**1. Objetivo e Abrangência**

Esta Política de Privacidade ("Política") descreve como a **Milo IA LTDA** ("Empresa", "Controlador", "nós") coleta, usa, compartilha e protege dados pessoais através da plataforma **Prophet**, em conformidade com:

* Lei Geral de Proteção de Dados (Lei nº 13.709/2018 - "LGPD")
* Marco Civil da Internet (Lei nº 12.965/2014)
* Código de Defesa do Consumidor (Lei nº 8.078/1990)
* Regulamentações complementares aplicáveis

O Prophet é uma plataforma de automação que permite criar e executar fluxos automatizados conectando diversos serviços e aplicações terceirizados.

## **2. Definições Importantes**

Conforme Art. 5º da LGPD:

* **Dados Pessoais:** Informação relacionada a pessoa natural identificada ou identificável
* **Dados Pessoais Sensíveis:** Dados sobre origem racial/étnica, convicção religiosa, opinião política, filiação sindical, dados de saúde, vida sexual, dados genéticos ou biométricos
* **Tratamento:** Toda operação com dados pessoais: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle, modificação, comunicação, transferência, difusão ou extração
* **Titular:** Pessoa natural a quem se referem os dados pessoais
* **Consentimento:** Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento

## **3. Dados Coletados**

### **3.1 Dados de Cadastro (Coleta Direta)**

**Dados obrigatórios:**

* Nome completo
* Endereço de e-mail
* Senha (armazenada com hash criptográfico)

### **3.2 Dados Processados pelas Automações**

⚠️ **IMPORTANTE:** O Prophet processa dados provenientes de serviços conectados **exclusivamente para executar as automações configuradas pelo usuário**.

**Características do processamento:**

* **Finalidade específica:** Apenas para executar a automação solicitada
* **Processamento temporário:** Dados transitam pela plataforma durante execução
* **Armazenamento mínimo:** Logs técnicos mantidos por 90 dias para auditoria e suporte
* **Sem acesso humano:** Processamento automatizado, sem visualização por colaboradores
* **Criptografia:** Todos os dados em trânsito e em repouso são criptografados

**Tipos de dados que podem ser processados:**

* Conteúdo de e-mails e mensagens (Gmail, Outlook, Slack, Teams)
* Dados de planilhas e documentos (Google Sheets, Excel, Notion)
* Informações de CRM (Pipedrive, HubSpot, Salesforce)
* Dados de redes sociais profissionais (LinkedIn)
* Webhooks e APIs configuradas pelo usuário
* Anexos e arquivos (quando necessário para automação)

**⚠️ Dados sensíveis:** Reconhecemos que dados sensíveis podem estar presentes no conteúdo processado. Implementamos controles para minimizar riscos:

* Processamento apenas pelo tempo necessário
* Criptografia em todas as etapas
* Logs mínimos sem conteúdo sensível
* Acesso restrito a sistemas automatizados

### **3.3 Dados Coletados Automaticamente**

* **Dados técnicos:** Endereço IP, user agent, sistema operacional
* **Dados de uso:** Páginas acessadas, tempo de sessão, funcionalidades utilizadas
* **Cookies:** Conforme nossa Política de Cookies
* **Logs de segurança:** Tentativas de acesso, eventos de autenticação

## **4. Bases Legais para Tratamento**

Todo tratamento está fundamentado nas bases legais do Art. 7º da LGPD:

### **4.1 Execução de Contrato (Art. 7º, V)**

**Aplicação:** Dados essenciais para prestação do serviço

* Criação e gestão de conta
* Execução de automações
* Processamento de pagamentos
* Suporte técnico

### **4.2 Consentimento (Art. 7º, I)**

**Aplicação:** Tratamentos opcionais com benefício ao usuário

* Newsletter e comunicações promocionais
* Funcionalidades beta e experimentais
* Pesquisas de satisfação
* Cookies não essenciais

**Características do consentimento:**

* Livre: Sem vício de vontade
* Informado: Com conhecimento das finalidades
* Inequívoco: Manifestação expressa
* Específico: Para finalidades determinadas
* Revogável: A qualquer momento

### **4.3 Legítimo Interesse (Art. 7º, IX)**

**Aplicação:** Interesses legítimos do controlador, respeitando direitos dos titulares

**Análise de balanceamento realizada:**

### **4.4 Cumprimento de Obrigação Legal (Art. 7º, II)**

**Aplicação:** Exigências legais e regulatórias

* Retenção fiscal (5 anos - Art. 173 CTN)
* Ordens judiciais
* Requisições de autoridades competentes
* Obrigações trabalhistas

## **5. Finalidades do Tratamento**

### **5.1 Finalidades Primárias**

**Prestação do serviço contratado:**

* Criar e gerenciar conta de usuário
* Autenticar e autorizar acesso
* Executar automações configuradas
* Conectar APIs e serviços terceiros
* Processar pagamentos e assinaturas
* Fornecer suporte técnico
* Enviar notificações operacionais críticas

### **5.2 Finalidades Secundárias**

**Melhorias e comunicação (com consentimento):**

* Análise de uso para desenvolvimento de funcionalidades
* Comunicações sobre atualizações do produto
* Pesquisas de satisfação
* Personalização da experiência
* Segurança e prevenção a fraudes

### **🚫 O que NÃO fazemos:**

* Não vendemos ou alugamos dados pessoais
* Não compartilhamos dados para marketing direto de terceiros
* Não realizamos decisões automatizadas com impacto significativo nos direitos do titular
* Não fazemos perfilamento discriminatório
* Não acessamos o conteúdo das automações para outros fins que não a execução

## **6. Integração com Google Workspace**

### **6.1 Compromisso de Uso Limitado**

O Prophet adere aos **Requisitos de Uso Limitado das APIs do Google**, utilizando dados obtidos exclusivamente para:

* Executar automações solicitadas pelo usuário
* Fornecer funcionalidades específicas autorizadas
* Garantir operação segura da integração

### **6.2 Práticas Específicas**

* **Autorização OAuth 2.0:** Acesso apenas com consentimento explícito
* **Escopo mínimo:** Solicitamos apenas permissões necessárias para funcionalidade específica
* **Processamento limitado:** Dados utilizados apenas para automação solicitada
* **Sem armazenamento desnecessário:** Retenção mínima conforme nossa política
* **Conformidade contínua:** Aderência às Políticas de Dados do Google

### **6.3 Revogação de Acesso**

Você pode revogar permissões a qualquer momento:

* Através das configurações da sua conta Google
* No painel de integrações do Prophet
* Solicitando via privacidade@oimilo.com

## **7. Compartilhamento de Dados**

### **7.1 Com Serviços Conectados pelo Usuário**

Compartilhamos dados **apenas** com serviços que você explicitamente conecta para executar automações (ex: Gmail, Slack, Notion).

**Controles implementados:**

* Compartilhamento apenas durante execução da automação
* Dados mínimos necessários para funcionalidade
* Criptografia em todas as transferências
* Logs de auditoria para transparência

### **7.2 Com Fornecedores de Serviço (Subprocessadores)**

Compartilhamos dados com fornecedores essenciais sob acordos rigorosos:

**Garantias contratuais:**

* Data Processing Agreements (DPA) assinados
* Certificações de segurança validadas
* Auditoria periódica de fornecedores
* Notificação obrigatória de incidentes

### **7.3 Por Obrigação Legal**

Podemos divulgar dados quando **estritamente necessário** para:

* Cumprir ordem judicial com fundamentação
* Atender requisição de autoridade competente
* Proteger direitos em processo judicial
* Prevenir fraudes com evidências concretas
* Atender obrigações regulatórias específicas

### **7.4 Em Reorganização Societária**

Em caso de fusão, aquisição ou reorganização:

* Manutenção integral dos compromissos desta Política
* Notificação prévia aos usuários com 30 dias de antecedência
* Direito de eliminação de dados antes da transferência
* Garantias contratuais de continuidade da proteção

## **8. Transferência Internacional de Dados**

### **8.1 Países de Destino**

Dados podem ser transferidos para:

* **Estados Unidos:** Fornecedores de infraestrutura (Supabase, Vercel)
* **União Europeia:** Fornecedores com adequação GDPR
* **Outros países:** Conforme necessário para integrações específicas

### **8.2 Salvaguardas Implementadas**

**Para países sem decisão de adequação:**

* **Cláusulas Contratuais Padrão (SCCs)** aprovadas
* **Certificações internacionais** (ISO 27001, SOC 2 Tipo II)
* **Avaliação de Impacto (TIA)** para transferências de alto risco
* **Medidas técnicas suplementares:**
  + Criptografia AES-256 em repouso
  + TLS 1.3 em trânsito
  + Controles de acesso rigorosos
  + Monitoramento contínuo

### **8.3 Direitos do Titular**

Você pode solicitar informações específicas sobre transferências através de privacidade@oimilo.com.

## **9. Segurança da Informação**

### **9.1 Medidas Técnicas**

**Criptografia:**

* **Em trânsito:** TLS 1.3 para todas as comunicações
* **Em repouso:** AES-256 para dados armazenados
* **Chaves:** Gestão segura com rotação automática

**Controle de Acesso:**

* Autenticação multifator obrigatória para administradores
* Princípio do menor privilégio
* Revisão trimestral de permissões
* Logs de auditoria para todos os acessos

**Monitoramento:**

* Detecção de intrusão em tempo real
* Análise comportamental de segurança
* Alertas automáticos para atividades suspeitas
* SIEM (Security Information and Event Management)

**Infraestrutura:**

* Backup criptografado diário com teste de restauração
* Segregação de ambientes (produção, teste, desenvolvimento)
* Patch management automatizado
* Disaster recovery com RTO de 4 horas

### **9.2 Medidas Organizacionais**

* **Políticas de segurança** documentadas e atualizadas anualmente
* **Treinamento obrigatório** em segurança para todos colaboradores
* **Acordos de confidencialidade** com todos os colaboradores e fornecedores
* **Comitê de segurança** com reuniões mensais
* **Testes de penetração** semestrais por empresa certificada
* **Gestão de incidentes** com procedimentos documentados

### **⚠️ Responsabilidade Compartilhada**

**Sua responsabilidade:**

* Manter credenciais seguras e confidenciais
* Usar senhas fortes e únicas
* Ativar autenticação de dois fatores
* Reportar atividades suspeitas imediatamente
* Manter software atualizado
* Não compartilhar acesso à conta

## **10. Retenção e Eliminação de Dados**

### **10.1 Períodos de Retenção**

### **10.2 Processo de Eliminação**

**Eliminação automática:**

* Rotinas automatizadas para exclusão conforme prazos
* Verificação de dependências legais antes da eliminação
* Log de auditoria das eliminações realizadas

**Eliminação por solicitação:**

* Análise de viabilidade legal em até 5 dias úteis
* Execução em até 10 dias úteis após confirmação
* Comprovante de eliminação enviado ao titular

**Exceções à eliminação:**

* Dados sob disputa judicial
* Informações necessárias para cumprimento de obrigação legal
* Dados anonimizados para estatísticas agregadas

## **11. Direitos dos Titulares**

### **Seus Direitos (Art. 18 da LGPD):**

### **11.1 Direito de Confirmação e Acesso (Incisos I e II)**

Confirmar se tratamos seus dados e obter cópia das informações.

### **11.2 Direito de Correção (Inciso III)**

Corrigir dados incompletos, inexatos ou desatualizados.

### **11.3 Direito de Anonimização, Bloqueio ou Eliminação (Inciso IV)**

Solicitar tratamento de dados desnecessários, excessivos ou tratados em desconformidade.

### **11.4 Direito de Portabilidade (Inciso V)**

Receber dados em formato estruturado, de uso comum e leitura por máquina.

### **11.5 Direito de Eliminação (Inciso VI)**

**IMPORTANTE:** Este direito não é absoluto. Dados podem ser mantidos quando:

* Necessários para cumprimento de obrigação legal
* Necessários para exercício de direitos em processo
* Uso exclusivo do controlador vedado acesso de terceiros

### **11.6 Direito de Informação sobre Compartilhamento (Inciso VII)**

Saber com quais entidades públicas e privadas compartilhamos dados.

### **11.7 Direito de Informação sobre Possibilidade de Não Consentir (Inciso VIII)**

Conhecer consequências de não fornecer consentimento.

### **11.8 Direito de Revogação de Consentimento (Inciso IX)**

Retirar consentimento a qualquer momento quando esta for a base legal.

### **11.9 Direito de Oposição (§ 2º)**

Opor-se a tratamento realizado com base em legítimo interesse mediante justificativa.

### **11.10 Direito de Revisão (Art. 20)**

Solicitar revisão de decisões automatizadas.

### **11.3 Como Exercer Seus Direitos**

**1. Envie solicitação para:** privacidade@oimilo.com

**2. Inclua as seguintes informações:**

* Nome completo e e-mail da conta
* Documento de identificação (para validação)
* Direito específico que deseja exercer
* Detalhamento da solicitação
* Forma preferida de resposta

**3. Prazos de atendimento:**

* **Confirmação de recebimento:** 48 horas
* **Resposta final:** 15 dias **corridos** (Art. 19 LGPD)
* **Prorrogação:** Até 15 dias adicionais em casos complexos (com justificativa)

**4. Sem custo:** Atendimento gratuito, exceto solicitações manifestamente infundadas ou excessivas.

## **12. Cookies e Tecnologias Similares**

### **12.1 Referência à Política Específica**

O uso de cookies e tecnologias similares é regulado por nossa **Política de Cookies**, disponível em [link] e acessível através do banner de consentimento.

### **12.2 Categorias Principais**

* **Essenciais:** Autenticação, segurança, funcionamento básico
* **Funcionais:** Preferências, personalização
* **Analytics:** Métricas de uso (dados agregados)
* **Marketing:** Campanhas próprias (com consentimento)

### **12.3 Gestão de Preferências**

Acesse o painel "Preferências de Cookies" disponível no rodapé de todas as páginas para gerenciar suas escolhas.

## **13. Menores de Idade**

### **13.1 Política Restritiva**

O Prophet **não é direcionado** a menores de 18 anos. Não coletamos **intencionalmente** dados pessoais de menores de idade.

### **13.2 Identificação Inadvertida**

Se identificarmos que coletamos dados de menor de 18 anos:

1. **Suspensão imediata** do tratamento
2. **Notificação aos pais/responsáveis** (quando possível)
3. **Eliminação dos dados** em até 15 dias
4. **Bloqueio de nova criação** de conta com os mesmos dados
5. **Relatório interno** para prevenção de recorrência

### **13.3 Procedimentos de Verificação**

* Declaração de maioridade no cadastro
* Análise de padrões suspeitos de uso
* Verificação adicional quando necessário
* Canal específico para denúncias: menores@oimilo.com

## **14. Comunicações e Marketing**

### **14.1 Tipos de Comunicação**

**Comunicações Operacionais (obrigatórias):**

* Confirmações de cadastro e alterações de conta
* Notificações de segurança e incidentes
* Alertas sobre mudanças nos termos
* Status do serviço e manutenções
* Faturas e informações de pagamento

**Comunicações Promocionais (opcionais - com consentimento):**

* Newsletter com novidades do produto
* Ofertas e promoções especiais
* Conteúdo educacional sobre automação
* Pesquisas de satisfação e feedback
* Convites para eventos e webinars

### **14.2 Gestão de Preferências**

**Opt-out facilitado:**

* Link "Descadastrar" em todos e-mails promocionais
* Painel de preferências na sua conta
* Solicitação via privacidade@oimilo.com
* Processamento em até 48 horas

**Granularidade:** Você pode escolher receber apenas tipos específicos de comunicação.

## **15. Integrações e Serviços de Terceiros**

### **15.1 Responsabilidades Compartilhadas**

⚠️ **IMPORTANTE:** Ao conectar serviços de terceiros, você nos autoriza a acessar dados conforme necessário para executar suas automações. Cada integração possui suas próprias políticas de privacidade que recomendamos consultar.

### **15.2 Principais Integrações**

**Google Workspace:**

* Regido pelas Políticas do Google
* OAuth 2.0 com escopos específicos
* Conformidade com Limited Use Requirements
* Revogação de acesso disponível a qualquer momento

**Microsoft 365:**

* Sujeito aos Termos de Privacidade da Microsoft
* Graph API com permissões mínimas
* Controles de segurança empresarial respeitados

**Meta Business (WhatsApp Business API):**

* Conformidade com políticas Meta
* Dados de mensagens processados conforme automação
* Webhook security implementado

**Outros Serviços (Slack, Notion, CRMs):**

* Due diligence de segurança realizada
* Contratos de processamento quando aplicável
* Monitoramento de conformidade contínuo

### **15.3 Controles Implementados**

* **Escopos mínimos:** Solicitamos apenas permissões necessárias
* **Auditoria regular:** Revisão trimestral de integrações ativas
* **Revogação facilitada:** Desconexão a qualquer momento pelo usuário
* **Transparência:** Lista completa de integrações disponível na conta

## **16. Avaliação de Impacto à Proteção de Dados (RIPD)**

### **16.1 Quando Realizamos**

Conduzimos RIPD (Data Protection Impact Assessment) para:

* Novas funcionalidades que envolvam alto risco
* Mudanças significativas no tratamento de dados
* Implementação de novas tecnologias
* Compartilhamento com novos parceiros
* Transferências internacionais de alto risco

### **16.2 Processo de RIPD**

1. **Mapeamento de riscos** aos direitos dos titulares
2. **Análise de necessidade e proporcionalidade**
3. **Identificação de medidas mitigatórias**
4. **Consulta ao DPO** em todos os casos
5. **Revisão pela equipe jurídica**
6. **Implementação de controles identificados**
7. **Monitoramento contínuo de eficácia**

### **16.3 Resultados**

RIPDs realizadas são documentadas e arquivadas por 5 anos, disponíveis para consulta da ANPD quando solicitado.

## **17. Encarregado de Proteção de Dados (DPO)**

### **17.1 Identificação**

**Encarregado (DPO):** [OBRIGATÓRIO - DESIGNAR FORMALMENTE]

**E-mail:** privacidade@oimilo.com

**Horário de atendimento:** Segunda a sexta, 9h às 18h (horário de Brasília)

**Telefone:** [INSERIR QUANDO DESIGNADO]

### **17.2 Responsabilidades Principais**

* **Conformidade:** Orientar organização sobre cumprimento da LGPD
* **Atendimento:** Receber e tratar solicitações de titulares
* **Cooperação:** Atuar como canal de comunicação com a ANPD
* **Auditoria:** Realizar verificações periódicas de conformidade
* **Treinamento:** Capacitar equipe sobre proteção de dados
* **Políticas:** Desenvolver e atualizar políticas internas

### **17.3 Independência**

O DPO possui independência funcional e reporta diretamente à alta administração, sem conflitos de interesse com outras responsabilidades.

## **18. Gestão de Incidentes de Segurança**

### **18.1 Detecção e Classificação**

**Sistemas de monitoramento contínuo:**

* SIEM (Security Information and Event Management)
* Alertas automáticos para atividades anômalas
* Análise comportamental de usuários
* Monitoramento de integridade de dados

**Classificação de incidentes:**

* **Nível 1 - Baixo:** Sem risco aos dados pessoais
* **Nível 2 - Médio:** Risco limitado e controlado
* **Nível 3 - Alto:** Alto risco aos direitos dos titulares
* **Nível 4 - Crítico:** Vazamento confirmado de dados sensíveis

### **18.2 Resposta a Incidentes**

**Procedimento padronizado (24/7):**

1. **Detecção (0-1h):**
   * Identificação e classificação inicial
   * Ativação da equipe de resposta
   * Isolamento de sistemas afetados
2. **Contenção (1-4h):**
   * Bloqueio de acesso não autorizado
   * Preservação de evidências
   * Avaliação do escopo do incidente
3. **Avaliação (4-24h):**
   * Análise detalhada do impacto
   * Identificação de dados envolvidos
   * Avaliação de riscos aos titulares
4. **Notificação (24-72h):**
   * ANPD: Em até 24h para incidentes de alto risco
   * Titulares: Quando houver risco alto aos direitos
   * Autoridades: Conforme obrigações específicas
5. **Remediação (contínuo):**
   * Correção de vulnerabilidades
   * Implementação de controles adicionais
   * Monitoramento reforçado
   * Relatório final de lições aprendidas

### **18.3 Transparência**

Publicamos relatório anual sobre incidentes (sem informações sensíveis) demonstrando nosso compromisso com a transparência.

## **19. Alterações nesta Política**

### **19.1 Tipos de Alteração**

**Alterações menores (administrativas):**

* Correções de redação sem mudança de significado
* Atualização de dados de contato
* Esclarecimentos que não alteram direitos

**Alterações substanciais:**

* Novas finalidades de tratamento
* Mudanças nas bases legais
* Alterações nos períodos de retenção
* Novos compartilhamentos ou transferências

### **19.2 Processo de Comunicação**

**Para alterações substanciais:**

1. **Notificação prévia** de 30 dias via e-mail
2. **Banner destacado** na plataforma
3. **Pop-up** no primeiro login após alteração
4. **Período de manifestação** para oposição
5. **Direito de cancelamento** sem ônus

**Para alterações menores:**

* Atualização da data de revisão
* Comunicação na próxima newsletter

### **19.3 Versionamento e Arquivo**

* Controle de versões numeradas
* Arquivo das últimas 5 versões disponível mediante solicitação
* Log de alterações mantido por auditoria

## **20. Jurisdição e Lei Aplicável**

### **20.1 Legislação Aplicável**

Esta Política é regida pelas leis da República Federativa do Brasil, especialmente:

* **Lei Geral de Proteção de Dados** (Lei nº 13.709/2018)
* **Marco Civil da Internet** (Lei nº 12.965/2014)
* **Código de Defesa do Consumidor** (Lei nº 8.078/1990)
* **Regulamentações da ANPD**

### **20.2 Resolução de Conflitos**

**Tentativas de resolução amigável:**

1. Contato direto via privacidade@oimilo.com
2. Mediação através de câmaras especializadas
3. Eventual recurso à ANPD
4. Via judicial como última instância

## **21. Canais de Atendimento e Contato**

### **21.1 Questões de Privacidade**

**E-mail principal:** privacidade@oimilo.com

**Prazo de resposta:** 48 horas para confirmação, 15 dias corridos para resposta final

**Horário:** Segunda a sexta, 9h às 18h (horário de Brasília)

### **21.2 Outros Contatos**

* **Suporte técnico:** suporte@oimilo.com
* **Comercial:** contato@oimilo.com
* **Denúncias (menores):** menores@oimilo.com
* **Website:** [www.oimilo.com](http://www.oimilo.com/)

### **21.3 ANPD - Autoridade Nacional de Proteção de Dados**

Para reclamações não resolvidas:

* **Website:** [gov.br/anpd](http://gov.br/anpd)
* **Peticionamento eletrônico:** Disponível no site oficial
* **Ouvidoria:** Canais oficiais da ANPD

## **22. Disposições Finais**

### **22.1 Aceite e Consentimento**

Ao utilizar o Prophet, você:

* ✅ Declara ter **lido integralmente** esta Política
* ✅ **Compreende** os tratamentos de dados descritos
* ✅ **Concorda** com os termos estabelecidos
* ✅ **Reconhece** ter capacidade legal para consentir
* ✅ **Entende** seus direitos e como exercê-los
* ✅ **Aceita** os riscos inerentes ao processamento descrito

### **22.2 Capacidade Legal**

O uso dos serviços requer capacidade civil plena. Menores de 18 anos não podem utilizar a plataforma.

### **22.3 Idioma**

Esta Política é redigida em português brasileiro. Em caso de tradução para outros idiomas, a versão em português prevalecerá em caso de conflito.

### **22.4 Separabilidade**

Se qualquer disposição desta Política for considerada inválida ou inexequível, as demais cláusulas permanecerão em pleno vigor e efeito.

### **22.5 Documentação Relacionada**

* **Termos de Uso do Prophet**
* **Política de Cookies**
* **Acordo de Nível de Serviço (SLA)**
* **Documentação Técnica das APIs**

**Milo IA LTDA**

CNPJ: 57.257.919/0001-82

© 2024 - Todos os direitos reservados

*Esta política foi desenvolvida em conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e melhores práticas de privacidade.*