Data protection impact assessment support file (DPIA / AIPD / EIPD) — Phimetra, version 2026-09-29

Intended for: the controller (the clinic using Phimetra) and its legal counsel or data protection officer (DPO). Structure based on the CNIL methodology and the Article 29 Working Party guidelines (WP248 rev. 01).

Purpose and scope of this document. Phimetra acts as a **processor** (Art. 28 GDPR) for the clinic, which is the **controller**. This file gathers the information Phimetra can provide about its service to help the clinic carry out its own impact assessment (Art. 35 GDPR). It does not replace that assessment: the decision to carry it out, its final content and its approval rest with the controller.

Items marked `To be completed by the controller` are deliberately left to the clinic: they depend on its organisation and choices, which Phimetra does not know.

Transparency. Phimetra holds **no certification** (neither HDS, ISO 27001 nor SOC 2) and has **not been externally audited**. Phimetra has **not appointed a DPO**; the dedicated contact is privacy@phimetra.com. The measures described below are stated by the publisher and reflect the service as of 29 September 2026.

1. Description of the processing

1.1 Purpose

Informative aesthetic pre-consultation: from a photo of the face taken by the patient, the service produces an analysis and, when the engine is active, a visual simulation, intended to prepare the discussion with the clinic. Phimetra is **not a medical device** and makes **no medical diagnosis**.

1.2 Data subjects

Adult patients of the clinic who use the pre-consultation journey.

1.3 Categories of data

Data	Nature	Status
Face photo and derived facial template	Biometric data and, depending on use, data concerning health — special category (Art. 9 GDPR)	Required for the service
Name, e-mail address, telephone	Identification and contact data	Optional
Results: analysis, simulation sessions, quotes, appointments, invitations	Data produced by the service; may reveal health-related information	Produced by the service
Consent	Time-stamped record of consent	Required
Access log	Account identifier (or “patient / anonymous”), date, type of data and identifiers, route, outcome, **hash** of the IP address (not the IP in clear)	Security and traceability

1.4 Data flows

1. **Patient's browser.** Face detection runs in the browser (MediaPipe); the models are served by phimetra.com, with no call to Google during capture.
2. **Phimetra server in France** (OVHcloud, server located in Strasbourg): reception over HTTPS, storage in an encrypted volume.
3. **Analysis** by Scaleway SAS, "Generative APIs" service, **Paris** data centres (Mistral Small 3.2 model; fallback Mistral Medium 3.5, same provider, same region).
4. **Visual simulation** by IONOS Cloud, AI Model Hub, in **Germany** (FLUX.2 [klein] 4B model, Black Forest Labs, Apache-2.0 licence).
5. **Recomposition on the server in France**: the treated area is placed back onto the original photo; the rest of the photo remains pixel-identical.
6. **Transactional e-mails** (confirmation, appointment, quote) by Scaleway Transactional Email (Paris). No e-mail contains a face image.

> **Status of the simulation engine as of 29/09/2026: activation in progress.** Until it is active, the simulation is unavailable. There is **no fallback engine outside the European Union**.

No photo, analysis or simulation is transferred outside the European Union. All exchanges (browser ↔ server, server ↔ sub-processors) are encrypted with TLS (HTTPS).

1.5 Recipients

- The clinic (controller), through its accounts on the application.
- Phimetra (processor): a single person, the publisher, has administrator access to production.
- The sub-processors listed in section 5, within the limits of their role.

Correspondence: messages sent to contact@phimetra.com and privacy@phimetra.com pass through Cloudflare Email Routing and are read in a Google (Gmail) mailbox. This channel is not used to process photos; photos must not be sent through it.

> **To be completed by the controller:** authorised persons within the clinic, and any other recipients on the clinic's side.

1.6 Retention periods (automatic purge every night, verified)

Data	Maximum period at Phimetra
Face photos and derived facial template	30 days after capture
Temporary simulation files	Deleted as soon as the result has been read, at the latest 2 hours later
Analyses, appointments, simulation sessions, quotes, invitations, access log	12 months after creation
Requests at Scaleway (analysis)	Not stored according to the provider, except abuse or server errors: 2 weeks at most
Inputs at IONOS (simulation)	Neither logged nor stored according to the provider

To be completed by the controller: retention period for data that the clinic exports or copies into its own tools (patient record, calendar, e-mail).

2. Legal basis

- **Article 9 (special categories)**: explicit consent of the patient (Art. 9(2)(a) GDPR), collected by the interface **before the photo is captured** and time-stamped.
- **Article 6 (lawfulness)**: the choice of legal basis rests with the controller.

To be completed by the controller: legal basis chosen under Article 6, and the arrangements offered by the clinic for withdrawing consent.

3. Necessity and proportionality

- **Data minimisation**: only the face photo is required; name, e-mail and telephone are optional. Face detection runs in the browser. No face image is sent by e-mail. The access log keeps a hash of the IP address, not the IP in clear.
- **Short retention**: photos deleted at the latest 30 days after capture; temporary simulation files at the latest after 2 hours; other data after 12 months (section 1.6).
- **No training**: neither Phimetra nor its AI sub-processors use the photos or results to train models (Phimetra's commitment; statements by Scaleway and IONOS in their terms).
- **No advertising on the patient journey**: the Meta advertising pixel never loads on the patient journey pages (and, on marketing pages, only after consent).
- **Location**: all processing of patient data takes place in the European Union (France, Germany).
- **Information of data subjects**: the interface informs the patient before capture and collects her consent; it informs her that this is an AI system (section 7).
- **Data subject rights** (access, rectification, erasure, withdrawal of consent, etc.): exercised with the clinic; Phimetra assists on request (privacy@phimetra.com).
- **End of contract**: deletion of the data and written certificate provided to the clinic.

4. Security measures

Measure	Description
Encryption in transit	TLS (HTTPS) between the browser and the server, and to each sub-processor.
Encryption at rest	Database (photos, analyses, appointments, log) and temporary simulation files in an encrypted **LUKS2 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, into memory.
Backups	Database backups made within the encrypted volume; off-server copies encrypted (AES-256).

Measure	Description
Access log	Every read, listing, export, creation, modification, deletion or sharing of a patient record through the application is logged (who, when, what, route, outcome, IP hash). Kept 12 months, accessible to the publisher; an extract is provided to the clinic on request for its own records. Administrator access to the database is also logged by the database (query logs).
Access control	A single person (the publisher) has administrator access to production; server access by SSH key only.
Automatic purges	Run every night on the server (periods in section 1.6).
Reduced exposure	No face image by e-mail; no Meta pixel on the patient journey; face detection models served by phimetra.com (no call to Google during capture); no fallback engine outside the EU.
Personal data breaches	Notification to the clinic within **48 hours** of Phimetra becoming aware.
Sub-processors	**30 days'** notice before any change; versioned, dated list on /legal/security.

Known limitations. There is **no end-to-end encryption**. Encryption at rest protects against access to the disks and copies; it **does not protect a compromised server while it is running**. Administration relies on a single person. No certification or external audit supports these measures.

5. Sub-processors

List in force as of 29/09/2026 (generated from the official list published on /legal/security):

Sub-processor / entity	Location	Role	Data processed	Safeguards	Since / status
OVHcloud OVH SAS, 2 rue Kellermann, 59100 Roubaix, France	France (Strasbourg) Outside the EEA: no	Hosting of the application server and database (VPS)	All service data, stored in an encrypted volume (LUKS2, AES-256) Patient data: yes	OVHcloud Data Processing Agreement incorporated in the terms of service Data processing agreement (link)	2026-07-17 Active
Scaleway — Generative APIs Scaleway SAS, 8 rue de la Ville l'Évêque, 75008 Paris, France	France (Paris) Outside the EEA: no	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 Patient data: yes	Scaleway data processing agreement (DPA) incorporated in the contract; no retention of requests and no training (provider statement) Data processing agreement (link)	2026-09-28 Active

Sub-processor / entity	Location	Role	Data processed	Safeguards	Since / status
IONOS Cloud — AI Model Hub IONOS Cloud (IONOS group entity named in the contract); inference in IONOS Cloud data centres in Germany	Germany Outside the EEA: no	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 Patient data: yes	IONOS Cloud data processing agreement incorporated in the contract; inputs not logged, not stored, not used for training (provider statement) Data processing agreement (link)	2026-09-28 Activation in progress
Scaleway — Transactional Email Scaleway SAS, 8 rue de la Ville l'Évêque, 75008 Paris, France	France (Paris) Outside the EEA: no	Delivery of transactional e-mails (confirmation, appointment, quote)	Recipient name and e-mail address, message content; never any face image Patient data: yes	Scaleway data processing agreement (DPA) incorporated in the contract Data processing agreement (link)	2026-09-28 Active
Stripe Stripe Payments Europe, Ltd., Dublin, Irlande	Ireland (EU) Outside the EEA: no	Payment of the clinic's subscription	Clinic billing data only — no patient data Patient data: no	Stripe Data Processing Agreement; receives no patient data Data processing agreement (link)	2026-05-01 Active

Change history

- **2026-09-29** — Earlier simulations stored at fal.ai have been deleted (478 requests, 369 files). No sub-processor added. Clarifications: IONOS Cloud entity named in the contract; link to the contracts of OVHcloud (OVH SAS).
- **2026-09-28** — All processing of patient data moves into the European Union: analysis from OpenRouter (United States) to Scaleway (Paris), simulation from fal.ai (United States) to IONOS Cloud (Germany), e-mails from Resend (United States) to Scaleway (Paris). Free fallback AI models are removed. The site is no longer relayed by the Cloudflare proxy.

Former sub-processors removed on 28-29/09/2026: OpenRouter (United States, analysis), free fallback AI models, fal.ai (United States, simulation), Resend (United States, e-mails), Cloudflare proxy (the site is no longer relayed by Cloudflare). Earlier simulations stored at fal.ai have been deleted (478 requests, 369 files).

6. Risks to the rights and freedoms of data subjects

Scales used (CNIL methodology): *negligible, limited, significant, maximum*. The levels below are an **estimate proposed by Phimetra**, to be discussed and **approved by the controller**, who may revise them according to its own context.

Risk	Risk sources and threats	Existing measures	Proposed residual risk
Illegitimate access to data Impact: disclosure of the face photo and of aesthetic or health-related information; invasion of privacy, embarrassment, non-material damage.	External attacker (application, server); compromise or error of a sub-processor; misuse of a clinic account or of administrator access; credential theft; photos sent through an unintended channel (e-mail).	TLS; LUKS2 encrypted volume with off-server key; encrypted off-server copies; SSH key-only access; single administrator; access log (including administrator queries); short retention (photos ≤ 30 days); no retention and no training stated by the AI sub-processors; no image by e-mail; no Meta pixel on the patient journey; 100% EU processing; notification within 48 h.	Severity: **significant** (Article 9 data) Likelihood: **limited** Points of attention: no end-to-end encryption; a compromised running server is not protected by encryption at rest; no external audit.
Unwanted modification of data Impact: incorrect analysis, appointment or quote; inaccurate information given to the patient.	External attacker; software error; handling error; inaccurate output of an AI model.	Logging of every creation, modification and deletion; restricted access; TLS; simulation recomposed onto the original photo (rest of the photo pixel-identical); service presented as informative, non-medical, with information on the use of AI.	Severity: **limited** Likelihood: **limited**
Disappearance of data Impact: loss of the analysis, appointments or quotes; new capture needed.	Hardware or hosting failure; administration error; malware; loss of access to the encryption key; unavailability of a sub-processor; dependence on a single administrator.	Backups within the encrypted volume; encrypted off-server copies (AES-256); key kept in Scaleway Secret Manager (off-server); deliberate absence of a fallback engine outside the EU (unavailability rather than transfer).	Severity: **limited** Likelihood: **limited** Point of attention: backup frequency and restore tests are not described in this file; ask Phimetra if needed.

To be completed by the controller: approval or revision of the risk levels; additional measures on the clinic's side (authorisations, workstations, breach-handling procedure).

7. EU Artificial Intelligence Act (AI Act)

- Phimetra is a **limited-risk** AI system, subject to the transparency obligations of **Article 50**: the patient is informed that she is interacting with an AI system and that the analysis and simulation are produced by such a system.
- Phimetra is not a medical device and makes no medical diagnosis.
- Models used: Mistral Small 3.2 (fallback Mistral Medium 3.5) for analysis, via Scaleway (Paris); FLUX.2 [klein] 4B (Black Forest Labs, Apache-2.0 licence) for simulation, via IONOS Cloud (Germany), activation in progress.

8. Items to be completed by the controller

Item	Clinic's answer
Legal basis chosen under Article 6 GDPR	
Information of patients: notices displayed at the practice, wording in the clinic's documents, privacy policy	
Retention period on the clinic's side (exported or copied data)	
Authorised persons and account management	
Approval of the risk levels (section 6) and additional measures	
Opinion of the clinic's DPO (if one has been appointed)	
Consultation of data subjects or their representatives (where appropriate)	
Decision and approval: name, position, date, signature	

Contact

Questions about this file, requests for an access log extract, assistance with data subject rights: privacy@phimetra.com. Please never send photos by e-mail.

Publisher: Wahib Znidah, sole proprietor (trading name SAYWA) — SIREN 888 001 054 — SIRET 888 001 054 00020 — 274 rue du Collège, 74950 Scionzier, France · Data protection: privacy@phimetra.com · Contact: contact@phimetra.com · Host: OVH SAS, 2 rue Kellermann, 59100 Roubaix, France (server located in Strasbourg).