

Política de Privacidade

LGPDCloud é um produto da Befavos Tecnologia LTDA.

Versão 1.1 | Revisada em 30 de setembro de 2026

Esta Política explica como tratamos dados pessoais no site, na plataforma LGPDCloud e nas interações comerciais, de suporte e de privacidade. Também distingue os dados tratados pela Befavos para suas próprias finalidades daqueles que tratamos por instrução de empresas clientes. Conhecer esta Política não significa consentir com todos os tratamentos: cada operação exige fundamento legal próprio.

Sumário

- | | |
|---|--|
| 1. Quem somos e como falar conosco | 7. Armazenamento, transferências e retenção |
| 2. A quem se aplica e nossos papéis | 8. Inteligência artificial e decisões automatizadas |
| 3. Quais dados podem ser tratados | 9. Crianças, adolescentes e dados sensíveis |
| 4. Para que usamos dados e com que fundamento | 10. Como protegemos dados e respondemos a incidentes |
| 5. Com quem os dados podem ser compartilhados | 11. Seus direitos e como exercer esses direitos |
| 6. Cookies e tecnologias semelhantes | 12. Atualizações e outros ambientes |

1. Quem somos e como falar conosco

A responsável pelo produto é Befavos Tecnologia LTDA, CNPJ nº 69.228.511/0001-61, com sede na Rua Leonel Mosele, nº 40, Sala 202, Edifício Ayrton de Menezes, Centro, Concórdia, Santa Catarina, CEP 89700-176. LGPDCloud é o nome do produto, não uma pessoa jurídica separada. Nosso site é <https://lgpdcloud.com.br>.

Nosso encarregado pelo tratamento de dados pessoais é Anderson Scotton. Para exercer direitos, esclarecer tratamentos ou relatar incidente com dados pessoais, escreva para dpo@lgpdcloud.com.br. Também é possível enviar correspondência à sede, aos cuidados do encarregado. Para suporte operacional, utilize suporte@lgpdcloud.com.br; para assuntos comerciais, contato@lgpdcloud.com.br.

2. A quem se aplica e nossos papéis

Esta Política alcança visitantes, interessados, representantes de clientes, usuários, consultores, participantes de ações organizadas pela Befavos e pessoas que interagem com nossos serviços. Formulários, páginas ou recursos operados para uma empresa cliente também podem tratar dados de colaboradores, consumidores, fornecedores e outros titulares dessa empresa.

Somos controladores quando decidimos finalidades e elementos essenciais de tratamentos próprios, como atender contatos comerciais, administrar nossa relação contratual, cumprir obrigações fiscais e proteger a plataforma. O fundamento legal é definido por operação e não decorre simplesmente da existência de um cadastro.

Atuamos como operadores quando armazenamos e organizamos dados inseridos pela empresa cliente ou enviados a seus formulários, seguindo suas instruções. Nesses casos, a empresa normalmente é a controladora e deve informar finalidades, bases legais, destinatários e retenção. Se nosso cliente for

operador de outra organização, a cadeia de instruções e autorizações deve ser respeitada. O aviso do cliente complementa esta Política para sua operação; nosso papel é definido pelo tratamento concreto.

O encarregado da Befavos não se torna automaticamente o encarregado das empresas clientes. Um serviço dessa natureza depende de contratação e designação próprias.

3. Quais dados podem ser tratados

3.1 Dados fornecidos diretamente

Podemos receber nome, e-mail, telefone, empresa, cargo, informações sobre interesse no serviço e conteúdo de mensagens em contatos, demonstrações, newsletter e suporte. Na contratação, tratamos os dados necessários do cliente, representante e responsável financeiro, como identificação, endereço, dados fiscais, informações de cobrança e registros de pagamento. Dados empresariais também podem identificar pessoas naturais, como empresários individuais e contatos nominativos.

No cadastro e uso da plataforma, tratamos identificação de usuários, e-mail, vínculo com organizações, papéis, permissões e informações necessárias à autenticação e recuperação de conta. Credenciais são protegidas por mecanismos próprios; não devem ser enviadas em chamados ou mensagens. Dados de autenticação adicional dependem do recurso habilitado.

3.2 Dados gerados durante o uso

Podem ser registrados endereço IP, data e hora, características do navegador e dispositivo, informações de sessão, eventos de autenticação, ações relevantes, falhas, preferências e registros de auditoria. Tais dados permitem operar o serviço, investigar acesso não reconhecido, proteger contas e demonstrar operações realizadas.

Podemos tratar informações de navegação, páginas e eventos de uso mediante tecnologias de medição identificadas na seção de cookies. Monitoramento de erros pode incluir metadados técnicos, aplicando redução e filtragem de conteúdo. Não se presume autorização para registrar o conteúdo completo de documentos, senhas ou formulários em ferramentas de análise.

3.3 Dados tratados por conta de empresas clientes

Os módulos podem receber cadastros profissionais; solicitações e respostas de titulares; consentimentos; preferências de cookies; documentos e contratos; dados de fornecedores; registros de incidentes; avaliações de risco e conformidade; anexos; tarefas; e evidências de operação. O conteúdo varia conforme a configuração e as informações inseridas pela empresa.

Treinamentos podem registrar nome, e-mail, vínculo profissional, matrícula, progresso, interações com aulas, respostas, tentativas, notas e certificados. Simulações autorizadas de phishing podem registrar destinatário, envio, entrega, interação e resultados técnicos. A empresa deve explicar o uso desses dados aos participantes e definir permissões e retenção. Simulações não devem coletar senhas reais.

Documentos e campos livres podem conter dados sensíveis ou informações de crianças e adolescentes. A inserção só deve ocorrer quando necessária, lícita e compatível com o módulo e suas salvaguardas. Esses dados não são exigidos de forma geral para contratar a plataforma.

3.4 Origem dos dados

Recebemos dados do próprio titular, de administradores e consultores autorizados, de empresas clientes, de prestadores necessários ao serviço e de integrações habilitadas, além dos registros técnicos gerados durante o uso. A origem e a finalidade de cada fluxo devem ser compatíveis com o contexto informado ao titular.

4. Para que usamos dados e com que fundamento

4.1 Contatos, demonstrações e diagnóstico

Usamos identificação, contato e informações fornecidas para responder mensagens, demonstrar o produto, produzir diagnóstico solicitado e conduzir negociações. Dependendo da relação com a pessoa, o fundamento pode ser procedimento preliminar solicitado por ela, execução de contrato ou legítimo interesse na comunicação empresarial pertinente, sujeito à análise de necessidade, expectativas e direitos.

Diagnósticos podem produzir pontuações e recomendações a partir de respostas da organização. Esses resultados são indicativos e exigem avaliação humana. Se houver processamento externo por IA, aplica-se a seção 8, com informação sobre o fluxo e minimização.

4.2 Cadastro, prestação e suporte

Dados necessários à conta, comunicação operacional e suporte são tratados para executar a relação com o titular quando ele for parte do contrato. Para usuários e representantes de contratos empresariais, avaliamos o fundamento adequado, inclusive legítimo interesse em disponibilizar e administrar o serviço solicitado pela organização. A base contratual não é aplicada automaticamente a qualquer pessoa mencionada por um cliente.

4.3 Cobrança e cumprimento de obrigações

Tratamos dados de representantes, cobrança, transações e documentos fiscais para pagamento, gestão contratual e obrigações legais ou regulatórias. Registros necessários à defesa de direitos podem ser conservados para exercício regular de direitos em procedimentos judiciais, administrativos ou arbitrais.

4.4 Segurança e prevenção de fraude

Registros técnicos e de acesso são usados para proteger contas, investigar incidentes e evitar uso indevido. Aplicamos obrigações legais quando existentes e legítimo interesse sujeito a avaliação e salvaguardas quando adequado. Dados sensíveis eventualmente necessários à identificação ou autenticação exigem hipótese específica do art. 11 da LGPD; não são tratados com base genérica em legítimo interesse.

4.5 Comunicação facultativa e melhoria

Newsletter e comunicações promocionais facultativas devem respeitar a escolha informada, com consentimento quando adotado para essa finalidade e mecanismo de descadastro. Contatos empresariais pertinentes eventualmente fundamentados em legítimo interesse devem ser proporcionais

e permitir oposição. Mensagens essenciais de segurança, faturamento e execução contratual têm finalidade distinta e podem continuar enquanto necessárias.

Medições opcionais de navegação utilizam consentimento conforme a seção 6. Melhorias podem utilizar dados efetivamente anonimizados e avaliações técnicas minimizadas. Não vendemos dados pessoais ou os disponibilizamos a terceiros para publicidade independente.

4.6 Operações da empresa cliente

Nos dados tratados como operadores, executamos instruções documentadas da controladora. A empresa cliente deve definir a hipótese legal de sua operação, inclusive regras próprias para dados sensíveis e de menores. O aceite da contratação pela empresa não substitui o fundamento necessário para tratar dados de outras pessoas.

Dados estritamente necessários são identificados no fluxo correspondente. A falta de informação obrigatória pode inviabilizar cadastro, suporte seguro ou contratação. Recusar finalidades opcionais não deve impedir o acesso às funções essenciais nem gerar tratamento discriminatório.

5. Com quem os dados podem ser compartilhados

5.1 Acesso autorizado

Equipes e prestadores autorizados da Befavos acessam apenas o necessário a suas funções, com dever de sigilo. Administradores e consultores autorizados do cliente podem acessar informações de sua organização conforme permissões. A empresa deve informar aos usuários quais gestores acompanham atividades e evidências.

5.2 Prestadores e integrações

O serviço pode envolver infraestrutura de hospedagem e armazenamento, proteção de tráfego, entrega de e-mails, pagamentos e observabilidade. As integrações identificadas no produto incluem Mercado Pago para pagamentos; Cloudflare para serviços de tráfego e armazenamento quando utilizados; Resend para mensagens e Mailtrap como contingência quando configurada; Sentry para monitoramento de erros; Google Analytics para medição de navegação; e Google Gemini no recurso de diagnóstico com IA quando habilitado.

Dados enviados são limitados à função: processadores de pagamento recebem informações necessárias ao pagamento; serviços de mensagens recebem destinatário e conteúdo necessário à entrega; ferramentas técnicas recebem metadados compatíveis; e IA deve receber apenas o contexto mínimo informado. A existência de integração no produto não significa que todos esses fornecedores recebam todos os dados ou que estejam ativos em cada ambiente.

A relação vigente de prestadores com função de operador ou suboperador, países, categorias de dados e garantias deve ser disponibilizada ao cliente antes da ativação do tratamento e pode ser solicitada ao encarregado. Prestadores que tratam dados para finalidades próprias, como deveres regulatórios de pagamentos, atuam conforme seu papel efetivo e seus avisos; isso não afasta nossa responsabilidade pelo compartilhamento que realizamos.

Integrações escolhidas pelo cliente seguem suas autorizações e configuração. Antes de habilitar ferramenta externa, o administrador deve verificar finalidade, permissões e aviso aplicável. Não autorizamos compartilhamento indiscriminado.

5.3 Autoridades e operações societárias

Podemos fornecer informações quando exigido por lei, ordem judicial ou requisição válida de autoridade competente, limitadas ao necessário e respeitadas as regras especiais de registros de acesso. Também podemos preservar evidências para exercício regular de direitos.

Em reorganização societária, aquisição ou transferência da operação, dados necessários poderão ser transmitidos ao sucessor, com proteção, transparência e continuidade das finalidades legítimas. Nova finalidade incompatível exige fundamento próprio e informação ao titular.

5.4 Publicações autorizadas

Políticas, formulários, páginas de consentimento, links documentais e verificação de certificados podem tornar informações acessíveis ao público ou a destinatários definidos pela empresa cliente. A publicação depende do propósito do recurso e da configuração autorizada; não torna públicos, por padrão, os demais dados do ambiente. O cliente deve evitar divulgação excessiva de nomes, assinaturas ou documentos.

6. Cookies e tecnologias semelhantes

Utilizamos cookies ou armazenamento equivalente para autenticação, segurança, continuidade da sessão e preferências. Recursos opcionais de estatística e marketing devem ser identificados separadamente, com finalidade, responsável e duração no painel de preferências.

O site contém integração com Google Analytics. Cookies e tecnologias opcionais de medição devem ser ativados somente após escolha válida quando dependam de consentimento. O fluxo deve permitir aceitar, rejeitar ou revisar categorias opcionais com facilidade equivalente e sem opções pré-selecionadas. A presença do banner, isoladamente, não garante que scripts estejam bloqueados.

Você pode revisar escolhas pelo mecanismo de preferências disponibilizado e também gerenciar cookies no navegador. Bloquear cookies estritamente necessários pode afetar login e funções essenciais. Para solicitar informações sobre as escolhas ou comunicar dificuldade no controle, utilize dpo@lgpdcloud.com.br.

Um banner instalado por empresa cliente em seu próprio site reflete as categorias e fornecedores definidos por ela. A política desse cliente deve explicar os tratamentos de seu site. Não presumimos que sua configuração seja idêntica à do site LGPLDCloud.

7. Armazenamento, transferências e retenção

7.1 Localização e transferência internacional

Dados podem ser processados na infraestrutura da Befavos e em serviços contratados. Serviços globais de tráfego, e-mail, observabilidade, estatística ou IA podem envolver processamento fora do Brasil, inclusive acesso remoto internacional. O local de processamento depende do serviço ativado; não há compromisso geral de residência exclusiva no Brasil.

Uma transferência internacional deve ter mecanismo válido da LGPLD e da regulamentação da ANPD, com transparência sobre finalidade, destinatários, países e garantias. Quando adotadas, as cláusulas-padrão contratuais devem ser incorporadas integralmente e preenchidas com o importador. Esta Política não substitui esse instrumento nem representa consentimento específico para transferência.

As informações específicas de transferência - finalidade, duração, países, destinatários, responsabilidades, medidas de segurança e direitos - devem acompanhar o fluxo ativado e ficar disponíveis em português pelo canal do encarregado e no aviso público aplicável. Quando forem adotadas cláusulas-padrão contratuais da ANPD, você pode solicitar seu inteiro teor, que será fornecido em até 15 dias, ressalvado prazo regulamentar distinto. A proteção de segredos comerciais não pode impedir acesso às garantias e informações legalmente asseguradas.

7.2 Critérios e prazos

Conservamos dados pelo tempo necessário à finalidade e às obrigações aplicáveis, com restrição de acesso após o encerramento quando necessária preservação. Prazos distintos são aplicados a cadastro, transações, segurança, evidências e telemetria; não adotamos prazo único para todos os dados.

Registros de acesso à aplicação sujeitos ao Marco Civil da Internet devem ser mantidos por seis meses, sob sigilo, podendo haver preservação específica por fundamento legal. Metadados de sessão usados para investigação de acessos possuem regra operacional de expiração de 90 dias após o encerramento da sessão; esses metadados não substituem os registros legais de acesso.

Cadastros e informações operacionais próprios são conservados enquanto necessários à relação e, após seu término, apenas na extensão justificada por obrigações, defesa de direitos ou atendimento pendente. Documentos fiscais seguem os prazos legais de sua categoria. Registros de incidentes observam a conservação regulamentar aplicável, por no mínimo cinco anos, inclusive incidentes não comunicados, ou prazo regulamentar superior aplicável. Contatos promocionais são mantidos enquanto houver finalidade legítima e escolha válida; a prova mínima do descadastro pode ser conservada para evitar novos envios indevidos.

Dados sob nossa operação para um cliente seguem suas instruções de retenção. Na contratação padrão, há janela de 30 dias após o término para solicitar exportação; o descarte operacional ocorre em até 60 dias após essa janela ou confirmação de entrega; resíduos de backup são removidos no ciclo aplicável em até 90 dias após o descarte operacional, resultando em prazo padrão máximo de 180 dias após o encerramento, ressalvada conservação legal específica e justificada. Esses prazos não afastam atendimento mais breve de direito legalmente exigível. Condição específica mais protetiva ou validamente negociada deve ser informada.

Evidências de auditoria, consentimentos, treinamentos e certificados podem exigir preservação distinta da telemetria. Permanência de evidência não implica exposição pública ilimitada ou conservação eterna de dados nominativos. A controladora deve definir prazo, finalidade probatória e eventual anonimização. Em exclusão ou anonimização, preservações excepcionais serão explicadas, sem conservar todo o ambiente por conveniência.

8. Inteligência artificial e decisões automatizadas

O diagnóstico pode utilizar Google Gemini quando habilitado para elaborar sugestões a partir de identificação da organização, pontuações e achados de conformidade. Texto livre pode conter informação pessoal ou confidencial e exige minimização. A integração e as condições comerciais efetivamente utilizadas devem ser informadas antes do envio de tais dados.

Outros recursos de IA externa exigem avaliação prévia, identificação do fornecedor e das categorias enviadas, instruções compatíveis e garantias de proteção, retenção e transferência. Não autorizamos treinamento de modelos gerais de terceiros com dados de clientes; a ativação com esses dados exige contrato compatível com essa restrição. Se essas garantias não existirem, o recurso deve operar sem dados pessoais ou informações confidenciais identificáveis, ou permanecer desativado para esse uso.

Pontuações, detecção de eventos e recomendações são recursos de apoio. A organização deve avaliar contexto, qualidade e limitações antes de decisões que afetem pessoas. O usuário pode solicitar informações sobre critérios e procedimentos e revisão de decisões tomadas unicamente com base em tratamento automatizado que afetem seus interesses, nos termos legais e com proteção dos segredos comerciais e industriais.

9. Crianças, adolescentes e dados sensíveis

O site comercial e a contratação são dirigidos a adultos. Empresas podem, em situações legítimas, utilizar módulos para aprendizes ou tratar informações de dependentes ou outros menores. Esses tratamentos exigem necessidade, hipótese legal aplicável, melhor interesse e salvaguardas apropriadas. A hipótese legal deve ser definida para cada operação; quando exigido consentimento, serão observadas suas condições específicas. Nos recursos destinados ou provavelmente acessados por menores, aplicam-se também as salvaguardas do Estatuto Digital da Criança e do Adolescente e de sua regulamentação, conforme o contexto e o risco.

Dados de saúde, biometria, origem racial, convicções e outras categorias sensíveis requerem fundamento específico e acesso restrito. Não solicitamos essas informações como requisito geral de demonstração ou assinatura. Se identificarmos tratamento incompatível, cooperaremos com a controladora para restringir, corrigir ou eliminar dados de forma segura, preservando obrigações legais e direitos. A identificação de dado de menor não autoriza sua destruição automática sem avaliação do contexto.

10. Como protegemos dados e respondemos a incidentes

Empregamos controles proporcionais de autenticação, permissões, segregação lógica de organizações, proteção das comunicações, credenciais, registros de operações, redução de informações em telemetria e resposta a incidentes. Cópias, recuperação e controles específicos seguem a documentação operacional aplicável. A Befavos mantém registros das operações de tratamento e revê suas medidas de proteção conforme o risco e a evolução técnica.

Nenhum sistema elimina todos os riscos. Essa circunstância não afasta nosso dever de segurança, prevenção, correção e responsabilidade. A proteção também depende de usuários manterem dispositivos seguros, acessos individuais e atenção a tentativas de fraude.

Nos incidentes envolvendo dados próprios em que sejamos controladores, avaliaremos risco e realizaremos comunicações obrigatórias. Quando atuarmos como operadores, avisaremos a empresa cliente conforme o Anexo de Tratamento de Dados, sem demora injustificada e em até 24 horas após ciência de comprometimento de dados pessoais. A controladora deverá avaliar comunicações à ANPD e aos titulares, observando os prazos legais, inclusive o prazo geral de três dias úteis quando aplicável.

11. Seus direitos e como exercer esses direitos

Você pode solicitar, conforme as condições legais: confirmação de tratamento e acesso; correção de dados; anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade; portabilidade conforme regulamentação; informação sobre compartilhamentos; informação sobre possibilidade de não consentir e suas consequências; revogação de consentimento; eliminação de dados tratados com consentimento, ressalvadas conservações legais; oposição a tratamento irregular; e revisão e informações sobre decisões exclusivamente automatizadas que afetem seus interesses.

Pedidos podem ser enviados gratuitamente a dpo@lgpdcloud.com.br. Informe seu nome, contato, relação com a plataforma e direito pretendido. Poderemos solicitar confirmação proporcional de identidade ou representação para evitar entrega indevida de dados. Não exigiremos senha nem documentação excessiva. Os direitos não dependem de plano pago.

Pedidos de confirmação ou acesso serão atendidos imediatamente em formato simplificado ou, por declaração completa, em até 15 dias contados da solicitação, conforme o art. 19 da LGPD. Outros pedidos seguem os prazos legais e regulamentares aplicáveis, com explicação de providências, impedimentos e informações complementares necessárias. A validação de identidade não autoriza postergação injustificada do atendimento.

Se o pedido envolver dados de uma empresa cliente sobre os quais atuamos como operadores, indicaremos a controladora quando possível e encaminharemos o pedido de forma segura em até dois dias úteis, auxiliando-a na execução e informando o encaminhamento. Nos dados próprios da Befavos, responderemos diretamente. Uma recusa ou retenção excepcional deve indicar fundamento e alcance, sem negativa genérica. Quando cabível, comunicaremos correção, eliminação, anonimização ou bloqueio aos agentes com quem compartilhamos os dados para que repitam a providência, ressalvadas as exceções legais comprovadas.

Você pode apresentar petição à Agência Nacional de Proteção de Dados (ANPD) e utilizar os demais meios legais, inclusive órgãos de defesa do consumidor quando cabíveis. Recomendamos contato inicial para solução do pedido; ele não elimina o direito de recorrer às autoridades.

12. Atualizações e outros ambientes

Manteremos identificação de versão e data. Alterações relevantes nas práticas serão comunicadas por canal adequado antes de sua adoção, salvo exigência legal ou urgência justificada. Se uma finalidade depender de consentimento novo ou específico, a simples publicação da Política não o substitui. Versões anteriores poderão ser solicitadas ao encarregado.

Links externos podem levar a ambientes com responsáveis e avisos próprios. Avalie o destino antes de fornecer informações. Essa orientação não afasta nossa responsabilidade por integrações e compartilhamentos realizados por nós.

Aplica-se a legislação brasileira, especialmente a LGPD e as regras da ANPD. Esta Política não impõe renúncia a direitos de titulares, foro obrigatório para solicitações de privacidade ou limitação de atuação de autoridades.