



Política de Privacidade

Versão completa revisada

Última atualização: 29 de maio de 2026

Documento público de privacidade, proteção de dados, segurança, verificação de idade, auditoria e conformidade.

Canal oficial de privacidade: privacidade@idadeid.com.br

Site oficial: www.idadeid.com.br

Resumo objetivo para titulares

A IdadeID é uma plataforma de verificação de idade e apoio à conformidade. Em geral, quando a solução é usada dentro do site, app, checkout, vending machine ou ambiente de um cliente, a IdadeID atua como Operadora, tratando dados conforme as instruções do cliente contratante, que normalmente é o Controlador.

A IdadeID busca coletar o mínimo necessário para verificar idade, prevenir fraude, proteger sessões técnicas e registrar eventos de auditoria. Como regra operacional, imagens faciais e documentos são tratados temporariamente e descartados após a análise, mantendo-se preferencialmente apenas metadados mínimos, como decisão, confiança, reason code, site_id, tenant_id, sessão e data/hora.

A IdadeID não vende dados pessoais, não utiliza dados de verificação para publicidade comportamental, não cria banco facial permanente e não permite que o navegador ou o widget decidam sozinho se uma verificação é válida. Validações críticas devem ocorrer no servidor e, em caso de falha relevante, a solução deve priorizar comportamento de falha segura.

Solicitações sobre dados pessoais, LGPD, incidentes ou privacidade devem ser enviadas ao canal oficial: privacidade@idadeid.com.br.

1. Introdução

A IdadeID é uma plataforma tecnológica de verificação de idade e apoio à conformidade, desenvolvida para auxiliar sites, plataformas, aplicativos, e-commerces, sistemas de checkout, pontos de venda digitais e demais ambientes digitais ou conectados na prevenção de acesso, cadastro, compra ou utilização indevida de produtos, serviços ou conteúdos sujeitos a restrição etária.

Esta Política de Privacidade descreve, de forma clara e transparente, como a IdadeID realiza o tratamento de dados pessoais no contexto da utilização de sua solução, incluindo dados coletados em processos de verificação de idade, dados técnicos de segurança, dados de auditoria, dados de clientes contratantes e dados de visitantes do site institucional.

A IdadeID adota como princípios orientadores a necessidade, a minimização de dados, a segurança da informação, a prevenção à fraude, a transparência, a responsabilização e a prestação de contas, nos termos da Lei Geral de Proteção de Dados Pessoais - LGPD, Lei nº 13.709/2018.

A solução da IdadeID é uma ferramenta tecnológica de apoio à verificação de idade e à gestão de risco. A decisão final sobre permitir, bloquear, restringir ou condicionar o acesso do usuário final a determinado site, serviço, conteúdo, compra ou funcionalidade caberá ao cliente contratante, observadas as obrigações legais, regulatórias, contratuais e setoriais aplicáveis ao seu próprio negócio.

Esta Política deve ser lida em conjunto com os Termos de Uso, contratos comerciais, aditivos de tratamento de dados, políticas específicas do cliente contratante e demais documentos aplicáveis à relação entre a IdadeID, seus clientes e os usuários finais.

2. Papel da IdadeID no tratamento de dados pessoais

A IdadeID poderá atuar como Operadora ou como Controladora de dados pessoais, conforme o contexto específico do tratamento realizado.

2.1 Atuação como Operadora de dados pessoais

No contexto da prestação dos serviços de verificação de idade aos seus clientes contratantes, a IdadeID atua predominantemente como Operadora de dados pessoais, nos termos da Lei Geral de Proteção de Dados Pessoais - LGPD.

Nessa hipótese, a IdadeID realiza o tratamento de dados pessoais em nome e segundo as instruções do cliente contratante, que, em regra, será o Controlador dos dados pessoais tratados no ambiente de seu site, aplicativo, plataforma, e-commerce, checkout, ponto de venda digital ou outro canal integrado à solução.

Como Operadora, a IdadeID poderá executar atividades técnicas necessárias à prestação do serviço, incluindo:

- a) coleta temporária de dados necessários ao processo de verificação de idade;
- b) processamento técnico de imagens, documentos ou dados informados, quando aplicável;
- c) geração de resultado técnico de verificação, como aprovação, negativa, inconclusão, necessidade de fallback ou indicador de risco;
- d) criação e validação de sessões técnicas de acesso;
- e) registro de eventos mínimos de auditoria, segurança, prevenção à fraude e rastreabilidade;
- f) suporte técnico à integração da solução com o ambiente do cliente contratante.

Nessa condição, a IdadeID não define a finalidade principal do tratamento, não escolhe o público final submetido à verificação, não determina quais produtos, serviços ou conteúdos exigem restrição etária e não toma a decisão comercial, jurídica ou regulatória final sobre permitir ou impedir o acesso do usuário final.

A decisão final sobre acesso, cadastro, compra, checkout, consumo de conteúdo, liberação de funcionalidade ou qualquer outra ação protegida caberá ao cliente contratante, observadas as leis, normas, regulamentos, políticas internas e obrigações setoriais aplicáveis ao seu negócio.

2.2 Atuação como Controladora de dados pessoais

A IdadeID poderá atuar como Controladora quando tratar dados pessoais para finalidades próprias, isto é, quando determinar diretamente os meios e finalidades do tratamento.

Isso poderá ocorrer, por exemplo, nas seguintes situações:

- a) gestão de cadastro de clientes, representantes, administradores e usuários do painel da IdadeID;
- b) gestão contratual, financeira, comercial, cobrança, faturamento e suporte;
- c) atendimento a solicitações enviadas por formulários, e-mail, canais comerciais ou canais de suporte;
- d) envio de comunicações institucionais, técnicas, operacionais ou comerciais relacionadas à IdadeID;

- e) segurança da própria plataforma, prevenção a fraudes, controle de acesso, logs administrativos e auditoria interna;
- f) cumprimento de obrigações legais, regulatórias, fiscais, contábeis ou determinações de autoridades competentes;
- g) melhoria, monitoramento e manutenção da plataforma, desde que observados os princípios da necessidade, minimização e segurança.

Nesses casos, a IdadeID será responsável por definir as finalidades do tratamento, adotar medidas adequadas de segurança, atender aos direitos dos titulares quando aplicável e cumprir as obrigações previstas na LGPD.

2.3 Responsabilidade do cliente contratante

O cliente contratante é responsável por definir a finalidade de uso da solução IdadeID em seu próprio ambiente digital ou físico, incluindo a identificação dos produtos, serviços, conteúdos, funcionalidades ou operações que exigem verificação de idade.

Também caberá ao cliente contratante:

- a) informar adequadamente seus usuários finais sobre o uso da solução IdadeID;
- b) indicar, quando necessário, a base legal aplicável ao tratamento realizado em seu ambiente;
- c) garantir que a utilização da solução seja compatível com sua própria Política de Privacidade, Termos de Uso e obrigações legais;
- d) configurar corretamente idade mínima, modo de verificação, regras de bloqueio, fallback e demais parâmetros disponíveis;
- e) evitar o uso da solução para finalidades incompatíveis, abusivas, discriminatórias, ilegais ou não informadas ao titular;
- f) decidir, sob sua responsabilidade, se determinado usuário final poderá ou não acessar, comprar, contratar ou utilizar determinado produto, serviço, conteúdo ou funcionalidade.

2.4 Instruções, limites e cooperação

A IdadeID tratará os dados pessoais de usuários finais conforme as instruções legítimas e documentadas do cliente contratante, os contratos aplicáveis, esta Política de Privacidade, eventuais aditivos de tratamento de dados e a legislação vigente.

A IdadeID poderá recusar, suspender ou limitar tratamentos solicitados pelo cliente contratante quando houver indícios de ilegalidade, abuso, violação de direitos de titulares, risco à segurança da plataforma, descumprimento contratual ou incompatibilidade com a LGPD.

Quando necessário, a IdadeID poderá cooperar com o cliente contratante para atendimento de solicitações de titulares, incidentes de segurança, auditorias, requisições de autoridades ou demais obrigações relacionadas à proteção de dados pessoais, observados os limites técnicos, legais e contratuais aplicáveis.

3. Escopo desta Política de Privacidade

Esta Política de Privacidade aplica-se ao tratamento de dados pessoais realizado pela IdadeID no contexto da disponibilização, operação, integração, manutenção, segurança e melhoria de sua plataforma de verificação de idade.

Esta Política se aplica, conforme o caso, aos seguintes públicos:

- a) usuários finais, isto é, pessoas que passam por processos de verificação de idade em sites, aplicativos, plataformas, e-commerces, checkouts, pontos de venda digitais, vending machines, sistemas de acesso ou outros ambientes integrados à solução IdadeID;
- b) clientes contratantes, incluindo empresas, representantes legais, administradores, colaboradores, operadores, parceiros comerciais e usuários autorizados que utilizam o painel, as APIs, os widgets, integrações, relatórios ou demais funcionalidades da IdadeID;
- c) visitantes do site institucional da IdadeID, incluindo pessoas que acessam páginas públicas, preenchem formulários, solicitam contato comercial, interagem com canais de atendimento ou demonstram interesse nos produtos e serviços da IdadeID;
- d) parceiros técnicos, comerciais e de integração, quando houver tratamento de dados pessoais necessário para viabilizar suporte, implantação, testes, integração, faturamento, segurança ou execução contratual.

Esta Política abrange, entre outras situações:

- a) processos de verificação de idade realizados por meio de selfie, imagem facial, análise técnica, inteligência artificial, documento ou outro método disponibilizado pela IdadeID;
- b) geração, validação e encerramento de sessões técnicas de acesso;
- c) registros de segurança, auditoria, prevenção à fraude, logs técnicos e eventos operacionais;
- d) uso do painel administrativo da IdadeID por clientes contratantes;
- e) integrações com plataformas externas, como e-commerces, sistemas de checkout, aplicativos, websites, APIs, plugins, widgets ou outros ambientes digitais;
- f) atendimento comercial, suporte técnico, billing, cobrança, comunicações operacionais e relacionamento com clientes;
- g) navegação no site institucional da IdadeID e utilização de formulários, páginas públicas e canais de contato.

Esta Política não substitui a Política de Privacidade, os Termos de Uso, avisos legais ou demais documentos próprios do cliente contratante. Quando a solução IdadeID for utilizada dentro de ambiente pertencente a um cliente contratante, esse cliente continuará responsável por informar seus usuários finais sobre as finalidades específicas do tratamento, a base legal aplicável, as regras de acesso ao seu serviço, produto ou conteúdo, bem como por cumprir suas próprias obrigações legais e regulatórias.

A IdadeID não se responsabiliza por tratamentos de dados realizados diretamente pelo cliente contratante, por plataformas terceiras, por meios de pagamento, por gateways, por sistemas de e-commerce, por ferramentas de marketing, por provedores externos ou por qualquer outro serviço que não esteja sob controle técnico, contratual ou operacional da IdadeID.

Caso o usuário final acesse a IdadeID por meio de site, aplicativo, plataforma ou canal de um cliente contratante, recomenda-se que também consulte a Política de Privacidade e os Termos de Uso desse cliente, pois poderão existir regras adicionais aplicáveis ao uso daquele ambiente.

4. Dados pessoais tratados pela IdadeID

A IdadeID adota os princípios da necessidade, adequação, minimização, segurança, prevenção e transparência no tratamento de dados pessoais, limitando a coleta e o processamento aos dados estritamente necessários para a verificação de idade, prevenção à fraude, segurança da sessão, auditoria técnica e cumprimento das obrigações contratuais e legais aplicáveis.

Os dados tratados podem variar conforme o tipo de integração utilizada pelo cliente contratante, o nível de risco do site, o modo de verificação configurado, a legislação aplicável ao segmento, a necessidade de fallback documental e as configurações técnicas da solução.

A IdadeID poderá tratar as seguintes categorias de dados pessoais:

4.1 Dados fornecidos ou capturados durante a verificação de idade

Durante o processo de verificação, a IdadeID poderá tratar dados fornecidos diretamente pelo usuário final ou capturados por meio da interface de verificação, sempre de forma proporcional à finalidade pretendida.

Esses dados podem incluir:

- a) imagem facial, selfie ou frame capturado durante o processo de verificação;
- b) imagem ou captura temporária de documento de identificação, quando aplicável como fallback ou etapa adicional de verificação;
- c) informações visíveis no documento necessárias para confirmação de idade, quando aplicável;
- d) respostas ou interações relacionadas a desafios de presença, liveness, movimentação, orientação facial ou validação antifraude;
- e) confirmação de consentimentos, ciência de avisos ou interação com telas de verificação, quando tecnicamente necessário;
- f) informações declaradas pelo usuário final, quando o fluxo exigir preenchimento manual de algum dado.

A IdadeID não tem como objetivo coletar dados excessivos, completos ou incompatíveis com a finalidade de verificação de idade. Sempre que possível, o tratamento será limitado à confirmação de que o usuário final atende ou não à idade mínima exigida pelo cliente contratante, sem necessidade de armazenamento permanente da imagem, do documento ou de dados completos de identificação civil.

4.2 Dados derivados do processo de verificação

A partir dos dados tratados no processo de verificação, a IdadeID poderá gerar informações técnicas ou inferidas necessárias para tomada de decisão, segurança, auditoria e prevenção à fraude.

Esses dados podem incluir:

- a) resultado da verificação, como aprovado, negado, inconclusivo, pendente ou fallback necessário;
- b) indicação de que o usuário aparenta ou comprova estar acima da idade mínima exigida;
- c) idade estimada ou faixa etária estimada, quando aplicável;
- d) pontuação ou score de confiança;

- e) indicadores de qualidade da captura, como baixa nitidez, iluminação inadequada, rosto ausente, documento ilegível ou imagem incompleta;
- f) indicadores de risco, fraude, spoofing, manipulação, inconsistência ou tentativa de burlar o processo;
- g) reason codes ou códigos técnicos de decisão, como imagem insuficiente, documento incompatível, falha de liveness, risco elevado ou verificação aprovada;
- h) metadados mínimos de auditoria relacionados ao resultado da verificação.

Sempre que possível, a IdadeID prioriza o armazenamento de metadados técnicos e registros de decisão, em vez do armazenamento das imagens originais utilizadas no processo.

4.3 Dados técnicos, de sessão e segurança

Para permitir o funcionamento seguro da solução, a IdadeID poderá tratar dados técnicos relacionados ao dispositivo, navegador, sessão, origem da requisição e ambiente de integração.

Esses dados podem incluir:

- a) endereço IP;
- b) data e hora da requisição;
- c) tipo de navegador, sistema operacional e dispositivo;
- d) identificadores técnicos de sessão;
- e) identificador do site, tenant, cliente contratante, integração ou ambiente de origem;
- f) domínio, origem, referer e parâmetros técnicos necessários para validação da integração;
- g) public key, site key ou identificadores públicos de integração;
- h) tokens temporários assinados, identificadores de sessão, jti, expiração e escopos de acesso;
- i) eventos técnicos de carregamento, validação, erro, timeout, bloqueio ou liberação;
- j) informações de rate limit, tentativa repetida, comportamento suspeito ou falha de validação;
- k) logs mínimos necessários para segurança, diagnóstico, auditoria, prevenção à fraude e melhoria operacional.

Esses dados são utilizados para proteger a integridade da verificação, reduzir tentativas de burla, validar domínios autorizados, impedir uso indevido da solução, evitar reutilização indevida de sessões e garantir rastreabilidade técnica.

4.4 Dados relacionados ao cliente contratante

Quando uma empresa contrata ou utiliza a IdadeID, poderão ser tratados dados pessoais de seus representantes, administradores, operadores, colaboradores ou usuários autorizados.

Esses dados podem incluir:

- a) nome e sobrenome;
- b) e-mail profissional;
- c) telefone ou canal de contato;
- d) cargo, função ou vínculo com a empresa;
- e) dados de login e autenticação no painel;

- f) permissões, perfil de acesso e histórico de ações administrativas;
- g) dados de cobrança, faturamento, plano contratado e uso da plataforma;
- h) comunicações comerciais, técnicas, contratuais ou de suporte;
- i) registros de atendimento, implantação, integração, solicitações e incidentes.

Esses dados são tratados para gestão contratual, suporte técnico, administração da conta, segurança da plataforma, faturamento, comunicação operacional, prevenção a fraude, cumprimento de obrigações legais e execução dos serviços contratados.

4.5 Dados de visitantes do site institucional

Quando uma pessoa acessa o site institucional da IdadeID, entra em contato, solicita demonstração, preenche formulário ou interage com canais comerciais, a IdadeID poderá tratar dados pessoais necessários para atendimento e relacionamento.

Esses dados podem incluir:

- a) nome;
- b) e-mail;
- c) telefone;
- d) empresa ou organização;
- e) cargo ou área de atuação;
- f) mensagem enviada pelo titular;
- g) origem do contato;
- h) dados técnicos de navegação estritamente necessários para segurança, funcionamento do site, estatísticas básicas e prevenção a abuso.

A IdadeID não utiliza esses dados para criar perfis comportamentais sensíveis, vender informações pessoais ou realizar rastreamento abusivo de titulares.

4.6 Dados de documentos, quando houver fallback documental

Em situações específicas, quando a verificação por selfie, imagem facial, liveness ou análise automatizada não for suficiente, o cliente contratante poderá configurar ou exigir etapa adicional de verificação documental.

Nesses casos, a IdadeID poderá tratar temporariamente imagem de documento de identificação ou informações extraídas dele, limitando-se ao necessário para confirmar a idade ou a elegibilidade do usuário final.

Os dados tratados podem incluir:

- a) tipo de documento;
- b) país ou órgão emissor, quando necessário;
- c) data de nascimento ou idade extraída;
- d) confirmação de que o usuário atende ou não à idade mínima exigida;
- e) qualidade da imagem;
- f) sinais de inconsistência, adulteração ou fraude;

- g) resultado da análise documental;
- h) código técnico da decisão.

Como regra, a IdadeID deve evitar o armazenamento permanente de imagem de documento, número completo de CPF, RG, nome completo, filiação, endereço, assinatura ou outros dados que não sejam indispensáveis para a finalidade de verificação de idade.

Quando for necessária retenção para auditoria, segurança, prevenção à fraude, obrigação legal ou solicitação documentada do cliente contratante, a IdadeID poderá armazenar apenas os metadados mínimos necessários, preferencialmente anonimizados, pseudonimizados ou protegidos por técnicas de segurança adequadas.

4.7 Dados que a IdadeID evita tratar ou armazenar

A IdadeID adota uma postura de redução de exposição e, por isso, evita coletar ou armazenar dados que não sejam necessários para a finalidade de verificação de idade, segurança e auditoria.

Como regra, a IdadeID não busca armazenar permanentemente:

- a) imagens faciais originais após a conclusão do processamento;
- b) imagens integrais de documentos após a análise;
- c) templates biométricos permanentes;
- d) banco de reconhecimento facial;
- e) CPF ou RG completo, salvo quando indispensável e justificado;
- f) nome completo do usuário final, salvo quando indispensável e justificado;
- g) data completa de nascimento, quando bastar registrar apenas a confirmação de maioridade;
- h) endereço residencial;
- i) dados financeiros do usuário final;
- j) dados de geolocalização precisa, salvo quando indispensável para segurança, antifraude ou obrigação legal;
- k) dados sensíveis não relacionados à finalidade da verificação de idade.

A IdadeID poderá registrar apenas informações mínimas como decisão, status da verificação, idade suficiente ou insuficiente, nível de confiança, motivo técnico da

decisão, identificador da sessão, identificador do site, identificador do cliente contratante, data e hora, e dados técnicos necessários à segurança e auditoria.

4.8 Dados de auditoria e eventos operacionais

Para fins de segurança, rastreabilidade, prevenção a fraude, suporte, diagnóstico e prestação de contas, a IdadeID poderá registrar eventos operacionais relacionados ao uso da solução.

Esses eventos podem incluir:

- a) carregamento do widget;
- b) solicitação de configuração pública do site;
- c) início de verificação;
- d) conclusão da verificação;

- e) aprovação, negativa ou fallback;
- f) criação, validação, expiração ou revogação de sessão de acesso;
- g) tentativa de uso em domínio não autorizado;
- h) falha de token, token expirado ou token inválido;
- i) tentativa suspeita de manipulação, remoção ou ocultação do widget;
- j) bloqueio, liberação ou interceptação de checkout;
- k) eventos de erro, timeout, falha de comunicação ou comportamento anômalo;
- l) ações administrativas realizadas no painel.

Esses registros são utilizados para comprovar funcionamento da solução, investigar incidentes, prevenir abuso, apoiar o cliente contratante, cumprir obrigações legais e demonstrar conformidade com medidas de segurança e responsabilidade.

4.9 Dados tratados por provedores e suboperadores

Para prestação da solução, a IdadeID poderá utilizar provedores de infraestrutura, armazenamento, processamento, segurança, inteligência artificial, envio de e-mails, monitoramento, billing, autenticação e demais serviços técnicos necessários.

Nesses casos, os dados compartilhados serão limitados ao necessário para execução da finalidade específica, observadas medidas contratuais, técnicas e organizacionais de proteção de dados.

Quando a IdadeID atuar como Operadora, tais provedores poderão atuar como suboperadores, conforme o contrato firmado com o cliente contratante e as regras aplicáveis de proteção de dados. A ANPD reconhece a importância de identificar corretamente os papéis de controlador, operador e demais agentes conforme a atividade concreta de tratamento.

4.10 Variação conforme risco, configuração e segmento

A quantidade e o tipo de dados tratados poderão variar conforme:

- a) idade mínima configurada pelo cliente;
- b) tipo de site, produto, serviço ou conteúdo protegido;
- c) nível de risco do segmento;
- d) modo de verificação contratado;
- e) exigência de fallback documental;
- f) necessidade de prevenção à fraude;
- g) obrigações legais ou regulatórias aplicáveis ao cliente contratante;
- h) configurações técnicas da integração;
- i) ocorrência de incidentes, erros, tentativas de burla ou uso indevido.

Em todos os casos, a IdadeID buscará limitar o tratamento ao mínimo necessário para cumprir as finalidades informadas nesta Política, nos contratos aplicáveis e nas instruções legítimas do cliente contratante.

5. Natureza dos dados biométricos e imagens faciais

A imagem facial, a selfie, os frames capturados durante a verificação, os dados extraídos de características faciais e eventuais informações técnicas utilizadas para análise de presença, liveness, autenticidade ou prevenção à fraude poderão, conforme o contexto, ser considerados dados pessoais sensíveis, especialmente quando utilizados para identificar, autenticar ou confirmar a identidade de uma pessoa natural.

A IdadeID reconhece que dados biométricos exigem nível elevado de proteção, governança e segurança, em razão de sua natureza sensível, de seu potencial de identificação única e dos riscos associados ao uso indevido, vazamento, reidentificação, discriminação, erro automatizado ou tratamento incompatível com a finalidade original.

A utilização de imagem facial pela IdadeID tem finalidade limitada e específica: apoiar tecnicamente a verificação de idade, a detecção de fraude, a validação de presença, a prevenção de spoofing e a geração de resultado técnico de verificação para o cliente contratante.

Como regra, a IdadeID não utiliza imagem facial para reconhecimento facial massivo, vigilância, rastreamento comportamental, identificação pública de pessoas, criação de perfis sensíveis, monitoramento contínuo ou formação de base permanente de reconhecimento facial.

A IdadeID também não tem como finalidade criar banco biométrico permanente, comercializar dados biométricos, vender informações faciais, treinar modelos próprios com imagens de usuários finais sem base legal adequada ou utilizar imagens capturadas para finalidades incompatíveis com a verificação de idade e segurança da operação.

Sempre que possível, o tratamento da imagem facial ocorre de forma temporária, transitória e limitada ao processamento necessário, sendo priorizado o descarte da imagem após a análise técnica e o armazenamento apenas de metadados mínimos de auditoria, tais como:

- a) resultado da verificação;
- b) indicação de idade suficiente ou insuficiente;
- c) score ou nível de confiança;
- d) reason code técnico da decisão;
- e) presença ou ausência de indícios de fraude;
- f) identificador da sessão;
- g) identificador do site e do cliente contratante;
- h) data e hora do evento;
- i) dados técnicos mínimos necessários para segurança e rastreabilidade.

Quando for necessário tratar imagem facial ou dado biométrico em razão de fallback, contestação, auditoria, segurança, investigação de fraude, obrigação legal, solicitação do cliente contratante ou configuração contratual específica, a IdadeID adotará medidas técnicas e administrativas proporcionais ao risco, incluindo controles de acesso, restrição de finalidade, logs de acesso, criptografia, retenção limitada e descarte seguro.

A IdadeID não armazena templates biométricos permanentes como regra operacional da solução, nem mantém base própria destinada à identificação recorrente de usuários finais em diferentes clientes, sites ou contextos. Qualquer mecanismo de recorrência, quando tecnicamente necessário,

deverá priorizar identificadores

pseudonimizados, hashes, tokens temporários, escopos limitados e segregação por cliente, site ou finalidade.

No caso de fallback documental ou comparação entre imagem facial e documento, o tratamento será limitado ao necessário para confirmar a idade, reduzir fraude e apoiar a decisão técnica, evitando-se o armazenamento permanente de documentos, imagens completas, CPF, RG, nome completo, data completa de nascimento ou outros dados civis quando não forem indispensáveis.

A IdadeID adota uma abordagem de privacidade desde a concepção e segurança por padrão, buscando reduzir a exposição de dados sensíveis, limitar o tempo de tratamento, restringir acessos internos, evitar reutilizações indevidas e impedir que dados biométricos sejam utilizados para finalidades não autorizadas ou incompatíveis.

A ANPD destaca que dados biométricos demandam tratamento rigoroso devido aos riscos à privacidade e aos direitos dos titulares, especialmente em tecnologias de reconhecimento facial, autenticação digital e aplicações automatizadas. Por isso, a IdadeID adota critérios de necessidade, proporcionalidade, transparência, prevenção, segurança e não discriminação na concepção e operação da solução.

6. Finalidades do tratamento de dados pessoais

A IdadeID trata dados pessoais apenas para finalidades legítimas, específicas, explícitas e compatíveis com a prestação de seus serviços de verificação de idade, segurança, prevenção à fraude, auditoria e conformidade.

Os dados pessoais tratados pela IdadeID poderão ser utilizados para as seguintes finalidades:

6.1 Verificação de idade

Realizar a verificação técnica de idade do usuário final, com o objetivo de apoiar o cliente contratante na prevenção de acesso, cadastro, compra, contratação ou utilização indevida de produtos, serviços, conteúdos ou funcionalidades sujeitos a restrição etária.

Essa finalidade pode envolver análise de imagem facial, selfie, liveness, estimativa de faixa etária, validação documental, fallback ou outros métodos técnicos disponibilizados pela IdadeID, conforme o modo contratado e o nível de risco configurado pelo cliente.

6.2 Prevenção de acesso indevido por menores de idade

Auxiliar o cliente contratante a reduzir o risco de acesso indevido por pessoas que não atendam à idade mínima exigida para determinado ambiente, produto, serviço, conteúdo, checkout, ponto de venda digital, vending machine ou funcionalidade protegida.

A IdadeID atua como ferramenta tecnológica de apoio, cabendo ao cliente contratante definir quais áreas, produtos, serviços ou operações exigem verificação de idade.

6.3 Segurança da sessão e controle de acesso

Criar, validar, renovar, expirar ou revogar sessões técnicas de acesso vinculadas a determinado site, cliente, domínio, integração, dispositivo, contexto ou operação protegida.

Essa finalidade inclui o uso de tokens temporários, identificadores técnicos, validação de origem, validação de domínio autorizado, verificação de public key ou site key, controle de expiração,

prevenção de reutilização indevida e bloqueio de sessões inválidas, suspeitas ou expiradas.

6.4 Prevenção à fraude, spoofing e tentativa de burla

Detectar, prevenir e registrar tentativas de fraude, manipulação, falsificação, uso de imagem indevida, deepfake, replay, documento inconsistente, alteração de contexto, remoção do widget, ocultação do modal, manipulação de parâmetros, uso em domínio não autorizado, chamadas suspeitas ou qualquer tentativa de burlar o processo de verificação.

Essa finalidade é essencial para preservar a segurança da solução, proteger o cliente contratante, reduzir risco regulatório e garantir maior confiabilidade ao processo de verificação.

6.5 Fallback documental

Quando a verificação inicial não for suficiente, for inconclusiva, apresentar baixa confiança ou quando o cliente contratante exigir nível maior de segurança, a IdadeID poderá tratar dados relacionados a documento de identificação para confirmar idade ou maioridade.

Essa finalidade é limitada à análise necessária para verificar se o usuário final atende à idade mínima exigida, detectar inconsistências e registrar metadados mínimos de auditoria.

Como regra, o fallback documental não tem finalidade de KYC completa, cadastro civil permanente ou formação de banco documental, salvo quando expressamente contratado, juridicamente justificado e tecnicamente implementado com salvaguardas adicionais.

6.6 Auditoria, rastreabilidade e prestação de contas

Registrar eventos técnicos e metadados mínimos necessários para comprovar que determinado processo de verificação foi iniciado, processado, concluído, negado, aprovado, expirado, contestado ou submetido a fallback.

Essa finalidade pode incluir registros como:

- a) data e hora da verificação;
- b) identificador do site;
- c) identificador do cliente contratante;
- d) identificador técnico da sessão;
- e) resultado da verificação;
- f) nível de confiança;
- g) reason code da decisão;
- h) status da sessão de acesso;
- i) eventos de erro, timeout, suspeita de fraude ou tentativa de burla.

A IdadeID prioriza o armazenamento de metadados técnicos de auditoria em vez de imagens faciais, documentos completos ou dados civis desnecessários.

6.7 Cumprimento de obrigações legais, regulatórias e contratuais

Tratar dados pessoais quando necessário para apoiar o cumprimento de obrigações legais, regulatórias, contratuais, fiscais, contábeis, administrativas ou determinações de autoridades competentes.

Essa finalidade pode incluir a manutenção de registros de segurança, comprovação de operação da solução, atendimento a solicitações de titulares, resposta a incidentes, cooperação com o cliente contratante e cumprimento de obrigações previstas em contrato.

6.8 Suporte técnico, diagnóstico e melhoria da plataforma

Utilizar dados técnicos, logs, eventos de erro, dados de integração e informações operacionais para prestar suporte ao cliente contratante, diagnosticar falhas, corrigir bugs, melhorar estabilidade, otimizar performance, reduzir erros de verificação, aumentar segurança e garantir continuidade operacional da plataforma.

Sempre que possível, essas atividades serão realizadas com dados anonimizados, pseudonimizados, agregados ou limitados ao mínimo necessário.

6.9 Gestão de clientes, contratos e billing

Tratar dados pessoais de clientes, representantes, administradores, operadores e usuários do painel para gestão de cadastro, autenticação, permissões, planos, assinaturas, cobrança, faturamento, suporte, comunicação operacional, histórico de uso, limites de plano e prevenção a abuso da plataforma.

Essa finalidade se aplica principalmente aos dados de clientes contratantes e usuários administrativos, não aos usuários finais submetidos à verificação.

6.10 Comunicações institucionais, comerciais e operacionais

Enviar comunicações relacionadas à operação da plataforma, alterações técnicas, segurança, suporte, avisos contratuais, atualizações de serviço, cobranças, propostas comerciais, demonstrações ou relacionamento com interessados que tenham solicitado contato ou interagido com a IdadeID.

A IdadeID não deverá utilizar dados sensíveis de usuários finais para marketing, segmentação comercial ou comunicação promocional.

6.11 Proteção da própria IdadeID, de seus clientes e de terceiros

Tratar dados pessoais quando necessário para proteger direitos, prevenir abuso, investigar uso indevido da plataforma, defender interesses legítimos em processos administrativos ou judiciais, preservar evidências de fraude, garantir segurança da infraestrutura e evitar danos à IdadeID, aos clientes contratantes, aos usuários finais ou a terceiros.

7. Bases legais para o tratamento de dados pessoais

A IdadeID realiza o tratamento de dados pessoais com fundamento nas hipóteses legais previstas na Lei Geral de Proteção de Dados Pessoais - LGPD, conforme o tipo

de dado tratado, a finalidade específica, o contexto da operação e o papel assumido pela IdadeID em cada atividade.

Quando a IdadeID atuar como Operadora, o tratamento será realizado em nome do cliente contratante, que, na condição de Controlador, será responsável por definir a base legal aplicável ao tratamento realizado em seu ambiente, bem como por informar adequadamente seus usuários finais.

Quando a IdadeID atuar como Controladora, em atividades próprias como gestão contratual, billing, suporte, segurança da plataforma, comunicações, auditoria interna e operação administrativa, a IdadeID será responsável por definir a base legal correspondente.

7.1 Bases legais para dados pessoais comuns

Para dados pessoais comuns, a IdadeID poderá realizar o tratamento com fundamento nas seguintes hipóteses legais, conforme aplicável:

- a) execução de contrato ou de procedimentos preliminares relacionados a contrato, especialmente para gestão da relação com clientes contratantes, criação de contas, administração do painel, suporte, implantação, cobrança, faturamento e prestação dos serviços contratados;
- b) cumprimento de obrigação legal ou regulatória, quando o tratamento for necessário para atender exigências legais, regulatórias, fiscais, contábeis, administrativas, solicitações de autoridades competentes ou deveres de conformidade aplicáveis;
- c) legítimo interesse, quando necessário para segurança da plataforma, prevenção à fraude, prevenção a abuso, proteção contra acessos indevidos, melhoria da solução, suporte técnico, auditoria, defesa de direitos e manutenção da integridade dos serviços, sempre observados os direitos e liberdades fundamentais dos titulares;
- d) exercício regular de direitos, inclusive em contratos, processos administrativos, judiciais ou arbitrais, quando necessário para preservação de evidências, defesa de interesses da IdadeID, de seus clientes ou de terceiros;
- e) proteção do crédito, quando aplicável a atividades de cobrança, faturamento, inadimplência, análise comercial ou gestão financeira da relação com clientes contratantes;
- f) consentimento, quando exigido ou adotado em situações específicas, desde que fornecido de forma livre, informada e inequívoca, podendo ser revogado pelo titular nos termos da LGPD.

O uso de legítimo interesse deverá considerar a finalidade do tratamento, a necessidade dos dados, a expectativa legítima do titular, os impactos aos direitos e liberdades fundamentais e a adoção de medidas de transparência e mitigação de riscos. A ANPD orienta que o legítimo interesse exige avaliação cuidadosa, especialmente em contextos de prevenção à fraude, segurança e dados de crianças e adolescentes.

7.2 Bases legais para dados pessoais sensíveis

Quando houver tratamento de dados pessoais sensíveis, incluindo imagem facial, dados biométricos, informações derivadas de análise facial ou dados extraídos de documento de identificação, a IdadeID observará as hipóteses específicas previstas no art. 11 da LGPD.

Conforme o contexto, o tratamento poderá ser fundamentado em:

- a) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, especialmente quando a verificação de idade envolver imagem facial, liveness, análise de documento, detecção de spoofing, validação de autenticidade ou prevenção de uso indevido da solução;
- b) cumprimento de obrigação legal ou regulatória pelo controlador, quando o cliente contratante estiver sujeito a dever legal, regulatório ou setorial de impedir acesso, cadastro, compra ou utilização de produtos, serviços, conteúdos ou funcionalidades por pessoas que não atendam à idade mínima exigida;
- c) exercício regular de direitos, quando necessário para defesa em processos administrativos, judiciais ou arbitrais, preservação de evidências, apuração de incidentes, contestação de

verificações ou demonstração de conformidade;

- d) consentimento específico e destacado, quando aplicável e juridicamente adequado ao caso concreto, especialmente em fluxos em que o cliente contratante opte por utilizar o consentimento como base legal complementar ou principal, observadas as exigências da LGPD.

A base de prevenção à fraude e segurança prevista no art. 11, II, "g", da LGPD é especialmente relevante para processos de identificação e autenticação em sistemas eletrônicos, desde que o tratamento seja necessário, proporcional, transparente e protegido por medidas adequadas de segurança.

7.3 Tratamento de dados de crianças e adolescentes

A IdadeID poderá tratar dados de adolescentes ou, em situações específicas, dados de pessoas que tentem acessar ambientes sujeitos a restrição etária, inclusive quando a finalidade for impedir acesso indevido, prevenir fraude ou proteger o próprio titular.

Nesses casos, o tratamento deverá observar o princípio do melhor interesse da criança e do adolescente, nos termos da LGPD, bem como os princípios da necessidade, minimização, transparência, segurança e prevenção.

A IdadeID não tem como finalidade estimular o acesso de menores a produtos, serviços ou conteúdos restritos. Ao contrário, a finalidade do tratamento é auxiliar o cliente contratante a evitar que pessoas abaixo da idade mínima exigida acessem, comprem ou utilizem ambientes, conteúdos, produtos ou serviços incompatíveis com sua faixa etária.

Quando o cliente contratante atuar como Controlador, caberá a ele definir e documentar a base legal aplicável ao tratamento de dados de crianças e adolescentes em seu próprio ambiente, observadas as exigências legais e regulatórias aplicáveis ao seu segmento.

7.4 Consentimento

O consentimento poderá ser utilizado em determinados fluxos, quando adequado, exigido ou definido pelo cliente contratante. No entanto, a IdadeID não depende exclusivamente de consentimento para todos os tratamentos, especialmente quando houver outras bases legais aplicáveis, como prevenção à fraude, segurança, cumprimento de obrigação legal, execução de contrato ou legítimo interesse.

Quando utilizado, o consentimento deverá ser apresentado de forma clara, destacada e específica, permitindo que o titular compreenda quais dados serão tratados, para qual finalidade e por quem.

A revogação do consentimento poderá limitar ou impedir a continuidade do processo de verificação, quando o tratamento dos dados for indispensável para confirmar idade, prevenir fraude ou liberar determinada ação protegida.

7.5 Responsabilidade do cliente contratante pela base legal

Quando a IdadeID atuar como Operadora, o cliente contratante será responsável por:

- a) definir a base legal adequada para o uso da solução em seu ambiente;
- b) informar seus usuários finais sobre a utilização da IdadeID;
- c) justificar a necessidade da verificação de idade para seu produto, serviço, conteúdo ou operação;
- d) configurar a solução de forma proporcional ao risco do seu segmento;
- e) evitar uso excessivo, discriminatório, abusivo ou incompatível com a finalidade informada;

f) manter sua própria Política de Privacidade, Termos de Uso e avisos legais atualizados.

A IdadeID poderá solicitar informações, documentos ou esclarecimentos ao cliente contratante quando houver dúvida razoável sobre a legalidade, proporcionalidade ou adequação do uso da solução.

7.6 Limitação e revisão das bases legais

A definição de base legal não autoriza tratamento ilimitado de dados pessoais. Mesmo quando houver base legal aplicável, a IdadeID observará os princípios da finalidade, adequação, necessidade, transparência, segurança, prevenção, não discriminação e responsabilização.

Caso uma nova funcionalidade, integração, segmento, método de verificação ou finalidade de tratamento seja implementada, a IdadeID poderá revisar a base legal aplicável e adotar medidas adicionais, como avaliação de impacto, reforço de transparência, ajuste de retenção, revisão contratual, segregação de dados ou alteração do fluxo de verificação.

8. Compartilhamento de dados pessoais

A IdadeID não vende dados pessoais, não comercializa bases de usuários finais, não compartilha imagens faciais ou documentos para publicidade comportamental e não utiliza dados sensíveis de verificação para formação de perfis comerciais.

O compartilhamento de dados pessoais, quando ocorrer, será limitado ao necessário para operação da plataforma, execução contratual, verificação de idade, prevenção à fraude, segurança da informação, auditoria, suporte técnico, cobrança, cumprimento de obrigações legais ou atendimento a determinações de autoridades competentes.

Quando a IdadeID atuar como Operadora, o tratamento e eventual compartilhamento de dados serão realizados conforme as instruções legítimas do cliente contratante, na qualidade de Controlador, observados os contratos aplicáveis e a legislação de proteção de dados. A LGPD prevê que o operador deve realizar o tratamento segundo as instruções fornecidas pelo controlador.

8.1 Compartilhamento com o cliente contratante

A IdadeID poderá compartilhar com o cliente contratante informações necessárias para permitir a operação da solução, a tomada de decisão pelo cliente, a auditoria e a segurança do ambiente protegido.

Essas informações podem incluir:

- a) resultado da verificação, como aprovado, negado, inconclusivo ou fallback necessário;
- b) indicação de idade suficiente ou insuficiente para a idade mínima configurada;
- c) nível de confiança ou score técnico;
- d) reason code da decisão;
- e) status da sessão de acesso;
- f) identificador técnico da sessão;
- g) data e hora da verificação;
- h) eventos de segurança, erro, expiração, tentativa suspeita ou tentativa de burla;
- i) dados mínimos necessários para suporte, auditoria, billing e prevenção a fraude.

Como regra operacional, a IdadeID evita compartilhar com o cliente contratante imagens faciais, imagens integrais de documentos, CPF, RG, nome completo, data completa de nascimento ou outros dados civis que não sejam indispensáveis para a finalidade contratada.

Quando o compartilhamento de dados mais sensíveis for necessário por configuração específica, exigência legal, auditoria, contestação, fallback documental ou obrigação contratual, ele deverá ocorrer de forma proporcional, segura, rastreável e limitada à finalidade específica.

8.2 Compartilhamento com provedores de infraestrutura e tecnologia

Para disponibilizar a solução, a IdadeID poderá utilizar provedores técnicos responsáveis por infraestrutura, hospedagem, banco de dados, armazenamento temporário, processamento, autenticação, segurança, monitoramento, envio de e-mails, logs, billing, antifraude, inteligência artificial, suporte e demais serviços necessários à operação da plataforma.

Esses provedores poderão tratar dados pessoais apenas na medida necessária para executar suas respectivas funções, observadas medidas contratuais, técnicas e organizacionais adequadas de proteção de dados.

Esses provedores não estão autorizados a utilizar dados pessoais tratados pela IdadeID para finalidades próprias incompatíveis, venda de dados, publicidade comportamental, formação de banco facial próprio ou qualquer finalidade alheia à prestação dos serviços contratados.

8.3 Compartilhamento com provedores de inteligência artificial e análise automatizada

A IdadeID poderá utilizar APIs, modelos ou provedores externos de inteligência artificial, visão computacional, análise documental, detecção de fraude, liveness ou processamento técnico para apoiar a verificação de idade e a segurança da solução.

Nesses casos, o envio de dados deverá ser limitado ao mínimo necessário para a análise específica. Sempre que possível, a IdadeID deverá priorizar:

- a) processamento temporário;
- b) redução de resolução ou compressão técnica quando suficiente;
- c) descarte da imagem após a análise;
- d) envio apenas dos dados necessários para a decisão;
- e) não utilização dos dados para treinamento de modelos de terceiros sem base legal adequada;
- f) contratos ou termos que prevejam confidencialidade, segurança e limitação de finalidade.

O uso de inteligência artificial pela IdadeID tem finalidade de apoio técnico à verificação de idade, prevenção à fraude e segurança, não devendo ser utilizado para vigilância, reconhecimento facial em massa, publicidade, rastreamento comportamental ou identificação de pessoas em contextos não relacionados à solução.

8.4 Suboperadores

Quando a IdadeID atuar como Operadora, determinados provedores contratados para auxiliar na execução dos serviços poderão atuar como suboperadores, tratando dados pessoais em apoio à prestação da solução ao cliente contratante.

A utilização de suboperadores deverá observar os contratos aplicáveis, as instruções do cliente contratante, as obrigações de segurança, confidencialidade, limitação de finalidade, retenção, descarte e conformidade com a LGPD. A ANPD orienta que a definição dos papéis de controlador, operador e demais agentes deve considerar a atividade concreta de tratamento.

A IdadeID poderá substituir, incluir ou remover provedores técnicos e suboperadores ao longo do tempo, desde que mantidas salvaguardas compatíveis com esta Política, com os contratos aplicáveis e com a legislação vigente.

8.5 Compartilhamento com meios de pagamento, cobrança e billing

Para gestão de planos, assinaturas, cobranças, faturamento, emissão de documentos fiscais, controle de inadimplência, conciliação financeira e suporte comercial, a IdadeID poderá compartilhar dados de clientes contratantes com provedores de pagamento, gateways, plataformas de cobrança, sistemas fiscais, contábeis ou financeiros.

Esse compartilhamento não deve envolver imagens faciais, documentos de usuários finais ou dados sensíveis do processo de verificação, salvo em hipótese excepcional, legalmente justificada e diretamente relacionada à finalidade específica.

8.6 Compartilhamento para suporte, implantação e integrações

A IdadeID poderá compartilhar dados técnicos mínimos com parceiros, plataformas, desenvolvedores, prestadores de suporte ou integradores quando necessário para instalação, configuração, diagnóstico, manutenção, correção de falhas ou funcionamento da solução.

Esse compartilhamento poderá envolver dados como:

- a) site_id;
- b) tenant_id;
- c) domínio autorizado;
- d) modo do widget;
- e) eventos técnicos;
- f) status de integração;
- g) logs de erro;
- h) configuração pública do site;
- i) dados administrativos do cliente contratante.

O compartilhamento deverá ser limitado ao necessário para resolver a demanda técnica, evitando exposição indevida de dados de usuários finais.

8.7 Compartilhamento com autoridades públicas, reguladores ou terceiros legalmente autorizados

A IdadeID poderá compartilhar dados pessoais quando necessário para cumprir obrigação legal, regulatória, ordem judicial, requisição de autoridade competente, investigação de fraude, defesa de direitos ou cooperação em procedimentos administrativos, judiciais ou arbitrais.

Nessas hipóteses, a IdadeID deverá avaliar a validade da solicitação, limitar o compartilhamento ao mínimo necessário e manter registros internos, sempre que aplicável e permitido pela legislação.

8.8 Compartilhamento em operações societárias

Em caso de reorganização societária, fusão, aquisição, incorporação, venda de ativos, investimento, due diligence, sucessão empresarial ou operação semelhante envolvendo a IdadeID, determinados dados pessoais poderão ser compartilhados com

partes envolvidas na operação, assessores jurídicos, auditores, investidores ou potenciais adquirentes.

Nesses casos, deverão ser adotadas medidas razoáveis de confidencialidade, segurança, limitação de acesso e preservação dos direitos dos titulares.

8.9 Limites do compartilhamento

A IdadeID não deverá compartilhar dados pessoais de forma incompatível com as finalidades descritas nesta Política, com os contratos aplicáveis ou com a LGPD.

Em especial, a IdadeID não deverá:

- a) vender dados pessoais de usuários finais;
- b) comercializar imagens faciais ou documentos;
- c) compartilhar dados sensíveis para publicidade comportamental;
- d) formar banco facial compartilhado entre clientes;
- e) permitir uso de dados de verificação para treinamento de modelos sem base legal adequada;
- f) permitir reuso de dados de usuários finais entre clientes diferentes sem fundamento jurídico, segregação e autorização aplicável;
- g) compartilhar mais dados do que o necessário para a finalidade específica.

8.10 Segurança no compartilhamento

Sempre que houver compartilhamento de dados pessoais, a IdadeID adotará medidas proporcionais ao risco, podendo incluir:

- a) contratos com cláusulas de proteção de dados;
- b) confidencialidade;
- c) controle de acesso;
- d) criptografia em trânsito e, quando aplicável, em repouso;
- e) segregação por cliente, site, tenant ou finalidade;
- f) logs de acesso;
- g) retenção limitada;
- h) descarte seguro;
- i) due diligence de fornecedores críticos;
- j) revisão periódica de provedores e suboperadores.

9. Transferência internacional de dados pessoais

A IdadeID poderá realizar transferência internacional de dados pessoais quando a operação da plataforma, a prestação dos serviços contratados, a verificação de idade, o processamento técnico, a hospedagem, o armazenamento, a segurança, o monitoramento, o suporte, o billing, a autenticação, o envio de comunicações ou o uso de provedores de inteligência artificial envolverem fornecedores, servidores, sistemas ou equipes localizados fora do Brasil.

A transferência internacional poderá ocorrer, por exemplo, quando a IdadeID utilizar provedores de:

- a) infraestrutura em nuvem;
- b) hospedagem e banco de dados;
- c) APIs de inteligência artificial, visão computacional ou análise documental;
- d) monitoramento, logs, observabilidade e segurança;
- e) autenticação, envio de e-mails e comunicações operacionais;
- f) meios de pagamento, billing, cobrança e faturamento;
- g) suporte técnico, diagnóstico ou prevenção à fraude;
- h) ferramentas administrativas necessárias à operação da plataforma.

A transferência internacional de dados pessoais será realizada apenas quando necessária para as finalidades descritas nesta Política, para execução dos contratos aplicáveis, para cumprimento de obrigação legal ou regulatória, para segurança da plataforma, para prevenção à fraude ou para funcionamento técnico da solução.

A IdadeID adotará medidas razoáveis e proporcionais para assegurar que a transferência internacional observe a LGPD, a regulamentação aplicável da Autoridade Nacional de Proteção de Dados - ANPD e os mecanismos legais cabíveis, incluindo, quando aplicável:

- a) decisões de adequação reconhecidas pela ANPD;
- b) cláusulas-padrão contratuais aprovadas pela ANPD;
- c) cláusulas contratuais específicas aprovadas pela ANPD;
- d) normas corporativas globais;
- e) contratos com obrigações de confidencialidade, segurança, limitação de finalidade, retenção e descarte;
- f) avaliação de fornecedores críticos;
- g) medidas técnicas de proteção, como criptografia, controle de acesso, segregação de dados, logs e retenção limitada;
- h) limitação do envio de dados ao mínimo necessário para a finalidade específica.

A Resolução CD/ANPD nº 19/2024 estabeleceu regras e procedimentos aplicáveis à transferência internacional de dados pessoais e aprovou o conteúdo das cláusulas-padrão contratuais no Brasil. Os agentes de tratamento que utilizavam cláusulas contratuais para transferência internacional tiveram prazo de 12 meses, contado da publicação da resolução, para incorporar as cláusulas-padrão aprovadas pela ANPD aos seus instrumentos contratuais.

Quando a transferência envolver imagem facial, dados sensíveis, documento de identificação ou dados derivados de verificação de idade, a IdadeID deverá adotar cautelas adicionais, buscando

limitar o volume de dados enviados, reduzir o tempo de processamento, evitar armazenamento permanente pelo fornecedor, impedir uso para treinamento de modelos sem base legal adequada e manter registros de auditoria compatíveis com o risco da operação.

Sempre que possível, a IdadeID deverá priorizar:

- a) processamento temporário;
- b) descarte após a análise;
- c) envio de dados reduzidos ou comprimidos quando tecnicamente suficiente;
- d) armazenamento de metadados em vez de imagens completas;
- e) segregação por cliente, site, tenant e finalidade;
- f) restrição contratual contra uso secundário dos dados;
- g) fornecedores com padrões reconhecidos de segurança e privacidade.

Quando a IdadeID atuar como Operadora, a transferência internacional será realizada em conformidade com as instruções legítimas do cliente contratante, os contratos aplicáveis, esta Política e a legislação vigente. Nessa hipótese, o cliente contratante, na qualidade de Controlador, poderá ser responsável por avaliar a base legal, a necessidade e a adequação da transferência internacional no contexto de seu próprio negócio.

Quando a IdadeID atuar como Controladora, será responsável por avaliar o mecanismo jurídico aplicável à transferência internacional realizada para suas próprias finalidades, como gestão contratual, suporte, cobrança, segurança da plataforma, comunicações institucionais, auditoria interna e operação administrativa.

A IdadeID não realizará transferência internacional de dados pessoais para finalidades incompatíveis com esta Política, com os contratos aplicáveis ou com a legislação de proteção de dados. Também não autorizará fornecedores internacionais a vender dados pessoais, utilizar dados sensíveis de verificação para publicidade comportamental, formar banco facial próprio, realizar reconhecimento facial em

massa ou utilizar imagens e documentos de usuários finais para treinamento de modelos sem base legal adequada e autorização aplicável.

10. Retenção, descarte e conservação de dados

A IdadeID mantém dados pessoais somente pelo tempo necessário para cumprir as finalidades descritas nesta Política de Privacidade, executar os serviços contratados, garantir segurança da plataforma, prevenir fraudes, registrar eventos mínimos de auditoria, atender solicitações de titulares, cumprir obrigações legais ou regulatórias e resguardar direitos da IdadeID, de seus clientes contratantes ou de terceiros.

A retenção dos dados poderá variar conforme a categoria do dado, a finalidade do tratamento, o papel da IdadeID como Controladora ou Operadora, as instruções do cliente contratante, o nível de risco do segmento, o tipo de integração utilizada, a existência de contestação, suspeita de fraude, incidente de segurança, obrigação legal ou necessidade de preservação de evidências.

Como regra geral, a IdadeID adota uma política de retenção mínima, priorizando o descarte de imagens e documentos após o processamento e a conservação apenas de metadados técnicos necessários para segurança, auditoria e rastreabilidade.

10.1 Imagens faciais, selfies e frames de verificação

As imagens faciais, selfies ou frames capturados durante o processo de verificação são tratados, como regra, de forma temporária e transitória, pelo tempo necessário para realizar a análise técnica de idade, liveness, qualidade da captura, prevenção à fraude ou validação da sessão.

Como regra operacional, a IdadeID não mantém armazenamento permanente de imagens faciais utilizadas na verificação, nem cria banco permanente de reconhecimento facial ou templates biométricos persistentes de usuários finais.

Após a conclusão do processamento, a IdadeID deverá priorizar o descarte da imagem facial e a retenção apenas de metadados mínimos, tais como:

- a) resultado da verificação;
- b) indicação de idade suficiente ou insuficiente;
- c) nível de confiança;
- d) reason code da decisão;
- e) identificador técnico da sessão;
- f) site_id;
- g) tenant_id;
- h) data e hora do evento;
- i) indicadores técnicos mínimos de risco, qualidade ou fraude.

A retenção excepcional de imagem facial poderá ocorrer apenas quando houver justificativa específica, como obrigação legal, solicitação documentada do cliente contratante, necessidade de auditoria, contestação da decisão, investigação de fraude, incidente de segurança, preservação de evidência ou configuração contratual específica compatível com a LGPD.

10.2 Imagens de documentos e fallback documental

Quando houver fallback documental, a imagem do documento deverá ser tratada apenas pelo tempo necessário para confirmar a idade, verificar qualidade, detectar inconsistência, prevenir fraude e gerar o resultado técnico da análise.

Como regra, a IdadeID não deve armazenar permanentemente imagem integral de documento, CPF, RG, nome completo, filiação, assinatura, endereço ou data completa de nascimento quando essas informações não forem indispensáveis para a finalidade contratada.

Sempre que possível, após a análise documental, a IdadeID deverá descartar a imagem do documento e manter apenas metadados mínimos, como:

- a) tipo de documento;
- b) idade suficiente ou insuficiente;
- c) required_age;
- d) over_required_age;
- e) nível de confiança;
- f) qualidade da captura;
- g) sinais de inconsistência ou fraude;

- h) decisão final;
- i) reason code;
- j) fallback_used;
- k) site_id;
- l) tenant_id;
- m) access_session_id ou verification_session_id;
- n) timestamp.

Caso seja necessária retenção excepcional de documento ou dado extraído do documento, essa retenção deverá ser limitada, justificada, protegida por controles reforçados e compatível com a finalidade específica.

10.3 Sessões de verificação e sessões de acesso

A IdadeID poderá manter registros relacionados a sessões de verificação e sessões técnicas de acesso pelo período necessário para validar o funcionamento da solução, comprovar a decisão técnica, evitar reutilização indevida, prevenir fraude, garantir rastreabilidade e apoiar auditoria.

Esses registros podem incluir:

- a) verification_session_id;
- b) access_session_id;
- c) status da sessão;
- d) data e hora de criação;
- e) data e hora de expiração;
- f) site_id;
- g) tenant_id;
- h) domínio de origem;
- i) token jti ou identificador técnico equivalente;
- j) escopo da sessão;
- k) status de validação, expiração, revogação ou erro.

Tokens de acesso e sessões técnicas deverão ter prazo limitado, escopo restrito e possibilidade de expiração ou revogação. A IdadeID não deve utilizar tokens permanentes de liberação de acesso como substitutos de nova verificação quando a legislação, o risco do segmento ou a configuração do cliente exigirem verificação recorrente.

10.4 Logs, eventos técnicos e auditoria

A IdadeID poderá manter logs, eventos técnicos e registros mínimos de auditoria pelo prazo necessário para segurança, rastreabilidade, prevenção à fraude, diagnóstico, suporte, billing, cumprimento contratual e defesa de direitos.

Esses registros poderão incluir eventos como:

- a) widget_loaded;
- b) config_requested;

- c) verification_started;
- d) approved;
- e) denied;
- f) fallback_required;
- g) session_created;
- h) session_validated;
- i) tamper_detected;
- j) widget_removed;
- k) checkout_intercepted;
- l) checkout_released;
- m) invalid_domain;
- n) invalid_token;
- o) erro técnico, timeout ou falha de comunicação.

Como parâmetro geral, logs e eventos técnicos poderão ser mantidos por até 365 dias, salvo quando prazo maior ou menor for necessário em razão de obrigação legal, exigência contratual, investigação de fraude, incidente de segurança, contestação, auditoria, exercício regular de direitos ou orientação documentada do cliente contratante.

10.5 Dados de clientes contratantes e usuários administrativos

Dados pessoais de clientes contratantes, representantes, administradores, operadores, usuários do painel, contatos comerciais e responsáveis financeiros poderão ser mantidos enquanto houver relação contratual ativa com a IdadeID e, após seu encerramento, pelo período necessário para cumprimento de obrigações legais, fiscais, contábeis, contratuais, regulatórias, prevenção à fraude, cobrança, auditoria e exercício regular de direitos.

Esses dados podem incluir informações cadastrais, dados de contato, registros de plano, cobrança, faturamento, suporte, permissões, logs administrativos e histórico de ações relevantes no painel.

10.6 Dados de visitantes do site institucional e leads comerciais

Dados fornecidos por visitantes do site institucional, leads, interessados, parceiros ou pessoas que solicitam contato poderão ser mantidos pelo tempo necessário para atendimento da solicitação, relacionamento comercial, envio de comunicações solicitadas, registro de histórico de contato, execução de procedimentos preliminares ou cumprimento de obrigações legais.

O titular poderá solicitar exclusão, oposição ou revisão do tratamento, observados os limites legais, contratuais e técnicos aplicáveis.

10.7 Retenção por obrigação legal, fraude, auditoria ou defesa de direitos

Mesmo após o término da finalidade principal, determinados dados poderão ser conservados quando necessário para:

- a) cumprimento de obrigação legal ou regulatória;
- b) auditoria e prestação de contas;

- c) prevenção, investigação ou comprovação de fraude;
- d) apuração de incidente de segurança;
- e) atendimento a autoridade competente;
- f) exercício regular de direitos em processo judicial, administrativo ou arbitral;
- g) cumprimento de contrato com o cliente contratante;
- h) cobrança, faturamento, contabilidade ou obrigações fiscais;
- i) proteção da IdadeID, dos clientes contratantes, dos titulares ou de terceiros.

Nesses casos, a IdadeID deverá limitar a conservação ao dado estritamente necessário, restringir o acesso, aplicar medidas de segurança adequadas e realizar o descarte quando a finalidade de conservação deixar de existir.

10.8 Anonimização, pseudonimização e descarte seguro

Sempre que possível, a IdadeID poderá substituir dados pessoais por dados anonimizados, agregados ou pseudonimizados, especialmente para estatísticas operacionais, melhoria da plataforma, métricas de performance, análise de falhas, segurança e billing.

O descarte de dados pessoais deverá ocorrer de forma segura, utilizando procedimentos técnicos compatíveis com o tipo de dado, o ambiente de armazenamento e o risco envolvido.

Quando a exclusão imediata não for tecnicamente possível, como em backups, logs distribuídos ou retenções operacionais, a IdadeID adotará medidas para impedir o uso ativo desses dados e promover sua eliminação conforme ciclos técnicos razoáveis de retenção e descarte.

10.9 Instruções do cliente contratante

Quando a IdadeID atuar como Operadora, os prazos de retenção poderão observar as instruções legítimas e documentadas do cliente contratante, desde que compatíveis com a LGPD, com os contratos aplicáveis e com as medidas de segurança da IdadeID.

A IdadeID poderá recusar instruções de retenção que sejam excessivas, desproporcionais, inseguras, incompatíveis com a finalidade contratada ou que possam gerar risco relevante aos titulares, à plataforma ou à conformidade legal.

10.10 Revisão periódica dos prazos de retenção

A IdadeID poderá revisar periodicamente seus prazos de retenção, critérios de descarte, categorias de dados armazenados e controles de segurança, especialmente quando houver alteração legal, regulatória, técnica, contratual, de risco ou de arquitetura da plataforma.

A LGPD prevê que o tratamento deve terminar quando a finalidade for alcançada ou quando os dados deixarem de ser necessários ou pertinentes, ressalvadas hipóteses legais de conservação. Por isso, a política da IdadeID deve ser orientada por retenção limitada, proporcionalidade e descarte seguro.

11. Segurança da informação

A IdadeID adota medidas técnicas, administrativas e organizacionais destinadas a proteger os dados pessoais tratados em sua plataforma contra acesso não autorizado, uso indevido, perda, destruição, alteração, vazamento, comunicação indevida, fraude, manipulação, tratamento inadequado ou qualquer forma de tratamento ilícito.

As medidas de segurança adotadas pela IdadeID são proporcionais à natureza dos dados tratados, ao risco da atividade, ao volume de informações processadas, à sensibilidade dos dados, ao contexto da verificação de idade, ao nível de risco do cliente contratante e às características técnicas da integração utilizada.

A IdadeID reconhece que nenhuma medida de segurança é absoluta ou capaz de eliminar integralmente todos os riscos. No entanto, a plataforma adota uma abordagem de segurança em camadas, privacidade desde a concepção, segurança por padrão, minimização de dados, validação server-side e falha segura, buscando reduzir riscos, limitar exposição e preservar a integridade da verificação.

11.1 Segurança na arquitetura da plataforma

A arquitetura da IdadeID é projetada para que decisões críticas não dependam exclusivamente do navegador, do widget, de cookies locais, de parâmetros de URL ou de dados não validados enviados pelo cliente.

Sempre que aplicável, a IdadeID adota medidas como:

- a) validação crítica no servidor;
- b) separação entre frontend, backend, banco de dados e integrações externas;
- c) APIs seguras para configuração, verificação, sessão, auditoria e billing;
- d) restrição de acesso a endpoints sensíveis;
- e) validação de origem, domínio, site_id, tenant_id e public key;
- f) segregação lógica de dados por cliente, site, tenant e finalidade;
- g) uso de service role apenas em ambiente backend seguro;
- h) aplicação de políticas de acesso no banco de dados, incluindo RLS quando aplicável;
- i) controle de permissões por perfil de usuário, como usuário comum, administrador do cliente e administrador master;
- j) separação entre dados operacionais, dados de auditoria, dados de billing e dados administrativos.

A IdadeID não deve expor no cliente chaves privadas, secrets, service role keys, regras sensíveis de billing, lógica crítica de aprovação ou qualquer mecanismo que permita ao navegador decidir sozinho se uma verificação é válida.

11.2 Segurança do widget e das integrações

O widget da IdadeID é uma camada de interface e integração, mas não deve ser a autoridade final sobre aprovação, liberação ou validade da sessão.

O widget poderá carregar configurações públicas a partir do servidor, utilizando identificadores públicos como site key ou public key, sem incluir dados sensíveis hardcoded no código distribuído ao cliente.

A IdadeID poderá adotar medidas para proteger o funcionamento do widget, incluindo:

- a) consulta server-side da configuração real do site;
- b) validação de domínio autorizado;
- c) validação de site ativo, tenant ativo, plano ativo e modo de widget;
- d) uso de tokens temporários assinados;
- e) verificação de integridade da sessão;
- f) detecção de remoção ou manipulação do elemento do widget;
- g) detecção de ocultação indevida do modal, iframe ou overlay;
- h) registro de eventos suspeitos;
- i) bloqueio seguro em caso de erro, domínio inválido, token inválido, configuração ausente, timeout ou comportamento anômalo.

Quando houver falha de validação, ausência de configuração, domínio não autorizado, token inválido, tentativa de manipulação ou inconsistência relevante, a solução deverá priorizar comportamento de falha segura, impedindo a liberação indevida quando tecnicamente possível.

11.3 Tokens, sessões e controle de acesso

A IdadeID utiliza sessões técnicas, tokens temporários e identificadores de validação com escopo limitado para proteger o processo de verificação e reduzir o risco de reutilização indevida.

As sessões e tokens poderão conter ou estar vinculados a informações como:

- a) tenant_id;
- b) site_id;
- c) public key ou identificador público da integração;
- d) domínio autorizado;
- e) contexto da verificação;
- f) escopo da sessão;
- g) data de emissão;
- h) data de expiração;
- i) identificador único da sessão ou jti;
- j) status de validação, expiração ou revogação.

Tokens e sessões devem ter duração limitada, possibilidade de revogação, validação server-side e vínculo com o contexto específico da verificação. A IdadeID não deve aceitar tokens fora de escopo, expirados, alterados, reutilizados de forma indevida ou incompatíveis com o site, domínio, tenant ou operação protegida.

11.4 Controle de acesso interno

A IdadeID adota controles internos para restringir o acesso a dados pessoais apenas a pessoas autorizadas e quando necessário para execução de suas funções.

Essas medidas podem incluir:

- a) autenticação de usuários administrativos;

- b) controle de permissões por perfil;
- c) princípio do menor privilégio;
- d) segregação entre usuários de cliente, administradores de tenant e administradores master;
- e) logs de ações administrativas relevantes;
- f) revisão de acessos;
- g) restrição de acesso a dados sensíveis;
- h) proteção de credenciais, secrets e chaves de API;
- i) bloqueio ou revogação de acessos indevidos, inativos ou comprometidos.

Ações administrativas críticas, como alteração de plano, configuração de site, domínio autorizado, política de verificação, acesso a logs, alteração de billing ou intervenção manual, deverão ser registradas para fins de auditoria.

11.5 Criptografia, comunicação segura e proteção de dados

A IdadeID poderá adotar criptografia em trânsito, criptografia em repouso quando aplicável, conexões seguras, armazenamento protegido, controle de acesso a bancos de dados, segregação de ambientes e mecanismos de proteção contra exposição indevida.

Entre as medidas aplicáveis, poderão estar:

- a) uso de HTTPS/TLS;
- b) proteção de credenciais e secrets;
- c) armazenamento seguro de chaves;
- d) criptografia de dados sensíveis quando aplicável;
- e) restrição de acesso direto ao banco de dados;
- f) proteção contra exposição pública de buckets, arquivos ou endpoints;
- g) descarte seguro de imagens e documentos após o processamento;
- h) armazenamento preferencial de metadados em vez de imagens completas;
- i) limitação de dados retornados ao cliente ou ao navegador.

A IdadeID deve evitar retornar ao frontend informações sensíveis, mensagens de erro internas, detalhes de infraestrutura, chaves, regras de negócio críticas ou dados pessoais desnecessários.

11.6 Monitoramento, logs e auditoria

A IdadeID poderá manter registros técnicos de segurança, auditoria e operação para detectar falhas, abusos, tentativas de fraude, tentativas de burla, manipulação de sessão, erros de integração, indisponibilidade, acessos suspeitos e comportamentos anômalos.

Esses registros podem incluir eventos como:

- a) widget_loaded;
- b) config_requested;
- c) verification_started;
- d) approved;
- e) denied;

- f) fallback_required;
- g) session_created;
- h) session_validated;
- i) session_expired;
- j) session_revoked;
- k) tamper_detected;
- l) widget_removed;
- m) checkout_intercepted;
- n) checkout_released;
- o) invalid_domain;
- p) invalid_token;
- q) rate_limit_triggered;
- r) admin_action;
- s) webhook_received;
- t) webhook_rejected.

Os logs devem ser utilizados para segurança, diagnóstico, auditoria, prevenção à fraude, billing, suporte técnico, cumprimento contratual, investigação de incidentes e exercício regular de direitos, sempre respeitando os princípios de necessidade, minimização e retenção limitada.

11.7 Rate limit, antifraude e proteção contra abuso

A IdadeID poderá aplicar mecanismos de proteção contra abuso, incluindo limitação de requisições, bloqueio temporário, validação de origem, validação de domínio autorizado, verificação de public key, proteção contra replay, controle de sessão, fingerprint técnico leve, análise de comportamento anômalo e registro de tentativas suspeitas.

Essas medidas podem ser aplicadas por IP, site, tenant, sessão, integração, domínio, endpoint ou outro critério técnico razoável, sempre com o objetivo de proteger a plataforma, os clientes contratantes, os titulares e a integridade da verificação.

A IdadeID deverá evitar coleta excessiva para fins antifraude, priorizando dados técnicos mínimos e proporcionais ao risco.

11.8 Segurança em integrações, webhooks e APIs

As APIs, webhooks e integrações da IdadeID deverão ser protegidos por mecanismos compatíveis com o risco da operação.

Quando aplicável, a IdadeID poderá utilizar:

- a) autenticação de APIs;
- b) validação de assinatura de webhooks;
- c) proteção contra replay;
- d) validação de payload;
- e) CORS restrito;

- f) rate limit;
- g) logs de requisição;
- h) idempotência em operações críticas;
- i) validação server-side de regras de plano, uso, sessão e domínio;
- j) respostas de erro que não revelem dados sensíveis ou detalhes internos da infraestrutura.

Webhooks de billing, integrações externas, plataformas de e-commerce, sistemas de checkout e provedores de pagamento devem ser validados antes de qualquer alteração crítica em conta, plano, assinatura, cobrança, limite de uso ou status operacional.

11.9 Segurança no tratamento de imagens e documentos

Imagens faciais, frames de verificação e documentos de identificação, quando tratados, exigem proteção reforçada em razão de sua sensibilidade.

A IdadeID deverá adotar medidas para reduzir a exposição desses dados, incluindo:

- a) processamento temporário sempre que possível;
- b) descarte após análise, salvo justificativa específica;
- c) limitação de acesso interno;
- d) não criação de banco facial permanente;
- e) não armazenamento de templates biométricos permanentes como regra;
- f) não utilização para publicidade comportamental;
- g) não utilização para reconhecimento facial em massa;
- h) retenção preferencial de metadados mínimos de auditoria;
- i) proteção reforçada quando houver fallback documental;
- j) restrição de compartilhamento com terceiros ao mínimo necessário.

Quando a imagem ou documento for enviado a provedor externo de análise, como APIs de inteligência artificial ou visão computacional, o envio deverá ser limitado ao necessário para a finalidade específica, com salvaguardas contratuais e técnicas compatíveis.

11.10 Gestão de incidentes de segurança

A IdadeID poderá manter procedimentos internos para identificação, análise, contenção, mitigação, registro e resposta a incidentes de segurança envolvendo dados pessoais.

Em caso de incidente que possa acarretar risco ou dano relevante aos titulares, a IdadeID avaliará as medidas cabíveis, incluindo comunicação ao cliente contratante, titulares afetados e Autoridade Nacional de Proteção de Dados, conforme a LGPD e a regulamentação aplicável.

A ANPD publicou a Resolução CD/ANPD nº 15/2024, que aprovou o Regulamento de Comunicação de Incidente de Segurança, com foco em mitigação de prejuízos, responsabilização, prestação de contas e boas práticas de governança e segurança.

Quando a IdadeID atuar como Operadora, comunicará o cliente contratante sobre incidentes relevantes de que tenha conhecimento, para que o cliente, como Controlador, possa avaliar suas obrigações legais e regulatórias.

11.11 Responsabilidade compartilhada com o cliente contratante

A segurança da solução também depende da configuração correta pelo cliente contratante e do uso adequado dos mecanismos de integração.

O cliente contratante é responsável por:

- a) instalar corretamente o widget, plugin, middleware, API ou integração;
- b) manter seu próprio ambiente seguro;
- c) configurar domínios autorizados corretamente;
- d) não expor chaves, tokens ou credenciais;
- e) não alterar indevidamente o código da solução;
- f) não tentar contornar validações críticas;
- g) manter seus usuários administrativos protegidos;
- h) comunicar suspeitas de incidente, uso indevido ou falha de integração;
- i) utilizar a solução conforme contrato, documentação e legislação aplicável.

A IdadeID não se responsabiliza por falhas, vazamentos, bypasses, manipulações ou incidentes causados exclusivamente por ambiente externo inseguro, instalação incorreta, alteração não autorizada, uso indevido pelo cliente, falha de plataforma terceira ou integração fora das orientações técnicas fornecidas.

11.12 Revisão contínua de segurança

A IdadeID poderá revisar, testar e aprimorar periodicamente seus controles de segurança, especialmente em razão de novas ameaças, alterações regulatórias,

mudanças de arquitetura, integrações com terceiros, evolução da plataforma, incidentes, auditorias ou aumento do nível de risco de determinado segmento.

As medidas de segurança poderão ser atualizadas sem aviso prévio quando necessárias para proteger a plataforma, os titulares, os clientes contratantes ou terceiros.

12. Direitos dos titulares de dados pessoais

Nos termos da Lei Geral de Proteção de Dados Pessoais - LGPD, os titulares de dados pessoais poderão exercer seus direitos em relação aos dados tratados pela IdadeID, observados os limites legais, técnicos, contratuais e o papel assumido pela IdadeID em cada atividade de tratamento.

Conforme aplicável, o titular poderá solicitar:

- a) confirmação da existência de tratamento de seus dados pessoais;
- b) acesso aos dados pessoais tratados;
- c) correção de dados incompletos, inexatos ou desatualizados;
- d) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD;
- e) portabilidade dos dados, observadas as normas aplicáveis da autoridade competente e os segredos comercial e industrial;
- f) eliminação dos dados pessoais tratados com base no consentimento, quando aplicável;

- g) informação sobre entidades públicas ou privadas com as quais houve compartilhamento de dados;
- h) informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- i) revogação do consentimento, quando o tratamento estiver baseado nessa hipótese legal;
- j) oposição a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, quando houver descumprimento da LGPD;
- k) revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, observados os limites legais aplicáveis.

A LGPD também prevê que o titular tem direito de peticionar em relação aos seus dados contra o controlador perante a Autoridade Nacional de Proteção de Dados - ANPD.

12.1 Como exercer os direitos

As solicitações relacionadas a dados pessoais tratados pela IdadeID poderão ser enviadas para:

privacidade@idadeid.com.br

A solicitação deverá conter informações mínimas que permitam identificar o titular e localizar o tratamento relacionado, como:

- a) nome ou identificação do solicitante, quando aplicável;
- b) e-mail de contato;
- c) descrição clara da solicitação;
- d) indicação do site, plataforma, cliente contratante ou ambiente onde ocorreu a verificação, quando aplicável;
- e) data aproximada da verificação ou interação;
- f) informações técnicas que ajudem na localização da sessão, caso disponíveis.

A IdadeID poderá solicitar informações adicionais estritamente necessárias para confirmar a identidade do solicitante, prevenir fraude, proteger dados de terceiros e evitar acesso indevido a informações pessoais.

12.2 Solicitações de usuários finais verificados em sites de clientes

Quando a solicitação envolver usuário final que realizou verificação de idade dentro de site, aplicativo, e-commerce, checkout, vending machine, plataforma ou ambiente de um cliente contratante, a IdadeID poderá atuar como Operadora de dados pessoais.

Nesses casos, o cliente contratante, na qualidade de Controlador, poderá ser o responsável principal por responder à solicitação do titular, definir a base legal aplicável e decidir sobre eliminação, bloqueio, retenção, oposição, portabilidade ou fornecimento de informações.

A IdadeID poderá:

- a) orientar o titular a contatar o cliente contratante quando este for o Controlador;
- b) encaminhar a solicitação ao cliente contratante, quando adequado;
- c) cooperar tecnicamente com o cliente contratante para localização e atendimento da solicitação;
- d) fornecer informações técnicas compatíveis com seu papel de Operadora;

e) preservar registros quando houver obrigação legal, auditoria, fraude, segurança ou exercício regular de direitos.

A ANPD orienta que a definição entre controlador e operador depende da atividade concreta de tratamento e das decisões tomadas sobre finalidade e meios do tratamento. Por isso, a resposta ao titular deve considerar o contexto específico em que os dados foram tratados.

12.3 Solicitações de clientes, leads e visitantes do site institucional

Quando a solicitação envolver dados tratados diretamente pela IdadeID para finalidades próprias, como cadastro de clientes, gestão contratual, billing, suporte, atendimento comercial, comunicações, segurança da plataforma ou navegação no site institucional, a IdadeID atuará como Controladora.

Nesses casos, a IdadeID avaliará a solicitação e responderá ao titular conforme a LGPD, podendo confirmar, corrigir, eliminar, anonimizar, bloquear, fornecer acesso ou justificar eventual impossibilidade de atendimento, conforme a situação concreta.

12.4 Limitações ao exercício dos direitos

O exercício dos direitos do titular não é absoluto e poderá estar sujeito a limitações previstas na LGPD, em contratos aplicáveis ou em obrigações legais e regulatórias.

A IdadeID poderá manter determinados dados mesmo após solicitação de exclusão, bloqueio ou oposição quando a conservação for necessária para:

- a) cumprimento de obrigação legal ou regulatória;
- b) auditoria e prestação de contas;
- c) prevenção, investigação ou comprovação de fraude;
- d) segurança da plataforma;
- e) apuração de incidentes;
- f) defesa em processos judiciais, administrativos ou arbitrais;
- g) cobrança, faturamento, obrigações fiscais ou contábeis;
- h) cumprimento de contrato com o cliente contratante;
- i) proteção de direitos da IdadeID, do cliente contratante, do titular ou de terceiros.

Nessas hipóteses, a IdadeID deverá limitar a retenção ao dado estritamente necessário, restringir o acesso, aplicar medidas de segurança e descartar os dados quando a finalidade de conservação deixar de existir.

12.5 Revisão de decisões automatizadas

Quando o resultado da verificação envolver tratamento automatizado que possa afetar interesses do titular, o titular poderá solicitar informações e, quando aplicável, revisão da decisão, nos termos da LGPD.

A revisão poderá considerar elementos como:

- a) resultado da verificação;
- b) nível de confiança;

- c) reason code técnico;
- d) qualidade da imagem ou documento;
- e) presença de indícios de fraude;
- f) necessidade de fallback documental;
- g) erro técnico, falha de captura ou inconsistência operacional.

A IdadeID poderá cooperar com o cliente contratante para revisar tecnicamente o evento, mas a decisão final sobre acesso, compra, cadastro, contratação ou liberação de funcionalidade poderá caber ao cliente contratante quando este atuar como Controlador.

12.6 Prazo e forma de resposta

A IdadeID responderá às solicitações dos titulares dentro dos prazos previstos na LGPD e na regulamentação aplicável, considerando a natureza da solicitação, o papel da IdadeID no tratamento, a necessidade de confirmação de identidade, a complexidade técnica e eventual necessidade de cooperação com o cliente contratante.

A LGPD prevê regras específicas para confirmação de tratamento e acesso aos dados, incluindo possibilidade de resposta em formato simplificado ou por declaração clara e completa, observados os prazos legais aplicáveis.

Quando a IdadeID não puder atender integralmente uma solicitação, informará, sempre que possível, os motivos da impossibilidade, respeitados os limites legais, comerciais, técnicos, de segurança e de proteção de dados de terceiros.

12.7 Segurança no atendimento das solicitações

Para proteger os titulares e evitar fraude, a IdadeID poderá adotar medidas de validação antes de atender solicitações relacionadas a dados pessoais.

A IdadeID não fornecerá dados pessoais a solicitantes que não comprovem legitimidade, identidade ou autorização suficiente para receber as informações solicitadas.

Solicitações feitas por representantes legais, procuradores ou responsáveis deverão ser acompanhadas de comprovação adequada de representação, quando necessário.

13. Responsabilidade do cliente contratante como controlador

Quando a IdadeID for utilizada em site, aplicativo, plataforma, e-commerce, checkout, vending machine, sistema de acesso, ponto de venda digital ou qualquer outro ambiente pertencente ou operado por um cliente contratante, o cliente será, em regra, o Controlador dos dados pessoais tratados no contexto de seu próprio negócio.

Nessa condição, caberá ao cliente contratante definir as finalidades do tratamento, a base legal aplicável, os produtos, serviços, conteúdos ou funcionalidades sujeitos à verificação de idade, a idade mínima exigida, o nível de risco do fluxo e a decisão final sobre permitir, negar, condicionar ou restringir o acesso do usuário final.

A IdadeID, quando atuar como Operadora, realizará o tratamento de dados pessoais em nome do cliente contratante, conforme suas instruções legítimas e documentadas, os contratos aplicáveis, esta Política de Privacidade e a legislação vigente.

13.1 Obrigações do cliente contratante

O cliente contratante é responsável por utilizar a solução IdadeID de forma adequada, proporcional, segura e compatível com a legislação aplicável ao seu segmento.

Entre outras obrigações, caberá ao cliente contratante:

- a) definir corretamente a finalidade de uso da verificação de idade em seu ambiente;
- b) identificar quais produtos, serviços, conteúdos, cadastros, compras, checkouts ou funcionalidades exigem restrição etária;
- c) configurar corretamente a idade mínima exigida;
- d) definir o nível de verificação adequado ao risco do seu segmento;
- e) informar seus usuários finais sobre o uso da IdadeID;
- f) manter sua própria Política de Privacidade, Termos de Uso e avisos legais atualizados;
- g) indicar a base legal aplicável ao tratamento realizado em seu ambiente;
- h) obter consentimentos ou apresentar avisos quando necessário;
- i) não utilizar a IdadeID para finalidades ilegais, abusivas, discriminatórias ou incompatíveis com a finalidade de verificação de idade;
- j) garantir que sua integração técnica esteja instalada corretamente;
- k) manter seu próprio site, app, checkout, backend, APIs e sistemas protegidos;
- l) não modificar, ocultar, remover ou contornar mecanismos de segurança da IdadeID;
- m) não expor publicamente secrets, tokens privados, credenciais ou chaves sensíveis;
- n) responder às solicitações dos titulares quando atuar como Controlador;
- o) cooperar com a IdadeID em casos de incidente, fraude, auditoria, requisição de autoridade ou solicitação de titular.

13.2 Decisão final de acesso, compra ou liberação

A IdadeID fornece uma solução tecnológica de apoio à verificação de idade, prevenção à fraude, controle de sessão e geração de evidências técnicas de auditoria.

A decisão final sobre permitir, negar, restringir ou condicionar o acesso do usuário final a determinado produto, serviço, conteúdo, cadastro, checkout, compra, área restrita, funcionalidade ou operação protegida caberá ao cliente contratante.

Essa decisão poderá considerar o resultado técnico fornecido pela IdadeID, as configurações do cliente, o segmento regulado, as obrigações legais aplicáveis, o risco da operação, políticas internas, documentação adicional, revisão manual ou qualquer outro critério legítimo definido pelo cliente.

A IdadeID não define, por conta própria, quais produtos ou serviços do cliente devem ser bloqueados, qual conteúdo é permitido ou proibido, qual usuário pode comprar, qual operação deve ser recusada ou qual obrigação legal específica incide sobre o negócio do cliente.

13.3 Base legal e transparência perante o usuário final

O cliente contratante será responsável por informar seus usuários finais, de forma clara e adequada, sobre o uso da IdadeID em seu ambiente, incluindo a existência de verificação de idade, a finalidade do tratamento, eventual uso de imagem facial, fallback documental, tecnologias antifraude e critérios gerais aplicáveis ao fluxo.

Também caberá ao cliente contratante definir e documentar a base legal aplicável ao tratamento realizado em seu ambiente, especialmente quando houver tratamento de dados sensíveis, dados biométricos, dados de adolescentes, fallback documental ou obrigações regulatórias específicas do segmento.

A IdadeID poderá disponibilizar textos de apoio, documentação técnica, modelos informativos ou orientações gerais, mas tais materiais não substituem a análise jurídica própria do cliente contratante.

13.4 Configuração, instalação e uso correto da solução

O cliente contratante é responsável por instalar, configurar e utilizar a IdadeID conforme a documentação técnica, as orientações fornecidas, o contrato aplicável e as melhores práticas de segurança.

Isso inclui, quando aplicável:

- a) cadastrar corretamente os domínios autorizados;
- b) utilizar a public key ou site key correspondente ao site correto;
- c) manter ativo apenas o site permitido pelo plano contratado, salvo contratação específica;
- d) configurar corretamente o modo de widget, checkout guard, middleware, API ou integração;
- e) validar o funcionamento da solução antes de publicar em produção;
- f) não reaproveitar indevidamente chaves, tokens ou sessões entre sites diferentes;
- g) não tentar burlar limites de plano, billing, verificação ou auditoria;
- h) não alterar o comportamento do widget de forma incompatível com a segurança da solução.

A IdadeID poderá bloquear, suspender, limitar ou revisar integrações que apresentem uso indevido, domínio inválido, configuração insegura, tentativa de burla, risco aos titulares, violação contratual ou incompatibilidade com a LGPD.

13.5 Responsabilidade pelo ambiente externo

A IdadeID não controla integralmente o ambiente técnico do cliente contratante, incluindo seu site, checkout, backend, hospedagem, plataforma de e-commerce, plugins, meios de pagamento, aplicativos, scripts de terceiros, gateways, sistemas internos, dispositivos físicos ou redes utilizadas.

Por isso, o cliente contratante será responsável por manter seu próprio ambiente seguro, atualizado e compatível com a integração da IdadeID.

A IdadeID não será responsável por falhas, vazamentos, bypasses, perda de dados, liberação indevida, indisponibilidade ou incidentes causados exclusivamente por:

- a) instalação incorreta da solução;
- b) alteração não autorizada do widget, plugin, API ou integração;

- c) remoção ou ocultação proposital do mecanismo de verificação;
- d) configuração incorreta de domínio, site, plano, idade mínima ou modo de verificação;
- e) falha no site, backend, checkout ou plataforma do cliente;
- f) falha de terceiros não controlados pela IdadeID;
- g) exposição de credenciais pelo cliente;
- h) uso de scripts conflitantes;
- i) tentativa de burla por parte do próprio cliente, usuário final ou terceiro;
- j) ausência de validação server-side no ambiente do cliente quando tecnicamente necessária.

13.6 Solicitações de titulares e autoridades

Quando o cliente contratante atuar como Controlador, caberá a ele responder às solicitações dos titulares relacionadas ao tratamento realizado em seu ambiente, bem como avaliar pedidos de acesso, correção, exclusão, oposição, revisão de decisão automatizada, portabilidade ou informação sobre compartilhamento.

A IdadeID poderá cooperar tecnicamente com o cliente contratante para localização de registros, validação de sessão, análise de eventos, exportação de metadados mínimos, investigação de fraude, resposta a incidentes ou atendimento de requisições de autoridades competentes.

A cooperação da IdadeID observará os limites técnicos, legais e contratuais aplicáveis, bem como a necessidade de preservar segurança, confidencialidade, direitos de terceiros, segredos comerciais e integridade da plataforma.

13.7 Uso proibido ou incompatível da solução

O cliente contratante não deverá utilizar a IdadeID para finalidades incompatíveis com verificação de idade, segurança, prevenção à fraude, controle de acesso, auditoria ou conformidade.

É proibido, entre outros usos:

- a) utilizar a IdadeID para vigilância indevida;
- b) utilizar a solução para reconhecimento facial em massa;
- c) criar banco biométrico próprio sem base legal adequada;
- d) discriminar usuários de forma ilegal ou abusiva;
- e) coletar dados além do necessário;
- f) reutilizar dados de verificação para marketing, publicidade comportamental ou enriquecimento de perfil;
- g) tentar extrair, armazenar ou reutilizar imagens faciais ou documentos fora da finalidade contratada;
- h) contornar regras de billing, plano, sessão, domínio ou segurança;
- i) usar a solução em produtos, serviços ou conteúdos ilegais;
- j) expor usuários finais a tratamento excessivo, desproporcional ou não informado.

A IdadeID poderá suspender ou encerrar o serviço quando identificar uso incompatível, abusivo, inseguro, ilegal ou em desacordo com esta Política, com os contratos aplicáveis ou com a legislação vigente.

13.8 Limitação da responsabilidade da IdadeID

A IdadeID será responsável pelos tratamentos que realizar sob sua própria governança, conforme seu papel em cada contexto.

Quando atuar como Operadora, a responsabilidade da IdadeID estará limitada ao tratamento realizado conforme as instruções legítimas do cliente contratante, os contratos aplicáveis, esta Política, a documentação técnica e a legislação de proteção de dados.

A IdadeID não assume responsabilidade pela decisão jurídica, comercial, regulatória ou operacional do cliente contratante sobre permitir ou impedir acesso, venda, cadastro, checkout, contratação, consumo de conteúdo ou uso de funcionalidade.

Também não assume responsabilidade por configurações incorretas, uso indevido, omissão de informações ao titular, ausência de base legal pelo cliente, descumprimento de obrigação setorial, falha em ambiente externo, bypass causado por integração insegura ou decisão final tomada pelo cliente em desacordo com o resultado técnico da verificação.

14. Limitações tecnológicas, inteligência artificial e decisões automatizadas

A IdadeID utiliza recursos tecnológicos para apoiar processos de verificação de idade, prevenção à fraude, análise de risco, validação de presença, detecção de inconsistências e geração de resultados técnicos de verificação.

Esses recursos podem incluir, conforme o modo contratado e a configuração do cliente:

- a) análise automatizada de imagem facial;
- b) estimativa de idade ou faixa etária;
- c) detecção de qualidade da captura;
- d) validação de presença ou liveness;
- e) identificação de sinais de spoofing, fraude, manipulação ou inconsistência;
- f) análise documental, quando houver fallback;
- g) scores de confiança;
- h) reason codes técnicos;
- i) regras automatizadas de aprovação, negativa, fallback ou revisão.

Embora a IdadeID adote medidas para aumentar a precisão, segurança e confiabilidade da solução, tecnologias de verificação automatizada, inteligência artificial, visão computacional, análise documental e detecção de fraude estão sujeitas a limitações técnicas, estatísticas e contextuais.

Entre as possíveis limitações estão:

- a) variações de iluminação, nitidez, enquadramento, reflexo, sombra ou qualidade da câmera;
- b) dificuldade de análise em imagens incompletas, desfocadas, comprimidas ou distorcidas;
- c) oclusões faciais, acessórios, baixa resolução, múltiplas pessoas na imagem ou ausência de rosto detectável;
- d) inconsistência entre dados fornecidos, imagem facial, documento ou contexto da sessão;

- e) erros de estimativa de idade em pessoas com aparência próxima à idade mínima exigida;
- f) possibilidade de falso positivo, falso negativo, resultado inconclusivo ou necessidade de fallback;
- g) limitações de modelos de inteligência artificial, provedores externos, APIs, infraestrutura, navegador, dispositivo, rede ou plataforma integrada;
- h) tentativas de fraude, spoofing, manipulação, replay, deepfake, adulteração de documento ou burla técnica;
- i) falhas de integração, indisponibilidade temporária, timeout, bloqueios por navegador, CSP, plataforma externa ou instabilidade de terceiros.

A IdadeID não garante que a solução será livre de erros, interrupções, falsos positivos, falsos negativos, tentativas de burla ou limitações técnicas. No entanto, a plataforma é projetada para reduzir riscos por meio de camadas de segurança, validação server-side, análise de confiança, fallback documental, registros de auditoria, detecção de comportamento suspeito e mecanismos de falha segura quando aplicável.

A solução da IdadeID deve ser compreendida como uma ferramenta tecnológica de apoio à decisão, segurança e conformidade, e não como garantia absoluta de idade, identidade, autenticidade documental, ausência de fraude ou conformidade plena do cliente contratante com todas as normas aplicáveis ao seu segmento.

A decisão final sobre permitir, negar, restringir ou condicionar acesso, cadastro, compra, checkout, contratação, consumo de conteúdo ou uso de funcionalidade caberá ao cliente contratante, considerando o resultado técnico fornecido pela IdadeID, suas próprias obrigações legais, políticas internas, nível de risco, configurações da solução e, quando necessário, revisão adicional.

14.1 Estimativa de idade e margem de erro

Quando a verificação utilizar estimativa visual de idade, o resultado será baseado em análise probabilística e poderá apresentar margem de erro, especialmente em casos de baixa qualidade de imagem, aparência próxima à idade mínima exigida, tentativa de fraude ou dados insuficientes.

Por isso, a IdadeID poderá utilizar regras conservadoras, níveis mínimos de confiança, reason codes, bloqueios automáticos, negativa, solicitação de nova captura ou fallback documental quando o resultado não for suficientemente seguro.

A ausência de aprovação automática não significa necessariamente que o usuário final seja menor de idade, assim como uma aprovação técnica não deve ser interpretada como identificação civil plena ou KYC completa, salvo quando houver contratação específica e controles adicionais.

14.2 Fallback e revisão

Quando a análise automatizada não for suficiente, apresentar baixa confiança, inconsistência, risco elevado ou falha técnica, a IdadeID poderá solicitar nova tentativa, nova captura, fallback documental, revisão técnica ou outro procedimento adicional compatível com a configuração do cliente contratante.

O fallback tem a finalidade de reduzir erros e aumentar a confiabilidade do processo, especialmente em casos limítrofes, imagens ruins, suspeita de fraude ou segmentos de maior risco.

14.3 Decisões automatizadas e direito de revisão

Determinados resultados da IdadeID poderão ser produzidos por tratamento automatizado de dados pessoais, incluindo sistemas algorítmicos ou de inteligência artificial.

Quando um resultado automatizado afetar interesses do titular, este poderá solicitar informações e, quando aplicável, revisão da decisão, nos termos da LGPD e da regulamentação aplicável. A ANPD vem tratando decisões automatizadas, transparência algorítmica e revisão de decisões baseadas em IA como temas relevantes para a proteção de dados pessoais.

A revisão poderá considerar elementos como:

- a) qualidade da imagem;
- b) falha de captura;
- c) resultado técnico;
- d) nível de confiança;
- e) reason code;
- f) necessidade de fallback;
- g) inconsistência documental;
- h) indício de fraude;
- i) erro técnico ou falha de integração.

Quando a IdadeID atuar como Operadora, a revisão poderá depender da participação do cliente contratante, que será o responsável pela decisão final de acesso, compra, cadastro ou liberação da funcionalidade.

14.4 Transparência e explicabilidade possível

A IdadeID buscará fornecer informações claras e compatíveis com a natureza da tecnologia utilizada, incluindo status da verificação, motivo técnico da decisão, necessidade de fallback ou erro operacional, quando aplicável.

No entanto, determinados detalhes técnicos, modelos, regras antifraude, parâmetros internos, pesos algorítmicos, mecanismos anti-burla, assinaturas de segurança, regras de risco e lógicas de detecção poderão ser protegidos por segurança da informação, segredo comercial, prevenção à fraude ou integridade da plataforma.

A transparência da IdadeID deverá equilibrar o direito do titular à informação com a necessidade de evitar que detalhes sensíveis sejam utilizados para burlar o sistema.

14.5 Dependência de terceiros e ambiente externo

A IdadeID poderá depender de provedores externos de infraestrutura, inteligência artificial, banco de dados, hospedagem, análise documental, autenticação, monitoramento, e-mail, billing, plataformas de e-commerce, gateways, APIs, navegadores, dispositivos, sistemas operacionais e conexão de internet.

Falhas, limitações, mudanças de política, indisponibilidade, bloqueios técnicos, lentidão, bugs, restrições de plataforma, alterações de navegador, CSP, scripts conflitantes ou instabilidade de terceiros poderão afetar temporariamente o funcionamento da solução.

A IdadeID adotará medidas razoáveis para reduzir impactos, mas não controla integralmente todos os ambientes externos onde a solução é instalada ou executada.

14.6 Limitação contra burla client-side

A IdadeID poderá utilizar widget, script, iframe, modal, checkout guard, middleware, API, plugin, adapter ou outros meios técnicos de integração.

Quando a integração depender apenas de elementos client-side, como JavaScript executado no navegador, existe risco técnico de manipulação, bloqueio, desativação, remoção ou tentativa de contorno por usuários avançados, extensões, configurações de navegador ou alterações no ambiente do cliente.

Por isso, a IdadeID recomenda que fluxos críticos sejam protegidos também por validação server-side, middleware, backend do cliente, API de validação, webhook, app/plugin oficial ou bloqueio antes da criação do pedido, cadastro, acesso ou operação protegida.

O widget é uma camada importante de verificação e experiência do usuário, mas não deve ser a única camada de segurança em segmentos de maior risco.

15. Uso de cookies e tecnologias similares

A IdadeID poderá utilizar cookies, local storage, session storage, tokens temporários, identificadores técnicos, pixels estritamente necessários, logs de sessão e tecnologias similares para permitir o funcionamento seguro da plataforma, manter sessões técnicas, validar verificações, proteger o acesso, prevenir fraudes, registrar eventos de auditoria, melhorar a estabilidade da solução e viabilizar integrações com sites, aplicativos, checkouts, e-commerces, plataformas externas e demais ambientes digitais.

Cookies e tecnologias similares são utilizados de forma proporcional à finalidade pretendida, observando os princípios da necessidade, minimização, transparência, segurança e prevenção previstos na LGPD.

A IdadeID não utiliza cookies ou tecnologias similares no processo de verificação de idade para vender dados pessoais, realizar publicidade comportamental baseada em dados sensíveis, criar perfis comerciais de usuários finais, monitorar navegação entre diferentes clientes sem finalidade legítima ou formar bases de rastreamento incompatíveis com a verificação de idade.

15.1 Cookies e tecnologias estritamente necessários

A IdadeID poderá utilizar cookies e tecnologias similares estritamente necessários para o funcionamento da solução.

Esses recursos podem ser utilizados para:

- a) manter o estado técnico da sessão de verificação;
- b) validar se uma sessão de acesso foi criada, expirada, revogada ou invalidada;
- c) evitar repetição indevida de verificações dentro do mesmo contexto permitido;
- d) proteger o processo contra fraude, replay, manipulação ou uso indevido;
- e) validar origem, domínio, site, tenant, public key ou contexto da integração;
- f) registrar eventos mínimos de segurança e auditoria;
- g) preservar a integridade do fluxo de acesso ou checkout;

- h) reduzir falhas técnicas, loops, erros de carregamento ou perda de sessão;
- i) lembrar preferências técnicas estritamente necessárias ao funcionamento da interface.

Esses cookies e tecnologias são necessários para a prestação do serviço e para a segurança da operação. A desativação desses recursos pelo navegador, dispositivo, extensão ou configuração do usuário poderá comprometer ou impedir o funcionamento da verificação de idade, da sessão de acesso, do checkout protegido ou de outra funcionalidade integrada.

15.2 Cookies de segurança e antifraude

A IdadeID poderá utilizar identificadores técnicos e mecanismos de segurança para detectar comportamento suspeito, tentativas repetidas, uso em domínio não autorizado, manipulação de sessão, remoção do widget, ocultação indevida de interface, tentativa de bypass, chamadas automatizadas, abuso de endpoints ou outras ações incompatíveis com a integridade da verificação.

Esses mecanismos poderão considerar dados como:

- a) identificador técnico de sessão;
- b) endereço IP;
- c) data e hora;
- d) domínio de origem;
- e) user agent;
- f) tipo de dispositivo e navegador;
- g) eventos de erro, bloqueio ou tentativa suspeita;
- h) status de validação do token;
- i) contexto técnico da verificação.

A IdadeID adota diretriz de coleta mínima para fins antifraude, priorizando sinais técnicos proporcionais ao risco da operação.

15.3 Tokens temporários e sessões técnicas

A IdadeID poderá utilizar tokens temporários assinados e identificadores de sessão para validar tecnicamente processos de verificação e acesso.

Esses tokens poderão conter ou estar vinculados a informações como:

- a) identificador da sessão;
- b) site_id;
- c) tenant_id;
- d) escopo da verificação;
- e) data de emissão;
- f) data de expiração;
- g) jti ou identificador único;
- h) status de validação, expiração ou revogação.

Tokens e sessões técnicas não devem ser tratados como autorização permanente de acesso. Eles devem possuir prazo limitado, escopo restrito, validação server-side e vínculo com o contexto específico da verificação.

A IdadeID não recomenda o uso de cookies permanentes ou de longa duração para liberação irrestrita de acesso a ambientes sujeitos a restrição etária, especialmente em segmentos sensíveis ou de maior risco.

15.4 Local storage, session storage e armazenamento no navegador

A IdadeID poderá utilizar local storage, session storage ou mecanismos equivalentes do navegador apenas quando necessário para funcionamento técnico da interface, continuidade temporária do fluxo, prevenção de erro, validação de sessão ou experiência mínima do usuário.

No entanto, a IdadeID não deve confiar exclusivamente em dados armazenados no navegador para decisões críticas de aprovação, liberação de acesso, billing, validação de idade ou autorização de checkout.

Qualquer dado vindo do navegador deverá ser validado no servidor antes de produzir efeitos críticos.

A IdadeID não armazena no navegador, como regra de segurança, chaves privadas, secrets, service role keys, lógica sensível de aprovação, dados biométricos persistentes, documentos, regras críticas de billing ou informações que permitam contornar a verificação.

15.5 Cookies analíticos e de desempenho

A IdadeID poderá utilizar cookies ou tecnologias similares de análise e desempenho em seu site institucional, painel ou ambientes próprios, com o objetivo de compreender métricas agregadas de uso, estabilidade, performance, erros, navegação, conversão, segurança e melhoria da experiência.

Quando esses cookies não forem estritamente necessários, a IdadeID deverá observar as exigências legais aplicáveis, incluindo transparência, base legal adequada e, quando necessário, mecanismo de consentimento ou opção de gerenciamento pelo titular.

No processo de verificação de idade em ambiente de clientes, a IdadeID deverá evitar o uso de cookies analíticos não essenciais que ampliem desnecessariamente a coleta de dados de usuários finais.

15.6 Cookies de marketing

A IdadeID poderá utilizar cookies de marketing ou tecnologias semelhantes em seu site institucional apenas quando houver finalidade legítima, transparência adequada e, quando aplicável, consentimento ou mecanismo de escolha pelo titular.

A IdadeID não deverá utilizar dados sensíveis coletados no processo de verificação de idade, imagens faciais, documentos, resultados de análise, scores de confiança ou informações de maioridade para publicidade comportamental, remarketing, segmentação comercial ou venda de dados.

Dados de usuários finais submetidos à verificação não devem ser usados para campanhas comerciais da IdadeID ou de terceiros.

15.7 Gestão de preferências e consentimento

Quando aplicável, a IdadeID poderá disponibilizar mecanismos para que o titular gerencie preferências relacionadas ao uso de cookies não essenciais, especialmente no site institucional e em ambientes próprios.

Cookies estritamente necessários, de segurança, autenticação, prevenção à fraude e manutenção da sessão técnica poderão permanecer ativos, pois são indispensáveis para funcionamento seguro da solução.

A ANPD recomenda que banners e políticas de cookies sejam claros, específicos e capazes de permitir ao titular compreender as finalidades dos cookies utilizados.

15.8 Cookies e tecnologias de terceiros

A IdadeID poderá utilizar tecnologias de terceiros em seu site institucional, painel, infraestrutura ou integrações, como provedores de hospedagem, autenticação, segurança, analytics, atendimento, cobrança, e-mail, monitoramento e inteligência artificial.

Esses terceiros poderão utilizar cookies ou identificadores próprios conforme suas respectivas políticas, contratos e configurações técnicas.

Quando a IdadeID atuar como Controladora, buscará limitar o uso de terceiros ao necessário e adotar fornecedores compatíveis com padrões adequados de proteção de dados.

Quando a IdadeID atuar como Operadora em ambiente de cliente contratante, o uso de tecnologias de terceiros deverá observar as instruções legítimas do cliente, os contratos aplicáveis e a finalidade da solução.

15.9 Responsabilidade do cliente contratante

O cliente contratante é responsável por informar seus usuários finais, em sua própria Política de Privacidade, Política de Cookies, Termos de Uso ou aviso equivalente, sobre o uso da IdadeID e de cookies ou tecnologias similares no ambiente sob seu controle.

Também caberá ao cliente contratante avaliar a necessidade de banner de cookies, consentimento, gestão de preferências, avisos específicos ou ajustes técnicos em seu próprio site, app, e-commerce, checkout, vending machine ou plataforma.

A IdadeID poderá fornecer orientações gerais, mas essas orientações não substituem a análise jurídica própria do cliente contratante.

15.10 Limitações técnicas

A desativação, bloqueio ou remoção de cookies, JavaScript, local storage, session storage ou tecnologias similares poderá comprometer ou impedir o funcionamento da verificação de idade, da sessão de acesso, do checkout protegido, do painel administrativo ou de outras funcionalidades da IdadeID.

Quando houver falha técnica, ausência de cookie necessário, token inválido, sessão expirada, domínio não autorizado, configuração ausente ou tentativa de manipulação, a IdadeID poderá adotar comportamento de falha segura, bloqueio, nova verificação, fallback ou recusa de validação, conforme o contexto e a configuração aplicável.

16. Alterações nesta Política de Privacidade

A IdadeID poderá atualizar, revisar ou alterar esta Política de Privacidade a qualquer momento, especialmente para refletir mudanças legais, regulatórias, técnicas, operacionais, comerciais, contratuais, de segurança, de arquitetura da plataforma, de fornecedores, de funcionalidades, de bases legais, de categorias de dados tratados, de prazos de retenção ou de formas de compartilhamento.

A versão vigente desta Política estará sempre disponível nos canais oficiais da IdadeID, com indicação da data da última atualização.

Quando houver alterações relevantes que possam impactar de forma significativa os titulares de dados pessoais, os clientes contratantes ou o modo de tratamento dos dados, a IdadeID poderá adotar medidas razoáveis de comunicação, tais como:

- a) publicação de aviso em seu site institucional;
- b) aviso no painel administrativo da plataforma;
- c) envio de comunicação por e-mail aos clientes contratantes;
- d) destaque temporário da alteração na própria Política;
- e) comunicação contratual específica, quando aplicável;
- f) atualização de documentos complementares, como Termos de Uso, contratos, aditivos de tratamento de dados, documentação técnica ou política de cookies.

Alterações meramente formais, editoriais, corretivas, organizacionais ou que não modifiquem substancialmente a forma de tratamento de dados poderão ser realizadas sem comunicação individual prévia, mantendo-se a versão atualizada disponível para consulta.

Quando a alteração envolver nova finalidade relevante de tratamento, nova categoria sensível de dados, novo compartilhamento substancial, mudança importante de base legal, alteração significativa de retenção, novo uso de tecnologia de alto risco ou modificação material na relação entre IdadeID e cliente contratante, a IdadeID avaliará a necessidade de comunicação adicional, ajuste contratual, atualização de avisos, obtenção de consentimento quando aplicável ou adoção de medidas complementares de transparência.

O uso contínuo dos serviços da IdadeID após a publicação de nova versão desta Política indicará ciência da versão vigente, sem prejuízo dos direitos dos titulares previstos na LGPD, dos direitos dos clientes contratantes previstos em contrato e das obrigações legais aplicáveis.

Quando a IdadeID atuar como Operadora, alterações relevantes nesta Política poderão exigir que o cliente contratante atualize seus próprios documentos, avisos, políticas, termos, banners ou comunicações aos usuários finais, especialmente quando a mudança afetar o fluxo de verificação, categorias de dados tratados, finalidade, retenção, compartilhamento ou uso de suboperadores.

Caberá ao cliente contratante avaliar, em seu próprio ambiente, se a atualização desta Política exige ajustes em sua Política de Privacidade, Termos de Uso, Política de Cookies, avisos de verificação de idade, contratos com usuários ou demais documentos legais.

A IdadeID poderá manter histórico de versões anteriores desta Política para fins de transparência, auditoria, governança, atendimento a solicitações, defesa de direitos e demonstração de conformidade.

17. Contato, encarregado e canal de privacidade

Para dúvidas, solicitações, reclamações, comunicações ou exercício de direitos relacionados ao tratamento de dados pessoais pela IdadeID, o titular poderá entrar em contato pelo canal oficial de privacidade:

privacidade@idadeid.com.br

Esse canal poderá ser utilizado para solicitações relacionadas a:

- a) confirmação de tratamento de dados pessoais;
- b) acesso a dados pessoais;
- c) correção, anonimização, bloqueio ou eliminação de dados;
- d) informações sobre compartilhamento de dados;
- e) revogação de consentimento, quando aplicável;
- f) oposição ao tratamento, quando cabível;
- g) revisão de decisão automatizada, quando aplicável;
- h) dúvidas sobre esta Política de Privacidade;
- i) comunicações relacionadas a segurança, fraude, incidente ou uso indevido da solução.

A IdadeID poderá solicitar informações adicionais estritamente necessárias para confirmar a identidade do solicitante, localizar o tratamento relacionado, proteger dados de terceiros, prevenir fraude e evitar acesso indevido a informações pessoais.

Quando a solicitação estiver relacionada a uma verificação realizada em ambiente de cliente contratante, como site, aplicativo, e-commerce, checkout, vending machine ou plataforma integrada, a IdadeID poderá atuar como Operadora. Nesse caso, o cliente contratante poderá ser o Controlador responsável pela resposta principal ao titular, e a IdadeID poderá cooperar tecnicamente para atendimento da solicitação, conforme a LGPD, os contratos aplicáveis e as instruções legítimas do cliente.

Quando a solicitação estiver relacionada a dados tratados diretamente pela IdadeID para finalidades próprias, como site institucional, atendimento comercial, suporte, billing, painel administrativo, contratos, segurança da plataforma ou comunicações institucionais, a IdadeID atuará como Controladora e responderá ao titular conforme a legislação aplicável.

17.1 Encarregado pelo tratamento de dados pessoais

A IdadeID poderá indicar encarregado pelo tratamento de dados pessoais, responsável por atuar como canal de comunicação entre a IdadeID, os titulares de dados pessoais, os clientes contratantes e a Autoridade Nacional de Proteção de Dados - ANPD, observadas as atribuições previstas na LGPD e na regulamentação aplicável.

Encarregado pelo Tratamento de Dados Pessoais: Vinicius Pauletti - IdadeID Canal oficial de privacidade: privacidade@idadeid.com.br Site: www.idadeid.com.br

17.2 Atendimento a autoridades e clientes contratantes

Comunicações formais de autoridades públicas, órgãos reguladores, clientes contratantes ou parceiros relacionadas à proteção de dados, incidentes, auditorias, requisições legais ou obrigações contratuais também poderão ser encaminhadas para:

privacidade@idadeid.com.br

A IdadeID poderá solicitar documentação complementar, identificação do solicitante, comprovação de poderes, referência contratual, número de processo, ordem formal ou demais informações necessárias para validação da solicitação.

17.3 Limites do canal de privacidade

O canal de privacidade não deve ser utilizado para suporte comercial comum, dúvidas de venda, negociação de planos, atendimento financeiro ou suporte técnico não relacionado à proteção de dados pessoais, salvo quando a solicitação também envolver privacidade, segurança, LGPD, dados pessoais ou direitos de titulares. Para assuntos comerciais e suporte ordinário, deverão ser utilizados os canais comerciais e operacionais divulgados no site oficial da IdadeID.

Solicitações genéricas, incompletas, abusivas, repetitivas, fraudulentas ou que coloquem em risco dados de terceiros poderão exigir validação adicional ou poderão ser respondidas dentro dos limites permitidos pela legislação aplicável.

17.4 Peticionamento perante a ANPD

O titular de dados pessoais tem o direito de peticionar em relação aos seus dados perante a Autoridade Nacional de Proteção de Dados - ANPD, observados os

procedimentos aplicáveis. A LGPD prevê a possibilidade de o titular peticionar contra o controlador perante a autoridade nacional.

A IdadeID recomenda que o titular, sempre que possível, entre em contato inicialmente pelo canal de privacidade indicado nesta Política, para que a solicitação possa ser analisada e respondida diretamente.

18. Disposições finais

Esta Política de Privacidade integra o conjunto de documentos legais, técnicos e contratuais da IdadeID, devendo ser interpretada em conjunto com os Termos de Uso, contratos comerciais, aditivos de tratamento de dados, propostas, documentação técnica, políticas de segurança, políticas de cookies e demais instrumentos aplicáveis à relação entre a IdadeID, seus clientes contratantes, parceiros e usuários finais.

A presente Política tem por objetivo informar, de forma transparente, como a IdadeID trata dados pessoais no contexto de sua plataforma, observando os princípios, direitos e obrigações previstos na Lei Geral de Proteção de Dados Pessoais - LGPD, Lei nº 13.709/2018, que disciplina o tratamento de dados pessoais no Brasil, inclusive em meios digitais.

Caso exista divergência entre esta Política de Privacidade e contrato específico firmado com cliente contratante, prevalecerão as disposições contratuais específicas naquilo que forem mais detalhadas, desde que compatíveis com a LGPD, com a regulamentação aplicável e com os direitos dos titulares de dados pessoais.

A eventual invalidade, nulidade ou inexistência de qualquer disposição desta Política não afetará a validade das demais cláusulas, que permanecerão em pleno vigor e efeito.

A omissão ou tolerância da IdadeID quanto ao descumprimento de qualquer obrigação prevista nesta Política, em contratos aplicáveis ou na documentação técnica não constituirá renúncia de direito, alteração contratual ou autorização para descumprimentos futuros.

A IdadeID poderá adotar medidas técnicas, administrativas, contratuais ou operacionais adicionais sempre que necessário para proteger dados pessoais, prevenir fraudes, responder a incidentes, cumprir obrigações legais, atender autoridades competentes, preservar direitos ou garantir a integridade da plataforma.

Em caso de incidente de segurança envolvendo dados pessoais que possa acarretar risco ou dano relevante aos titulares, a IdadeID adotará as medidas cabíveis conforme

seu papel no tratamento, a LGPD, a regulamentação da ANPD e os contratos aplicáveis. A ANPD publicou a Resolução CD/ANPD nº 15/2024, que regulamenta procedimentos de comunicação de incidentes de segurança envolvendo dados pessoais.

Quando atuar como Operadora, a IdadeID poderá comunicar e cooperar com o cliente contratante, para que este, na condição de Controlador, avalie as providências legais, regulatórias e operacionais cabíveis. Quando atuar como Controladora, a IdadeID avaliará diretamente as medidas aplicáveis, incluindo eventual comunicação a titulares, autoridades ou partes envolvidas, quando exigido pela legislação.

Esta Política não deve ser interpretada como promessa de segurança absoluta, garantia infalível de identificação, garantia plena de conformidade legal do cliente contratante ou substituição da análise jurídica própria de cada negócio. A IdadeID fornece uma solução tecnológica de apoio à verificação de idade, segurança, prevenção à fraude e auditoria, cabendo ao cliente contratante avaliar suas obrigações legais, regulatórias e setoriais específicas.

A disponibilização e utilização da solução IdadeID deve observar esta Política, os Termos de Uso, os contratos aplicáveis e a documentação técnica correspondente, sem prejuízo dos direitos assegurados aos titulares de dados pessoais pela LGPD.

A versão vigente desta Política de Privacidade será sempre aquela publicada nos canais oficiais da IdadeID, identificada pela respectiva data de atualização.

Última atualização: 29 de maio de 2026 Canal de privacidade: privacidade@idadeid.com.br
Encarregado pelo Tratamento de Dados Pessoais: Vinicius Pauletti - IdadeID Site oficial: www.idadeid.com.br

© 2026 IdadeID. Todos os direitos reservados.