

Política de Privacidade

Version 1.0

Última atualização: 2026-08-04

Aplica-se a: Peoplelane para macOS

1. Controlador e contato

Oliver Gepp

Hübeliweg 11

3052 Zollikofen

Suíça

E-mail: support@peoplelane.app

"Nós" nesta política se refere à pessoa acima. "Peoplelane" e "o app" se referem ao aplicativo Peoplelane para macOS. Esta política descreve apenas o app; o site peoplelane.app é regido por um aviso separado.

2. Resumo

- Tudo o que você registra no Peoplelane é armazenado no seu Mac.
- O app não contém análise de uso, publicidade, rastreamento nem relatório de falhas.
- O Peoplelane pode ser usado sem conta. Nenhuma conta é necessária.
- O app faz conexões de rede de saída apenas para as finalidades listadas na seção 5.
- O conteúdo que você registrou é transmitido a terceiros apenas quando você aciona uma solicitação de IA, ou como arquivo de backup criptografado, caso você tenha apontado sua pasta de backup para um local sincronizado por um serviço em nuvem (ver seção 10).

3. Quem é responsável por quê

O Peoplelane é um auxiliar de memória para leads, gestores, mentores e coaches. As informações que você registra são, em grande parte, informações sobre outras pessoas — geralmente membros da sua equipe.

Você decide o que registrar. Conforme a legislação de proteção de dados aplicável, você é responsável por esse conteúdo, incluindo informar as pessoas envolvidas quando a lei exigir.

Nós não recebemos esse conteúdo. Ele não é armazenado em nossos servidores, e não temos acesso técnico a ele. Quando você envia conteúdo a um provedor de IA (seção 6), esse provedor o processa por sua instrução e sob o acordo entre você e esse provedor.

4. Dados armazenados no seu dispositivo

4.1 Conteúdo que você insere

- Perfis de pessoas: nome, projeto, cliente, localização, tipos de cuidado, periodicidade de contato, dias de trabalho, percentual de trabalho, data de nascimento, dados de contato privados, uma nota de texto livre sobre salário, notas, foto, tags
- Contexto privado registrado para uma pessoa
- Interações: o texto livre original que você inseriu ("braindump"), um resumo, o tipo e a data da interação, quatro avaliações em escala de 1 a 5 (humor, carga de trabalho, status do projeto, desenvolvimento), tópicos, riscos, atualizações de contexto privado anotadas para essa interação, perguntas abertas, uma recomendação de próximo contato
- Metas de desenvolvimento
- Follow-ups
- Campos personalizados definidos pelo usuário e seus valores
- O estado das entradas na caixa de eventos (lida, adiada, descartada)

Esses dados são armazenados em um arquivo de banco de dados local no seu Mac, dentro do diretório de suporte de aplicativos do app. O arquivo como um todo não é criptografado separadamente pelo app; ele é protegido pelas permissões de arquivo do macOS e, se você a tiver ativado, pelo FileVault. Dentro desse arquivo, o contexto privado registrado para uma pessoa, os dados de contato privados e a nota de salário são cada um criptografado com AES-256-GCM, usando uma chave mantida no Chaveiro do macOS (ver seção 4.3). Atualizações de contexto privado anotadas em uma interação individual não são cobertas por isso e são armazenadas como texto simples, como todo o restante desta lista.

4.2 Configurações

As preferências do aplicativo são armazenadas no sistema padrão de preferências do macOS: configurações de notificação e horário do resumo, idioma da interface e tema, estado do bloqueio do app e tempo limite de inatividade, a referência à pasta de backup selecionada e os limites de status. A configuração do seu provedor de IA (provedor, modelo, ordem e o registro de data/hora da sua confirmação de compartilhamento de dados) é armazenada no banco de dados local.

4.3 Chaveiro do macOS

- Chaves de API dos provedores de IA. São armazenadas somente para este dispositivo e não são sincronizadas com o iCloud.
- A chave de criptografia de campo que protege seu contexto privado, seus dados de contato privados e sua nota de salário (seção 4.1). É armazenada somente para este dispositivo e não é sincronizada com o iCloud. Se o arquivo de banco de dados bruto fosse copiado para outro Mac fora do próprio recurso de backup e restauração do app, esses três campos não poderiam ser lidos lá, porque a chave nunca deixa o dispositivo que a criou.
- A chave de criptografia de backup. Se o Chaveiro do iCloud estiver ativo no seu Mac, essa

chave é sincronizada com seus outros Macs usando o mesmo ID Apple, para que os backups possam ser restaurados neles. Ver seção 10.

As chaves de API não são gravadas no banco de dados local, em exportações ou em arquivos de log.

5. Conexões de saída

Toda conexão de rede revela seu endereço IP e metadados gerais de conexão ao serviço destinatário. Além disso, o app se conecta aos seguintes destinatários:

- O provedor de IA que você configurar — para estruturar texto livre, reescrever texto, extrair follow-ups ou verificar se um provedor configurado está acessível. Transmitido: para essas funções de IA, uma instrução fixa e o texto que você envia (ver seção 6); para uma verificação de conexão, apenas uma frase de teste fixa, nunca seu conteúdo. Somente quando você aciona uma função de IA, ou testa a conexão de um provedor em Configurações.
- Supabase, verificação de versão — para informá-lo sobre atualizações recomendadas e obrigatórias. Transmitido: versão do app e string de versão do macOS. A cada inicialização, fora do modo de demonstração.
- Apple e RevenueCat — para determinar o status da sua assinatura e para comprar ou restaurar. Transmitido: dados de compra e de direito de uso, e um identificador anônimo gerado pela RevenueCat. Ao iniciar o app, e quando você abre a tela de assinatura, compra ou restauração.
- Hugging Face — para baixar o modelo de reconhecimento de voz uma única vez. Nenhum conteúdo seu é transmitido. Na primeira vez que você usa o dictation.
- E-mail de suporte — para responder à sua mensagem. Transmitido: sua mensagem e, se você deixar a opção ativada, versão do app, versão do macOS, modelo do Mac e idioma configurado. Somente quando você envia o e-mail pelo seu próprio programa de correio.

5.1 Verificação de versão

Ao iniciar, o app solicita os requisitos de versão atuais a uma Edge Function do Supabase. A solicitação contém a versão do app e a string de versão do macOS. Nada do que você registrou é transmitido. Esses dois valores são armazenados por nós junto com um registro de data/hora, para que possamos ver quais versões de app e macOS estão em uso. Os registros não contêm nenhum identificador que os vincule a você ou ao seu dispositivo. A verificação é ignorada no modo de demonstração e quando o app foi compilado sem credenciais de servidor.

5.2 Assinaturas

As compras são processadas pela Apple através da Mac App Store. Não recebemos seus dados de pagamento. A RevenueCat processa dados de compra e de direito de uso em nosso nome,

para que o app possa determinar se uma assinatura está ativa. O app não transmite à RevenueCat nenhum nome de usuário, endereço de e-mail ou conteúdo; a RevenueCat gera seu próprio identificador anônimo.

O app consulta a RevenueCat sobre o status da sua assinatura quando é iniciado, para que os recursos que você pagou fiquem disponíveis imediatamente, e novamente quando você abre a tela de assinatura. Isso não ocorre no modo de demonstração.

6. Recursos de IA

O suporte de IA é opcional. No macOS 26 ou posterior, o app pré-configura o Apple Intelligence — que roda no seu dispositivo e não precisa de chave de API — como único provedor na primeira vez que é iniciado sem uma configuração de IA própria; em versões anteriores do macOS nada é pré-configurado. Um provedor que envia dados pela internet nunca é pré-configurado, e cada solicitação de IA é acionada por você.

Provedores disponíveis. OpenAI, Anthropic, Google Gemini, xAI Grok, OpenRouter, qualquer endpoint compatível com OpenAI cujo endereço você mesmo insira (que também pode ser um serviço rodando na sua própria máquina), e o Apple Intelligence, que roda no seu dispositivo.

Conexão direta. As solicitações vão do seu Mac diretamente ao provedor selecionado. Não operamos nenhum servidor intermediário, não recebemos nenhuma cópia da solicitação e não temos acesso à resposta.

O que é transmitido. Uma instrução fixa e o texto que você envia. O nome armazenado da pessoa não faz parte da solicitação; o app insere um placeholder neutro em vez disso. O contexto privado armazenado, foto, data de nascimento, nota de salário, dados de contato, interações anteriores, metas e follow-ups não são transmitidos. Para a função de reescrita, apenas o texto que você selecionou é transmitido.

Confirmação antes da primeira transmissão. Antes da primeira solicitação após você configurar ou alterar um provedor, o app pede que você confirme que os dados serão enviados a esse provedor. Se sua lista contiver apenas provedores que rodam no seu dispositivo, nenhum dado é enviado pela rede e o app não pergunta.

Teste de conexão. Configurações permite testar se um provedor configurado está acessível, um por um ou todos de uma vez. Isso envia uma frase de teste fixa — nunca seu conteúdo — a esse provedor, junto com sua chave de API. Ocorre no momento em que você aciona o teste, sem a confirmação descrita acima, porque nenhum conteúdo seu está envolvido.

Vários provedores. Se você configurar mais de um provedor, o app usa o primeiro. Se essa solicitação falhar, o mesmo texto é enviado automaticamente ao próximo provedor da sua lista, sem perguntar novamente. Isso acontece quando um provedor retorna um erro de servidor, não conhece o modelo que você configurou, ou reporta uma cota ou limite de taxa — e também quando o Apple Intelligence é o primeiro da lista e está indisponível no seu Mac, ou seu texto é mais longo que a janela de contexto dele. Uma solicitação que você pretendia processar no seu dispositivo pode, assim, ser enviada a um provedor na internet. Configure apenas provedores aos

quais você esteja disposto a enviar seu conteúdo. Se seu conteúdo precisar permanecer no seu Mac, configure o Apple Intelligence como único provedor.

Processamento pelo provedor. O que acontece com o texto transmitido é regido pelos termos e pela política de privacidade desse provedor. Provedores podem reter dados de entrada por um período de tempo ou usá-los para detecção de abuso. Leia os termos do provedor que você selecionar.

Resultados são rascunhos. Os resultados de IA são exibidos para revisão. Nada é armazenado até que você o confirme.

Precisão. O conteúdo gerado por IA pode estar incompleto ou errado, inclusive de formas que não são óbvias. Não o use como única base para decisões sobre emprego, pessoal ou disciplina.

Sua responsabilidade. Você decide se pode transmitir um determinado conteúdo a um provedor externo. Para dados como informações de saúde, opiniões religiosas ou políticas, afiliação sindical, orientação sexual ou processos criminais, isso geralmente requer uma base legal específica. Considere se um provedor local no dispositivo é suficiente para seu propósito.

7. Dictation

O dictation roda no seu dispositivo. O reconhecimento de voz é realizado localmente por um modelo Core ML; o áudio não é transmitido para reconhecimento.

Na primeira vez que você usa o dictation, o modelo é baixado uma única vez do huggingface.co e depois mantido localmente. Esse download não contém nenhum conteúdo seu.

O áudio é gravado em um arquivo temporário enquanto você dita e excluído após a transcrição. O acesso ao microfone requer sua permissão, que o macOS solicita.

8. Bloqueio do app

O Peoplelane oferece um bloqueio de app opcional e um bloqueio automático após um período de inatividade que você configura.

A autenticação é realizada pelo macOS com Touch ID, Apple Watch ou sua senha de login, dependendo do que seu Mac suporta. O app recebe apenas o resultado da autenticação. Nenhum dado biométrico é acessível ao app.

9. Notificações

As notificações são geradas no seu dispositivo e não são enviadas por nenhum servidor. Seu texto consiste em frases fixas e contagens, por exemplo o número de pessoas que precisam de atenção. As notificações não contêm nomes nem conteúdo das suas anotações.

10. Backups e exportações

Backups. O app grava um backup em três momentos: uma vez por dia calendário quando você o abre, a cada vez que você o encerra, e sempre que você aciona um manualmente. Cada backup é um arquivo separado, nomeado conforme o momento em que foi gravado. Os backups são criptografados no seu Mac com AES-256-GCM. A chave é mantida no Chaveiro do macOS. Não temos acesso aos seus backups nem à chave.

Backups antigos são removidos automaticamente. O app mantém um backup por dia nos últimos sete dias, um por semana nos últimos trinta dias, e um por mês no último ano; qualquer coisa mais antiga é excluída. Como o backup de encerramento é gravado antes dessa limpeza ser executada, encerrar o app várias vezes ao dia produz vários arquivos, dos quais apenas o mais recente sobrevive ao dia. Se sua pasta de backup for sincronizada por um serviço em nuvem, cada um desses arquivos é transferido por esse serviço antes de ser removido novamente.

Local do backup. Por padrão, os backups são armazenados em uma pasta específica do app no seu Mac. Você pode selecionar uma pasta diferente. Se você selecionar uma pasta sincronizada por um serviço em nuvem, os arquivos de backup criptografados são transferidos por esse serviço.

Chave de backup. Se o Chaveiro do iCloud estiver ativo no seu Mac, a chave de backup é sincronizada com seus outros Macs usando o mesmo ID Apple, para que os backups possam ser restaurados neles. A Apple armazena o conteúdo do Chaveiro do iCloud criptografado de ponta a ponta. Você também pode exportar a chave e importá-la em outro Mac. Se a chave for perdida, os backups existentes não podem mais ser descriptografados.

Exportações. Você pode exportar os dados de uma pessoa como Markdown, JSON ou PDF. As exportações não são criptografadas e podem conter tudo o que foi registrado sobre essa pessoa, incluindo contexto privado. Depois de salvar uma exportação, protegê-la é responsabilidade sua.

11. Registro (logging)

O app grava entradas técnicas no sistema de log do macOS: nomes de provedor e modelo, códigos de status HTTP, tipos de erro, durações e identificadores internos. Texto livre, respostas de IA e chaves de API não são gravados nesses logs em versões lançadas. O conteúdo de solicitações e respostas só é registrado em builds de desenvolvimento, que não são distribuídos. Essas entradas de log permanecem no seu Mac. Elas não são transmitidas a nós.

12. Exclusão e retenção

No seu dispositivo. O conteúdo que você registra permanece até que você o exclua; o app não o exclui por conta própria. Duas coisas são limpas automaticamente: registros de estado de entradas da caixa de entrada depois de expirarem, e arquivos de backup mais antigos, conforme a regra de retenção descrita na seção 10.

Excluir uma pessoa no editor arquiva o registro e pode ser desfeito. A exclusão permanente é realizada a partir do arquivo e remove a pessoa junto com suas interações, metas, follow-ups

vinculados e estado da caixa de entrada.

Backups não são afetados pela exclusão. Arquivos de backup criados antes de uma exclusão ainda contêm os dados excluídos, e restaurar tal backup os trará de volta. Se você também quiser que os dados sejam removidos dos backups, exclua os arquivos de backup.

Exportações não são afetadas pela exclusão. Arquivos que você exportou permanecem onde você os salvou.

Desinstalação. Remover o app não necessariamente remove a pasta de dados, as entradas do Chaveiro ou as preferências. Exclua-as você mesmo se quiser que os dados desapareçam.

Dados que mantemos. Três categorias, e apenas estas:

- Registros de verificação de versão: versão do app, versão do macOS e um registro de data/hora. Nenhum período de exclusão automática está implementado.
- Dados de compra e de direito de uso mantidos pela RevenueCat em nosso nome. Estão vinculados a um identificador anônimo gerado pela RevenueCat, não ao seu nome ou endereço de e-mail.
- Correspondência de suporte: sua mensagem, seu endereço de e-mail e os detalhes de diagnóstico que você escolheu incluir. Mantemos por quanto tempo precisarmos para tratar sua consulta e qualquer acompanhamento. Nenhum período de exclusão automática está implementado.

Você pode nos solicitar a exclusão de qualquer um desses dados; ver seção 14.

13. Bases legais

Onde o GDPR se aplica:

- Verificação de versão e bloqueio de atualização: nosso interesse legítimo em fornecer software funcional e atualizado (art. 6(1)(f) do GDPR)
- Processamento de assinaturas: execução do contrato (art. 6(1)(b) do GDPR)
- Correspondência de suporte: execução do contrato e nosso interesse legítimo em responder consultas (art. 6(1)(b) e (f) do GDPR)

A transmissão a um provedor de IA é realizada por sua instrução. Você determina a finalidade e a base legal do conteúdo que transmite.

Conforme a Lei Federal Suíça de Proteção de Dados, o tratamento por uma pessoa privada não requer uma justificativa específica. Tratamos os dados descritos acima de acordo com os princípios dessa lei, em particular legalidade, boa-fé, proporcionalidade, limitação de finalidade e segurança dos dados.

14. Seus direitos

Em relação aos dados que mantemos — ou seja, os dados descritos na seção 12 sob "Dados que mantemos" — você pode solicitar acesso, correção, exclusão e, quando aplicável, restrição do tratamento, oposição e portabilidade de dados. Escreva para support@peoplelane.app.

Registros de verificação de versão e os dados mantidos pela RevenueCat não carregam nenhum identificador que nos permita atribuí-los a você, portanto podemos não conseguir localizar seus registros e atender a uma solicitação relacionada a eles. Correspondência de suporte é diferente: ela chega até nós a partir do seu próprio endereço, então uma solicitação sobre ela sempre pode ser atendida.

Você pode registrar uma reclamação junto a uma autoridade de supervisão: na Suíça, o Comissário Federal de Proteção de Dados e Informação; no EEE, a autoridade do seu país de residência.

Solicitações de pessoas que você registrou no Peoplelane devem ser dirigidas a você, não a nós. Não temos acesso a esses dados.

15. Transferências internacionais

Dependendo de onde os serviços listados na seção 5 são operados, os dados podem ser processados fora da Suíça e do Espaço Econômico Europeu — em particular pela Apple, RevenueCat, Hugging Face e o provedor de IA que você escolheu. Qual provedor de IA, e portanto qual país, é sua decisão.

16. Segurança

O app roda no sandbox do macOS com o hardened runtime ativado. Conexões de rede usam TLS; conexões não criptografadas são possíveis apenas com endpoints na sua própria máquina ou rede local que você mesmo configure. Segredos são mantidos no Chaveiro do macOS, backups são criptografados com AES-256-GCM, e nenhum conteúdo que você registra é armazenado em nossos servidores.

Nenhuma medida técnica pode eliminar todos os riscos. Mantenha o macOS atualizado, use a criptografia completa de disco e proteja os arquivos exportados.

17. Crianças

O Peoplelane é uma ferramenta para uso profissional e não é direcionada a crianças.

18. Alterações a esta política

Podemos alterar esta política quando o app for alterado. A versão e a data no topo mostram o estado atual. A versão atual está disponível no app em Configurações.

19. Idioma de referência

A versão em inglês desta Política de Privacidade é a versão com validade jurídica. As traduções

são fornecidas por conveniência.