

Política de privacidade

Hineh Tecnologia Ltda · CNPJ 69.280.849/0001-62

Versão 1.0 · 9 de outubro de 2026

Aprovação e última revisão: 10/10/2026 · Direção da Hineh

Próxima revisão: até 10/10/2027 ou antes, em caso de mudança relevante.

Edição pública: 10/10/2026

[Consultar a versão no site da Hineh](#)

Esta política informa como a Hineh Tecnologia Ltda trata dados pessoais em seus produtos e serviços, incluindo projetos de transcrição de áudio, processamento de imagens e integração com serviços externos, e em suas relações comerciais. Dirige-se aos titulares dos dados e aos clientes que contratam a Hineh.

Quando um produto possui aviso de privacidade próprio, esse aviso detalha as regras daquele produto e complementa esta política. Prazos de retenção mais curtos previstos no aviso específico ou no contrato de um serviço prevalecem e não são ampliados pelos prazos desta política. A execução destas regras segue os Procedimentos de proteção de dados e terceiros, e as medidas de segurança estão na Política de segurança da informação.

1 Quem somos e como falar conosco

A Hineh desenvolve software e serviços de inteligência artificial. O canal de privacidade da Hineh é privacidade@hineh.com.br e atende aos produtos e serviços da Hineh, inclusive aos que possuem aviso de privacidade próprio. Por esse endereço, titulares, clientes e outras pessoas podem enviar dúvidas, solicitações de direitos e relatos de incidentes ou vulnerabilidades.

As atribuições de encarregado pelo tratamento de dados pessoais são exercidas pela função de privacidade da Hineh, pelo mesmo endereço. Essa função coordena o atendimento aos titulares, os registros de tratamento e a avaliação de fornecedores.

2 Papéis da Hineh

A Hineh atua como controladora quando define as finalidades e os meios essenciais do tratamento, como no cadastro, na cobrança, no relacionamento com clientes e usuários e na segurança de seus próprios serviços.

A Hineh atua como operadora quando processa dados em nome de um cliente, segundo suas instruções documentadas, como nos projetos personalizados. Nesses casos, o cliente, como controlador, define a finalidade, a hipótese legal e a relação com os titulares, e os papéis e as obrigações de cada parte devem constar do contrato. A existência de uma conta na plataforma não transfere à Hineh a decisão sobre o uso dos dados de terceiros incluídos pelo cliente.

O papel da Hineh deve ser identificado por atividade, e um mesmo serviço pode envolver os dois papéis.

3 Dados tratados e finalidades

Devem ser tratados apenas os dados necessários à finalidade de cada serviço. Nos projetos personalizados, devem ser tratadas somente as categorias de dados previstas no contrato e nas instruções documentadas do cliente. Antes de iniciar um tratamento ou alterar materialmente seu escopo, a Hineh deve registrar a finalidade, as categorias de dados e de titulares, a origem, os sistemas, os destinatários, os países de tratamento e os prazos de retenção.

Cadastro e relacionamento

Para cadastro, contratação, suporte, cobrança e segurança dos serviços, a Hineh trata dados de identificação e contato, informações da conta e os registros necessários à operação. Dados de cartão de pagamento são tratados pelos provedores de pagamento, conforme o fluxo de cada serviço.

Transcrição de áudio

Nos serviços de transcrição de áudio, são tratados o conteúdo que o usuário decide gravar, enviar ou conectar, como áudio, transcrições, notas e documentos, e os dados da conta associada. As gravações realizadas pela aplicação dependem de ação do usuário.

Integrações com serviços externos

As integrações com serviços externos devem respeitar as permissões concedidas pelo titular da conta e os acessos autorizados no serviço de origem, e o conteúdo obtido deve ser usado somente nas funcionalidades habilitadas pelo usuário. A desconexão deve impedir novas consultas e iniciar a revogação ou a eliminação das credenciais mantidas pela Hineh.

Quando o usuário autoriza um aplicativo de terceiro a consultar seus dados na Hineh, os dados consultados passam a ser tratados também por esse terceiro, conforme os termos dele. A revogação impede novas consultas, mas não apaga os dados já recebidos pelo terceiro. Da mesma forma, a exclusão na Hineh não altera os arquivos originais mantidos em serviços integrados.

Processamento de imagens

Nos projetos de processamento de imagens, são tratados os dados e as imagens previstos na especificação do projeto, além dos resultados produzidos. A coleta deve priorizar fotografias dos objetos e locais necessários à análise. Nomes, rostos, documentos e outros identificadores que não sejam necessários devem ser evitados na coleta ou removidos antes do envio a fornecedores. Não se deve acrescentar reconhecimento facial, identificação biométrica ou avaliação de pessoas sem nova definição de escopo e análise de proteção de dados.

Dados sensíveis e dados de crianças e adolescentes

Dados pessoais sensíveis, dados de crianças e adolescentes e atividades que possam produzir risco elevado exigem avaliação específica antes do início do tratamento. Clientes devem evitar o envio desse conteúdo quando ele não for necessário. Se houver recebimento incidental, o conteúdo deve ser restringido, avaliado e eliminado ou tratado conforme instrução do controlador e hipótese legal apropriada.

4 Hipóteses legais e limites de uso

Quando atua como controladora, a Hineh deve associar cada finalidade a uma hipótese legal pertinente, como a execução de contrato e de procedimentos relacionados ao serviço, o cumprimento de obrigação legal, o exercício regular de direitos, o legítimo interesse precedido de avaliação ou o consentimento, quando exigido. O consentimento não deve ser usado como justificativa genérica para toda a operação. O fundamento legal de cada tratamento deve constar de seu registro e, quando houver, do aviso específico do produto.

Quando atua como operadora, a hipótese legal é definida pelo cliente controlador.

Quando a Hineh atua como operadora, o conteúdo de clientes deve ser usado somente conforme as instruções documentadas do cliente. Em qualquer papel, o conteúdo de clientes não deve ser utilizado pela Hineh para publicidade, comercialização de dados ou treinamento de modelos de uso geral. O envio a serviços de inteligência artificial deve se limitar ao conteúdo necessário à tarefa, com avaliação das condições de uso, retenção e eventual treinamento do fornecedor. O acesso humano ao conteúdo deve ser restrito às situações justificadas de suporte, segurança, cumprimento de obrigação legal ou atendimento de direitos, com autorização compatível com a atividade.

Mudanças de finalidade, novas categorias de dados e novos destinatários devem passar por avaliação e instrução documentada antes do uso.

5 Compartilhamento com fornecedores e terceiros

A Hineh utiliza fornecedores conforme cada serviço, em categorias como provedor de nuvem, banco de dados gerenciado, provedor de inteligência artificial, envio de mensagens por e-mail, suporte e meios de pagamento. Os fornecedores de cada produto devem ser indicados em seu aviso específico, e os de cada projeto personalizado, na relação entregue ao cliente nos termos contratuais.

O inventário de terceiros deve conter somente os fornecedores efetivamente envolvidos em cada serviço. A utilização de um fornecedor em um serviço não autoriza seu acesso aos dados de outro serviço ou projeto.

Antes de permitir que um fornecedor acesse ou processe dados pessoais, a Hineh deve avaliar a finalidade, a necessidade do compartilhamento, as categorias de dados, a localização, as medidas de segurança, a subcontratação, a retenção, a eliminação, a resposta a incidentes e o apoio ao exercício de direitos. Os contratos devem delimitar finalidade e instruções, confidencialidade e segurança, subcontratação, assistência aos titulares e ao controlador, comunicação de incidentes, transferência internacional e devolução ou eliminação ao término do serviço. Fornecedores que tratem dados pessoais devem ser reavaliados ao menos anualmente e sempre que ocorrer mudança relevante, incidente ou alteração de condições contratuais.

Quando a Hineh atua como operadora, a utilização e a substituição de suboperadores devem respeitar a autorização e as condições acordadas com o cliente.

Dados pessoais também podem ser compartilhados com autoridades públicas quando houver obrigação legal ou determinação de autoridade competente.

6 Transferência internacional

Parte dos dados tratados pela Hineh é armazenada ou processada por fornecedores fora do Brasil, inclusive nos Estados Unidos.

O armazenamento ou o acesso a dados pessoais a partir de outro país deve ser identificado no inventário, inclusive quando realizado por fornecedores e suboperadores. Antes da transferência, a função de privacidade deve verificar o fundamento aplicável e a adoção de um mecanismo admitido pela LGPD e pela regulamentação da Autoridade Nacional de Proteção de Dados, como cláusulas contratuais padrão brasileiras, quando cabíveis. Cláusulas de outra jurisdição não devem ser consideradas automaticamente suficientes para atender às exigências brasileiras.

Quando a Hineh atua como operadora, a transferência deve observar também as condições acordadas com o cliente.

7 Retenção e eliminação

Os prazos de retenção devem ser associados a cada categoria de dados e ao evento que inicia sua contagem. O encerramento da finalidade, a expiração do prazo ou uma solicitação válida de eliminação deve iniciar o descarte, ressalvadas as hipóteses legais de conservação. A retenção não pode ser ampliada apenas porque a manutenção dos dados é tecnicamente possível. Os prazos abaixo são os limites gerais por categoria de serviço.

Transcrição de áudio

O áudio enviado para transcrição deve ser eliminado após o processamento. Quando o usuário escolher expressamente o envio de um arquivo para inspeção de suporte, a cópia deve permanecer privada, restrita à investigação e por até 14 dias. Logs de diagnóstico técnico devem ter retenção de até 14 dias. Transcrições, notas e dados associados à conta podem permanecer durante sua utilização, e a exclusão da conta deve concluir a eliminação desses dados nos sistemas ativos em até 15 dias, observadas as exceções legais.

Integrações com serviços externos

Credenciais de integrações devem ser removidas ou invalidadas quando houver desconexão. Índices e informações derivadas das integrações só devem permanecer enquanto necessários ao serviço autorizado, e a exclusão da conta deve concluir a eliminação desses dados nos sistemas ativos em até 15 dias, observadas as exceções legais.

Processamento de imagens

Nos projetos em que o cliente mantém as imagens em seu próprio ambiente e autoriza seu processamento pela Hineh, as cópias temporárias devem ser eliminadas após a conclusão da tarefa. Em caso de falha, a permanência para reproprocessamento deve ser limitada a 24 horas a partir da criação da cópia. Imagens brutas temporárias devem ser excluídas das cópias de segurança.

Resultados e metadados necessários à prestação do serviço podem permanecer durante o contrato e por até 30 dias após seu encerramento, para devolução e conclusão da eliminação. Logs técnicos devem ter retenção de até 14 dias, e registros de acesso e auditoria, de até 180 dias, ressalvadas obrigações legais de guarda. As cópias de segurança desse perfil de projeto devem

expirar em até 35 dias de sua criação, prazo que pode terminar após a exclusão dos sistemas ativos.

Campanhas e registros operacionais

Identificadores pseudonimizados de campanhas podem ser conservados por até 180 dias. Registros operacionais pseudonimizados estritamente necessários à segurança e à integridade podem permanecer por até 24 meses. Esses prazos não autorizam a conservação de conteúdo eliminado nem ampliam os limites específicos de retenção de cada serviço.

Cópias de segurança, fornecedores e exceções

Durante o ciclo de expiração das cópias de segurança, dados eliminados dos sistemas ativos devem permanecer inacessíveis ao uso cotidiano. Se houver restauração, as exclusões pendentes devem ser reaplicadas antes da liberação do ambiente.

Os prazos desta seção referem-se às cópias mantidas pela Hineh. Fornecedores podem manter registros próprios conforme seus termos, e essa retenção deve ser considerada na avaliação prevista na seção 5.

A conservação por obrigação legal, determinação de autoridade ou exercício regular de direitos deve ter fundamento, escopo, responsável e prazo de revisão registrados, com acesso restrito, e os dados devem ser eliminados ao término da necessidade.

No encerramento de um projeto personalizado, os dados devem ser devolvidos ao cliente, quando cabível, por canal seguro e em até 30 dias, salvo prazo mais curto contratado, e eliminados nos prazos desta seção. A confirmação de encerramento deve distinguir a eliminação concluída daquela ainda sujeita à expiração de cópias de segurança ou à confirmação de fornecedores.

8 Direitos dos titulares

O titular pode solicitar confirmação da existência de tratamento e acesso aos dados, correção, informações sobre compartilhamento e, quando cabível, portabilidade, anonimização, bloqueio, eliminação, oposição, revogação do consentimento e revisão de decisões automatizadas que afetem seus interesses.

As solicitações podem ser enviadas a privacidade@hineh.com.br, e o atendimento não deve impor cobrança ao titular. A confirmação de identidade deve ser proporcional ao risco e utilizar, sempre que possível, a conta autenticada ou um canal já associado ao titular. Documentos adicionais não devem ser solicitados sem necessidade.

Quando a Hineh atuar como controladora, a confirmação e o acesso devem ser fornecidos de forma simplificada imediatamente ou por declaração completa em até 15 dias, nos termos da LGPD. As demais solicitações devem receber tratamento nos prazos legais aplicáveis, com informação clara ao titular sobre a medida adotada, eventuais impedimentos e sua justificativa.

Quando atuar como operadora, a Hineh deve encaminhar a solicitação ao controlador sem demora injustificada e prestar a assistência necessária à resposta, sem decidir por conta própria sobre dados que o cliente controla.

O titular também pode peticionar à Autoridade Nacional de Proteção de Dados e aos órgãos competentes.

9 Segurança

A Política de segurança da informação estabelece as medidas de proteção aplicáveis aos produtos e serviços da Hineh, incluindo acesso mínimo e nominal, autenticação multifator, criptografia em trânsito e em repouso, separação entre os ambientes de produção e de desenvolvimento, registros de acesso e tratamento de incidentes. A aplicação concreta varia por serviço e pode ser detalhada no contrato de cada projeto. Nenhuma medida de segurança constitui garantia absoluta de invulnerabilidade.

10 Incidentes com dados pessoais

Suspeitas de incidente podem ser relatadas a privacidade@hineh.com.br e devem ser tratadas conforme o Plano de resposta a incidentes da Hineh.

Quando a Hineh atua como operadora, deve comunicar ao cliente controlador, sem demora injustificada, o incidente que envolva ou possa afetar dados tratados em seu nome, no prazo contratado ou, na ausência de prazo específico, em até 24 horas da ciência. A comunicação à Autoridade Nacional de Proteção de Dados e aos titulares é atribuição do controlador.

Quando a Hineh atua como controladora e o incidente pode acarretar risco ou dano relevante aos titulares, a Hineh deve comunicá-lo à Autoridade Nacional de Proteção de Dados e aos titulares afetados em até três dias úteis da ciência de que o incidente afetou dados pessoais. A comunicação aos titulares deve usar linguagem simples e ser feita de forma direta e individual sempre que possível.

11 Revisão desta política

A direção deve revisar esta política ao menos anualmente e quando houver alteração relevante de serviço, finalidade, fornecedor ou obrigação aplicável. Cada versão deve indicar o responsável, a data de aprovação e a próxima revisão, e as alterações devem ser refletidas nos avisos específicos e nos contratos pertinentes.

Esta política observa a Lei nº 13.709/2018, especialmente as hipóteses legais de tratamento, os direitos dos titulares, a transferência internacional e a segurança dos dados, a Resolução CD/ANPD nº 15/2024, sobre comunicação de incidentes, e a Resolução CD/ANPD nº 19/2024, sobre transferência internacional de dados.