

PROTEÇÃO DE DADOS PESSOAIS NA BIOGENESES

Política de Privacidade

VERSÃO 2.0

Esta Política explica o tratamento de dados pessoais relacionado aos serviços da BIOGENESES TECHNOLOGY LTDA, CNPJ nº 48.151.976/0001-91, com sede em São Miguel do Oeste/SC. Aplica-se ao site, às contas, aos dispositivos vinculados, aos módulos e às integrações utilizados conforme a contratação e a configuração.

A versão 2.0 foi publicada em 9 de outubro de 2026. A Política é instrumento de transparência, não autorização irrestrita para coleta, compartilhamento ou uso de dados. O tratamento deve ter finalidade, necessidade, base legal e salvaguardas compatíveis com a Lei nº 13.709/2018 - LGPD e demais normas aplicáveis.

Recursos e fluxos variam entre módulos. Referências a integração ou categoria explicam o tratamento quando utilizado, sem afirmar que todo usuário esteja sujeito a todos os fluxos. Informações específicas podem ser solicitadas a contato@biogeneses.com.br.

1. IDENTIDADE E PAPÉIS NO TRATAMENTO

A Biogeneses é controladora dos tratamentos cujas finalidades e meios essenciais determina, como cadastro e gestão de suas contas, segurança, relacionamento comercial, faturamento e obrigações próprias. Seu canal de privacidade é contato@biogeneses.com.br; o WhatsApp de atendimento é +55 49 99100-9100.

Para conteúdos operacionais inseridos pelo Cliente, este pode ser controlador e a Biogeneses operadora, quando os trata em seu nome segundo instruções lícitas. O papel depende da atividade concreta, não apenas do nome contratual. A Biogeneses pode ser controladora de finalidade distinta no mesmo ambiente, que deve ser identificada e justificada.

O Cliente não substitui titulares nem renuncia aos direitos deles. A Biogeneses deve respeitar instruções válidas, auxiliar obrigações pertinentes e não usar conteúdos para finalidade incompatível. Se um pedido exigir atuação do Cliente controlador, deve haver orientação e cooperação, sem recusa genérica baseada na divisão de papéis.

2. ESCOPO, NECESSIDADE E PRINCÍPIOS

A Política abrange pessoas relacionadas a contas, equipes, contatos de notificação, clientes, fornecedores, operadores e portais, na medida em que os módulos realizem o tratamento. Dados de empresa ou equipamento são pessoais quando relacionados a pessoa natural identificada ou identificável; contexto e possibilidade de vinculação importam.

Coleta e uso devem observar finalidade, adequação, necessidade, qualidade, transparência, segurança, prevenção, não discriminação e responsabilização. Acesso deve limitar-se à função. Informação em fonte pública não perde sua proteção nem autoriza reutilização incompatível com a finalidade da divulgação.

O Cliente deve evitar dados desnecessários em nomes de equipamentos, campos livres, anexos, mensagens e relatórios. Serviços que demandem dados de saúde, pacientes ou outras categorias sensíveis exigem avaliação, contratação e instruções adequadas, com salvaguardas próprias. Não há autorização genérica para qualquer conteúdo pessoal.

3. CATEGORIAS DE DADOS

Identificação e vínculo

Nome, CPF, CNPJ, instituição ou empresa vinculada, endereço e campos necessários ao fluxo de cadastro, contrato, operação ou faturamento.

Contato e relacionamento

E-mail, telefone/WhatsApp, contatos adicionais, preferências, suporte e mensagens necessárias às comunicações habilitadas.

Acesso e segurança

Conta, sessão, permissões, códigos ou tokens de verificação, credenciais e informações de autenticação, IP e navegador/dispositivo.

Perfil

Foto obtida da integração com WhatsApp quando disponível; nome ou identificador usado na geração de avatar.

Equipamentos e operação

Serial, MAC, hardware, leituras, eventos, configurações, comandos, rede e controle, quando vinculados a pessoas ou responsáveis.

Gestão, fiscal e pagamento

Dados de clientes, fornecedores e operadores, documentos, pagador, valores, vencimentos e conciliação, conforme módulos. Dados bancários dependem do meio e da operação.

Auditoria e localização técnica

Geração e consulta de documentos, períodos, conta, IP, navegador e geolocalização aproximada por IP; localização de tablet nos recursos habilitados que a utilizem.

Conteúdo sob instruções do Cliente

Dados de pessoas em registros, formulários e documentos, inclusive sensíveis apenas quando necessários e legitimamente abrangidos pelo serviço.

Uma leitura ambiental nem sempre identifica alguém; associá-la a conta ou responsável pode fazê-lo. Foto de perfil não é, por si só, cadastro biométrico para reconhecimento. Não se afirma captura automática de imagem, áudio ou biometria por todos os módulos. Tratamento dessa natureza exige informação e fundamento próprios.

4. ORIGENS E MODOS DE COLETA

Dados podem ser fornecidos em cadastro, contratação, configurações, suporte e operação; recebidos do Cliente sobre pessoas de sua equipe ou atividade; ou gerados por dispositivos, acesso, auditoria e funcionalidades. O Cliente deve ter fundamento para dados de terceiros e informar-lhes o tratamento, sem presumir que seu próprio aceite vincule todos os titulares.

Consultas de CEP e CNPJ podem utilizar ViaCEP e BrasilAPI conforme o formulário. Mensageria pode fornecer informações do número de WhatsApp, inclusive foto quando disponível. Validar contato por código não garante correção de todos os dados cadastrais.

Localização por IP é estimativa que pode refletir provedor, proxy ou rede, não posição física exata. Localização de tablet habilitada depende do dispositivo e de suas permissões. Limites de precisão devem orientar o uso; não se presume rastreamento contínuo de todo usuário.

5. FINALIDADES E BASES LEGAIS

Cadastro e execução

Identificar a parte e prestar serviço solicitado: contrato ou procedimentos preliminares a pedido do titular, quando cabível; representantes e terceiros que não sejam parte exigem avaliação da base pertinente.

Vínculos e suporte

Permissões, atendimento e continuidade: contrato quando pertinente, ou legítimo interesse com necessidade, expectativas e avaliação dos direitos afetados.

Segurança

Proteger contas, apurar acessos e prevenir fraude: legítimo interesse ponderado, exercício de direitos ou obrigação legal concreta, conforme a operação.

Faturamento

Documentos, conciliação e obrigações fiscais/contábeis efetivas: execução contratual e obrigação legal identificável, na extensão necessária.

Prova e defesa

Registros necessários à apuração e ao exercício regular de direitos: fundamento correspondente, acesso e retenção limitados.

Notificações operacionais

Informações necessárias e alertas configurados: base adequada à relação e à função, legitimidade dos contatos adicionais e transparência dos canais.

Comunicações comerciais opcionais

Publicidade conforme preferência: consentimento específico quando adotado ou exigido; outro fundamento requer análise própria, informação e oposição cabível.

Conteúdo e dados sensíveis

Instruções lícitas do controlador e bases da finalidade; sensíveis requerem hipótese específica do art. 11 da LGPD, indispensabilidade e salvaguardas.

Aceite de termos ou ciência desta Política não autorizam todo tratamento indistintamente. Consentimento necessário deve ser livre, informado, específico, demonstrável e separado de finalidades não necessárias ao serviço. Pode ser revogado pelos meios disponíveis ou pelo canal, sem prejuízo de análise de outra base legítima para retenção ou finalidade distinta.

Legítimo interesse não serve automaticamente a qualquer uso, exige necessidade e balanceamento e não substitui hipóteses de dados sensíveis. Obrigação legal deve corresponder a exigência efetiva; citar norma sanitária não impõe CPF em todo relatório.

6. AUTENTICAÇÃO, PERFIL E ACESSO

Fluxos podem usar códigos por e-mail ou WhatsApp, sessões, permissões e credenciais próprias. Cadastro e login não utilizam necessariamente os mesmos canais ou controles. IP, navegador e registros auxiliam segurança e apuração, sem constituir prova absoluta de identidade ou localização.

Foto disponível pelo WhatsApp pode apresentar o perfil. Avatar alternativo pode ser gerado a partir de nome ou identificador, conforme a seção de fornecedores. Não se declara reconhecimento biométrico a partir dessa apresentação.

Os métodos de autenticação e as medidas de proteção das credenciais variam conforme o serviço e o equipamento. Senhas, códigos e outros dados de autenticação recebem controles de acesso e proteção compatíveis com sua finalidade e risco. O usuário deve preservá-los e utilizar os canais de suporte adequados, evitando sua divulgação em relatórios públicos ou ambientes sem proteção.

7. COOKIES, ARMAZENAMENTO LOCAL E ESCOLHAS

Cookies e tecnologias semelhantes são utilizados conforme o módulo para sessão, segurança e preferências. A sessão principal segue a configuração do ambiente. Módulos podem usar nomes próprios, como BIOGENESES_CONTACT no contato e HRTGBSESSID no HRTGB. Presença e nomes variam com os fluxos e ajustes técnicos compatíveis.

Sessão e segurança

Mantêm autenticação, estado e proteção. Bloqueá-los pode impedir acesso ou conclusão de funcionalidades. Necessidade é avaliada pela finalidade, não pelo nome do cookie.

Conveniência

identificador_sessao e metodo_sessao podem facilitar retorno ao login após expiração; telefone_sessao pode aparecer em fluxos legados. Não substituem verificações de acesso.

Armazenamento no navegador

Tema, modelos e estado de trabalho podem usar localStorage ou sessionStorage nos módulos correspondentes. Excluir armazenamento pode remover preferências ou trabalho não transmitido.

Recursos externos

Fontes, avatares e proteção de formulário podem receber dados técnicos e usar tecnologias próprias, conforme o recurso carregado.

O usuário pode consultar, bloquear e excluir armazenamento pelos controles do navegador e ajustar as preferências disponíveis no serviço. Quando tecnologias não necessárias dependerem de consentimento, a escolha deve ser informada e específica, com possibilidade de revogação. A exclusão ou o bloqueio de tecnologias necessárias pode afetar o acesso e o funcionamento de recursos. Dúvidas, pedidos e ajustes que não estejam disponíveis na interface podem ser encaminhados ao canal de privacidade.

8. MENSAGENS, ALERTAS E PREFERÊNCIAS

E-mail, WhatsApp, SMS e canais integrados podem transmitir códigos, suporte, cobrança e alertas. O tratamento inclui destinatário, conteúdo, fila e registros de entrega quando disponíveis. Dados enviados a grupo ou contato podem ser acessados por seus participantes; o Cliente deve configurar destinatários e conteúdo de modo proporcional.

Preferências comerciais devem ser respeitadas por canal e finalidade. Cancelar publicidade não encerra automaticamente a conta ou elimina dados, nem cancela por si só mensagens estritamente necessárias à prestação em curso. Pode-se solicitar esclarecimento e revisão das preferências e exercer os direitos cabíveis.

Contatos adicionais precisam de informação e fundamento adequado. O Cliente não impõe consentimento genérico em nome deles. Canal de alarme e de privacidade têm funções distintas; falha de entrega não elimina atendimento de direitos ou comunicação de incidente legalmente exigida.

9. FORNECEDORES E COMPARTILHAMENTO

Hospedagem e e-mail	Infraestrutura e SMTP, incluindo Hostinger conforme configuração, para aplicações, armazenamento e mensagens. Acesso depende da função e dos controles pertinentes.
Mensageria	n8n e gateways/integradores de WhatsApp, incluindo Evolution quando usado, para fluxos habilitados. Esses componentes não comprovam integração oficial com API da Meta.
Pagamento e cobrança	Instituições do meio escolhido, inclusive Banco do Brasil em boleto ou Pix habilitado, recebem dados de pagador e transação necessários à operação e suas obrigações.
Consulta e formulário	ViaCEP, BrasilAPI e Cloudflare Turnstile, quando utilizados, recebem consulta ou dados técnicos necessários. Turnstile depende da habilitação e configuração.
Apresentação web	ui-avatars pode receber nome ou identificador na URL e dados de navegador, como IP, ao carregar avatar. CDNs e fontes externas, inclusive rsms.me quando carregada, recebem requisições e dados técnicos pertinentes.
Localização por IP	ipwho.is pode receber IP público nos fluxos de auditoria de relatórios que consultam geolocalização aproximada. O resultado pode ficar em cache; não comprova localização física exata.
Pessoas autorizadas	Cliente, administradores, responsáveis, destinatários e usuários de portais acessam conforme permissão e finalidade. Exportar ou enviar documento amplia destinatários conforme a operação autorizada.

Autoridades e direitos Divulgação necessária a obrigação, requisição válida ou exercício de direitos exige avaliação de legitimidade, necessidade e limites.

Fornecedores variam com módulo e contratação. Compartilhamento deve limitar-se à finalidade e ser acompanhado de medidas e instrumentos adequados ao papel de cada participante. Integração não autoriza divulgação irrestrita. Controladoria independente, operação e suboperação devem ser avaliadas em cada atividade.

Não se autoriza venda de dados pessoais ou uso incompatível. Novas finalidades e destinatários relevantes exigem avaliação e transparência, com consentimento ou requisitos específicos quando legalmente necessários. Detalhes do fluxo podem ser solicitados, preservados direitos e segurança de terceiros.

10. RELATÓRIOS, AUDITORIA, PORTAIS E LOCALIZAÇÃO

Geração, consulta e compartilhamento de documentos podem registrar conta, nome e cadastro pertinente, instituição, equipamento, período, sessão, IP e navegador. Fluxos habilitados podem enriquecer auditoria com localização aproximada por IP. Rastreabilidade não torna todo dado cadastral necessário a qualquer destinatário.

Portais, relatórios e mensagens devem expor informações compatíveis com finalidade e permissão. O Cliente deve evitar dados desnecessários em documentos distribuídos. Um relatório não deve conceder acesso irrestrito a outros clientes ou a segredos de autenticação.

Localização operacional de tablet, quando habilitada, deve limitar-se à finalidade, às permissões e ao módulo pertinente. Não se afirma GPS contínuo em todas as páginas nem biometria de operadores. Identificação, matrícula e registros de atuação permanecem sujeitos à necessidade e às instruções lícitas.

11. DADOS SENSÍVEIS, CRIANÇAS E ADOLESCENTES

Saúde e outros dados sensíveis não são necessários ao simples monitoramento ambiental em toda contratação. Se o serviço legitimamente os abranger, o controlador deve identificar hipótese do art. 11 da LGPD, demonstrar necessidade e aplicar controles. Operação depende de instruções e escopo válidos; a Biogeneses deve avaliar instruções incompatíveis com a lei, sem tratá-las como autorização irrestrita.

Cadastro contratual não é direcionado intencionalmente a crianças. Conteúdo de Cliente pode envolver crianças ou adolescentes em operação legítima. Prevalecem melhor interesse, fundamento apropriado, transparência adequada e participação ou autorização de responsáveis quando exigida. A presença de dados não autoriza exploração promocional ou tratamento excessivo.

Dados sensíveis ou de menores fora da finalidade ou sem fundamento exigem avaliação de restrição, regularização, comunicação ao controlador e eliminação cabível. Proibição genérica de conteúdo não afasta deveres sobre dados efetivamente recebidos.

12. RETENÇÃO, ELIMINAÇÃO E BACKUPS

Retenção considera finalidade, contratação, necessidade operacional e obrigações legais concretas. Não há prazo único para cadastro, leituras, documentos, logs e backups. Encerramento ou revogação não autorizam retenção indefinida; conservação permitida exige fundamento e limites identificados no atendimento.

Conta e atendimento

Durante a finalidade legítima e, depois, somente para conservação justificada. Dados desnecessários devem ser eliminados ou adequadamente anonimizados.

Acesso à aplicação

O art. 15 do Marco Civil prevê guarda mínima de seis meses para provedores sujeitos à obrigação, sob sigilo e segurança. A regra é observada quando aplicável; não define prazo de todos os dados.

Fiscal, cobrança e defesa

Prazos concretos da obrigação fiscal/contábil, preservação de prova e exercício de direitos, sem extensão além do fundamento.

Operação e leituras

Retenção ou agregação do módulo, contratação e necessidades legais do processo. O Cliente deve conhecer limites e preservar documentos sob sua responsabilidade.

Incidentes

A Resolução CD/ANPD nº 15/2024 prevê guarda mínima de cinco anos de seus registros, inclusive dos incidentes não comunicados, no âmbito do regulamento.

Backups

Cópias podem permanecer até ciclos de substituição e eliminação pertinentes, com acesso restrito e sem reutilização incompatível. Limites técnicos não autorizam retorno indiscriminado de dados cuja eliminação deva ser respeitada.

Pedidos devem alcançar tratamentos sob responsabilidade da Biogeneses e ser encaminhados ao controlador pertinente quando necessário. Conservação lícita exige explicação de categorias, razões e limites. Não se promete eliminação instantânea de todas as cópias ou um ciclo uniforme não verificado, nem se usa limitação técnica como justificativa genérica para negar direitos.

13. SEGURANÇA E DEVERES DE PROTEÇÃO

A Biogeneses deve adotar medidas técnicas e administrativas adequadas aos dados e riscos, incluindo gestão de acessos, autenticação, confidencialidade, integridade, atualização, auditoria e continuidade compatíveis com o serviço. Escolha e operação de fornecedores também devem considerar segurança e obrigações correspondentes.

Risco zero não existe, mas isso não elimina prevenir, corrigir, responder e reparar na forma legal. Não se afirma arquitetura, criptografia, certificação ou periodicidade de backup idênticas em todos os módulos. Informações pertinentes podem ser fornecidas sem expor segredos que facilitem abuso.

Cliente e usuários devem proteger acessos, revisar permissões, evitar dados excessivos e comunicar suspeitas. Cooperação não transfere integralmente a segurança da Biogeneses ou de outro agente. Cada participante responde conforme sua atuação e regime legal.

14. INCIDENTES E COMUNICAÇÃO

Suspeitas de acesso indevido, perda, alteração ou divulgação de dados devem ser comunicadas a contato@biogeneses.com.br com informações úteis, sem publicação de credenciais ou conteúdos alheios. A avaliação apura dados, riscos, contenção e necessidade de comunicação. Falha de internet, equipamento ou mensagem não prova, isoladamente, incidente com dados pessoais.

Quando puder haver risco ou dano relevante aos titulares, o controlador deve comunicar ANPD e pessoas afetadas no prazo aplicável. A regra geral da Resolução CD/ANPD nº 15/2024 é três dias úteis do conhecimento de que o incidente afetou dados pessoais, observados regimes e exceções efetivamente aplicáveis. Não se presume enquadramento da Biogeneses em prazo ampliado.

Investigação incompleta não autoriza adiar indevidamente comunicação obrigatória: devem ser observadas comunicação preliminar justificada, complementação e exigências do regulamento. Como operadora, a Biogeneses deve informar o controlador sem demora injustificada e cooperar. A comunicação deve ser clara e útil, sem esconder fatos relevantes por motivo reputacional.

15. DIREITOS DOS TITULARES

- Confirmar tratamento, acessar dados e corrigir informações incompletas, inexatas ou desatualizadas.
- Requerer anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou desconformes, e eliminação de dados tratados com consentimento nas hipóteses legais, ressalvadas conservações permitidas.
- Saber com quem houve compartilhamento, conhecer a possibilidade e consequências de não consentir e revogar consentimento quando utilizado.

- Solicitar portabilidade na forma da regulamentação, sem prejuízo dos demais direitos, observados segredos comercial e industrial nos limites legais.
- Opor-se a tratamento sem consentimento quando houver descumprimento da lei e exercer oposição ou preferência cabível à finalidade.
- Solicitar revisão de decisão unicamente automatizada que afete interesses e informações pertinentes sobre critérios e procedimentos, resguardados os limites legais.
- Peticionar à ANPD e aos órgãos competentes e buscar tutela judicial ou de defesa do consumidor quando aplicável.

Pedidos são gratuitos nos casos legais. Confirmação e acesso seguem o art. 19 da LGPD: resposta simplificada imediata ou declaração clara e completa em até quinze dias, conforme a hipótese. Outros pedidos observam regras próprias; esse prazo não autoriza postergar toda urgência ou obrigação distinta.

Identidade e legitimidade podem ser verificadas proporcionalmente para evitar exposição a terceiros, sem exigência excessiva ou impedimento artificial. Limitação, conservação ou impossibilidade concreta deve ter fundamento e orientação. Inadimplência não impede atendimento; propriedade intelectual não justifica recusa genérica de acesso aos próprios dados.

16. TRANSFERÊNCIAS INTERNACIONAIS

Hospedagem, comunicação, segurança e infraestrutura podem envolver tratamento em outros países ou acesso internacional conforme o fluxo real. A avaliação inclui destinatários e transferências posteriores. Nacionalidade de fornecedor ou menção a conformidade estrangeira não prova regularidade, sozinha.

Transferência sujeita à LGPD exige base legal e mecanismo válido, como adequação aplicável, cláusulas contratuais, normas corporativas ou outra hipótese pertinente. A Resolução CD/ANPD nº 19/2024 disciplina essas ferramentas. Cláusulas-padrão utilizadas devem ser validamente incorporadas; publicar a Política não substitui o instrumento necessário.

A adequação da Resolução CD/ANPD nº 32/2026 deve ser considerada dentro do próprio escopo, sem extensão automática a qualquer país, destinatário ou transferência subsequente. Não se presume consentimento para todo fluxo nem um mesmo instrumento já contratado para todos. Informações sobre finalidade, duração, países, agentes e salvaguardas devem ser disponibilizadas quando exigidas e podem ser solicitadas ao canal.

17. CANAL DE PRIVACIDADE E ENCARREGADO

**Responsável pelo
atendimento**

BIOGENESES TECHNOLOGY LTDA - CNPJ nº
48.151.976/0001-91 - São Miguel do Oeste/SC.

Direitos e privacidade contato@biogeneses.com.br

**Atendimento
complementar**

WhatsApp +55 49 99100-9100.

Informe pedido e meio de retorno com dados suficientes para localizar o contexto, sem documentos ou dados sensíveis desnecessários. O canal deve encaminhar a solicitação à equipe competente e, quando pertinente, ao Cliente controlador, sem impedir cooperação. Atualizações e justificativas devem ser acessíveis.

O canal de privacidade recebe solicitações sobre proteção de dados e permite obter informações sobre os responsáveis pelo atendimento. Quando a indicação de encarregado for exigida, sua identidade e seus contatos formais serão divulgados de maneira clara e acessível, conforme o art. 41 da LGPD e a Resolução CD/ANPD nº 18/2024. A identificação aplicável também poderá ser consultada por esse canal.

18. VERSÕES, RELATÓRIOS E GOVERNANÇA DOCUMENTAL

A Política deve refletir tratamentos, fornecedores e exigências relevantes. Alterações materiais precisam de comunicação adequada e, quando necessário, informação ou consentimento específico. Publicação não converte aceites antigos nem autoriza retroativamente finalidade incompatível. O histórico deve identificar documentos e versões correspondentes.

Relatórios e outros documentos podem referenciar os termos para esclarecer emissão, uso e contexto contratual. Governança documental deve preservar versão pertinente, finalidade, destinatários e autenticidade, sem atribuir valor regulatório ou autoria não comprovados.

Este documento está sujeito aos termos de uso da plataforma, disponíveis em https://www.biogeneses.com.br/termo_uso.php.

A remissão disciplina aspectos contratuais e não reduz direitos da LGPD, não transforma esta Política em consentimento genérico e não afasta obrigações dos agentes. Normas obrigatórias e direitos dos titulares prevalecem em caso de conflito.

BIOGENESES TECHNOLOGY LTDA - CNPJ 48.151.976/0001-91

São Miguel do Oeste/SC - contato@biogeneses.com.br

Documento vigente desde 09/10/2026. Gerado eletronicamente em 26/10/2026 13:01.