Estamos conformes à LGPD!

Veja o que isso significa >

alignio

Somos Operadores de Dados

A alignio exerce, preponderantemente, o papel de Operador na prestação de seus serviços:

- Todos os dados pessoais processados são obtidos junto ao **Cliente** (Controlador);
- Esses dados são tratados **apenas conforme as ordens e finalidades do Cliente** e conforme o Contrato/DPA;
- A inserção, alteração e deleção dos dados obedecem à determinação do Cliente ou às regras legais aplicáveis;
- Temos interesse legítimo em **prestar o serviço**, mas **não comercializamos dados** e nos obrigamos a não utilizar dados identificáveis do Cliente para finalidades próprias fora do contrato.

Importante

Em atividades específicas de **benchmarking estatístico** e **melhoria de produto** com base em dados **agregados e anonimizados**, a alignio poderá atuar como **Controladora Conjunta do dataset estatístico anonimizado**, limitada às finalidades descritas em contrato e aos princípios da LGPD.

1. Obedecemos ao Princípio da Finalidade

Tratamos dados pessoais sempre de acordo com as finalidades previamente informadas ao Cliente, e somente:

- Para o cumprimento de obrigação legal ou regulatória pelo Cliente;
- Quando necessário para a execução do Contrato e do DPA (Data Processing Agreement);
- Para a proteção da vida ou da incolumidade física do Titular ou de terceiro;
- Para segurança, prevenção a fraude e abuso, e integridade operacional (quando aplicável e documentado).

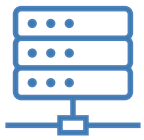
2. Obedecemos ao Princípio da Adequação e Necessidade

- Nossas soluções e processos são desenhados para operar com o **mínimo de informações pessoais necessárias**;
- Apenas dados estritamente adequados e necessários são processados;
- Controles técnicos reduzem exposição de dados pessoais em relatórios e rotinas;
- **IA:** não realizamos extrapolações e inferências indevidas sobre pessoas físicas quando isso não for necessário à finalidade do Cliente;
- **Benchmarking:** somente com dados **agregados/anonimizados**, sem identificação direta ou indireta de clientes.

3. Obedecemos ao Princípio da Transparência, Qualidade e Livre Acesso aos Dados

- Nossos tratamentos seguem padrões transparentes e previsíveis com garantia de qualidade;
- Mantemos procedimentos para atendimento pelo Encarregado/DPO e equipe de privacidade;
- Fornecemos ao Cliente informações e relatórios sobre o tratamento e as medidas de segurança aplicáveis ao contexto contratado.

4. Fornecemos Prontamente Informações sobre o Tratamento de Dados



- Informações sobre as finalidades específicas do tratamento;
- Quanto à forma e duração do tratamento;
- Sobre responsabilidades de Controlador/Operador/Suboperadores;
- E sobre os direitos do Titular, conforme a LGPD e a governança do Cliente.

5. Tratamento de Dados Pessoais Sensíveis

- A alignio **não utiliza** dados pessoais sensíveis para finalidades discriminatórias;
- Quando o Cliente, por sua operação, necessitar tratar categorias especiais, aplicamos controles reforçados de acesso, registro e segurança;
- Orientamos o Cliente a limitar a coleta ao estritamente necessário e a formalizar bases legais e avisos aplicáveis.

6. Política de Privacidade

- Possuímos política de privacidade própria para dados pessoais que coletamos em canais institucionais (site, formulários, contatos e usuários de ferramentas online);
- Para o tratamento operacional como Operadora (BPO/ERP/integrações/IA/benchmarking), aplicamos instrumentos **contratuais específicos** (Contrato + Cláusulas LGPD + DPA + anexos).

Baixe aqui a Política de Privacidade

7. Data Protection Officer (DPO)

- Contamos com Encarregado/DPO capacitado para exercer as atividades previstas na LGPD;
- Mantemos canal de contato para comunicações de privacidade e solicitações relacionadas a titulares e clientes.

8. Contratos de Confidencialidade

- Firmamos contratos de confidencialidade e cláusulas de proteção de dados com colaboradores, prestadores e terceiros;
- Implementamos regras internas de acesso por função e necessidade;
- Exigimos compromissos equivalentes de terceiros que atuem como suboperadores.

9. Cloud

- Utilizamos serviços de computação em nuvem com controles de segurança compatíveis com o risco do tratamento;
- Aplicamos criptografia em trânsito e em repouso;
- Mantemos segregação lógica por cliente (tenant isolation) e políticas de acesso restrito;
- Exigimos cláusulas contratuais e padrões mínimos de segurança de provedores e suboperadores.

10. SLD (Security Development Lifecycle)

- Adotamos ciclo de desenvolvimento seguro (SDLC/SLD) com boas práticas de segurança desde o desenho do produto;
- Revisamos mudanças relevantes de arquitetura, integrações e permissões;
- Controlamos credenciais e acessos (segredos, chaves, tokens) e registramos atividades críticas.

11. Inventário 

- Mantemos inventário dos dados tratados por tipo, finalidade, base legal aplicável (quando cabível), e fluxos de compartilhamento;
- Registramos suboperadores e integrações (ex.: ERPs, cloud, mensageria, ferramentas analíticas);
- O inventário é atualizado conforme demanda: novos clientes, alteração contratual, novos módulos, mudanças de responsáveis e integrações.

12. Governança no Tratamento de Dados

- Temos normas internas, procedimentos e controles para mitigação de riscos no tratamento;
- Nossos processos possuem rastreabilidade do início ao fim (logs, trilhas e auditoria);
- Mantemos gestão de acessos por função (RBAC), segregação por cliente e revisão periódica de permissões.

IA e automações

- Implementamos “guardrails” para evitar vazamento e contaminação entre clientes;
- Preferimos pseudonimização/minimização em pipelines;
- Não utilizamos dados identificáveis de clientes para treinar modelos de uso geral. Quando aplicável, (i) modelos isolados por cliente, ou (ii) dados anonimizados.

13. Avaliação Periódica de Vulnerabilidades

- Realizamos revisões preventivas periódicas para detectar vulnerabilidades em software, infraestrutura e processos;
- Mantemos plano de correção e priorização por criticidade;
- Testamos controles de acesso e eventuais pontos de extração/exportação de dados.

14. Plano de Comunicação para Incidente de Segurança

- Atuamos para mitigar incidentes que acarretem risco ou dano ao Cliente;
- Mantemos planos de contingência e procedimentos de comunicação ao Cliente;
- Em incidentes relevantes, suportamos o Cliente com informações técnicas para decisões de comunicação a titulares/ANPD, quando aplicável.

15. Validação do Término do Contrato de Tratamento

- Ao término do contrato, realizamos procedimentos de devolução/eliminação conforme acordado e conforme requisitos legais de retenção;

- Fornecemos evidências e relatórios quando contratualmente previsto;

- Mantemos controles para garantir que cópias e backups sigam políticas de retenção e descarte.

16. Segurança da Informação

Aplicamos medidas de segurança aptas a proteger dados de acessos não autorizados e de situações acidentais ou ilícitas.

- Controle de acesso com mecanismos físicos e lógicos;
- Criptografia, logs e monitoramento;
- Segregação por cliente e rastreabilidade;
- Treinamento interno e medidas preventivas contra erro humano;
- Políticas de continuidade e recuperação.

Referências Legais

Legislação principal

- Lei nº 13.709/2018 (LGPD)
- Lei nº 13.853/2019

Normas e diretrizes da ANPD

- Resolução CD/ANPD nº 1/2021
- Resolução CD/ANPD nº 2/2022
- Guia Orientativo de Segurança da Informação (ANPD)
- Guia de Tratamento de Dados (ANPD)

Normas e padrões de segurança

- ISO/IEC 27001 e 27002
- ISO/IEC 27701
- NIST Privacy Framework

Legislação complementar

- Marco Civil da Internet (Lei nº 12.965/2014)
- Código de Defesa do Consumidor (Lei nº 8.078/1990)
- Código Civil Brasileiro (Lei nº 10.406/2002)

Contexto regulatório da alignio

- Responsabilidade de operadores de dados
- Contratos Controlador x Operador (DPA)
- Segurança da informação e incidentes
- Anonimização e prevenção de reidentificação
- Uso de Inteligência Artificial com dados pessoais

Av. Brigadeiro Faria Lima 1811, sala 1119
Jd. Paulistano - São Paulo - SP
alignio.tech