φ phimetra

Standard template — version 2026-11-10 — **the version signed by the parties prevails** · Download the PDF (English)

Data Processing Agreement

Article 28 of Regulation (EU) 2016/679 (GDPR)

This agreement governs the processing of personal data carried out by the Processor on behalf of the clinic as part of the Phimetra aesthetic pre-consultation service. It supplements the subscription agreement and prevails over it in all matters relating to data protection.

1. Parties and roles

The client clinic (hereinafter "the Controller") determines the purposes and means of the processing and is the controller within the meaning of Article 4(7) GDPR. Wahib Znidah, sole proprietor trading as SAYWA, publisher of the Phimetra service, established in France (hereinafter "the Processor"), processes the data solely on behalf of the Controller, within the meaning of Article 4(8) GDPR.

2. Subject matter, duration, nature and purpose of the processing

The Processor performs a morphological analysis of a photograph of the face and produces an indicative visual simulation (before/after preview), intended to prepare the aesthetic consultation conducted by the Controller. These results are indicative and constitute neither a diagnosis nor a guarantee of outcome. The processing lasts for the duration of the subscription taken out by the Controller, and until the deletion provided for in clauses 10 and 11.

3. Categories of data and data subjects

Data subjects: adult patients of the clinic. Categories of data processed:

- photograph of the face and about thirty geometric measurements computed from it (angles, proportions, asymmetries) — no lanc
  persons; these measurements are t
  the explicit consent of the data subj
- name, e-mail address and telephone
- analysis results, simulations, appoin
- timestamp and content of the conse
- access log (account identifier, date, t

Cookie consent

Essential cookies keep the site working. Marketing cookies are optional. Privacy.

Decline marketing | Allow marketing

4. Documented instructions

The Processor processes the data only on documented instructions from the Controller. The Controller's use of the service (uploading a photograph, launching an analysis or a simulation) constitutes such instructions. The Processor never uses photographs or results to train artificial intelligence models, nor for any purpose of its own; its AI sub-processors (Scaleway, IONOS) also state that they do not use them for training. If the Processor considers that an instruction infringes the GDPR, it shall immediately inform the Controller.

5. Confidentiality of authorised persons

A single person, the publisher, has administrator access to the production environment. That person is bound by confidentiality and informed of their data protection obligations.

6. Security of processing (Article 32)

The Processor implements the following technical and organisational measures:

- encryption in transit: TLS (HTTPS) between the browser and the server, and to each sub-processor;
- encryption at rest: the database (photos, analyses, appointments, log) and temporary simulation files are stored in a LUKS2 encrypted volume (AES-256-XTS, argon2id key derivation); the key is not stored on the server: it is kept in Scaleway Secret Manager (Paris) and only read at start-up, in memory;
- backups made inside this encrypted volume; off-server copies encrypted (AES-256);
- access log: every read, listing, export, creation, modification, deletion or sharing of a patient record through the application is recorded (author, date, data concerned, route, outcome, hash of the IP address) and kept for 12 months; an extract is provided to the Controller on request for its own records; administrator access to the database is logged by the database;
- administrator access to production restricted to a single person (the publisher); server access by SSH key only;
- no face image is ever sent by e-mail; the Meta advertising pixel never loads on the pages of the patient journey;
- face-detection models (MediaPipe) served by phimetra.com, with no call to Google during capture.

Limitations: there is no end-to-end encryption; encryption at rest protects against access to the disks and copies, not against a compromised server while it is running. The Processor holds no certification (HDS, ISO 27001, SOC 2) and has not commissioned an external audit. Detailed description: phimetra.com/legal/security

7. Sub-processors

The Controller gives general authorisati
shall inform the Controller of any intenc
the Controller to object. The Processor
contract (Article 28(4) GDPR).

Cookie consent

Essential cookies keep the site working. Marketing cookies are optional. Privacy.

- OVHcloud — OVH SAS, 2 rue Kellermann, 59100 Roubaix, France — France (Strasbourg) : Hosting of the application server and database (VPS). All service data, stored in an encrypted volume (LUKS2, AES-256).
- Scaleway — Generative APIs — Scaleway SAS, 8 rue de la Ville l'Évêque, 75008 Paris, France — France (Paris) : Analysis of the photo by an AI model (Mistral Small 3.2; fallback Mistral Medium 3.5, same provider, same region). Face photo and analysis instructions, for the duration of processing; the provider states it does not store requests (except abuse or server errors, up to 2 weeks) and does not use them for training.
- IONOS Cloud — AI Model Hub — IONOS Cloud (IONOS group entity named in the contract); inference in IONOS Cloud data centres in Germany — Germany : Rendering of the visual simulation (FLUX.2 [klein] 4B model); the treated area is then recomposed onto the original photo on our server in France. Face photo, for the duration of rendering; the provider states inputs are neither logged nor stored and not used for training. (being activated — until then, the simulation is limited to an approximate preview computed on the server in France; no engine outside the European Union is used instead, except the option described in section 8)
- fal.ai (option de la clinique) — Features & Labels, Inc., 2261 Market St. Suite 10467, San Francisco, CA 94114, USA — United States (outside the EU) : Visual simulation in the United States, only if the clinic has expressly authorised it in its dashboard AND the patient has consented; that choice is recorded. By default, the simulation stays in the European Union: Germany if the paid engine answers, otherwise the server in France. Medical privacy always forces the European Union. The public path without an account stays in France.. Face photo and instruction for the area to simulate, for the duration of the rendering only.
- Scaleway — Transactional Email — Scaleway SAS, 8 rue de la Ville l'Évêque, 75008 Paris, France — France (Paris) : Delivery of transactional e-mails (confirmation, appointment, quote). Recipient name and e-mail address, message content; never any face image.
- Stripe — Stripe Payments Europe, Ltd., Dublin, Irlande — Ireland (EU) : Payment of the clinic's subscription. Clinic billing data only — no patient data.

Versioned and dated list, with its history: phimetra.com/legal/security

8. Transfers outside the European Union

The application and database are hosted at OVHcloud in Strasbourg (France). Photo analysis is performed by Scaleway in Paris. By default, the simulation stays in the European Union: in Germany if the paid engine answers, otherwise in France. Processing by fal.ai (United States) happens only if the clinic has expressly authorised it in its dashboard AND the patient has consented. Medical privacy always forces the European Union. The public path wi
sent to the patient stays in the Europea
and the patient has consented. Stored
and at rest. Contact details and appoin

Cookie consent

Essential cookies keep the site working. Marketing cookies are optional. Privacy.

9. Assistance to the Controller

Taking into account the nature of the pr

- in responding to requests from data subjects exercising their rights (access, rectification, erasure, restriction, portability, objection);
- in carrying out, where required, the data protection impact assessment (DPIA) and the prior consultation of the supervisory authority; a DPIA support file is provided;
- in meeting its obligations in the event of a data breach: the Processor notifies the Controller of any personal data breach within 48 hours of becoming aware of it, together with the information available to it for the notification provided for in Article 33.

10. Retention

Data is deleted automatically, by deletion jobs run every night:

- face photographs: no later than 30 days after capture; the geometric measurements are kept with the analysis (next item);
- temporary simulation files: as soon as the result has been read, and no later than 2 hours afterwards;
- analyses, appointments, simulation sessions, quotes, invitations and access log: 12 months after creation.

11. End of the agreement and fate of the data

At the end of the subscription, the Processor deletes the Controller's data: within 30 days of termination at the Controller's request, and at the latest upon expiry of the periods in clause 10. It provides the Controller with a written certificate of deletion. It retains no copy, except where retention is required by law.

12. Audits and documentation

The Processor makes available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR. The Controller may conduct an audit, itself or through a mandated auditor, once in any twelve-month period, at its own expense, subject to 30 days' written notice and without disrupting the service provided to other clients.

13. Governing law and supervisory authority

This agreement is governed by French law. The supervisory authority competent for the Processor is the Commission nationale de l'informatique et des libertés (CNIL). For a Controller established in another Member State, the supervisory authority of that State (in Spain, the Agencia Española de Protección de Datos, AEPD) remains competent for its

14. Contact

All communications relating to this agr
sent to privacy@phimetra.com. The Pro
is the dedicated point of contact.

Cookie consent

Essential cookies keep the site working. Marketing cookies are optional. Privacy.

Signatures

Made in two copies. The Controller's fields are to be completed by the clinic.

Controller (the clinic)

Company name

Address

Registration number

Represented by

Title

Place

Date

Signature

Processor

Wahib Znidah, sole proprietor (entrepreneur individuel)

Trade name: SAYWA (Phimetra service)

SIREN 888 001 054

contact@phimetra.com

privacy@phimetra.com

Place

Date

Signature

Signature and questions

Download the PDF, complete the "Controller" block and send the signed copy, or any question, to: privacy@phimetra.com

Download the PDF (English)

← Security and privacy

Cookie consent

Essential cookies keep the site working. Marketing cookies are optional. Privacy.

Cookie consent

Essential cookies keep the site working. Marketing cookies are optional. Privacy.