

PRIVACIDADE EM CADA RELAÇÃO

POLÍTICA DE PRIVACIDADE

GENTTRA | Pessoas, cultura e liderança

Versão 1.0 · Elaborada em 05 de outubro de 2026

Mover carreiras e empresas exige cuidar das informações que as pessoas confiam à GENTTRA. Esta Política explica quais dados podem ser tratados, para quais finalidades, com quem podem ser compartilhados e como exercer seus direitos.

1. Quem somos e quando esta Política se aplica

A **Genttra Consultoria e Serviços de RH Ltda**, CNPJ **YZ.A36.018/0001-98**, é a empresa responsável pelas operações descritas nesta Política, conforme o papel exercido em cada atividade. Atua em consultoria e serviços de RH, desenvolvimento de pessoas, cultura e liderança. A Política abrange visitantes, candidatos, colaboradores, representantes de clientes, fornecedores, parceiros e usuários dos canais.

Seu alcance inclui o site institucional, Carreiras/Talentos, Área do Cliente, Contratos, Academy, GED, Helpdesk, Linha Ética, Gestão de Qualidade (Qualiz) e Nexo ERP, bem como contatos, documentos físicos e atividades presenciais relacionadas aos serviços. Avisos específicos podem detalhar determinada operação.

2. Nosso papel no tratamento

Nas operações em que decide os objetivos e a forma de uso dos dados, a GENTTRA atua como **controladora**. Nos serviços em que trata dados por instrução documentada de um cliente, atua como **operadora**. O papel depende da atividade e do contrato; um mesmo projeto pode reunir operações com papéis distintos.

Quando um cliente é o controlador, suas orientações e seu aviso de privacidade também devem ser considerados. A GENTTRA auxilia o atendimento de solicitações relativas aos dados sob sua responsabilidade e informa o encaminhamento necessário.

Canal de privacidade: dpo@genttra.com.brSite institucional: genttra.com.br

DADOS E CANAIS DE COLETA

Dados e canais de coleta

3. Quais dados podem ser tratados

As informações variam conforme sua relação com a GENTTRA e o serviço utilizado. Solicitamos apenas os dados pertinentes à atividade. Informações relativas a empresas também são dados pessoais quando permitem identificar uma pessoa física.

Contexto	Dados e uso relacionado
Contato e relacionamento	Nome, e-mail, telefone/WhatsApp, empresa, cargo, solução de interesse e mensagem, para responder contatos e preparar propostas.
Carreiras e recrutamento	Nome, contato, cidade/UF, currículo, formação, experiências, qualificações, candidatura, entrevistas e registros de etapas. Foto, quando disponibilizada, não substitui critérios profissionais.
Colaboradores e usuários	Identificação, matrícula, nascimento, admissão, cargo, departamento, centro de custo, unidade, foto de perfil e dados necessários à relação de trabalho ou ao acesso aos sistemas.
Academy e desenvolvimento	Inscrições, participação, progresso, avaliações, resultados de aprendizagem e certificados. Projetos de desempenho, PDI e liderança podem usar informações profissionais pertinentes.
Clientes, contratos e GED	Dados de representantes, contatos, documentos contratuais, assinaturas, arquivos, registros de acesso e documentos necessários à execução e comprovação de serviços.
Faturas e Nexo ERP	Dados cadastrais, fiscais e bancários quando necessários, faturas, situação de pagamento, compras, ordens, despesas, reembolsos, comprovantes, aprovadores e histórico de movimentações.
Helpdesk e Qualiz	Perfil do solicitante, descrição, anexos, respostas, ocorrências, responsáveis, prazos e providências adotadas.
Linha Ética e ouvidoria	Relato, vínculo informado, protocolo, anexos e informações de envolvidos. Nome e contato, quando o relato for identificado, além de registros necessários à apuração.
Navegação e segurança	Dados técnicos que podem ser gerados pelo serviço, como IP, dispositivo, navegador, sessão, data/hora, tentativas de acesso e registros de atividade.

Não inclua senhas, documentos completos ou dados de terceiros em campos livres e anexos quando essas informações não forem necessárias. Dados de saúde e outros dados sensíveis merecem cuidado adicional.

FINALIDADES E FUNDAMENTO LEGAL

Finalidades e fundamento legal

4. De onde vêm as informações

Os dados podem ser fornecidos por você em formulários, contas, mensagens, currículos, entrevistas e arquivos; por clientes e empregadores em projetos contratados; por pessoas autorizadas, fornecedores ou referências profissionais; e pelos próprios sistemas durante sua utilização. Fontes públicas não autorizam uso indiscriminado: finalidade, contexto e direitos do titular continuam sendo considerados.

5. Para que utilizamos dados e em qual hipótese legal

Cada operação deve ter uma hipótese legal compatível com sua finalidade. A leitura desta Política ou o simples uso de um site não representam consentimento geral para qualquer tratamento.

Atividade	Finalidade e hipóteses legais possíveis
Contatos e serviços	Responder pedidos, negociar e executar serviços: procedimentos preliminares solicitados pelo titular ou execução de contrato. Relações com representantes de empresas podem exigir avaliação de legítimo interesse.
Recrutamento	Conduzir a candidatura e comunicar etapas: procedimentos preliminares relacionados a possível contratação, conforme o contexto. Banco de talentos e outras utilizações exigem finalidade própria e base avaliada separadamente.
Trabalho e obrigações	Administrar vínculos, documentos, treinamentos obrigatórios e registros fiscais: cumprimento de obrigação legal/regulatória e execução de contrato, quando aplicáveis.
Gestão e proteção	Administrar acessos, atendimento, qualidade, pagamentos e prevenir fraude: execução de contrato, obrigação legal, exercício regular de direitos ou legítimo interesse, conforme a operação.
Comunicação e análises	Comunicações opcionais e análises adicionais: consentimento quando necessário ou outra hipótese devidamente avaliada. O legítimo interesse exige necessidade, transparência e ponderação dos direitos do titular.

Dados sensíveis recebem avaliação específica das hipóteses do art. 11 da LGPD. Legítimo interesse não é fundamento para tratar dados sensíveis. Quando o consentimento for a hipótese adequada, ele deve ser específico, demonstrável e, para dados sensíveis, destacado.

Participar de uma seleção não garante contratação. A candidatura não autoriza, por si só, divulgação pública do currículo nem sua utilização irrestrita em outras oportunidades.

COMPARTILHAMENTO E AMBIENTE DIGITAL

Compartilhamento e ambiente digital

6. Com quem dados podem ser compartilhados

O compartilhamento deve se limitar à finalidade e aos dados necessários: equipes autorizadas da GENTTRA; clientes vinculados ao processo seletivo ou ao serviço; fornecedores de hospedagem, armazenamento, autenticação, comunicação e suporte; profissionais contábeis, jurídicos e de auditoria; instituições financeiras e provedores de cobrança; e autoridades, quando houver fundamento legal.

Na Área do Cliente há integração de cobranças com o **Asaas**. Dados cadastrais e de faturamento necessários à emissão, acompanhamento e conciliação de cobranças podem ser enviados ao provedor. O tratamento realizado por ele segue seu papel contratual e seu próprio aviso de privacidade. A GENTTRA não solicita o envio de senha bancária por formulários ou chamados.

Em seleções para clientes, o compartilhamento de currículo e avaliações deve estar ligado à oportunidade e ao destinatário informado. Anexos de chamados, contratos, comprovantes e relatos não devem circular além das pessoas autorizadas. A GENTTRA não autoriza comercialização de bases de candidatos ou colaboradores.

7. Serviços em outros países

Fornecedores de tecnologia podem armazenar dados ou permitir seu acesso fora do Brasil. Quando houver transferência internacional, a operação deve ser identificada e sustentada por mecanismo válido previsto na LGPD e nas regras da ANPD, como cláusulas-padrão contratuais quando cabíveis. O mecanismo, os destinatários e as informações aplicáveis podem ser solicitados pelo canal de privacidade.

8. Cookies, sessões e tecnologias semelhantes

Os portais podem utilizar cookies, armazenamento local e identificadores necessários para manter sessões, lembrar preferências, proteger acessos e permitir funcionalidades. Recusar ou apagar recursos estritamente necessários pode afetar o funcionamento do serviço.

Recursos opcionais de publicidade, análise ou rastreamento devem ter finalidade, fornecedor e duração informados no respectivo canal. Quando exigível, sua ativação dependerá de escolha válida do titular, com meio de revisar a preferência. O fato de esta Política mencionar essas tecnologias não confirma que todas estejam instaladas em cada site.

Links e integrações com redes sociais, WhatsApp ou outros serviços levam a ambientes com práticas próprias. Verifique o aviso do serviço de destino antes de fornecer informações adicionais.

CUIDADOS COM PESSOAS E CONSERVAÇÃO

Cuidados com pessoas e conservação

9. Dados sensíveis, crianças e adolescentes

Dados de saúde, origem racial ou étnica, religião, opinião política, filiação sindical, vida sexual, genética e biometria vinculada a uma pessoa exigem proteção reforçada. Em RH e saúde e segurança do trabalho, a coleta deve ficar restrita às informações indispensáveis, com acesso compatível com a responsabilidade de cada profissional.

As atividades não são destinadas a crianças de forma geral. Havendo tratamento de dados de crianças ou adolescentes, inclusive em aprendizagem profissional, a operação deve observar seu melhor interesse, a idade, a necessidade e as hipóteses legais aplicáveis. Para dados de crianças, deve ser obtido consentimento específico e destacado de pelo menos um responsável quando essa for a hipótese exigida, ressalvadas as exceções legais.

10. Confidencialidade da Linha Ética

A Linha Ética permite relatos anônimos ou identificados. Relatos, evidências e informações de envolvidos devem ser acessados somente por pessoas autorizadas para recebimento, análise e apuração. O relato não será publicado no site. A escolha pelo anonimato não impede que o conteúdo ou o próprio anexo revele a identidade do manifestante.

Não prometemos anonimato técnico absoluto: registros de segurança e metadados podem existir. A confidencialidade deve ser preservada, observadas necessidades de apuração, defesa de direitos e obrigações legais. A identidade do manifestante não deve ser divulgada indiscriminadamente aos envolvidos.

11. Por quanto tempo conservamos informações

A duração depende da finalidade, do vínculo e das obrigações legais. Cadastros e candidaturas devem ser revistos quando o processo terminar; documentos de trabalho, contratos e registros fiscais podem exigir conservação por prazos próprios; relatos e apurações podem exigir guarda para exercício de direitos. A existência de uma conta não justifica retenção ilimitada.

Encerrada a necessidade, os dados devem ser eliminados, bloqueados ou efetivamente anonimizados, conforme a situação. Obrigações legais, processos e outras hipóteses autorizadas podem impedir a exclusão imediata. Cópias de segurança devem seguir ciclos de substituição e restrição de uso. Prazos e critérios específicos podem ser consultados pelo canal de privacidade.

12. Avaliações e decisões automatizadas

Quando houver decisão tomada exclusivamente por tratamento automatizado que afete seus interesses, você pode pedir revisão e informações claras sobre critérios e procedimentos, resguardados os segredos comerciais e industriais. Esta Política não declara a existência de seleção automatizada em todos os serviços. A GENTTRA orienta avaliações profissionais por critérios pertinentes e não discriminatórios.

DIREITOS, SEGURANÇA E CONTATO

Direitos, segurança e contato

13. Seus direitos e como fazer uma solicitação

Você pode pedir confirmação e acesso; correção; anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados de forma irregular; portabilidade nos termos da regulamentação; eliminação dos dados tratados com consentimento, ressalvadas as hipóteses de conservação; informações sobre compartilhamento; informação sobre a possibilidade de não consentir e suas consequências; e revogação do consentimento. Pode também se opor ao tratamento sem consentimento em caso de descumprimento da LGPD e solicitar revisão de decisão exclusivamente automatizada.

Escreva para dpo@genttra.com.br, informe seu nome, o contexto do relacionamento e o pedido. A confirmação de identidade deve ser proporcional ao risco e realizada por meio seguro. Não envie documento completo de identificação sem necessidade. Representantes devem demonstrar poderes para agir em nome do titular.

O atendimento é gratuito. Confirmação e acesso podem ser fornecidos em formato simplificado imediatamente ou por declaração completa em até 15 dias, conforme o art. 19 da LGPD. Outros pedidos seguem os prazos legais aplicáveis. Se não pudermos atender de imediato, informaremos o motivo e, quando cabível, o controlador responsável. Você também pode procurar a ANPD e os órgãos de defesa do consumidor.

14. Segurança e incidentes

A proteção deve combinar acessos limitados por função, sigilo profissional, cuidados com arquivos e credenciais e medidas técnicas e administrativas proporcionais aos riscos. Esses compromissos orientam a operação e não constituem garantia de ausência de incidentes. Comunique perda, exposição indevida ou acesso suspeito ao canal de privacidade, sem encaminhar dados além do necessário.

Incidentes devem ser investigados e contidos. Quando um incidente puder causar risco ou dano relevante, o controlador deve comunicar à ANPD e aos titulares conforme os critérios, procedimentos e prazos legais aplicáveis.

15. Versões e informações complementares

A versão aprovada deve permanecer acessível nos canais da GENTTRA, com indicação da data de atualização. Mudanças relevantes de finalidade ou tratamento devem receber transparência adequada e nova avaliação de base legal. Avisos específicos complementam esta Política, sem reduzir direitos legais.

Fontes oficiais: [LGPD, Lei nº 13.709/2018 \(texto vigente\)](#); [ANPD: Regulamento de Comunicação de Incidentes; Resolução CD/ANPD nº 19/2024 \(transferências internacionais\)](#). Consulta: 05/10/2026.

Controle de publicação: documento elaborado para aprovação institucional. Razão social e CNPJ foram incluídos conforme informação fornecida pela empresa. Antes da divulgação oficial, a GENTTRA deve divulgar a identidade do encarregado e assegurar que os avisos de cada canal reflitam fornecedores, cookies e prazos efetivamente adotados.