

Política de Privacidade

Esta Política explica como a Cohearo trata dados pessoais e quais escolhas e direitos estão disponíveis para você.

Versão 0.1.7

Vigência a partir de 9 de setembro de 2026

1. Escopo e papéis

Esta Política explica como a Cohearo coleta, usa, compartilha, conserva e protege dados pessoais por meio de seus aplicativos, sites, APIs e integrações.

A Cohearo é operada por **RECHIA & MILOCO DESENVOLVIMENTO DE SOFTWARES LTDA**, CNPJ 65.175.527/0001-00, Rua Visconde do Rio Branco, 1488, Conj. 909, Andar 09 — Condomínio Universe Life Square, Bloco Comercial, Centro, Curitiba — PR, Brasil. Contato: contact@cohearo.com.

A Cohearo é controladora dos dados de conta, cobrança, segurança, suporte e operação do produto cujas finalidades determina. Para o conteúdo fornecido aos nossos serviços em nuvem, o cliente pode determinar as finalidades e atuar como controlador, enquanto a Cohearo trata esse conteúdo conforme suas instruções, como operadora quando aplicável. Os papéis dependem da atividade de tratamento.

O cliente deve ter base legal e fornecer os avisos exigidos antes de gravar pessoas ou tratar seu conteúdo. Uma transcrição não é automaticamente um dado pessoal sensível, mas pode conter informações de saúde, biométricas, religiosas, políticas ou outras informações sensíveis. Nesse caso, o cliente deve cumprir os requisitos aplicáveis, inclusive o artigo 11 da LGPD. O tratamento realizado pela própria Cohearo também deve cumprir os requisitos que lhe são aplicáveis.

2. Áudio, transcrições e nuvem

A gravação de áudio e a transcrição ocorrem localmente no dispositivo. O áudio não é enviado aos servidores da Cohearo nem a provedores de aprimoramento por IA. O sistema operacional, backups ou outros programas podem tratar arquivos locais conforme suas próprias configurações.

Dado	Tratamento e conservação
Gravação de áudio	Local no dispositivo, com política de limpeza automática de 72 horas. A limpeza depende da execução do aplicativo.
Transcrição local e edições	Permanecem localmente até o usuário excluí-las, remover os dados do aplicativo ou desinstalá-lo, sujeitas aos backups do dispositivo.

Dado	Tratamento e conservação
Transcrição na nuvem do plano Gratuito	Armazenada por até 7 dias e então excluída do armazenamento ativo em nuvem, salvo exclusão anterior pelo usuário.
Transcrições sincronizadas criadas durante um plano pago	Mantidas por prazo indeterminado nos termos dos Termos até o usuário excluí-las ou encerrar a conta. A mudança posterior para o plano Gratuito não reduz esse prazo.

Quando houver escolha de uso apenas local, a sincronização é opcional. Dados sincronizados podem incluir texto da transcrição, títulos, notas, edições, resultados de aprimoramento, instruções predefinidas ou personalizadas, identificação de falantes, marcações de tempo, idioma, metadados do dispositivo e aplicativo, identificadores do conteúdo e metadados de compartilhamento ou espaço de trabalho necessários ao recurso escolhido.

As representações numéricas da voz usadas para distinguir falantes ficam no dispositivo. Identificadores e nomes de perfis de falantes podem ser sincronizados, mas as representações da voz não são enviadas.

3. Informações tratadas

Conforme os recursos usados, tratamos:

- **Conta e identidade:** email, identificadores da conta, perfil opcional, idioma, eventos de autenticação e informações retornadas por provedores de login compatíveis.
- **Conteúdo do cliente:** conteúdo e metadados sincronizados descritos acima, solicitações e resultados de aprimoramento e conteúdo enviado pela API ou pelo Model Context Protocol (MCP).
- **Cobrança:** plano, teste e permissões, moeda, país de cobrança, referências de faturas e transações e metadados limitados de pagamento. A Stripe trata os dados do cartão; a Cohearo não armazena o número completo.
- **Suporte:** mensagens, anexos e informações fornecidas ao pedir ajuda.
- **Análise opcional:** após consentimento, eventos de uso, navegação, características do dispositivo e aplicativo e contexto técnico geral. A reprodução de sessão está desativada.
- **Diagnóstico:** nenhum relatório é enviado no modo local. No modo nuvem, relatórios de falha e erro ficam ativados por padrão e podem ser desativados em Configurações. Antes do envio, filtramos automaticamente campos conhecidos de conteúdo pessoal, como nomes de gravações, predefinições e falantes, endereços de email e caminhos de arquivos. A filtragem não é perfeita, e um valor digitado pelo usuário pode aparecer inesperadamente no contexto de um erro.

- **Segurança e rede:** endereço IP, horário, agente do usuário, identificadores do dispositivo e aplicativo, resultados de autenticação e autorização, eventos de chaves rejeitadas e limites de uso e registros limitados para impedir abusos e investigar incidentes. Filtramos campos conhecidos de segredos e conteúdo nos registros.

Não vendemos dados pessoais nem os compartilhamos com anunciantes ou corretores de dados. Não usamos transcrições para treinar modelos de IA da Cohearo ou de terceiros.

4. Finalidades e bases legais

Finalidade	Base legal típica
Conta, sincronização, aprimoramentos, API e MCP	Execução de contrato ou providências solicitadas antes da contratação
Assinaturas, faturas e pagamentos	Execução de contrato e obrigação legal
Autenticação, prevenção de abuso, limites e segurança	Interesse legítimo na integridade do serviço; obrigação legal quando aplicável
Suporte e mensagens de serviço	Execução de contrato e interesse legítimo
Análise opcional do produto	Consentimento
Diagnóstico e confiabilidade	Interesse legítimo, com controles disponíveis para desativação
Cumprimento da lei, disputas e demandas	Obrigação legal e exercício regular de direitos

Quando usamos interesse legítimo, avaliamos necessidade, proporcionalidade e direitos afetados. O consentimento pode ser retirado sem afetar o tratamento lícito anterior.

5. Provedores e integrações

Compartilhamos as informações razoavelmente necessárias para cada função:

- **AWS** hospeda nossos serviços principais. O armazenamento de contas e transcrições em produção fica em São Paulo, Brasil. Serviços globais, como a entrega de conteúdo, podem tratar dados de requisições em outros locais.
- **Stripe** trata assinaturas, pagamentos, fraude e cobrança nos Estados Unidos.
- **OpenRouter**, nos Estados Unidos, e provedores de modelos subsequentes tratam pedidos de aprimoramento conforme abaixo. Os locais de processamento são separados do local do nosso armazenamento em nuvem.
- **PostHog**, hospedada nos Estados Unidos, recebe dados analíticos somente após consentimento. Os eventos são conservados por um ano no plano atual. O cookie de consentimento dura 180 dias, quando perguntamos novamente. Respeitamos o Global Privacy Control, oferecemos desativação no produto e mantemos a reprodução de sessão desativada.

- **Sentry** trata diagnósticos na configuração atual da região da União Europeia, sujeita à filtragem e aos controles de desativação.
- **Cloudflare** hospeda o site público e fornece DNS. Sua rede global recebe dados de requisições do site, como endereço IP, informações do navegador e horário da visita.
- **Google** trata informações de login quando o usuário escolhe o login do Google.

Os provedores podem usar suboperadores. Você pode solicitar mais informações sobre destinatários e salvaguardas pelo contact@cohearo.com. Alterações relevantes seguem o processo de aviso abaixo.

Aprimoramento por IA

Quando solicitado, a Cohearo envia pelo OpenRouter o texto necessário ao aprimoramento. A solicitação pode incluir a transcrição, instruções predefinidas ou personalizadas e estrutura técnica limitada. O áudio não é enviado.

A retenção zero de dados está ativada na nossa conta da OpenRouter, restringindo o encaminhamento aos serviços que ela identifica como compatíveis com essa política para o conteúdo de inferência. A Cohearo não usa suas transcrições para treinar modelos de IA. Essa configuração não se aplica ao conteúdo armazenado na sua conta da Cohearo nem a um assistente externo que você conecte separadamente. Consulte nossa página de Segurança e tratamento de dados e a política da OpenRouter para conhecer seu alcance.

API e MCP

Um cliente de API ou MCP habilitado pode acessar conteúdo e recursos dentro dos escopos e permissões concedidos. A Cohearo trata o conteúdo da requisição, dados de autenticação, metadados da operação, uso e cotas e registros de segurança necessários para fornecer e proteger o acesso. O cliente controla quais ferramentas externas conecta e deve avaliar suas práticas de privacidade e segurança.

Escolhas de análise e diagnóstico

A análise de terceiros permanece desativada até o consentimento. A escolha pode ser alterada nas configurações, e o Global Privacy Control é respeitado. Separadamente, a Cohearo conta visualizações de páginas e cliques de download do site público em sua própria infraestrutura no Brasil, sem cookies nem identificadores entre visitas, inclusive quando a análise é recusada. Diagnósticos nunca são enviados no modo local; no modo nuvem, ficam ativados por padrão e podem ser desativados em Configurações. Essas escolhas não impedem registros estritamente necessários de segurança, cobrança ou operação.

Após o consentimento, a PostHog pode receber endereços de páginas, sites de origem, endereço IP e localização aproximada, detalhes do navegador e dispositivo, eventos de navegação, interação e desempenho e eventos da conta, como cadastro ou mudanças de assinatura. Ela usa um cookie e um identificador no armazenamento local. Ao se cadastrar ou entrar, esse identificador pode ser associado à conta e à atividade anterior de navegação realizada com consentimento. Podemos usar pesquisas na página. A reprodução de sessão exige atualização

da política e novo consentimento antes de ser ativada.

No painel, Dados e Privacidade em Configurações controla a análise da conta: a desativação interrompe eventos de conta enviados pelo servidor e a coleta no painel nos dispositivos em que você entra. A escolha no site público é específica de cada navegador; use Preferências de cookies em cada navegador no qual aceitou. Revogar o consentimento interrompe a coleta e remove o cookie da PostHog daquele navegador. Cookies necessários de login e segurança são separados.

6. Conservação, exclusão e anonimização

Conservamos dados pelos períodos indicados aqui ou enquanto necessários para prestar o serviço, cumprir a lei, resolver disputas e proteger o serviço.

O conteúdo excluído da nuvem é removido ou programado para exclusão dos sistemas ativos. A exclusão da conta é concluída em até 30 dias após uma solicitação válida, salvo prazo legal menor. Registros limitados de tributos, contabilidade, prevenção de fraude, segurança ou demandas podem ser conservados quando necessário.

Cópias podem permanecer temporariamente em backups até expirarem conforme seu ciclo de conservação. Registros limitados de cobrança, uso ou segurança também podem permanecer quando sua conservação for necessária e lícita. Remover identificadores diretos nem sempre torna um registro anônimo; continuamos protegendo os dados pessoais conservados e restringindo seu uso. O conteúdo local e os backups do dispositivo permanecem sob seu controle e conforme as configurações do provedor de backup.

Atualmente, eventos analíticos são conservados por até um ano. O cookie de consentimento do navegador dura 180 dias; registros das decisões de consentimento são conservados conforme necessário para comprovar a escolha. As contagens do site sem cookies são agregadas e não vinculadas a uma conta. Os prazos de registros operacionais, de segurança e diagnóstico variam por sistema e se limitam às necessidades operacionais, legais e de segurança.

7. Segurança e incidentes

Usamos salvaguardas adequadas ao tratamento, incluindo controle de acesso, privilégio mínimo, criptografia em trânsito, banco de dados e armazenamento de objetos criptografados em repouso, gestão de segredos, monitoramento, limites de uso e procedimentos de incidentes. Nenhum serviço garante segurança absoluta. O usuário deve proteger dispositivos, conta, chaves de API e clientes conectados.

Investigamos, contemos, corrigimos e documentamos incidentes suspeitos. Em incidente confirmado com dados pessoais que possa causar risco ou dano relevante, a Cohearo notificará a ANPD e os titulares conforme exigido — em geral, em até três dias úteis segundo o regulamento atual da ANPD, sujeito ao seu escopo e às exceções permitidas. O prazo de comunicação é contado do nosso conhecimento de que dados pessoais foram afetados. Prevalece prazo menor imposto por outra lei ou contrato aplicável. Uma comunicação inicial pode ser complementada conforme a apuração. Como operadora, a Cohearo notificará e auxiliará o

cliente responsável quando exigido.

8. Transferências internacionais

Alguns provedores e suboperadores podem tratar dados fora do Brasil. Usamos salvaguardas contratuais, organizacionais e técnicas adequadas e buscamos aplicar, quando necessário, um mecanismo de transferência permitido pelo artigo 33 da LGPD. Cláusulas contratuais europeias ou termos gerais de um provedor não comprovam, por si sós, o cumprimento dos requisitos brasileiros.

Estamos revisando as salvaguardas e o mecanismo da LGPD para cada fluxo internacional. Atualizaremos esta seção conforme essa revisão for concluída; esta Política não certifica o mecanismo de transferência de um provedor específico.

9. Seus direitos

Sujeito à lei aplicável, o titular pode pedir confirmação do tratamento; acesso; correção; anonimização, bloqueio ou exclusão de dados desnecessários, excessivos ou ilícitos; portabilidade quando regulamentada; informação sobre compartilhamento; informação sobre negar consentimento; revogação do consentimento; exclusão de dados tratados por consentimento, observadas as exceções; revisão de decisões unicamente automatizadas quando aplicável; oposição; e petição à ANPD.

Para confirmação e acesso conforme o artigo 19 da LGPD, fornecemos resposta simplificada imediatamente ou declaração clara e completa em até 15 dias do pedido. Os demais pedidos seguem o prazo exigido para cada direito e jurisdição; não aplicamos prazo geral de 30 dias quando houver regra menor.

A exportação está disponível na conta e inclui informações da conta, transcrições, pastas, predefinições, participação em organizações, histórico de assinatura e uso e metadados de chaves de API. Senhas e valores de chaves secretas não são incluídos. Você também pode nos contatar para exercer seus direitos de acesso e portabilidade, inclusive para dados pessoais não disponíveis nessa exportação. Envie outros pedidos, inclusive exclusão da conta, a contact@cohearo.com. Podemos verificar identidade e poderes. Quando a Cohearo trata conteúdo somente por conta de um cliente, podemos direcionar o pedido a esse controlador e auxiliá-lo conforme exigido. A exclusão da conta é concluída em até 30 dias após pedido válido, salvo prazo legal menor.

10. Crianças, alterações e contato

A Cohearo é destinada a pessoas com 18 anos ou mais. Não coletamos intencionalmente dados pessoais de crianças ou adolescentes, e o serviço não está preparado para as proteções que esses dados exigem. Se você acredita que uma pessoa menor de 18 anos criou uma conta, escreva para contact@cohearo.com.

Publicamos atualizações com versão e data de vigência e mantemos versões anteriores disponíveis. Avisamos os titulares das contas por email antes de alterações relevantes entrarem

em vigor. Uma política alterada não substitui o consentimento quando uma nova autorização for exigida.

RECHIA & MILOCO DESENVOLVIMENTO DE SOFTWARES LTDA CNPJ 65.175.527/0001-00 Rua Visconde do Rio Branco, 1488, Conj. 909, Andar 09 Condomínio Universe Life Square, Bloco Comercial, Centro, Curitiba — PR, Brasil contact@cohearo.com

Versão 0.1.7 · Vigência a partir de 9 de setembro de 2026