

Procedimentos de proteção de dados e terceiros

Hineh Tecnologia Ltda · CNPJ 69.280.849/0001-62

Versão 1.1 · 8 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](#)

Estes procedimentos estabelecem como a Hineh autoriza o tratamento de dados pessoais, atende solicitações, controla a retenção e o descarte de informações e avalia fornecedores. Aplicam-se aos produtos e serviços da Hineh, incluindo projetos de transcrição de áudio, processamento de imagens e integração com serviços externos, assim como aos sócios, profissionais e terceiros que tenham acesso a essas informações.

O canal de privacidade da Hineh é privacidade@hineh.com.br. As regras específicas de cada serviço devem constar de seu aviso de privacidade e, quando aplicável, do contrato de tratamento de dados. A execução de um projeto deve respeitar essas regras e as instruções documentadas do cliente, observada a legislação aplicável.

1 Inventário e autorização de tratamento

Papéis e responsabilidades

A Hineh atua como controladora quando define as finalidades e os meios essenciais do tratamento, como na administração de suas relações comerciais e no atendimento aos usuários. Atua como operadora quando processa conteúdo em nome de um cliente e segundo suas instruções. O papel deve ser identificado por atividade; a existência de uma conta na plataforma não transfere à Hineh a decisão sobre o uso dos dados de terceiros incluídos pelo cliente.

A direção responde pela adoção destes procedimentos. A função de privacidade coordena solicitações de titulares, registros e avaliação de terceiros. O responsável técnico executa os controles de acesso, retenção e eliminação. Essas funções podem ser exercidas pela mesma pessoa em uma equipe pequena, com registro das decisões e dos responsáveis por sua execução.

Registro antes do uso dos dados

Antes de iniciar um tratamento ou alterar materialmente seu escopo, o responsável pelo serviço deve registrar a finalidade, as categorias de dados e titulares, a origem, os sistemas envolvidos, os destinatários, os países de tratamento, as permissões de acesso e os prazos de retenção e eliminação. O registro deve identificar o controlador, os operadores e o fundamento legal aplicável. Quando atuar como operadora, a Hineh deve obter e registrar as instruções e os limites definidos pelo cliente.

Devem ser tratados apenas os dados necessários à finalidade autorizada. Dados sensíveis, informações de crianças e adolescentes ou atividades que possam produzir risco elevado exigem

avaliação específica antes do início do tratamento. A mudança de finalidade, a inclusão de novas categorias de dados ou a contratação de um novo destinatário exige revisão do registro e das autorizações aplicáveis.

Conteúdo e integrações

Nos serviços de transcrição de áudio, gravações realizadas pela aplicação dependem de ação do usuário. Integrações com serviços externos devem respeitar as permissões concedidas pelo titular da conta e os acessos autorizados no serviço de origem. A desconexão deve impedir novas consultas e iniciar a revogação ou eliminação das credenciais mantidas pela Hineh.

Projetos de classificação de imagens devem 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.

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.

2 Atendimento a titulares e clientes

Solicitações de confirmação de tratamento, acesso, correção, portabilidade, informação sobre compartilhamentos, oposição, revogação de consentimento ou eliminação podem ser encaminhadas a privacidade@hineh.com.br. O atendimento não deve impor cobrança ao titular.

A função de privacidade deve registrar a data de recebimento, a solicitação, o serviço envolvido, as verificações de identidade estritamente necessárias e a providência adotada. 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. A entrega de conteúdo ou sua eliminação deve respeitar as instruções do controlador e os direitos de outras pessoas. O registro do atendimento deve conter a decisão, a execução e a resposta enviada, preservando apenas as informações necessárias à comprovação.

3 Retenção e eliminação

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

Projetos de 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, sem reutilização para outras finalidades. Logs de diagnóstico técnico devem ter retenção de até 14 dias e conter o mínimo necessário para investigar falhas.

Transcrições, notas e dados associados à conta podem permanecer durante sua utilização. 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. A exclusão da conta deve concluir a eliminação desses dados nos sistemas ativos em até 15 dias, observadas as exceções legais.

Projetos de processamento de imagens

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

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; registros de acesso e auditoria, de até 180 dias, ressalvadas obrigações legais de guarda. Esses registros devem evitar imagens, conteúdo integral de requisições e credenciais.

As cópias de segurança desse perfil de projeto devem expirar em até 35 dias de sua criação. O prazo de 35 dias se aplica a cada cópia e pode terminar após a exclusão dos sistemas ativos. O cronograma de encerramento deve informar a data limite para a expiração da última cópia que ainda contenha os dados.

Registros de campanhas e operação

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. Dados pseudonimizados continuam sujeitos às regras de proteção de dados quando puderem ser relacionados a uma pessoa.

Execução e exceções

A eliminação deve abranger bancos de dados, objetos armazenados, arquivos temporários, filas, índices e demais cópias sob responsabilidade da Hineh, conforme o escopo de cada operação. O responsável técnico deve aplicar os mecanismos adequados a cada sistema, registrar falhas e concluir as correções necessárias. A evidência de eliminação deve identificar o escopo e o resultado, sem reproduzir o conteúdo descartado.

Em todos os serviços, os prazos máximos e o ciclo de expiração de backups devem constar do inventário e das condições aplicáveis ao serviço. Durante esse ciclo, 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. Prazos mais curtos estabelecidos no aviso de privacidade ou no contrato de um serviço devem ser respeitados e não são ampliados pelos prazos previstos para outras categorias de projeto.

A conservação por obrigação legal, determinação de autoridade ou exercício regular de direitos deve ter fundamento, escopo, responsável e prazo de revisão registrados. Os dados devem permanecer separados do uso ordinário, com acesso restrito, e ser eliminados ao término da necessidade. Anonimização só substitui a eliminação quando não for razoavelmente possível reidentificar os titulares.

4 Encerramento e devolução de dados

O encerramento de contrato, conta, integração ou autorização de acesso deve produzir um registro de execução proporcional ao escopo, com as seguintes etapas:

1. Identificar o solicitante autorizado, os sistemas, dados, fornecedores e acessos abrangidos, além da data efetiva do encerramento.
2. Interromper novas coletas e processamentos quando cessar a autorização. Revogar acessos, sessões e credenciais que deixem de ser necessários. No desligamento de um profissional, a revogação deve ocorrer imediatamente após a comunicação, independentemente da conclusão da devolução de dados.
3. Quando cabível, devolver os dados ao cliente por canal seguro, em formato estruturado e usual, após confirmar o destinatário e a autorização. Nos projetos personalizados, a devolução deve ocorrer em até 30 dias do encerramento, salvo prazo mais curto contratado. Ela não deve ampliar o prazo de eliminação aplicável ao serviço.
4. Eliminar os dados nos sistemas ativos nos prazos da seção 3, acionar os fornecedores envolvidos e registrar a expiração prevista dos backups e as exceções legais.

5. Entregar ao cliente, quando solicitado, confirmação do escopo concluído, das datas e de eventual retenção residual justificada, com sua data limite ou condição de término.

A Hineh deve distinguir a eliminação concluída daquela ainda sujeita à expiração de backups ou à confirmação de fornecedores. A declaração de encerramento não pode afirmar eliminação integral enquanto houver cópias conhecidas cuja retenção ainda esteja em curso.

A exclusão na Hineh não altera automaticamente os arquivos originais mantidos pelo cliente ou em serviços integrados. Cópias que o próprio cliente tenha exportado ou compartilhado permanecem sob sua gestão. A Hineh deve explicar esses limites e prestar a assistência cabível.

5 Avaliação e contratação de terceiros

Antes de permitir que um fornecedor acesse ou processe dados pessoais, o responsável pelo serviço e a função de privacidade devem avaliar a finalidade, a necessidade do compartilhamento, as categorias de dados, a criticidade e as condições de tratamento. A avaliação deve considerar segurança, confidencialidade, controle de acesso, localização dos dados, subcontratação, retenção, eliminação, resposta a incidentes e apoio ao exercício de direitos.

A documentação pode incluir termos de tratamento de dados, informações técnicas, relatórios de auditoria e certificações pertinentes ao serviço contratado. A existência de certificação, isoladamente, não dispensa a análise do tratamento específico. O resultado deve registrar a decisão, as restrições, os responsáveis e a próxima revisão. Lacunas relevantes devem ser resolvidas ou ter medidas compensatórias documentadas antes do início do compartilhamento.

Os instrumentos contratuais devem delimitar finalidade e instruções, obrigações de confidencialidade e segurança, condições para subcontratação, assistência a titulares e ao controlador, comunicação de incidentes, transferência internacional e devolução ou eliminação ao término do serviço. Quando a Hineh atuar como operadora, a utilização e a substituição de suboperadores devem respeitar a autorização e as condições acordadas com o cliente.

O inventário de terceiros deve conter somente os fornecedores efetivamente envolvidos em cada serviço. A utilização de um fornecedor em um projeto não autoriza seu acesso aos dados de outros projetos. O acesso deve se limitar aos dados necessários à atividade contratada, por contas e credenciais com escopo compatível.

Fornecedores que tratem dados pessoais ou sustentem atividades críticas devem ser reavaliados ao menos anualmente e sempre que ocorrer mudança relevante, incidente ou alteração de condições contratuais. O encerramento da relação deve incluir revogação de acessos, devolução ou eliminação e registro das confirmações recebidas.

6 Transferências e prestação de contas

O armazenamento ou 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 ANPD, como cláusulas contratuais padrão brasileiras, quando cabíveis. Cláusulas de outra jurisdição não devem ser consideradas automaticamente suficientes para atender às exigências brasileiras.

Suspeitas de acesso indevido, perda ou divulgação não autorizada devem ser encaminhadas ao responsável por incidentes. A função de privacidade deve participar da avaliação dos titulares e clientes afetados e das comunicações exigíveis. Quando atuar como operadora, a Hineh deve informar o controlador sem demora injustificada e fornecer elementos para sua avaliação, observados os prazos contratuais e legais.

Os registros de tratamento, solicitações, avaliações de terceiros e encerramento devem permitir identificar quem decidiu, o que foi executado, quando e com qual resultado. A evidência deve ser proporcional à atividade e protegida por acesso restrito. Uma política ou um procedimento formaliza uma regra; sua execução deve ser demonstrada pelos registros pertinentes quando necessário.

A direção deve revisar estes procedimentos ao menos anualmente e quando houver mudança relevante nos serviços, nos riscos ou nas obrigações aplicáveis. Alterações devem receber versão e data, ser comunicadas às pessoas responsáveis por sua execução e refletidas nos avisos e contratos pertinentes.

Estes procedimentos observam a Lei nº 13.709/2018, especialmente os direitos dos titulares, as hipóteses de conservação e as regras para tratamento por operadores, e a Resolução CD/ANPD nº 19/2024 sobre transferência internacional de dados.