

COMPROMISSO E GOVERNANÇA

POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

GENTTRA | Diretrizes de governança e tratamento
Versão 1.0 · Elaborada em 05 de outubro de 2026

1. Objetivo e abrangência

Esta Política estabelece regras para o tratamento de dados pessoais pela GENTTRA em consultoria e serviços de RH, recrutamento, desenvolvimento, gestão de colaboradores, relações comerciais e atividades administrativas. Deve ser observada pela direção, lideranças, colaboradores e demais pessoas que atuem em nome da empresa, conforme seu vínculo e suas responsabilidades.

Aplica-se a dados digitais e físicos e a todo o seu ciclo de vida, inclusive nos sites institucional e Carreiras/Talentos, Área do Cliente, Contratos, Academy, GED, Helpdesk, Linha Ética, Qualiz e Nexo ERP. Fornecedores e parceiros devem receber obrigações compatíveis com os serviços contratados.

2. Princípios e conceitos essenciais

As operações devem respeitar finalidade, adequação, necessidade, livre acesso, qualidade, transparência, segurança, prevenção, não discriminação e responsabilização. Cada equipe deve demonstrar por que coleta um dado, quem precisa acessá-lo e quando seu uso deve terminar.

Dado pessoal permite identificar uma pessoa direta ou indiretamente. **Dado sensível** exige as hipóteses e proteções específicas previstas na lei. **Controlador** decide finalidade e meios; **operador** trata por instrução do controlador. Dados pseudonimizados continuam pessoais quando a identificação puder ser recuperada. Anonimização exige avaliar o risco real de reidentificação.

3. Responsabilidade institucional

A empresa responsável é **Genttra Consultoria e Serviços de RH Ltda**, CNPJ **YZ.A36.018/0001-98**. A Direção deve aprovar esta Política, assegurar recursos e designar responsáveis pela execução. O canal **dpo@genttra.com.br** recebe questões de privacidade. A designação e a divulgação do encarregado devem atender à LGPD e à regulamentação; o endereço de e-mail não comprova, isoladamente, essa designação.

RESPONSÁVEIS E REGISTRO DAS OPERAÇÕES

Responsáveis e registro das operações

4. Atribuições de cada participante

Responsável	Deveres
Direção	Aprovar diretrizes, decidir riscos relevantes, garantir recursos e supervisionar prestação de contas. A responsabilidade do agente de tratamento não é transferida ao encarregado.
Encarregado	Receber comunicações de titulares e da ANPD, orientar equipes, apoiar inventário, contratos, riscos e incidentes. Deve ter recursos, acesso à direção e tratamento de conflitos de interesse.
Gestores de processos	Identificar dados e finalidades, revisar permissões, registrar bases e retenção, orientar a equipe e comunicar mudanças e incidentes.
Tecnologia e administradores	Executar controles de acesso, manutenção, registros, proteção de arquivos, continuidade e descarte técnico; fornecer evidências e apoiar a resposta a incidentes.
RH, Financeiro e áreas operacionais	Restringir documentos às atividades necessárias, conferir destinatários e manter registros, obrigações e canais sob sua gestão.
Colaboradores e terceiros	Usar dados apenas no trabalho autorizado, manter sigilo, concluir orientações e relatar riscos. Não copiar bases para contas pessoais ou ferramentas não aprovadas.

5. Inventário e definição dos papéis

Cada área deve manter registro de suas operações com: responsável; sistema; origem; categorias de dados e titulares; finalidade; base legal; papel da GENTTRA; destinatários e operadores; países envolvidos; retenção; controles; e procedimento para direitos e descarte. Projetos de clientes devem incluir instruções documentadas e limites de atuação.

A GENTTRA não deve reutilizar dados recebidos como operadora em campanhas próprias, outros clientes, banco de talentos independente ou treinamento de modelos sem nova análise jurídica, finalidade legítima e autorização contratual cabível. Decisões próprias podem caracterizar atuação como controladora, independentemente do nome dado no contrato.

6. Mudanças e proteção desde a concepção

Novos formulários, integrações, permissões, relatórios e automações devem passar por avaliação antes da ativação. Configurações iniciais devem reduzir exposição, campos e compartilhamentos. O inventário deve ser revisto quando houver mudança de finalidade, fornecedor, público, risco ou tecnologia.

BASES LEGAIS E PRÁTICAS DE RH

Bases legais e práticas de RH

7. Escolha da hipótese legal

A base legal deve ser definida e registrada antes do tratamento. A equipe deve avaliar contrato ou procedimentos preliminares, obrigação legal/regulatória, exercício regular de direitos, legítimo interesse, consentimento e demais hipóteses cabíveis, sem eleger uma única base para toda a empresa. Bases para dados sensíveis exigem análise do art. 11; legítimo interesse não se aplica a esses dados.

Consentimento deve ter finalidade delimitada, linguagem clara, prova da escolha e revogação acessível. Não pode estar embutido em aceite genérico, campo previamente marcado ou condicionado a atividade que dele não dependa. Em relações de trabalho, é necessário avaliar se a escolha é efetivamente livre.

O legítimo interesse exige registro de finalidade legítima, necessidade, expectativa do titular, ponderação de impactos e salvaguardas. A publicidade de um dado não dispensa essa avaliação. Os dados coletados devem ser compatíveis com a finalidade original e com os direitos do titular.

8. Recrutamento e banco de talentos

Solicitar informações relacionadas à vaga e informar a finalidade, os destinatários e a duração ou critério de conservação. Currículos, entrevistas, referências e avaliações devem ter acesso restrito à seleção correspondente. Foto, estado civil, religião, saúde e outras informações pessoais não devem servir a discriminação ou exclusão sem fundamento legítimo.

Verificação de referências e antecedentes exige pertinência, proporcionalidade e análise jurídica. Não coletar histórico irrestrito apenas por conveniência. Para manter currículo em banco de talentos após a seleção, estabelecer finalidade, base, prazo, transparência e possibilidade de exercício de direitos próprios.

9. Colaboradores, aprendizagem e dados sensíveis

Dados de admissão, matrícula, cargo, unidade, departamento, treinamentos e desempenho devem ser usados por pessoas autorizadas. Registros de saúde e segurança do trabalho precisam de acesso separado e limitado; gestores devem receber somente o necessário à sua função, sem exposição indiscriminada de diagnósticos.

Dados de crianças e adolescentes, inclusive aprendizes, exigem avaliação do melhor interesse e regras adequadas à idade. Deve-se documentar a hipótese legal e, quando necessário, a participação do responsável legal. A coleta não pode gerar exposição ou riscos desproporcionais.

10. People Analytics, avaliações e IA

Priorizar dados agregados e evitar grupos tão pequenos que revelem identidades. Não inserir currículos, relatos ou documentos internos em serviços de IA não autorizados. Ferramentas aprovadas exigem análise de finalidade, fornecedores, retenção, transferência e uso para treinamento. Avaliações devem permitir contestação e atender aos direitos sobre decisões exclusivamente automatizadas.

REGRAS PARA OS PORTAIS E DOCUMENTOS

Regras para os portais e documentos

11. Segregação de acesso por finalidade

Permissões devem ser individuais e concedidas pelo mínimo necessário, considerando empresa, setor, titular e processo. Um cargo de gestão não autoriza acesso irrestrito. A equipe técnica deve aplicar as restrições no servidor, inclusive em arquivos, exportações e endereços acessados diretamente.

Ambiente	Regra de proteção
Institucional / Carreiras	Formulários claros e campos necessários. Vagas públicas não tornam públicos currículos ou perfis. Usuários administrativos devem acessar somente setores e processos autorizados.
Área do Cliente / Contratos	Separar clientes e representantes. Documentos e faturas de um cliente não podem ser expostos a outro. Downloads e assinaturas exigem autorização compatível com o contrato.
GED	Restringir por setor, documento e finalidade. Links, visualizações e downloads devem respeitar o mesmo controle. Evitar links permanentes públicos para arquivos pessoais.
Academy	Progresso, avaliações e certificados devem ser acessados pelo participante e por responsáveis autorizados. Não publicar listas nominais de resultados sem justificativa.
Helpdesk	Solicitante acessa suas demandas; gestor, as atribuídas; administrador, o alcance necessário à administração. Anexos, respostas e avisos seguem a mesma restrição.
Linha Ética	Receber e apurar com sigilo reforçado. Separar identidade do manifestante quando possível. Impedir exposição dos relatos e verificar conflitos de interesse da equipe de apuração.
Qualiz	Compartilhar ocorrências e evidências somente com os responsáveis pela análise e ação. Reduzir dados pessoais em painéis gerenciais e relatórios de qualidade.
Nexo ERP	Dados de compras, despesas, bancos e comprovantes ficam limitados ao solicitante e aos responsáveis das etapas. Notificações, substituições de aprovadores e relatórios devem respeitar essa necessidade.

12. Arquivos, exportações e ambiente físico

Conferir destinatários e permissões antes de enviar documentos. Exportações e PDFs devem conter somente os dados necessários. Validar anexos, limitar formatos e proteger seu armazenamento. Documentos impressos devem ficar em local restrito, com retirada controlada e descarte seguro; não deixá-los expostos em mesas ou impressoras.

SEGURANÇA, FORNECEDORES E TRANSFERÊNCIAS

Segurança, fornecedores e transferências

13. Controles técnicos e administrativos

As medidas devem ser proporcionais ao risco e acompanhadas de evidências de execução: contas individuais; credenciais protegidas; autenticação adicional nos acessos de maior risco quando disponível; expiração de sessões; revogação de acesso no desligamento; revisões de privilégios; atualização de sistemas; proteção de tráfego e armazenamento conforme a arquitetura; registros de eventos; e testes de restauração de cópias de segurança.

Credenciais, tokens e segredos não podem aparecer em documentos, código público, mensagens ou relatórios. Ambientes de teste devem preferir dados fictícios ou anonimizados. Acesso de suporte precisa ser autorizado, temporário e rastreável. Logs não devem registrar senhas, dados sensíveis ou conteúdo completo sem necessidade.

Integrações entre portais devem transmitir apenas os campos previstos, validar autorização e impedir mistura entre clientes ou perfis. Segurança deve abranger o acesso direto às APIs e aos arquivos, não apenas os elementos visíveis da interface.

14. Contratação e acompanhamento de fornecedores

Antes da contratação, avaliar função do fornecedor, dados acessados, capacidade de segurança, subcontratação, países e descarte. Contratos devem definir instruções, confidencialidade, responsabilidades, auxílio aos titulares, comunicação rápida de incidentes, retenção, retorno ou eliminação, evidências e condições de subcontratação.

A integração com **Asaas** deve limitar o envio aos dados necessários às cobranças e à conciliação. A área responsável deve conferir o papel do provedor, suas condições e a informação aos titulares. O mesmo procedimento vale para hospedagem, autenticação, comunicação, armazenamento e novas integrações.

15. Transferência internacional

Inventariar armazenamento e acesso por equipes ou fornecedores no exterior, distinguir coleta direta de transferência e definir mecanismo válido para cada fluxo. Quando usadas cláusulas-padrão da ANPD, observar o conteúdo obrigatório, informações complementares e requisitos de transparência da Resolução nº 19/2024 e alterações.

Contratos genéricos, localização declarada de um servidor ou afirmação do fornecedor de que cumpre a LGPD não substituem a avaliação do mecanismo. Pedidos de informações e cópias de cláusulas devem ser atendidos conforme a regulamentação, protegidos os segredos legalmente resguardados.

16. Cookies e comunicações opcionais

Manter inventário por site com finalidade, fornecedor e duração das tecnologias. Distinguir recursos necessários de opcionais, viabilizar escolhas quando exigidas e registrar alterações. Cancelamentos de comunicações promocionais devem ser respeitados; avisos necessários ao serviço seguem a hipótese legal correspondente.

DIREITOS, CONSERVAÇÃO E ELIMINAÇÃO

Direitos, conservação e eliminação

17. Procedimento para solicitações de titulares

Pedidos recebidos por qualquer área devem ser encaminhados ao canal de privacidade e registrados com data, contexto e responsável. Confirmar a identidade por meio proporcional e seguro; localizar os dados em sistemas, documentos e operadores; avaliar o papel da GENTTRA; decidir a providência; responder de forma clara; e registrar as medidas realizadas.

O atendimento deve contemplar confirmação e acesso, correção, anonimização, bloqueio e eliminação cabíveis, portabilidade, informação sobre compartilhamento e consentimento, revogação, oposição nas hipóteses legais e revisão de decisões exclusivamente automatizadas. Atender também solicitações legítimas de representantes e responsáveis legais.

Confirmação e acesso: formato simplificado imediatamente ou declaração completa em até 15 dias, conforme o art. 19. Demais pedidos: observar os prazos próprios vigentes. Se a GENTTRA for operadora, auxiliar o controlador e encaminhar a solicitação com segurança. Negativas ou limitações devem indicar justificativa; os direitos de terceiros e a guarda legal precisam ser considerados.

18. Tabela de temporalidade

Cada processo deve ter prazo ou critério documentado com marco inicial, motivo, base de conservação e responsável. A tabela deve distinguir contatos e propostas; candidatos e banco de talentos; colaboradores e saúde ocupacional; treinamento; contratos e faturas; compras e reembolsos; chamados e ocorrências; relatos éticos; logs; e cópias de segurança.

A área jurídica ou profissional responsável deve validar os prazos associados às obrigações trabalhistas, fiscais, contratuais e à defesa de direitos. Não adotar prazo único nem retenção perpétua para todas as categorias. Revisar bases inativas, anexos e exportações que continuem guardados fora do sistema principal.

19. Descarte e bloqueio de uso

Ao encerrar a finalidade e inexistir hipótese legítima de conservação, eliminar de forma segura ou anonimizar de modo efetivo. Comunicar a providência a operadores e destinatários quando cabível. Registrar categoria, critério, data e responsável pelo descarte, sem criar uma nova cópia integral dos dados eliminados.

Dados preservados por obrigação ou litígio devem ter acesso restrito e uso limitado à justificativa de guarda. Backups seguem ciclo documentado de substituição; restaurações devem reaplicar eliminações e restrições. Retirar um registro da tela ou movê-lo para uma lixeira não comprova eliminação definitiva.

20. Transparência e prestação de contas

Manter avisos claros nos pontos de coleta e a Política de Privacidade aprovada acessível. Informação deve abranger finalidade, necessidade, compartilhamento e canal de direitos. Alterações relevantes não podem ficar ocultas em documentos internos ou somente no código dos sistemas.

RESPOSTA A INCIDENTES

Resposta a incidentes

21. Comunicação interna imediata

Quem identificar perda, acesso indevido, envio ao destinatário errado, publicação de arquivo, comprometimento de credencial ou outra suspeita deve informar imediatamente o canal **dpo@genttra.com.br** e os responsáveis internos de tecnologia e gestão. Não aguardar confirmação completa, não apagar evidências e não investigar por conta própria acessando dados adicionais.

22. Conter, apurar e avaliar

Etapa	Providência e evidência
Receber e registrar	Anotar ciência, origem, sistemas, pessoas responsáveis e ações iniciais. Abrir registro protegido; limitar o acesso à equipe de resposta.
Conter e preservar	Reduzir exposição, suspender acessos ou integrações afetadas, preservar registros e evidências com integridade. Documentar medidas e seus horários.
Analisar o impacto	Identificar dados, titulares, volume, duração, destinatários, consequências e salvaguardas. Avaliar dados sensíveis, menores, autenticação, finanças e outros fatores de risco relevante.
Decidir e comunicar	Controlador avalia dever de comunicar à ANPD e aos titulares. Encarregado e assessoria responsável apoiam conteúdo, meios e prazos; registrar a decisão inclusive se não houver comunicação.
Recuperar e corrigir	Restabelecer serviços com verificação, orientar titulares, corrigir causa, revisar acessos e contratos e documentar ações preventivas.

23. Comunicação externa e prazos

Quando o incidente puder acarretar risco ou dano relevante, o controlador deve comunicar à ANPD e aos titulares em **até 3 dias úteis** contados da ciência de que o incidente afetou dados pessoais, observadas a Resolução CD/ANPD nº 15/2024, eventuais regras específicas e hipóteses legais diferenciadas. Falta de informação completa não autoriza deixar o prazo transcorrer: seguir o procedimento de comunicação preliminar e complementação aplicável.

A comunicação deve apresentar natureza dos dados, riscos, medidas e contato, conforme o regulamento. Como operadora, a GENTTRA deve informar o controlador sem demora injustificada e cooperar. Comunicações externas devem ser coordenadas por responsável autorizado.

24. Registro e acompanhamento

Manter registro dos incidentes, inclusive os não comunicados, por **no mínimo 5 anos**, conforme o regulamento. Documentar fatos, impactos, critérios de decisão, medidas e acompanhamento. O registro deve ter acesso restrito e conter apenas as evidências necessárias.

IMPLEMENTAÇÃO, REVISÃO E REFERÊNCIAS

Implementação, revisão e referências

25. Treinamento, verificação e riscos

A GENTTRA deve orientar profissionais na entrada e nas mudanças relevantes, com conteúdo adaptado às funções. Reforçar boas práticas sobre currículos, anexos, e-mail, dados sensíveis, credenciais e relatos éticos. Manter registro de participação e canais para dúvidas.

Gestores devem verificar permissões, pendências de titulares, contratos, descarte e incidentes de seus processos. Tratamentos com maior risco exigem avaliação documentada e, quando cabível ou solicitado pela ANPD, Relatório de Impacto à Proteção de Dados Pessoais. Falhas precisam gerar responsável e prazo de correção; métricas não devem criar exposição adicional.

26. Descumprimento e revisão

Descumprimentos devem ser apurados com confidencialidade, proporcionalidade, direito de defesa e respeito à legislação e ao vínculo aplicável. Consequências contratuais ou disciplinares dependem de análise do caso; não são automáticas. Relatar riscos de boa-fé não deve gerar retaliação.

A revisão deve ocorrer periodicamente e quando houver mudança legal, incidente relevante, novo serviço, fornecedor, integração ou risco. A Direção deve aprovar alterações e comunicar equipes e terceiros afetados. A Política de Privacidade, avisos, contratos e procedimentos devem permanecer coerentes com esta Política.

27. Condições para adoção institucional

A vigência inicia após aprovação formal da Direção. Razão social e CNPJ constam conforme informação fornecida pela empresa. Antes da adoção, identificar e divulgar o encarregado; formalizar responsabilidades e substituição; validar inventário e tabela de temporalidade; avaliar fornecedores e transferências; conferir cookies e avisos; e verificar controles e atendimento do canal de privacidade.

Essas definições precisam corresponder à operação real. A presente versão estabelece diretrizes e não certifica conformidade técnica ou jurídica de todos os portais. A documentação de aprovação deve ficar em registro próprio da empresa, com responsável, data e versão.

28. Referências oficiais e documentos relacionados

Referências consultadas em 05/10/2026:

- [Lei nº 13.709/2018 - LGPD, texto vigente.](#)
- [Resolução CD/ANPD nº 15/2024 - comunicação de incidentes.](#)
- [Resolução CD/ANPD nº 18/2024 - atuação do encarregado.](#)
- [Resolução CD/ANPD nº 19/2024 - transferências internacionais.](#) Considerar alterações e retificações vigentes.

Documentos relacionados: Política de Privacidade; Código de Ética e Conduta da GENTTRA; avisos de coleta; contratos com clientes e operadores; inventário; tabela de temporalidade; procedimentos de acesso, atendimento de direitos e resposta a incidentes.