Dossiê de apoio à avaliação de impacto (AIPD / RIPD / DPIA) — Phimetra, versão 2026-09-29

Destinatários: o responsável pelo tratamento (controlador — a clínica que utiliza a Phimetra) e seu assessor jurídico ou encarregado de proteção de dados (DPO). Estrutura baseada na metodologia da CNIL e nas diretrizes do Grupo de Trabalho do Artigo 29 (WP248 rev. 01). O documento se refere ao Regulamento Geral sobre a Proteção de Dados da União Europeia (RGPD).

Objeto e alcance do documento. A Phimetra atua como **operador (subcontratante)** (art. 28 do RGPD) da clínica, que é o **responsável pelo tratamento (controlador)**. Este dossiê reúne as informações que a Phimetra pode fornecer sobre o seu serviço para ajudar a clínica a realizar a sua própria avaliação de impacto sobre a proteção de dados (art. 35 do RGPD). Ele não substitui essa avaliação: a decisão de realizá-la, seu conteúdo final e sua aprovação cabem ao responsável pelo tratamento.

Os itens marcados `A completar pelo responsável pelo tratamento` são deliberadamente deixados à clínica: dependem da sua organização e das suas escolhas, que a Phimetra não conhece.

Transparência. A Phimetra **não possui nenhuma certificação** (nem HDS, nem ISO 27001, nem SOC 2) e **não passou por nenhuma auditoria externa**. A Phimetra **não designou um encarregado (DPO)**; o contato dedicado é privacy@phimetra.com. As medidas descritas abaixo são declaradas pelo editor e refletem o estado do serviço em 29/09/2026.

1. Descrição do tratamento

1.1 Finalidade

Pré-consulta estética **informativa**: a partir de uma foto do rosto tirada pela paciente, o serviço gera uma análise e, quando o motor está ativo, uma simulação visual, destinadas a preparar a conversa com a clínica. A Phimetra **não é um dispositivo médico** e **não faz nenhum diagnóstico médico**.

1.2 Titulares dos dados

Pacientes adultas da clínica que utilizam o percurso de pré-consulta.

1.3 Categorias de dados

Dado	Natureza	Caráter
Foto do rosto e modelo facial derivado	Dado biométrico e, conforme o uso, dado relativo à saúde — categoria especial (art. 9 do RGPD)	Necessário ao serviço
Nome, e-mail, telefone	Dados de identificação e de contato	Facultativos
Resultados: análise, sessões de simulação, orçamentos, consultas agendadas, convites	Dados produzidos pelo serviço; podem revelar informações relativas à saúde	Produzidos pelo serviço
Consentimento	Prova do consentimento, com registro de data e hora	Necessário

Dado	Natureza	Caráter
Registro de acessos	Identificador da conta (ou «paciente / anônima»), data, tipo de dados e identificadores, rota, resultado, **hash** do endereço IP (não o IP em claro)	Segurança e rastreabilidade

1.4 Fluxos de dados

1. **Navegador da paciente.** A detecção do rosto é feita no navegador (MediaPipe); os modelos são servidos por phimetra.com, sem nenhuma chamada ao Google durante a captura.
2. **Servidor da Phimetra na França** (OVHcloud, servidor localizado em Estrasburgo): recepção por HTTPS, armazenamento em um volume criptografado.
3. **Análise** pela Scaleway SAS, serviço «Generative APIs», data centers de **Paris** (modelo Mistral Small 3.2; reserva Mistral Medium 3.5, mesmo provedor, mesma região).
4. **Simulação visual** pela IONOS Cloud, AI Model Hub, na **Alemanha** (modelo FLUX.2 [klein] 4B, Black Forest Labs, licença Apache-2.0).
5. **Recomposição no servidor na França**: a área tratada é recolocada sobre a foto original; o restante da foto permanece idêntico pixel a pixel.
6. **E-mails transacionais** (confirmação, consulta, orçamento) pela Scaleway Transactional Email (Paris). Nenhum e-mail contém imagem do rosto.

> **Situação do motor de simulação em 29/09/2026: em ativação.** Enquanto não estiver ativo, a simulação fica indisponível. **Não existe nenhum motor de reserva fora da União Europeia**.

Nenhuma foto, análise ou simulação é transferida para fora da União Europeia. Todas as trocas (navegador ↔ servidor, servidor ↔ suboperadores) são criptografadas por TLS (HTTPS).

1.5 Destinatários

- A clínica (responsável pelo tratamento), por meio das suas contas no aplicativo.
- A Phimetra (operador): uma única pessoa, o editor, tem acesso de administrador à produção.
- Os suboperadores listados na seção 5, nos limites da sua função.

Correspondência: as mensagens enviadas a contact@phimetra.com e privacy@phimetra.com passam pelo Cloudflare Email Routing e são lidas em uma caixa do Google (Gmail). Esse canal não é usado para tratar fotos; não se deve enviar fotos por ele.

> **A completar pelo responsável pelo tratamento:** pessoas autorizadas na clínica e outros eventuais destinatários do lado da clínica.

1.6 Prazos de conservação (exclusão automática todas as noites, verificada)

Dados	Prazo máximo na Phimetra
Fotos do rosto e modelo facial derivado	30 dias após a captura
Arquivos temporários de simulação	Apagados assim que o resultado é lido, no máximo 2 horas depois
Análises, consultas, sessões de simulação, orçamentos, convites, registro de acessos	12 meses após a criação

Dados	Prazo máximo na Phimetra
Solicitações na Scaleway (análise)	Não armazenadas segundo o provedor, exceto abuso ou erro de servidor: no máximo 2 semanas
Entradas na IONOS (simulação)	Nem registradas nem armazenadas segundo o provedor

A completar pelo responsável pelo tratamento: prazo de conservação dos dados que a clínica exporta ou copia para as suas próprias ferramentas (prontuário, agenda, e-mail).

2. Base legal

- **Artigo 9 (categorias especiais)**: consentimento explícito da paciente (art. 9.2.a do RGPD), coletado pela interface **antes da captura** da foto, com registro de data e hora.
- **Artigo 6 (licitude)**: a escolha da base legal cabe ao responsável pelo tratamento.

A completar pelo responsável pelo tratamento: base legal escolhida nos termos do artigo 6 e modalidades de revogação do consentimento oferecidas pela clínica.

3. Necessidade e proporcionalidade

- **Minimização**: apenas a foto do rosto é necessária; nome, e-mail e telefone são facultativos. A detecção do rosto é feita no navegador. Nenhuma imagem do rosto é enviada por e-mail. O registro de acessos guarda um hash do IP, não o IP em claro.
- **Conservação curta**: fotos excluídas no máximo 30 dias após a captura; arquivos temporários de simulação no máximo após 2 horas; demais dados após 12 meses (seção 1.6).
- **Sem treinamento**: nem a Phimetra nem os seus suboperadores de IA usam as fotos ou os resultados para treinar modelos (compromisso da Phimetra; declarações da Scaleway e da IONOS em seus termos).
- **Sem publicidade no percurso da paciente**: o pixel publicitário da Meta nunca é carregado nas páginas do percurso da paciente (e, nas páginas de marketing, somente após consentimento).
- **Localização**: todo o tratamento de dados de pacientes ocorre na União Europeia (França, Alemanha).
- **Informação aos titulares**: a interface informa a paciente antes da captura e coleta o seu consentimento; informa-a de que se trata de um sistema de IA (seção 7).
- **Direitos dos titulares** (acesso, retificação, exclusão, revogação do consentimento etc.): são exercidos junto à clínica; a Phimetra a auxilia mediante solicitação (privacy@phimetra.com).
- **Fim do contrato**: exclusão dos dados e declaração escrita entregue à clínica.

4. Medidas de segurança

Medida	Descrição
Criptografia em trânsito	TLS (HTTPS) entre o navegador e o servidor, e para cada suboperador.

Medida	Descrição
Criptografia em repouso	Banco de dados (fotos, análises, consultas, registro) e arquivos temporários de simulação em um volume criptografado **LUKS2 (AES-256-XTS, derivação de chave argon2id)**. A chave **não fica armazenada no servidor**: é mantida no Scaleway Secret Manager (Paris) e só é lida na inicialização, em memória.
Backups	Backups do banco feitos dentro do volume criptografado; cópias fora do servidor criptografadas (AES-256).
Registro de acessos	Toda leitura, listagem, exportação, criação, modificação, exclusão ou compartilhamento de um prontuário de paciente pelo aplicativo é registrado (quem, quando, o quê, rota, resultado, hash do IP). Mantido por 12 meses e consultável pelo editor; um extrato é fornecido à clínica, mediante solicitação, para os seus próprios prontuários. Os acessos de administrador ao banco também são registrados pelo próprio banco (logs de consultas).
Controle de acesso	Uma única pessoa (o editor) tem acesso de administrador à produção; acesso ao servidor somente por chave SSH.
Exclusões automáticas	Executadas todas as noites no servidor (prazos na seção 1.6).
Redução da exposição	Nenhuma imagem do rosto por e-mail; sem pixel da Meta no percurso da paciente; modelos de detecção do rosto servidos por phimetra.com (nenhuma chamada ao Google durante a captura); nenhum motor de reserva fora da UE.
Violações de dados	Notificação à clínica em até **48 horas** após a Phimetra tomar conhecimento.
Suboperadores	Aviso prévio de **30 dias** antes de qualquer mudança; lista versionada e datada em /legal/security.

Limitações conhecidas. Não há criptografia de ponta a ponta. A criptografia em repouso protege contra o acesso aos discos e às cópias; **não protege um servidor comprometido em funcionamento**. A administração depende de uma única pessoa. Nenhuma certificação ou auditoria externa respalda essas medidas.

5. Suboperadores

Lista em vigor em 29/09/2026 (gerada a partir da lista oficial publicada em /legal/security):

Suboperador / entidade	Localização	Função	Dados tratados	Garantias	Desde / situação
OVHcloud OVH SAS, 2 rue Kellermann, 59100 Roubaix, France	França (Estrasburgo) Fora do EEE: não	Hospedagem do servidor da aplicação e do banco de dados (VPS)	Todos os dados do serviço, armazenados em um volume criptografado (LUKS2, AES-256) Dados de pacientes: sim	Acordo de tratamento de dados da OVHcloud incorporado aos termos de serviço Acordo de tratamento de dados (link)	2026-07-17 Ativo

Suboperador / entidade	Localização	Função	Dados tratados	Garantias	Desde / situação
Scaleway — Generative APIs Scaleway SAS, 8 rue de la Ville l'Évêque, 75008 Paris, France	França (Paris) Fora do EEE: não	Análise da foto por um modelo de IA (Mistral Small 3.2; reserva Mistral Medium 3.5, mesmo provedor, mesma região)	Foto do rosto e instruções de análise, durante o processamento; o provedor declara não armazenar as solicitações (exceto abuso ou erro de servidor, no máximo 2 semanas) nem usá-las para treinamento Dados de pacientes: sim	Acordo de tratamento de dados (DPA) da Scaleway incorporado ao contrato; sem retenção das solicitações nem treinamento (declaração do provedor) Acordo de tratamento de dados (link)	2026-09-28 Ativo
IONOS Cloud — AI Model Hub IONOS Cloud (entidade do grupo IONOS designada no contrato); inferência nos data centers da IONOS Cloud na Alemanha	Alemanha Fora do EEE: não	Geração da simulação visual (modelo FLUX.2 [klein] 4B); a área tratada é depois recomposta sobre a foto original em nosso servidor na França	Foto do rosto, durante a geração; o provedor declara não registrar nem armazenar as entradas nem usá-las para treinamento Dados de pacientes: sim	Contrato de tratamento da IONOS Cloud incorporado ao contrato; entradas não registradas, não armazenadas, não usadas para treinamento (declaração do provedor) Acordo de tratamento de dados (link)	2026-09-28 Em ativação
Scaleway — Transactional Email Scaleway SAS, 8 rue de la Ville l'Évêque, 75008 Paris, France	França (Paris) Fora do EEE: não	Envio dos e-mails transacionais (confirmação, consulta, orçamento)	Nome e e-mail do destinatário, conteúdo da mensagem; nunca imagens do rosto Dados de pacientes: sim	Acordo de tratamento de dados (DPA) da Scaleway incorporado ao contrato Acordo de tratamento de dados (link)	2026-09-28 Ativo
Stripe Stripe Payments Europe, Ltd., Dublin, Irlande	Irlanda (UE) Fora do EEE: não	Pagamento da assinatura da clínica	Somente dados de faturamento da clínica — nenhum dado de pacientes Dados de pacientes: não	Acordo de tratamento de dados da Stripe; não recebe nenhum dado de pacientes Acordo de tratamento de dados (link)	2026-05-01 Ativo

Histórico de alterações

- **2026-09-29** — As simulações anteriores armazenadas na fal.ai foram excluídas (478 solicitações, 369 arquivos). Nenhum suboperador adicionado. Esclarecimentos: entidade da IONOS Cloud designada no contrato; link para os contratos da OVHcloud (OVH SAS).
- **2026-09-28** — Todo o processamento de dados de pacientes passa para a União Europeia: a análise sai da OpenRouter (Estados Unidos) para a Scaleway (Paris), a simulação da fal.ai (Estados Unidos) para a IONOS Cloud (Alemanha) e os e-mails da Resend (Estados Unidos) para a Scaleway (Paris). Os modelos de IA gratuitos de reserva foram removidos. O site deixou de passar pelo proxy da Cloudflare.

Antigos suboperadores retirados em 28-29/09/2026: OpenRouter (Estados Unidos, análise), modelos de IA gratuitos de reserva, fal.ai (Estados Unidos, simulação), Resend (Estados Unidos, e-mails), proxy da Cloudflare (o site deixou de passar pela Cloudflare).

As simulações anteriores armazenadas na fal.ai foram excluídas (478 solicitações, 369 arquivos).

6. Riscos para os direitos e liberdades dos titulares

Escalas utilizadas (metodologia da CNIL): *insignificante, limitado, importante, máximo*. Os níveis abaixo são uma **estimativa proposta pela Phimetra**, a ser discutida e **validada pelo responsável pelo tratamento**, que pode revê-los conforme o seu próprio contexto.

Risco	Fontes de risco e ameaças	Medidas existentes	Risco residual proposto
Acesso ilegítimo aos dados Impacto: divulgação da foto do rosto e de informações estéticas ou relativas à saúde; violação da privacidade, constrangimento, dano moral.	Atacante externo (aplicativo, servidor); comprometimento ou erro de um suboperador; uso abusivo de uma conta da clínica ou de um acesso de administrador; roubo de credenciais; envio de fotos por um canal não previsto (e-mail).	TLS; volume criptografado LUKS2 com chave fora do servidor; cópias fora do servidor criptografadas; acesso SSH somente por chave; um único administrador; registro de acessos (inclusive consultas de administrador); conservação curta (fotos ≤ 30 dias); sem retenção e sem treinamento segundo os suboperadores de IA; nenhuma imagem por e-mail; sem pixel da Meta no percurso da paciente; tratamento 100 % na UE; notificação em 48 h.	Gravidade: **importante** (dados do artigo 9) Probabilidade: **limitada** Pontos de atenção: sem criptografia de ponta a ponta; um servidor comprometido em funcionamento não é protegido pela criptografia em repouso; sem auditoria externa.
Modificação indesejada dos dados Impacto: análise, consulta ou orçamento incorretos; informação imprecisa fornecida à paciente.	Atacante externo; erro de software; erro de manuseio; resultado impreciso de um modelo de IA.	Registro de toda criação, modificação e exclusão; acessos restritos; TLS; simulação recomposta sobre a foto original (restante idêntico pixel a pixel); serviço apresentado como informativo, não médico, com informação sobre o uso de IA.	Gravidade: **limitada** Probabilidade: **limitada**
Desaparecimento dos dados Impacto: perda da análise, das consultas ou dos orçamentos; necessidade de nova captura.	Falha de hardware ou da hospedagem; erro de administração; software malicioso; perda de acesso à chave de criptografia; indisponibilidade de um suboperador; dependência de um único administrador.	Backups dentro do volume criptografado; cópias fora do servidor criptografadas (AES-256); chave mantida no Scaleway Secret Manager (fora do servidor); ausência assumida de motor de reserva fora da UE (indisponibilidade em vez de transferência).	Gravidade: **limitada** Probabilidade: **limitada** Ponto de atenção: a frequência dos backups e os testes de restauração não são descritos neste dossiê; solicitar à Phimetra se necessário.

A completar pelo responsável pelo tratamento: validação ou revisão dos níveis de risco; medidas complementares do lado da clínica (autorizações, estações de trabalho, procedimento de gestão de violações).

7. Regulamento europeu de Inteligência Artificial (AI Act)

- A Phimetra é um sistema de IA de **risco limitado**, sujeito às obrigações de transparência do **artigo 50**: a paciente é informada de que interage com um sistema de IA e de que a análise e a simulação são produzidas por esse sistema.
- A Phimetra não é um dispositivo médico e não faz diagnóstico médico.
- Modelos utilizados: Mistral Small 3.2 (reserva Mistral Medium 3.5) para a análise, via Scaleway (Paris); FLUX.2 [klein] 4B (Black Forest Labs, licença Apache-2.0) para a simulação, via IONOS Cloud (Alemanha), em ativação.

8. Itens a completar pelo responsável pelo tratamento

Item	Resposta da clínica
Base legal escolhida nos termos do artigo 6 do RGPD	
Informação às pacientes: avisos afixados no consultório, menções nos documentos da clínica, política de privacidade	
Prazo de conservação do lado da clínica (dados exportados ou copiados)	
Pessoas autorizadas e gestão de contas	
Validação dos níveis de risco (seção 6) e medidas complementares	
Parecer do encarregado (DPO) da clínica (se houver)	
Consulta aos titulares ou aos seus representantes (se for o caso)	
Decisão e aprovação: nome, cargo, data, assinatura	

Contato

Dúvidas sobre este dossiê, pedido de extrato do registro de acessos, auxílio com os direitos dos titulares: privacy@phimetra.com. Por favor, nunca envie fotos por e-mail.

Editor: Wahib Znidah, empresário individual (nome comercial SAYWA) — SIREN 888 001 054 — SIRET 888 001 054 00020 — 274 rue du Collège, 74950 Scionzier, França · Proteção de dados: privacy@phimetra.com · Contato: contact@phimetra.com · Hospedagem: OVH SAS, 2 rue Kellermann, 59100 Roubaix, França (servidor localizado em Estrasburgo).