

Aviso de Privacidade

VERSÃO 1.3 | MINUTA PARA REVISÃO

Documento temporário para leitura e validação interna. Não está vigente e não representa oferta ou contrato definitivo.

AVISO DE PRIVACIDADE

MINUTA 1.3 - NÃO PUBLICAR SEM VALIDAÇÃO DO AMBIENTE DE PRODUÇÃO E REVISÃO JURÍDICA

Controlador: MEU HORARIO INTERMEDIACOES E AGENCIAMENTO DE SERVICOS LTDA

Aplicativo: Pinho - Plataforma de serviços

CNPJ: 60.775.565/0001-72

Canal de privacidade: suporte@pinho.app

Versão e data: 1.3 - 4 de outubro de 2026

1. ESCOPO

Este Aviso explica como a Plataforma trata dados de Usuários, visitantes, representantes e colaboradores de Estabelecimentos Parceiros, Agentes Comerciais e demais pessoas que interajam com o aplicativo, site, checkout e atendimento.

Para tratamentos realizados exclusivamente pelo Estabelecimento Parceiro ou por produto financeiro contratado diretamente com terceiro, esses participantes poderão atuar como controladores próprios e disponibilizar avisos adicionais.

2. DADOS TRATADOS

2.1. Cadastro necessário para finalizar o pedido

- e-mail;
- telefone;
- nome completo;
- CPF;
- data de nascimento;
- fotografia de perfil, somente se esse recurso permanecer disponível e o Usuário optar por utilizá-lo.

É possível acessar a Plataforma, entrar na página de um Estabelecimento, adicionar Serviços ao pedido e visualizar seu resumo sem concluir esse cadastro. Para finalizar o pedido, o Usuário deverá informar os dados cadastrais acima, inclusive quando já tiver iniciado uma sessão por login externo.

O endereço não integra o cadastro geral. Em compras com cartão de crédito, poderá ser solicitado um endereço de faturamento para validação da transação, prevenção a fraude ou autenticação 3DS. O Usuário poderá escolher salvar esse endereço para compras futuras. Sem essa escolha, o endereço será usado apenas durante o fluxo da compra e não será mantido no cadastro da Plataforma, ressalvados registros estritamente necessários para segurança, prova da transação ou cumprimento de obrigação legal.

A Plataforma também gera ou recebe dados vinculados ao uso, aos pedidos, à segurança e aos pagamentos, descritos abaixo. Esses registros também podem ser dados pessoais para fins da LGPD, mesmo quando não são documentos de identificação.

2.2. Conta e autenticação

- identificadores de conta;
- hash da senha tratado pelo serviço de autenticação, quando o Usuário escolher login por e-mail e senha;
- tokens de sessão;
- dados autorizados no login externo, limitados ao identificador da conta utilizada para acesso, nome, e-mail, confirmação do e-mail e fotografia de perfil, quando disponibilizada;
- eventos de acesso e segurança.

A Plataforma não recebe a senha escolhida para a conta utilizada para acesso. O código analisado não solicita acesso ao Google serviços adicionais da conta utilizada para acesso ou outros produtos Google.

2.3. Uso do aplicativo

- carrinho;
- serviços e estabelecimentos visualizados;
- preferências;
- data e horário;
- pedidos, cancelamentos, reagendamentos e não comparecimentos;
- avaliações, fotografias, comentários e comunicações.

2.4. Pagamentos

- valor, moeda, método, parcelas e status;
- bandeira e últimos dígitos, quando disponibilizados;
- identificadores de transação;
- resultado de autenticação, quando aplicável;
- informações de antifraude;
- sinais técnicos do dispositivo e identificador de dispositivo (fingerprint) para prevenção a fraude;
- resultados de autenticação 3DS, quando esse mecanismo for exigido na compra;
- estornos, reembolsos e chargebacks.

A coleta de cartão utilizará integração segura de pagamento. O navegador enviará número completo, validade e código de segurança diretamente ao ambiente do fornecedor especializado com controles compatíveis com os

padrões do setor de pagamentos. Esses dados completos não serão recebidos pelo backend nem persistidos na base de dados da Plataforma.

O Prestador devolverá um token transitório para a operação. A Plataforma tratará esse token pelo tempo e para as finalidades necessárias à transação, sem utilizá-lo como cadastro permanente do cartão. O token não permite à Plataforma recuperar o número completo ou o código de segurança.

Também são tratados dados de Pix, identificadores de pagamento, autorização, captura, comprovante de venda, informações de divisão de valores, juros, valores aprovados ou negados, reembolsos e tempos do processamento, conforme aplicável.

2.5. Dados técnicos

- endereço IP;
- data e hora;
- dispositivo, sistema operacional e versão;
- idioma;
- identificadores do aplicativo;
- logs, erros, desempenho e eventos de segurança;
- cookies, SDKs e tecnologias semelhantes descritos na Política de Cookies.

2.6. Analytics e publicidade, somente depois da implementação e das escolhas aplicáveis

- identificador pseudônimo de navegador ou dispositivo;
- páginas e telas visualizadas;
- eventos de navegação e conversão;
- origem da visita, campanha e parâmetros de atribuição;
- duração e características da sessão;
- informações de navegador, dispositivo e localização aproximada;
- interações com anúncios e campanhas.

CPF, data de nascimento, endereço, telefone, e-mail, nome ou dados completos de pagamento não deverão ser enviados intencionalmente ao Google Analytics ou ao Meta Pixel.

2.7. Infraestrutura e proteção

- endereço IP, cabeçalhos HTTP, URL solicitada, data, hora e características da conexão;
- eventos de CDN, firewall, mitigação de abuso, disponibilidade e segurança processados pela Cloudflare;
- logs técnicos necessários à entrega, diagnóstico e proteção dos serviços.

O sitemap do site é um arquivo público destinado a mecanismos de busca. Ele não cria perfil do Usuário nem instala cookies por si só. A visita de robôs ou usuários às páginas poderá, entretanto, gerar os logs normais de infraestrutura.

2.8. Atendimento

- mensagens, protocolos, anexos, histórico de solução e eventuais gravações, quando previamente informadas.

2.9. Dados de Estabelecimentos e Agentes

- razão social, nome fantasia, CNPJ, inscrição, endereço, contato e dados bancários;
- dados de sócios, administradores, beneficiários finais, representantes e usuários autorizados;
- documentos de identidade, poderes de representação e validações de KYC/KYB;
- informações fiscais, notas fiscais, extratos, comissões e repasses.

3. FONTES

3.1. Os dados podem ser obtidos

- diretamente do titular;
- automaticamente no uso;
- do Google, mediante autorização;
- de Estabelecimentos Parceiros;
- de Agentes Comerciais;
- de prestadores de pagamento, autenticação, antifraude, infraestrutura e suporte;
- de fontes públicas e bureaus permitidos para validação, prevenção a fraude e cumprimento legal.

4. FINALIDADES E BASES LEGAIS

4.1. Cadastro e autenticação

Finalidade: criar e proteger contas.

Base típica: execução de contrato e prevenção a fraude.

4.2. Pedidos e agenda

Finalidade: formar, confirmar, alterar e acompanhar contratações.

Base típica: execução de contrato.

4.3. Pagamento e divisão de valores

Finalidade: processar, autenticar, dividir, conciliar, estornar, reembolsar e defender transações.

Base típica: execução de contrato, obrigação legal, prevenção a fraude e exercício de direitos.

4.4. KYC/KYB

Finalidade: identificar participantes, validar poderes, cumprir exigências do prestador financeiro e prevenir ilícitos.

Base típica: execução de contrato, obrigação legal/regulatória, proteção do crédito e prevenção a fraude.

4.5. Atendimento

Finalidade: responder solicitações, resolver disputas e manter provas.

Base típica: execução de contrato e exercício de direitos.

4.6. Segurança

Finalidade: detectar abuso, fraude, incidentes e acessos indevidos.

Base típica: legítimo interesse, proteção do crédito e exercício de direitos.

4.7. Avaliações e fotos

Finalidade: publicar conteúdo escolhido pelo Usuário e moderar abusos.

Base típica: execução de contrato, consentimento quando cabível e legítimo interesse.

4.8. Comunicações

Finalidade: enviar mensagens transacionais e marketing autorizado.

Base típica: execução de contrato, legítimo interesse ou consentimento, conforme o conteúdo.

4.9. Melhoria

Finalidade: analisar desempenho, estabilidade e uso.

Base típica: legítimo interesse com minimização ou consentimento para tecnologia não essencial quando exigido.

4.10. Google Analytics

Finalidade: medir audiência, desempenho, navegação e conversões para melhorar os serviços.

Base prevista: consentimento para ativação dos cookies ou identificadores não essenciais.

4.11. Meta Pixel

Finalidade: mensurar campanhas, atribuir conversões, limitar repetição e, se habilitado, formar públicos publicitários.

Base prevista: consentimento prévio para publicidade e rastreamento não essenciais.

4.12. Cloudflare

Finalidade: disponibilizar conteúdo, resolver DNS, entregar páginas, proteger contra abuso, ataques e indisponibilidade.

Base típica: execução de contrato, legítimo interesse em segurança e proteção dos direitos da Plataforma e de terceiros.

4.13. Agentes Comerciais

Finalidade: atribuir indicações, apurar comissões, validar documentos fiscais, prevenir fraude e gerir o contrato.

Base típica: execução de contrato, obrigação legal e exercício de direitos.

5. COMPARTILHAMENTO

5.1. Os dados necessários poderão ser compartilhados com

- Estabelecimentos Parceiros, para execução e atendimento do Pedido;
- Prestadores de Pagamentos, participantes do arranjo, bancos, antifraude e autenticação;
- Google, no fluxo de login federado;
- fornecedor de infraestrutura, para autenticação, banco de dados, APIs e recursos de infraestrutura utilizados pela Plataforma;
- Cloudflare, para hospedagem ou entrega de conteúdo, DNS, desempenho e segurança, conforme os produtos efetivamente contratados;
- Google Analytics, depois de habilitado e consentido, para medição de audiência e desempenho;
- Meta, depois de habilitado e consentido, para mensuração e atribuição de campanhas por meio do Meta Pixel;
- fornecedores de comunicação, suporte, assinatura, monitoramento e segurança;
- contadores, auditores e assessores sujeitos a confidencialidade;
- autoridades e terceiros diante de obrigação, ordem válida ou exercício de direitos;
- sucessores em operação societária, com salvaguardas adequadas.

A Plataforma não vende dados pessoais.

O compartilhamento com Google Analytics e Meta não deverá incluir intencionalmente os dados cadastrais diretamente identificáveis listados neste Aviso. A configuração técnica deverá impedir que parâmetros de URL, campos de formulário ou eventos exponham essas informações.

6. PAPÉIS DOS PARTICIPANTES

A Plataforma e o Estabelecimento poderão atuar como controladores independentes para finalidades próprias. O Estabelecimento deverá limitar o uso dos dados recebidos à execução, atendimento, emissão fiscal e obrigações legítimas.

O fornecedor especializado poderá atuar como controlador independente quando decidir sobre KYC, prevenção a fraude, conta de pagamento, liquidação ou obrigações regulatórias.

Fornecedor que tratar dados somente segundo instruções documentadas poderá atuar como operador.

7. LOGIN GOOGLE

A Plataforma usa login federado compatível com OpenID Connect. No fluxo atual, não são solicitadas permissões para acessar arquivos, mensagens, contatos ou calendário.

Poderão ser recebidos identificador estável da conta utilizada para acesso, nome, e-mail, indicação de e-mail verificado e fotografia, conforme os escopos de autenticação e os dados disponibilizados pelo titular.

A Plataforma não recebe a senha do provedor de identidade. A revogação da autorização poderá exigir o uso de outro método para acessar a conta Pinho.

8. RETENÇÃO

Os dados serão mantidos pelo período necessário às finalidades. Depois serão eliminados ou anonimizados, salvo conservação permitida ou exigida para obrigações legais, prevenção a fraude, auditoria, segurança, cobrança ou exercício de direitos.

A tabela interna de retenção deverá definir prazos para cadastro, pedidos, documentos fiscais, pagamentos, KYC, gravações, logs, cookies, avaliações, agentes e provas de aceite antes da publicação.

9. TRANSFERÊNCIA INTERNACIONAL

fornecedor de infraestrutura, fornecedores globais de tecnologia poderão armazenar, acessar ou tratar dados fora do Brasil ou por equipes localizadas em outros países. A região principal do banco de dados não impede todos os acessos ou transferências internacionais realizados por fornecedores e suboperadores.

Serão adotados mecanismos permitidos pela LGPD e regulamentação da ANPD, além de medidas contratuais, técnicas e organizacionais proporcionais. A Plataforma deverá manter registro da região contratada, países relevantes, instrumentos de transferência e lista de suboperadores.

Os países e fornecedores efetivos deverão constar do inventário interno.

10. SEGURANÇA

São adotadas medidas proporcionais, como controle de acesso, autenticação, permissões por função, registros, criptografia quando aplicável, segregação de ambientes, cópias de segurança e gestão de incidentes.

O fornecedor de infraestrutura declara manter controles auditados segundo SOC 2 Type 2 e certificação ISO 27001. Sua documentação informa proteção criptográfica de discos e backups e uso de conexões protegidas. O serviço de autenticação armazena hash de senha com bcrypt, e não a senha em texto simples.

Essas características do fornecedor não tornam a Pinho automaticamente conforme com a LGPD nem garantem risco zero. A segurança é responsabilidade compartilhada: a Pinho deve configurar corretamente chaves, Row Level Security, funções, permissões, sessões, backups, regiões, logs e acessos administrativos.

Chaves públicas destinadas ao navegador não substituem controle de acesso. Segredos administrativos não deverão ser expostos no cliente, em repositórios públicos, logs ou atendimento.

O fluxo de cartão utiliza integração segura para enviar os dados ao ambiente responsável pelo processamento e devolver à Plataforma apenas um token transitório. A Pinho deverá preservar evidências atualizadas dos controles de segurança aplicáveis e avaliar periodicamente as obrigações relacionadas ao checkout.

Nenhum sistema é imune. Incidentes com risco ou dano relevante serão avaliados e comunicados conforme a legislação e a regulamentação.

11. DIREITOS

11.1. O titular poderá solicitar, nos limites legais

- confirmação e acesso;
- correção;
- anonimização, bloqueio ou eliminação;
- portabilidade;
- informações sobre compartilhamentos;
- informação, revogação e consequências do consentimento;
- oposição a tratamento irregular;
- revisão de decisões automatizadas quando cabível;
- petição à ANPD e a órgãos de defesa do consumidor.

O titular também poderá retirar ou alterar, a qualquer momento, a escolha relativa a Google Analytics e Meta Pixel. A retirada impedirá novas ativações opcionais, sem afetar tratamentos anteriores realizados validamente.

12. EXERCÍCIO DE DIREITOS E EXCLUSÃO

Solicitações: suporte@pinho.app.

A Plataforma poderá verificar a identidade de modo proporcional. A exclusão da conta interromperá usos desnecessários, mas não apagará imediatamente dados cuja conservação seja permitida ou obrigatória.

13. CRIANÇAS E ADOLESCENTES

A Plataforma não se destina ao cadastro autônomo de crianças. Serviços em benefício de menor deverão ser contratados e supervisionados por responsável legal, sempre considerando o melhor interesse.

14. DECISÕES AUTOMATIZADAS

Poderão ser usadas regras automatizadas para prevenção a fraude, segurança, ordenação de resultados, atribuição de indicações e análise de transações.

Quando uma decisão produzir efeitos relevantes e estiver sujeita à LGPD, o titular poderá solicitar informações e revisão cabíveis.

15. ALTERAÇÕES E CONTATO

Alterações relevantes serão comunicadas por meio adequado.

Controlador: MEU HORARIO INTERMEDIACOES E AGENCIAMENTO DE SERVICOS LTDA - CNPJ 60.775.565/0001-72.

Canal de privacidade/encarregado: suporte@pinho.app.

Atendimento geral: suporte@pinho.app e WhatsApp (16) 99294-4224.