φ phimetra

Modèle standard — version 2026-11-10 — **la version signée par les parties fait foi** · Télécharger le PDF (français)

Accord de sous-traitance

Article 28 du Règlement (UE) 2016/679 (RGPD)

Le présent accord encadre le traitement de données à caractère personnel que le Sous-traitant effectue pour le compte de la clinique dans le cadre du service de pré-consultation esthétique Phimetra. Il complète le contrat d'abonnement et prévaut sur celui-ci pour tout ce qui concerne la protection des données.

1. Parties et rôles

La clinique cliente (ci-après « le Responsable ») détermine les finalités et les moyens du traitement : elle est responsable du traitement au sens de l'article 4, 7) du RGPD. Wahib Znidah, entrepreneur individuel exerçant sous le nom commercial SAYWA, éditeur du service Phimetra, établi en France (ci-après « le Sous-traitant »), traite les données uniquement pour le compte du Responsable, au sens de l'article 4, 8) du RGPD.

2. Objet, durée, nature et finalité du traitement

Le Sous-traitant réalise l'analyse morphologique d'une photographie du visage et produit une simulation visuelle indicative (aperçu avant/après), destinées à préparer la consultation esthétique menée par le Responsable. Ces résultats sont indicatifs et ne constituent ni un diagnostic ni un engagement de résultat. Le traitement dure pendant toute la durée de l'abonnement souscrit par le Responsable, puis jusqu'à la suppression prévue aux clauses 10 et 11.

3. Catégories de données et de personnes concernées

Personnes concernées : les patientes et patients adultes de la clinique. Catégories de données traitées :

- photographie du visage et une trent
  (angles, proportions, asymétries) —
  comparaison de personnes ; ces me
  l'article 9 du RGPD ; le Responsable
  capture ;
- nom, adresse e-mail et numéro de t

Consentement aux cookies

Les cookies essentiels assurent le fonctionnement. Les cookies marketing sont facultatifs. Confidentialité

Refuser le marketing

Accepter le marketing

- résultats d'analyse, simulations, rendez-vous, devis et invitations produits par le service ;
- horodatage et contenu du consentement recueilli ;
- journal des accès (identifiant du compte, date, type d'opération, empreinte de l'adresse IP).

4. Instructions documentées

Le Sous-traitant traite les données uniquement sur instruction documentée du Responsable. L'utilisation du service par le Responsable (envoi d'une photo, lancement d'une analyse ou d'une simulation) constitue cette instruction. Le Sous-traitant n'utilise jamais les photographies ni les résultats pour entraîner des modèles d'intelligence artificielle, ni pour aucune finalité propre ; ses sous-traitants d'IA (Scaleway, IONOS) déclarent également ne pas les utiliser pour l'entraînement. Si le Sous-traitant estime qu'une instruction contrevient au RGPD, il en informe immédiatement le Responsable.

5. Confidentialité des personnes autorisées

Une seule personne, l'éditeur, dispose d'un accès administrateur à l'environnement de production. Elle est tenue à la confidentialité et informée de ses obligations en matière de protection des données.

6. Sécurité du traitement (article 32)

Le Sous-traitant met en œuvre les mesures techniques et organisationnelles suivantes :

- chiffrement en transit : TLS (HTTPS) entre le navigateur et le serveur, et vers chaque sous-traitant ultérieur ;
- chiffrement au repos : la base de données (photos, analyses, rendez-vous, journal) et les fichiers temporaires de simulation sont stockés 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 réalisées dans ce 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 (auteur, date, données concernées, route, résultat, empreinte de l'adresse IP) et conservé 12 mois ; un extrait est fourni au Responsable, sur demande, pour ses propres dossiers ; les accès administrateur à la base sont journalisés par la base ;
- accès administrateur à la production réservé à une seule personne (l'éditeur) ; accès au serveur par clé SSH uniquement ;
- aucune image de visage n'est envoyée par e-mail ; le pixel publicitaire Meta ne se charge jamais sur les pages du parcours patient ;
- modèles de détection du visage (Me
  capture.

Limites : il n'y a pas de chiffrement de b
disques et aux copies, pas contre un se
aucune certification (HDS, ISO 27001, S
: phimetra.com/legal/security

Consentement aux cookies

Les cookies essentiels assurent le fonctionnement. Les cookies marketing sont facultatifs. Confidentialité

7. Sous-traitants ultérieurs

Le Responsable autorise de manière générale le recours aux sous-traitants ultérieurs listés ci-dessous. Le Sous-traitant informe le Responsable de tout ajout ou remplacement envisagé avec un préavis de 30 jours, afin de lui permettre d'émettre des objections. Le Sous-traitant impose à chaque sous-traitant ultérieur des obligations de protection des données par contrat (article 28, paragraphe 4, du RGPD).

- OVHcloud — OVH SAS, 2 rue Kellermann, 59100 Roubaix, France — France (Strasbourg) : Hébergement du serveur applicatif et de la base de données (VPS). Toutes les données du service, stockées dans un volume chiffré (LUKS2, AES-256).
- Scaleway — Generative APIs — Scaleway SAS, 8 rue de la Ville l'Évêque, 75008 Paris, France — France (Paris) : 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.
- 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 : 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. (en cours d'activation — d'ici là, la simulation se limite à un aperçu approximatif calculé sur le serveur en France ; aucun moteur hors de l'Union européenne n'est utilisé à la place, sauf l'option prévue à l'article 8)
- fal.ai (option de la clinique) — Features & Labels, Inc., 2261 Market St. Suite 10467, San Francisco, CA 94114, USA — États-Unis (hors UE) : Simulation visuelle aux États-Unis, uniquement si la clinique l'a expressément autorisée dans son tableau de bord ET que la patiente y a consenti ; ce choix est enregistré. Par défaut, la simulation reste dans l'Union européenne : Allemagne si le moteur payant répond, sinon le serveur en France. Confidentialité médicale impose toujours l'Union européenne. Le parcours public sans compte reste en France.. Photo du visage et consigne de la zone à simuler, pour la seule durée du rendu.
- Scaleway — Transactional Email — Scaleway SAS, 8 rue de la Ville l'Évêque, 75008 Paris, France — France (Paris) : Envoi des e-mails transactionnels (confirmation, rendez-vous, devis). Nom et adresse e-mail du destinataire, contenu du message ; jamais d'image du visage.
- Stripe — Stripe Payments Europe, Ltd., Dublin, Irlande — Irlande (UE) : Paiement de l'abonnement de la clinique. Données de facturation de la clinique uniquement — aucune donnée de patiente.

Liste versionnée et datée, avec son historique : phimetra.com/legal/security

8. Transferts hors de l'Union européenne

L'application et la base sont hébergées
faite chez Scaleway à Paris. Par défaut
moteur payant répond, sinon en France
expressément autorisé dans son tablea
impose toujours l'Union européenne. Le

Consentement aux cookies

Les cookies essentiels assurent le fonctionnement. Les cookies marketing sont facultatifs. Confidentialité

Le lien envoyé à la patiente reste dans l'Union européenne, sauf si la clinique a autorisé un traitement hors UE et que la patiente y a consenti. Les photos stockées le sont en France, 30 jours au plus. Chiffrement en transit et au repos. Les coordonnées et les rendez-vous restent hébergés en France.

9. Assistance au Responsable

Compte tenu de la nature du traitement, le Sous-traitant aide le Responsable :

- à répondre aux demandes d'exercice des droits des personnes (accès, rectification, effacement, limitation, portabilité, opposition) ;
- à réaliser, le cas échéant, l'analyse d'impact relative à la protection des données (AIPD) et la consultation préalable de l'autorité de contrôle ; un dossier d'aide à l'AIPD est fourni ;
- à respecter ses obligations en cas de violation de données : le Sous-traitant notifie au Responsable toute violation de données à caractère personnel dans les 48 heures suivant le moment où il en a connaissance, avec les éléments dont il dispose pour la notification prévue à l'article 33.

10. Conservation

Les données sont supprimées automatiquement, par des purges exécutées chaque nuit :

- photographies du visage : au plus tard 30 jours après la capture ; les mesures géométriques sont conservées avec l'analyse (ligne ci-dessous) ;
- fichiers temporaires de simulation : dès que le résultat est lu, au plus tard 2 heures après ;
- analyses, rendez-vous, sessions de simulation, devis, invitations et journal des accès : 12 mois après leur création.

11. Fin du contrat et sort des données

À la fin de l'abonnement, le Sous-traitant supprime les données du Responsable : dans les 30 jours suivant la résiliation si le Responsable le demande, et au plus tard à l'expiration des durées de la clause 10. Il remet au Responsable une attestation écrite de suppression. Il ne conserve aucune copie, sauf obligation légale de conservation.

12. Audits et documentation

Le Sous-traitant met à la disposition du Responsable toutes les informations nécessaires pour démontrer le respect des obligations prévues à l'article 28 du RGPD. Le Responsable peut faire réaliser un audit, par lui-même ou par un auditeur mandaté, u
préavis écrit de 30 jours et sans perturb

13. Droit applicable et autorité de contrôle

Le présent accord est régi par le droit f
est la Commission nationale de l'inform

Consentement aux cookies

Les cookies essentiels assurent le fonctionnement. Les cookies marketing sont facultatifs. Confidentialité

autre État membre, l'autorité de contrôle de cet État (en Espagne, l'Agencia Española de Protección de Datos, AEPD) reste compétente pour ses propres obligations en tant que responsable du traitement.

14. Contact

Toute communication relative au présent accord, notamment les notifications et les demandes d'assistance, est adressée à privacy@phimetra.com. Le Sous-traitant n'a pas désigné de délégué à la protection des données ; cette adresse est le point de contact dédié.

Signatures

Fait en deux exemplaires. Les champs du Responsable du traitement sont à compléter par la clinique.

Responsable du traitement (la clinique)

Dénomination

Adresse

Numéro d'immatriculation

Représentée par

Qualité

Lieu

Date

Signature

Sous-traitant

Wahib Znidah, entrepreneur individuel

Nom commercial : SAYWA (service Phimetra)

SIREN 888 001 054

contact@phimetra.com

privacy@phimetra.com

Lieu

Date

Signature

Signature et questions

Téléchargez le PDF, complétez le bloc «

toute question, à : privacy@phimetra.c

Télécharger le PDF (français)

Consentement aux cookies

Les cookies essentiels assurent le fonctionnement. Les cookies marketing sont facultatifs. Confidentialité

Consentement aux cookies

Les cookies essentiels assurent le fonctionnement. Les cookies marketing sont facultatifs. Confidentialité