

Registro de operações de tratamento

VERSÃO 1.3 | MINUTA PARA REVISÃO

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

REGISTRO PRELIMINAR DE OPERAÇÕES DE TRATAMENTO - LGPD

DOCUMENTO INTERNO - NÃO PUBLICAR

Versão: 1.3 - 4 de outubro de 2026

1. CADASTRO DO CONSUMIDOR

Titulares: usuários e consumidores.

Dados diretamente solicitados para finalizar o pedido: e-mail, telefone, nome completo, CPF e data de nascimento. O endereço de faturamento é solicitado apenas em compras com cartão de crédito e só integra o cadastro para compras futuras mediante escolha do Usuário.

Dados opcionais a confirmar: fotografia de perfil.

Finalidades: criar a conta, identificar o usuário, permitir contratação, prevenir duplicidade ou fraude, atender e cumprir obrigações.

Base legal preliminar: procedimentos preliminares e execução de contrato; obrigação legal quando aplicável; exercício regular de direitos e prevenção a fraude em operações específicas.

Compartilhamentos: fornecedor de infraestrutura e fornecedores estritamente necessários.

Retenção: definir na tabela de retenção.

Riscos: acesso indevido, fraude de identidade, uso excessivo do CPF e exposição indevida do endereço de faturamento.

Salvaguardas: minimização, RLS, controle de acesso, mascaramento, logs, criptografia, revisão de permissões e canal de direitos.

Ponto de decisão: documentar por que CPF e data de nascimento são necessários em cada etapa. Se forem necessários somente para pagamento ou prevenção a fraude, considerar coleta progressiva no checkout em vez do primeiro acesso.

2. AUTENTICAÇÃO POR E-MAIL E SENHA

Dados: e-mail, hash de senha, identificadores de conta, tokens de acesso e renovação, IP e eventos de segurança.

Finalidades: autenticar, manter sessão, recuperar conta e prevenir acesso indevido.

Base legal preliminar: execução de contrato e legítimo interesse em segurança, com teste de balanceamento.

Operador principal: fornecedor de infraestrutura.

Controles: bcrypt no serviço de autenticação, PKCE no fluxo aplicável, expiração e rotação de tokens, proteção contra credenciais vazadas, política de senha, MFA a avaliar e revogação de sessões.

3. LOGIN FEDERADO GOOGLE

Dados: identificador Google, nome, e-mail, confirmação do e-mail, fotografia e tokens necessários ao fluxo.

Escopos esperados: openid, email e profile.

Não solicitar: serviços adicionais da conta utilizada para acesso ou outros escopos sem finalidade nova, avaliação e transparência específicas.

Finalidade: criar ou acessar a conta por método escolhido pelo usuário.

Base legal preliminar: execução de contrato.

Participantes: Google e fornecedor de autenticação.

Controles: tela de consentimento correta, redirect URI restrito, PKCE/state, validação do emissor e audience, revogação e método alternativo de acesso.

4. PEDIDOS E AGENDAMENTOS

Dados: usuário, estabelecimento, serviço, variação, profissional, data, hora, preço, status, histórico de alteração e registros de atendimento.

Finalidades: formar e executar a contratação, oferecer suporte, produzir prova e resolver disputas.

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

Compartilhamento: estabelecimento e colaboradores com permissão necessária.

Controles: isolamento por estabelecimento, acesso mínimo a contato do cliente, trilha de alterações e retenção definida.

5. PAGAMENTOS

Dados recebidos pela Pinho: token de pagamento transitório, identificadores, método, bandeira e últimos dígitos quando fornecidos, valores, parcelas, status, autorizações, recusas, reembolsos, chargebacks, divisão de valores e IP.

Dados enviados diretamente ao Prestador por integração segura de pagamento: número completo, validade e CVV.

Finalidades: processar, conciliar, reembolsar, combater fraude e exercer direitos.

Base legal preliminar: execução de contrato, obrigação legal, proteção do crédito, prevenção a fraude e exercício de direitos, conforme a operação.

Controles: não registrar PAN/CVV, mascarar logs, limitar token à finalidade e validade, manter documentação de segurança aplicável do fornecedor e testar o fluxo antes da produção.

6. AVALIAÇÕES E CONTEÚDO

Dados: nota, texto, fotografia, conta, serviço, pedido e escolha de ocultar perfil.

Finalidades: publicar experiência, moderar abuso e melhorar confiança.

Base legal preliminar: execução dos recursos da Plataforma; consentimento para determinados conteúdos; legítimo interesse sujeito a teste.

Riscos: exposição indevida, difamação, imagem de terceiros e dados sensíveis escritos livremente.

Controles: aviso antes da publicação, moderação, denúncia, opção de exclusão, limitação de upload e remoção de metadados de imagem quando possível.

7. GOOGLE ANALYTICS

Status: planejado, não encontrado ativo no código analisado.

Dados: client ID pseudônimo, sessão, páginas, eventos, origem, dispositivo, navegador e geolocalização aproximada.

Finalidade: mensuração de audiência e desempenho.

Base proposta: consentimento prévio.

Controles: bloquear antes do consentimento; não enviar identificadores diretos; revisar URLs e eventos; reduzir retenção; desativar recursos publicitários não necessários; contrato e transferência internacional; retirada simples.

8. META PIXEL

Status: planejado, não encontrado ativo no código analisado.

Dados: identificadores pseudônimos, páginas, eventos, campanhas, características técnicas e IP recebido pela Meta.

Finalidade: atribuição e mensuração de campanhas; públicos somente se aprovados.

Base proposta: consentimento prévio.

Controles: bloquear antes do consentimento; proibir envio de CPF, e-mail, telefone, endereço, nome, data de nascimento e conteúdo de formulários; revisar eventos e parâmetros; documentar eventual correspondência avançada separadamente; retirada simples.

9. CLOUDFLARE

Dados: IP, cabeçalhos HTTP, URL, data, hora, dispositivo, identificadores e eventos de segurança conforme produtos ativos.

Finalidades: hospedagem/entrega, DNS, CDN, firewall, disponibilidade e prevenção a abuso.

Base preliminar: execução do serviço e legítimo interesse em segurança.

Controles: confirmar produtos, cookies, logs, duração, região e DPA; restringir acessos; configurar retenção mínima; documentar transferência internacional.

10. FORNECEDOR DE INFRAESTRUTURA

Serviços identificados: banco Postgres, autenticação, API e potencialmente armazenamento.

Dados: cadastro, conta, pedidos, operações, sessões e demais registros definidos pela Pinho.

Papel preliminar: operador da Pinho para serviços contratados; poderá haver suboperadores.

Controles declarados pelo fornecedor: SOC 2 Type 2, ISO 27001, criptografia de discos/backups e conexões protegidas.

Responsabilidades da Pinho: região, chaves, RLS, grants, funções SECURITY DEFINER, usuários administrativos, logs, backups, retenção, resposta a incidentes e revisão de suboperadores.

11. SITEMAP E INDEXAÇÃO

O sitemap contém URLs públicas e não é, por si só, operação de perfilamento. Deve excluir rotas autenticadas, parâmetros pessoais, pedidos e páginas não destinadas à indexação.

12. TESTES DE LEGÍTIMO INTERESSE A PRODUZIR

- segurança e prevenção a abuso;
- logs técnicos;
- prevenção a fraude fora de hipótese legal mais específica;
- melhoria de produto sem consentimento;
- moderação de avaliações;
- comunicações institucionais não estritamente contratuais.

Cada teste deve registrar finalidade, necessidade, expectativa do titular, impacto, salvaguardas, direito de oposição e conclusão.