la clé de chiffrement ; indisponibilité d'un sous-traitant ; dépendance à un administrateur unique.	Sauvegardes dans le volume chiffré ; copies hors serveur chiffrées (AES-256) ; clé conservée chez Scaleway Secret Manager (hors serveur) ; absence de moteur de repli hors UE assumée (indisponibilité plutôt que transfert).	Gravité : limitée Vraisemblance : limitée Point de vigilance : fréquence des sauvegardes et tests de restauration non décrits dans ce dossier ; à demander à Phimetra si nécessaire.

À compléter par le responsable du traitement : validation ou révision des niveaux de risque ; mesures complémentaires côté clinique (habilitations, postes de travail, procédure de gestion des violations).

7. Règlement européen sur l'IA (AI Act)

- Phimetra est un système d'IA à **risque limité**, soumis aux obligations de transparence de l'**article 50** : la patiente est informée qu'elle interagit avec un système d'IA et que l'analyse et la simulation sont produites par un tel système.
- Phimetra n'est pas un dispositif médical et ne fait pas de diagnostic médical.

- Modèles utilisés : Mistral Small 3.2 (repli Mistral Medium 3.5) pour l'analyse, via Scaleway (Paris) ; FLUX.2 [klein] 4B (Black Forest Labs, licence Apache-2.0) pour la simulation, via IONOS Cloud (Allemagne), en cours d'activation.

8. Points à compléter par le responsable du traitement

Rubrique	Réponse de la clinique
Base légale retenue au titre de l'article 6 RGPD	
Information des patientes : affichage en cabinet, mentions dans les documents de la clinique, politique de confidentialité	
Durée de conservation côté clinique (données extraites ou recopiées)	
Personnes habilitées et gestion des comptes	
Validation des niveaux de risque (section 6) et mesures complémentaires	
Avis du DPO de la clinique (s'il en existe un)	
Consultation des personnes concernées ou de leurs représentants (le cas échéant)	
Décision et validation : nom, fonction, date, signature	

Contact

Questions sur ce dossier, demande d'extrait du journal des accès, assistance pour les droits des personnes : privacy@phimetra.com. Merci de ne jamais envoyer de photos par e-mail.