

Política de Privacidade de Dados Pessoais

POL-SGSI-005

Histórico de Alterações

Nº	Data	Elaborado por:	Aprovado por:	Revisões
01	02/12/2025	Ricardo Bittar	Claudia Moraes	Emissão Inicial

1. Objetivo e abrangência

A iMonitore valoriza a privacidade e a proteção de dados pessoais. Esta Política descreve, de forma clara e completa, como tratamos dados pessoais no contexto:

1. das relações com candidatos, clientes, prestadores de serviço, fornecedores, parceiros comerciais, público em geral, leads e usuários dos sistemas fornecidos;
2. da operação do nosso negócio (prospecção, contratação, faturamento, suporte e segurança); e
3. do fornecimento da plataforma de Gestão do Ciclo de Vida do Consentimento (“Plataforma”), utilizada por clientes para coletar, gerenciar e arquivar registros de consentimento de usuários finais.

Esta Política é aplicável a dados pessoais tratados em meios físicos e digitais, incluindo sistemas, aplicações, logs e comunicações, conforme a legislação aplicável, especialmente a Lei nº 13.709/2018 (LGPD).

Esta Política também se aplica aos titulares que interagem com os canais digitais da iMonitore, incluindo visitantes do site institucional, leads, potenciais clientes e usuários dos sistemas fornecidos, inclusive quando houver coleta de dados por meio de cookies e tecnologias similares.

Importante: no contexto da Plataforma, a iMonitore pode atuar como Operadora de dados pessoais de usuários finais em nome de clientes (Controladores). Nesses casos, o cliente definirá as finalidades e decisões do tratamento, e a iMonitore executará o tratamento conforme instruções contratuais (ver Seção 4).

2. Definições principais

Para fins desta Política:

- Dado pessoal: informação relacionada a pessoa natural identificada ou identificável.
- Dado pessoal sensível: dado sobre origem racial/étnica, convicção religiosa, opinião política, filiação sindical, dado de saúde, vida sexual, genético ou biométrico.
- Titular: pessoa natural a quem os dados se referem.
- Controlador: quem toma decisões sobre o tratamento.
- Operador: quem realiza o tratamento em nome do controlador.
- Tratamento: qualquer operação com dados (coletar, armazenar, usar, compartilhar, eliminar etc.).
- Registro de consentimento: evidências e metadados que comprovam a manifestação de vontade do titular (ex.: preferências, data/hora, propósito, contexto e histórico).

3. Princípios e diretrizes (LGPD e alinhamento à ISO/IEC 27701)

A iMonitore conduz o tratamento observando princípios como finalidade, adequação, necessidade, transparência, segurança, prevenção, não discriminação e responsabilização.

A iMonitore mantém um Programa de Privacidade com práticas alinhadas à ISO/IEC 27701 (gestão de informações de privacidade), integradas à gestão de segurança da informação (ex.: controles de acesso, trilhas de auditoria, gestão de riscos e fornecedores). Isso não implica declaração de certificação, salvo se formalmente indicado em documento próprio.

4. Papéis da iMonitore: Controladora e Operadora (quando aplicável)

4.1. iMonitore como Controladora

A iMonitore é Controladora principalmente quando trata dados de:

- candidatos a vagas;
- prestadores de serviço e representantes de fornecedores;
- representantes e contatos de clientes (compras, jurídico, TI, privacidade, administradores de conta);
- visitantes do site institucional e contatos comerciais (quando aplicável).

4.2. iMonitore como Operadora (Plataforma de Consentimento)

Na Plataforma, em regra:

- o cliente (empresa que contrata a Plataforma) é o Controlador dos dados dos usuários finais;
- a iMonitore atua como Operadora, processando dados estritamente para prestar o serviço, manter segurança, suportar auditorias e cumprir obrigações legais/contratuais.

As regras específicas de operação como Operadora (incluindo suboperadores, medidas e responsabilidades) podem ser detalhadas em Contrato/DPA/Aditivo de Proteção de Dados firmado com o cliente.

5. Categorias de titulares e dados tratados

Abaixo, descrevemos as categorias mais comuns de dados pessoais tratados pela iMonitore. Podemos tratar apenas o mínimo necessário para cada finalidade.

5.1. Candidatos

- Identificação e cadastro: nome, data de nascimento, estado civil (quando necessário).
- Contato: e-mail, telefone, endereço.
- Dados profissionais: histórico profissional, treinamentos, e referências, .

5.2. Prestadores de serviço e partes relacionadas

- dados de identificação e contato profissional;
- dados contratuais e fiscais (ex.: notas, retenções);
- dados de acesso a ambientes e sistemas (quando necessário).

5.3. Representantes de clientes e fornecedores (B2B)

- nome, e-mail, telefone, empresa, cargo;
- dados de conta (usuário administrador), permissões e trilhas de auditoria;
- comunicações de suporte (tickets, e-mails, gravações, quando aplicável e informado).

5.4. Usuários finais (Plataforma de gestão de consentimento)

A depender da implementação do cliente, a Plataforma pode tratar:

(a) Dados para identificação/autenticação (quando aplicável):

- identificadores fornecidos pelo cliente (ex.: ID interno, hash/pseudônimo, e-mail mascarado/hasheado), conforme arquitetura do projeto.

(b) Dados técnicos e de uso:

- IP, data/hora, fuso, user-agent, idioma, informações do dispositivo e do navegador, identificadores de sessão e eventos técnicos necessários para segurança e operação.

(c) Dados do ciclo de vida do consentimento (registros de consentimento):

- preferências e escolhas do titular (ex.: consentiu/não consentiu por finalidade/categoria);
- carimbo de data e hora, versão do texto/aviso exibido, canal/origem (site/app), identificador do banner/fluxo, versão de políticas apresentadas, parâmetros regionais/legais configurados;
- histórico de alterações, revogações, renovações e expirações;
- evidências técnicas (ex.: identificador do registro, logs de integridade, prova de apresentação do aviso, trilhas de auditoria).

Nota: dependendo do desenho do cliente, o registro de consentimento pode, indiretamente, revelar preferências relacionadas a categorias potencialmente sensíveis (ex.: consentimento para compartilhar “dados de saúde”). Quando isso ocorrer, tratamos com controles reforçados de segurança e minimização.

5.5. Público geral, leads e potenciais clientes

- nome, e-mail, função e informações fornecidas em formulários ou interações digitais.

6. Fontes de coleta

Os dados podem ser coletados:

- diretamente do titular (cadastros, contratos, comunicações);
- de clientes/fornecedores (no contexto B2B);
- automaticamente por sistemas (logs, segurança, trilhas de auditoria);
- por integrações configuradas pelo cliente na Plataforma (quando aplicável).

7. Finalidades do tratamento e bases legais (LGPD)

A iMonitore trata dados pessoais para finalidades legítimas e compatíveis com a relação com o titular. As bases legais variam conforme o contexto:

7.1. Candidatos

Finalidades:

- Condução de processos seletivos;
- Avaliação para eventual formalização de vínculo contratual.

Bases legais usuais:

- Legítimo Interesse;
- Execução de atividades preliminares a um contrato.

7.2. Relação B2B com clientes e fornecedores (Controladora)

Finalidades:

- cadastro e gestão de contas;
- contratação, faturamento, cobrança, gestão financeira;
- suporte técnico, comunicações operacionais e de segurança;
- melhoria do serviço, governança e continuidade do negócio.

Bases legais usuais:

- execução de contrato;
- legítimo interesse (ex.: relacionamento B2B, melhoria e segurança);
- cumprimento de obrigação legal (fiscal/contábil etc.).

7.3. Operação da Plataforma de consentimento (em regra, Operadora)

Finalidades (para usuários finais):

- coletar, registrar, armazenar, consultar, atualizar e comprovar consentimentos e preferências;
- propagar sinais de consentimento/revogação a sistemas integrados conforme configuração do cliente;
- produzir relatórios, trilhas de auditoria e evidências;
- manter segurança, prevenir fraudes e garantir disponibilidade e integridade do serviço.

Base legal:

- como Operadora, a iMonitore trata os dados conforme a base legal definida pelo cliente Controlador (frequentemente o consentimento, quando o fundamento do cliente for consentimento) e sob instruções contratuais.
- a iMonitore pode tratar dados técnicos mínimos adicionais com base em execução de contrato e legítimo interesse para segurança e prevenção de abuso, sem desviar das finalidades do serviço.

8. Como a Plataforma gerencia o ciclo de vida do consentimento

A Plataforma foi desenhada para suportar governança e evidência do consentimento, incluindo:

1. Apresentação do aviso e coleta (banner/central de preferências/fluxo in-app), com parâmetros de versão;
2. Registro e arquivamento do evento (data/hora, contexto, versão do texto, finalidades/categorias, identificadores técnicos);
3. Gestão contínua (alteração de preferências, granularidade por finalidade, renovação/expiração quando configurado);
4. Revogação: registro do evento de revogação e disponibilização ao cliente (e integrações);
5. Auditoria e comprovação: trilhas de auditoria, exportação de evidências e relatórios;
6. Retenção e descarte: conforme parâmetros contratuais, prazos legais e configurações do cliente (Seção 11).

9. Compartilhamento de dados pessoais

A iMonitore pode compartilhar dados pessoais nas seguintes hipóteses:

9.1. Prestadores e suboperadores (fornecedores)

Podemos utilizar fornecedores para:

- hospedagem/infraestrutura em nuvem;
- envio de e-mails transacionais;
- sistemas de atendimento (helpdesk/tickets);
- monitoramento, logs e segurança;
- ferramentas corporativas necessárias ao negócio.

Esses fornecedores atuam sob obrigações contratuais de confidencialidade, segurança e proteção de dados, com acesso limitado ao necessário.

9.2. Compartilhamento com clientes (Plataforma)

No contexto da Plataforma, os dados e registros de consentimento são disponibilizados ao cliente Controlador e a integrações que ele configurar (por exemplo, ferramentas de analytics, tag managers e provedores de anúncios), sempre conforme instruções do cliente e desenho técnico do projeto.

9.3. Autoridades e obrigações legais

Podemos compartilhar dados para:

- cumprir obrigação legal/regulatória;
- atender ordem judicial, administrativa ou requisição válida;
- proteger direitos da iMonitore, clientes e terceiros.

10. Transferências internacionais de dados

- Em razão da utilização de infraestrutura tecnológica e/ou serviços de suporte localizados no exterior, os dados pessoais tratados pela iMonitore poderão ser transferidos para os Estados Unidos da América (EUA), sempre em estrita conformidade com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD), com a Resolução CD/ANPD nº 19/2024 e demais normas aplicáveis.

Tais transferências ocorrerão exclusivamente quando necessárias para a execução de atividades legítimas e compatíveis com as finalidades informadas neste Aviso, tais como a operação de sistemas, armazenamento em nuvem, suporte técnico, execução de contratos, cumprimento de obrigações legais ou exercício regular de direitos em processos administrativos ou judiciais.

As transferências internacionais são realizadas com fundamento nas hipóteses previstas no art. 33 da LGPD, mediante a adoção de mecanismos jurídicos adequados, incluindo, conforme aplicável, cláusulas contratuais que assegurem níveis de proteção de dados compatíveis com a legislação brasileira, bem como a avaliação das salvaguardas técnicas e organizacionais adotadas pelo destinatário.

Adicionalmente, a iMonitore adota medidas técnicas e organizacionais de segurança destinadas a proteger os dados pessoais transferidos, assegurando sua confidencialidade, integridade e disponibilidade, de acordo com boas práticas de governança e segurança da informação.

- **11. Retenção, arquivamento e descarte**

A iMonitore retém dados pelo tempo necessário para cumprir finalidades legítimas e obrigações legais/contratuais.

Diretrizes típicas:

- dados cadastrais, contratuais, financeiros e registros de uso dos sistemas,: conforme prazos legais aplicáveis;
- dados contratuais B2B e evidências de suporte/auditoria: durante a vigência do contrato e por período adicional necessário para exercício regular de direitos e conformidade;
- registros de consentimento (Plataforma): conforme contrato e configurações do cliente, e pelo período necessário para comprovação, auditoria e defesa relacionada às finalidades do consentimento.

Quando aplicável, realizamos anonimização, pseudonimização ou eliminação segura.

12. Segurança da informação e controles de privacidade

A iMonitore adota medidas técnicas e administrativas proporcionais aos riscos, como:

- controle de acesso por perfil e necessidade (least privilege);
- autenticação forte (incluindo MFA quando aplicável);
- criptografia em trânsito e em repouso;

- segregação de ambientes, gestão de segredos e chaves;
- logs, trilhas de auditoria e monitoramento de segurança;
- gestão de vulnerabilidades, correções e testes;
- backup, continuidade e recuperação;
- treinamento e conscientização de pessoas autorizadas envolvidas no tratamento de dados pessoais;
- governança de fornecedores e suboperadores.

13. Direitos dos titulares (LGPD) e como exercer

Nos termos da LGPD, o titular pode solicitar, quando aplicável:

- confirmação da existência de tratamento;
- acesso, correção e atualização;
- anonimização, bloqueio ou eliminação (quando cabível);
- portabilidade (quando aplicável);
- informação sobre compartilhamentos;
- informação sobre a possibilidade de não consentir e consequências;
- revogação do consentimento (quando o tratamento se basear em consentimento);
- revisão de decisões automatizadas (quando aplicável).

13.1. Como solicitar

Solicitações devem ser encaminhadas ao nosso canal de privacidade:

Encarregado (DPO) / Canal de Privacidade: ICTS DESENVOLVIMENTO DE SISTEMAS E TECNOLOGIA LTDA - PROTIVITI
E-mail: privacidade@imonitore.com.br

Podemos solicitar informações adicionais para confirmar a identidade e prevenir fraudes.

13.2. Usuários finais da Plataforma

Se você é usuário final de um cliente que usa a Plataforma, em regra, o cliente é o Controlador e deve ser o primeiro ponto de contato para seus direitos. A iMonitore, como Operadora, prestará suporte ao cliente para atender solicitações válidas, conforme contrato e instruções.

14. Crianças e adolescentes

A Plataforma e os serviços da iMonitore não são direcionados intencionalmente a crianças. Caso um cliente utilize a Plataforma em contextos que envolvam crianças/adolescentes, deverá garantir as bases legais e requisitos aplicáveis. A iMonitore atuará conforme instruções e salvaguardas contratuais.

15. Decisões automatizadas e perfilamento

A iMonitore não utiliza dados pessoais para decisões exclusivamente automatizadas que produzam efeitos jurídicos relevantes sobre titulares, salvo se previsto em contrato/uso específico e com transparência adequada. No contexto da Plataforma, “automatizações” costumam se restringir a aplicar preferências e propagar sinais de consentimento/revogação conforme regras configuradas pelo cliente.

16. Cookies e tecnologias similares

Quando aplicável (site institucional e/ou console da Plataforma), podemos utilizar cookies e tecnologias semelhantes para:

- funcionamento e segurança;
- preferências e experiência;
- métricas e melhoria.

O detalhamento e gerenciamento das preferências de cookies constará em Aviso de Cookies e/ou central de preferências, quando disponível.

17. Incidentes de segurança

Em caso de incidente com risco relevante aos titulares, adotaremos medidas de contenção e resposta, incluindo avaliação de impacto, registro e comunicações necessárias a clientes/controladores e, quando aplicável, às autoridades e titulares, conforme a LGPD e obrigações contratuais.

18. Contato

Caso você tenha dúvidas sobre esta Política, nossas práticas de tratamento de dados pessoais ou desejar exercer quaisquer de seus direitos de acordo com a lei geral de proteção de dados, entre em contato nosso encarregado pelo tratamento de dados pessoais Protiviti - ICTS Desenvolvimento de Sistemas e Tecnologia Ltda, representada pelo Fernando Fleider, através do e-mail: privacidade@imonitore.com.br.

18. Atualizações desta Política

Podemos atualizar esta Política para refletir mudanças legais, técnicas ou operacionais. A versão vigente estará indicada no topo do documento e mudanças relevantes serão comunicadas por canais apropriados (por exemplo, aviso no site/console ou comunicação aos clientes B2B).

Recomenda-se que os titulares revisem periodicamente esta Política para se manterem informados sobre eventuais atualizações.