Dossier de apoyo a la evaluación de impacto (EIPD / AIPD / DPIA) — Phimetra, versión 2026-09-29

Destinatarios: el responsable del tratamiento (la clínica que utiliza Phimetra) y su asesor jurídico o delegado de protección de datos (DPD). Estructura basada en la metodología de la CNIL y en las directrices del Grupo de Trabajo del Artículo 29 (WP248 rev. 01).

Objeto y alcance del documento. Phimetra actúa como **encargado del tratamiento** (art. 28 RGPD) por cuenta de la clínica, que es el **responsable del tratamiento**. Este dossier reúne la información que Phimetra puede aportar sobre su servicio para ayudar a la clínica a realizar su propia evaluación de impacto relativa a la protección de datos (art. 35 RGPD). No sustituye dicha evaluación: la decisión de realizarla, su contenido final y su aprobación corresponden al responsable del tratamiento.

Los apartados marcados `A completar por el responsable del tratamiento` se dejan deliberadamente a la clínica: dependen de su organización y de sus decisiones, que Phimetra desconoce.

Transparencia. Phimetra **no dispone de ninguna certificación** (ni HDS, ni ISO 27001, ni SOC 2) y **no ha sido objeto de ninguna auditoría externa**. Phimetra **no ha designado un DPD**; el contacto específico es privacy@phimetra.com. Las medidas descritas a continuación son declaradas por el editor y reflejan el estado del servicio a 29/09/2026.

1. Descripción del tratamiento

1.1 Finalidad

Preconsulta estética **informativa**: a partir de una foto del rostro tomada por la paciente, el servicio genera un análisis y, cuando el motor está activo, una simulación visual, destinados a preparar la conversación con la clínica. Phimetra **no es un producto sanitario** y **no emite ningún diagnóstico médico**.

1.2 Interesados

Pacientes adultas de la clínica que utilizan el recorrido de preconsulta.

1.3 Categorías de datos

Dato	Naturaleza	Carácter
Foto del rostro y plantilla facial derivada	Dato biométrico y, según el uso, dato relativo a la salud — categoría especial (art. 9 RGPD)	Necesario para el servicio
Nombre, correo electrónico, teléfono	Datos identificativos y de contacto	Facultativos
Resultados: análisis, sesiones de simulación, presupuestos, citas, invitaciones	Datos generados por el servicio; pueden revelar información relativa a la salud	Generados por el servicio
Consentimiento	Prueba del consentimiento, con sello de tiempo	Necesario

Dato	Naturaleza	Carácter
Registro de accesos	Identificador de la cuenta (o «paciente / anónimo»), fecha, tipo de datos e identificadores, ruta, resultado, **huella (hash)** de la dirección IP (no la IP en claro)	Seguridad y trazabilidad

1.4 Flujos de datos

1. **Navegador de la paciente.** La detección del rostro se realiza en el navegador (MediaPipe); los modelos se sirven desde phimetra.com, sin ninguna llamada a Google durante la captura.
2. **Servidor de Phimetra en Francia** (OVHcloud, servidor ubicado en Estrasburgo): recepción por HTTPS, almacenamiento en un volumen cifrado.
3. **Análisis** por Scaleway SAS, servicio «Generative APIs», centros de datos de **París** (modelo Mistral Small 3.2; respaldo Mistral Medium 3.5, mismo proveedor, misma región).
4. **Simulación visual** por IONOS Cloud, AI Model Hub, en **Alemania** (modelo FLUX.2 [klein] 4B, Black Forest Labs, licencia Apache-2.0).
5. **Recomposición en el servidor en Francia**: la zona tratada se vuelve a colocar sobre la foto original; el resto de la foto permanece idéntico píxel a píxel.
6. **Correos transaccionales** (confirmación, cita, presupuesto) por Scaleway Transactional Email (París). Ningún correo contiene imágenes del rostro.

Estado del motor de simulación a 29/09/2026: en proceso de activación. Mientras no esté activo, la simulación no está disponible. **No existe ningún motor de respaldo fuera de la Unión Europea**.

Ninguna foto, análisis o simulación se transfiere fuera de la Unión Europea. Todos los intercambios (navegador ↔ servidor, servidor ↔ subencargados) están cifrados mediante TLS (HTTPS).

1.5 Destinatarios

- La clínica (responsable del tratamiento), a través de sus cuentas en la aplicación.
- Phimetra (encargado del tratamiento): una sola persona, el editor, tiene acceso de administrador a producción.
- Los subencargados enumerados en la sección 5, dentro de los límites de su función.

Correspondencia: los mensajes enviados a contact@phimetra.com y privacy@phimetra.com pasan por Cloudflare Email Routing y se leen en un buzón de Google (Gmail). Este canal no se utiliza para tratar fotos; no deben enviarse fotos por él.

A completar por el responsable del tratamiento: personas autorizadas dentro de la clínica y otros posibles destinatarios por parte de la clínica.

1.6 Plazos de conservación (supresión automática cada noche, verificada)

Datos	Plazo máximo en Phimetra
Fotos del rostro y plantilla facial derivada	30 días después de la captura
Archivos temporales de simulación	Se borran en cuanto se lee el resultado, como máximo 2 horas después

Datos	Plazo máximo en Phimetra
Análisis, citas, sesiones de simulación, presupuestos, invitaciones, registro de accesos	12 meses después de su creación
Solicitudes en Scaleway (análisis)	No se conservan según el proveedor, salvo abuso o error del servidor: 2 semanas como máximo
Entradas en IONOS (simulación)	Ni registradas ni almacenadas según el proveedor

A completar por el responsable del tratamiento: plazo de conservación de los datos que la clínica exporta o copia en sus propias herramientas (historia clínica, agenda, correo).

2. Base jurídica

- **Artículo 9 (categorías especiales)**: consentimiento explícito de la paciente (art. 9.2.a RGPD), recabado por la interfaz **antes de la captura** de la foto y con sello de tiempo.
- **Artículo 6 (licitud)**: la elección de la base jurídica corresponde al responsable del tratamiento.

A completar por el responsable del tratamiento: base jurídica elegida en virtud del artículo 6 y modalidades de retirada del consentimiento ofrecidas por la clínica.

3. Necesidad y proporcionalidad

- **Minimización**: solo es necesaria la foto del rostro; nombre, correo y teléfono son facultativos. La detección del rostro se realiza en el navegador. No se envía ninguna imagen del rostro por correo. El registro de accesos conserva una huella de la IP, no la IP en claro.
- **Conservación breve**: fotos suprimidas como máximo 30 días después de la captura; archivos temporales de simulación como máximo a las 2 horas; resto de datos a los 12 meses (sección 1.6).
- **Sin entrenamiento**: ni Phimetra ni sus subencargados de IA utilizan las fotos ni los resultados para entrenar modelos (compromiso de Phimetra; declaraciones de Scaleway e IONOS en sus condiciones).
- **Sin publicidad en el recorrido de la paciente**: el píxel publicitario de Meta nunca se carga en las páginas del recorrido de la paciente (y, en las páginas de marketing, solo tras el consentimiento).
- **Ubicación**: todos los tratamientos de datos de pacientes se realizan en la Unión Europea (Francia, Alemania).
- **Información a los interesados**: la interfaz informa a la paciente antes de la captura y recaba su consentimiento; le informa de que se trata de un sistema de IA (sección 7).
- **Derechos de los interesados** (acceso, rectificación, supresión, retirada del consentimiento, etc.): se ejercen ante la clínica; Phimetra la asiste cuando lo solicite (privacy@phimetra.com).
- **Fin del contrato**: supresión de los datos y certificado escrito entregado a la clínica.

4. Medidas de seguridad

Medida	Descripción
Cifrado en tránsito	TLS (HTTPS) entre el navegador y el servidor, y hacia cada subencargado.
Cifrado en reposo	Base de datos (fotos, análisis, citas, registro) y archivos temporales de simulación en un volumen cifrado **LUKS2 (AES-256-XTS, derivación de clave argon2id)**. La clave **no se almacena en el servidor**: se conserva en Scaleway Secret Manager (París) y solo se lee al arrancar, en memoria.
Copias de seguridad	Copias de la base realizadas dentro del volumen cifrado; copias fuera del servidor cifradas (AES-256).
Registro de accesos	Se registra cada lectura, listado, exportación, creación, modificación, supresión o compartición de un expediente de paciente a través de la aplicación (quién, cuándo, qué, ruta, resultado, huella de IP). Se conserva 12 meses y es consultable por el editor; se entrega un extracto a la clínica, a petición, para sus propios expedientes. Los accesos de administrador a la base también quedan registrados por la propia base (registros de consultas).
Control de accesos	Una sola persona (el editor) tiene acceso de administrador a producción; acceso al servidor solo mediante clave SSH.
Supresiones automáticas	Se ejecutan cada noche en el servidor (plazos en la sección 1.6).
Reducción de la exposición	Ninguna imagen del rostro por correo; sin píxel de Meta en el recorrido de la paciente; modelos de detección del rostro servidos desde phimetra.com (ninguna llamada a Google durante la captura); ningún motor de respaldo fuera de la UE.
Violaciones de seguridad	Notificación a la clínica en un plazo de **48 horas** desde que Phimetra tenga conocimiento de ella.
Subencargados	Preaviso de **30 días** antes de cualquier cambio; lista versionada y fechada en /legal/security.

Limitaciones conocidas. No hay cifrado de extremo a extremo. El cifrado en reposo protege frente al acceso a los discos y a las copias; **no protege un servidor comprometido en funcionamiento**. La administración depende de una sola persona. Ninguna certificación ni auditoría externa respalda estas medidas.

5. Subencargados del tratamiento

Lista vigente a 29/09/2026 (generada a partir de la lista oficial publicada en /legal/security):

Subencargado / entidad	Ubicación	Función	Datos tratados	Garantías	Desde / estado
OVHcloud OVH SAS, 2 rue Kellermann, 59100 Roubaix, France	Francia (Estrasburgo) Fuera del EEE: no	Alojamiento del servidor de la aplicación y de la base de datos (VPS)	Todos los datos del servicio, almacenados en un volumen cifrado (LUKS2, AES-256) Datos de pacientes: sí	Acuerdo de encargo del tratamiento de OVHcloud incluido en las condiciones del servicio Contrato de encargo del tratamiento (enlace)	2026-07-17 Activo

Subencargado / entidad	Ubicación	Función	Datos tratados	Garantías	Desde / estado
Scaleway — Generative APIs Scaleway SAS, 8 rue de la Ville l'Évêque, 75008 Paris, France	Francia (París) Fuera del EEE: no	Análisis de la foto por un modelo de IA (Mistral Small 3.2; respaldo Mistral Medium 3.5, mismo proveedor, misma región)	Foto del rostro e instrucciones de análisis, durante el tratamiento; el proveedor declara no conservar las solicitudes (salvo abuso o error del servidor, 2 semanas como máximo) ni utilizarlas para entrenamiento Datos de pacientes: sí	Contrato de encargo (DPA) de Scaleway incluido en el contrato; sin conservación de las solicitudes ni entrenamiento (declaración del proveedor) Contrato de encargo del tratamiento (enlace)	2026-09-28 Activo
IONOS Cloud — AI Model Hub IONOS Cloud (entidad del grupo IONOS designada en el contrato); inferencia en los centros de datos de IONOS Cloud en Alemania	Alemania Fuera del EEE: no	Generación de la simulación visual (modelo FLUX.2 [klein] 4B); la zona tratada se recompone después sobre la foto original en nuestro servidor en Francia	Foto del rostro, durante la generación; el proveedor declara no registrar ni almacenar las entradas ni utilizarlas para entrenamiento Datos de pacientes: sí	Contrato de encargo de IONOS Cloud incluido en el contrato; entradas no registradas, no almacenadas, no utilizadas para entrenamiento (declaración del proveedor) Contrato de encargo del tratamiento (enlace)	2026-09-28 En proceso de activación
Scaleway — Transactional Email Scaleway SAS, 8 rue de la Ville l'Évêque, 75008 Paris, France	Francia (París) Fuera del EEE: no	Envío de los correos transaccionales (confirmación, cita, presupuesto)	Nombre y dirección de correo del destinatario, contenido del mensaje; nunca imágenes del rostro Datos de pacientes: sí	Contrato de encargo (DPA) de Scaleway incluido en el contrato Contrato de encargo del tratamiento (enlace)	2026-09-28 Activo
Stripe Stripe Payments Europe, Ltd., Dublin, Irlande	Irlanda (UE) Fuera del EEE: no	Pago de la suscripción de la clínica	Solo datos de facturación de la clínica — ningún dato de pacientes Datos de pacientes: no	Acuerdo de tratamiento de datos de Stripe; no recibe ningún dato de pacientes Contrato de encargo del tratamiento (enlace)	2026-05-01 Activo

Historial de cambios

- **2026-09-29** — Se han suprimido las simulaciones anteriores almacenadas en fal.ai (478 solicitudes, 369 archivos). No se añade ningún subencargado. Precisiones: entidad de IONOS Cloud designada en el contrato; enlace a los contratos de OVHcloud (OVH SAS).
- **2026-09-28** — Todos los tratamientos de datos de pacientes pasan a la Unión Europea: el análisis pasa de OpenRouter (Estados Unidos) a Scaleway (París), la simulación de fal.ai (Estados Unidos) a IONOS Cloud (Alemania) y los correos de Resend (Estados Unidos) a Scaleway (París). Se eliminan los modelos de IA gratuitos de respaldo. El sitio ya no pasa por el proxy de Cloudflare.

Antiguos subencargados retirados el 28-29/09/2026: OpenRouter (Estados Unidos, análisis), modelos de IA gratuitos de respaldo, fal.ai (Estados Unidos, simulación), Resend (Estados Unidos, correos), proxy de Cloudflare (el sitio ya no pasa por Cloudflare). Se han suprimido las simulaciones anteriores almacenadas en fal.ai (478 solicitudes, 369 archivos).

6. Riesgos para los derechos y libertades de los interesados

Escalas utilizadas (metodología de la CNIL): *insignificante, limitado, importante, máximo*. Los niveles siguientes son una **estimación propuesta por Phimetra**, que debe ser debatida y **validada por el responsable del tratamiento**, quien puede revisarlos según su propio contexto.

Riesgo	Fuentes de riesgo y amenazas	Medidas existentes	Riesgo residual propuesto
Acceso ilegítimo a los datos Impacto: divulgación de la foto del rostro y de información estética o relativa a la salud; intromisión en la intimidad, incomodidad, daño moral.	Atacante externo (aplicación, servidor); compromiso o error de un subencargado; uso abusivo de una cuenta de la clínica o de un acceso de administrador; robo de credenciales; envío de fotos por un canal no previsto (correo).	TLS; volumen cifrado LUKS2 con clave fuera del servidor; copias fuera del servidor cifradas; acceso SSH solo con clave; un único administrador; registro de accesos (incluidas las consultas de administrador); conservación breve (fotos ≤ 30 días); ni conservación ni entrenamiento según los subencargados de IA; ninguna imagen por correo; sin píxel de Meta en el recorrido de la paciente; tratamiento 100 % en la UE; notificación en 48 h.	Gravedad: **importante** (datos del artículo 9) Probabilidad: **limitada** Puntos de atención: sin cifrado de extremo a extremo; un servidor comprometido en funcionamiento no está protegido por el cifrado en reposo; sin auditoría externa.
Modificación no deseada de los datos Impacto: análisis, cita o presupuesto erróneos; información inexacta facilitada a la paciente.	Atacante externo; error de software; error de manipulación; resultado inexacto de un modelo de IA.	Registro de toda creación, modificación y supresión; accesos restringidos; TLS; simulación recompuesta sobre la foto original (resto de la foto idéntico píxel a píxel); servicio presentado como informativo, no médico, con información sobre el uso de la IA.	Gravedad: **limitada** Probabilidad: **limitada**
Desaparición de los datos Impacto: pérdida del análisis, las citas o los presupuestos; necesidad de una nueva captura.	Avería de hardware o del proveedor de alojamiento; error de administración; software malicioso; pérdida de acceso a la clave de cifrado; indisponibilidad de un subencargado; dependencia de un único administrador.	Copias de seguridad dentro del volumen cifrado; copias fuera del servidor cifradas (AES-256); clave conservada en Scaleway Secret Manager (fuera del servidor); ausencia asumida de motor de respaldo fuera de la UE (indisponibilidad antes que transferencia).	Gravedad: **limitada** Probabilidad: **limitada** Punto de atención: la frecuencia de las copias y las pruebas de restauración no se describen en este dossier; solicitarlas a Phimetra si es necesario.

A completar por el responsable del tratamiento: validación o revisión de los niveles de riesgo; medidas adicionales por parte de la clínica (autorizaciones, puestos de trabajo, procedimiento de gestión de violaciones de seguridad).

7. Reglamento europeo de Inteligencia Artificial (RIA / AI Act)

- Phimetra es un sistema de IA de **riesgo limitado**, sujeto a las obligaciones de transparencia del **artículo 50**: se informa a la paciente de que interactúa con un sistema de IA y de que el análisis y la simulación los genera dicho sistema.
- Phimetra no es un producto sanitario y no emite diagnósticos médicos.
- Modelos utilizados: Mistral Small 3.2 (respaldo Mistral Medium 3.5) para el análisis, a través de Scaleway (París); FLUX.2 [klein] 4B (Black Forest Labs, licencia Apache-2.0) para la simulación, a través de IONOS Cloud (Alemania), en proceso de activación.

8. Apartados a completar por el responsable del tratamiento

Apartado	Respuesta de la clínica
Base jurídica elegida en virtud del artículo 6 RGPD	
Información a las pacientes: carteles en la consulta, menciones en los documentos de la clínica, política de privacidad	
Plazo de conservación por parte de la clínica (datos exportados o copiados)	
Personas autorizadas y gestión de cuentas	
Validación de los niveles de riesgo (sección 6) y medidas adicionales	
Dictamen del DPD de la clínica (si lo hubiera)	
Consulta a los interesados o a sus representantes (en su caso)	
Decisión y aprobación: nombre, cargo, fecha, firma	

Contacto

Preguntas sobre este dossier, solicitud de un extracto del registro de accesos, asistencia para los derechos de los interesados: privacy@phimetra.com. Por favor, no envíe nunca fotos por correo electrónico.

Editor: Wahib Znidah, empresario individual (nombre comercial SAYWA) — SIREN 888 001 054 — SIRET 888 001 054 00020 — 274 rue du Collège, 74950 Scionzier, Francia · Protección de datos: privacy@phimetra.com · Contacto: contact@phimetra.com · Alojamiento: OVH SAS, 2 rue Kellermann, 59100 Roubaix, Francia (servidor ubicado en Estrasburgo).