POLÍTICA DE RETENÇÃO E DESCARTE DE DADOS PESSOAIS

1. OBJETIVO E FUNDAMENTOS

A presente Política de Retenção e Descarte de Dados Pessoais estabelece os critérios, prazos e procedimentos adotados pela **Aizen Tecnologia Ltda**., sociedade empresária inscrita no CNPJ sob o nº 63.740.359/0001-15, com sede na Rua Henri Dunant, 792, Apt 2306, Santo Amaro, São Paulo/SP, CEP 04709-110 (“**Aizen**”) para retenção, armazenamento e eliminação de dados pessoais tratados no âmbito de suas atividades, em observância aos princípios da necessidade e finalidade estabelecidos nos incisos III e I do artigo 6º da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - "LGPD"), garantindo que dados pessoais sejam mantidos apenas pelo período estritamente necessário ao cumprimento das finalidades para as quais foram coletados, ao atendimento de obrigações legais e regulatórias, ou ao exercício regular de direitos em processos judiciais, administrativos ou arbitrais.

Esta política fundamenta-se no princípio de que dados pessoais não devem ser armazenados indefinidamente, mas apenas enquanto justificáveis por finalidade legítima, base legal adequada ou obrigação regulatória específica. A eliminação tempestiva de dados que não mais atendam a tais critérios constitui medida essencial de proteção à privacidade dos titulares, reduzindo riscos associados a incidentes de segurança e garantindo conformidade com a legislação de proteção de dados.

2. ABRANGÊNCIA E APLICAÇÃO

Esta política aplica-se a todos os dados pessoais tratados pela Aizen, independentemente do formato em que estejam armazenados (digital ou físico), do sistema ou repositório utilizado, da localização geográfica de armazenamento ou da finalidade de tratamento. Abrange dados pessoais de usuários da plataforma, colaboradores, prestadores de serviço, candidatos a vagas de emprego, parceiros comerciais e quaisquer outras pessoas naturais cujos dados sejam tratados pela Aizen no curso de suas atividades empresariais.

Todos os colaboradores, prestadores de serviço, administradores de sistemas e demais pessoas que, em razão de suas funções, tenham acesso a dados pessoais ou responsabilidade sobre sistemas de armazenamento devem conhecer e observar rigorosamente as disposições desta política, sendo a inobservância dos prazos e procedimentos aqui estabelecidos considerada infração às normas internas de proteção de dados, sujeita a medidas disciplinares conforme a gravidade do descumprimento.

3. CATEGORIAS DE DADOS E PRAZOS DE RETENÇÃO

Os dados pessoais tratados pela Aizen são categorizados conforme sua natureza e finalidade de tratamento, sendo estabelecidos prazos específicos de retenção para cada

categoria, considerando-se as bases legais aplicáveis, obrigações regulatórias do setor financeiro e necessidade de preservação para exercício regular de direitos.

DADOS CADASTRAIS DE USUÁRIOS

Dados cadastrais básicos fornecidos no momento do registro na plataforma, incluindo nome completo, número de inscrição no Cadastro de Pessoas Físicas, endereço de correio eletrônico, número de telefone celular e outras informações de identificação e contato, são mantidos durante todo o período em que a conta do usuário permanecer ativa na plataforma, acrescidos de período adicional de cinco anos contados a partir da data de encerramento da conta, seja por solicitação do próprio usuário ou por iniciativa da Aizen.

O prazo de cinco anos após encerramento da conta justifica-se pela necessidade de cumprimento de obrigações legais e regulatórias aplicáveis ao setor financeiro, especialmente aquelas relacionadas à prevenção à lavagem de dinheiro e financiamento ao terrorismo estabelecidas pela Lei nº 9.613/1998 e regulamentação do Conselho de Controle de Atividades Financeiras, bem como pela preservação de informações necessárias ao exercício regular de direitos em eventual litígio decorrente da relação contratual, considerando-se os prazos prescricionais aplicáveis. Decorrido o prazo de cinco anos sem que subsista obrigação legal, regulatória ou necessidade de defesa em litígio específico, os dados cadastrais são eliminados de forma definitiva e segura.

DADOS FINANCEIROS DE OPEN BANKING

Dados financeiros obtidos mediante integração com o sistema de Open Banking, incluindo informações sobre transações bancárias, saldos de contas correntes e de poupança, extratos, histórico de movimentações, informações sobre cartões de crédito e débito, investimentos, empréstimos e financiamentos, são tratados com base no consentimento específico fornecido pelo titular conforme regulamentação do Banco Central do Brasil estabelecida pela Resolução Conjunta BCB/CMN nº 1/2020.

Os dados de Open Banking são mantidos enquanto o consentimento estiver ativo e válido, observando-se o prazo máximo de doze meses estabelecido pela regulamentação, renovável mediante manifestação expressa do titular. Após a revogação do consentimento pelo titular ou a expiração do prazo de validade sem renovação, o acesso a novos dados bancários cessa imediatamente, porém os dados já coletados e armazenados anteriormente à revogação ou expiração são mantidos pelo prazo adicional de cinco anos, fundamentado nas mesmas bases legais aplicáveis aos dados cadastrais, notadamente cumprimento de obrigações regulatórias do setor financeiro e preservação para defesa de direitos.

Esse prazo estendido de retenção, mesmo após revogação do consentimento, ampara-se na mudança de base legal de consentimento para cumprimento de obrigação legal e legítimo interesse do controlador, conforme previsto nos incisos II e IX do artigo 7º da LGPD, sendo os titulares informados sobre tal prática na Política de Privacidade da plataforma.

DADOS DE NAVEGAÇÃO E USO DA PLATAFORMA

Dados técnicos e de navegação coletados automaticamente durante a utilização da plataforma, incluindo endereços de protocolo de Internet, identificadores únicos de dispositivo, tipo e versão de sistema operacional e navegador, dados de geolocalização aproximada, horários de acesso, páginas visitadas, funcionalidades utilizadas, tempo de permanência e padrões de interação, são mantidos enquanto a conta do usuário permanecer ativa, acrescidos de período adicional de doze meses após o encerramento da conta.

O prazo de doze meses pós-encerramento justifica-se pela necessidade de manter capacidade de investigação de eventuais atividades fraudulentas ou ilícitas que possam ter ocorrido durante o período de utilização da plataforma, bem como pela preservação de logs necessários à comprovação de conformidade com obrigações regulatórias caso sejam objeto de fiscalização ou auditoria por autoridades competentes. Transcorrido esse prazo, os dados de navegação são anonimizados de forma irreversível ou eliminados.

HISTÓRICO DE CONVERSAS COM A ALEAH

As interações dos usuários com a Aleah, assistente virtual baseada em inteligência artificial, incluindo mensagens trocadas, perguntas formuladas, respostas fornecidas, contexto de conversações e metadados associados, são armazenadas enquanto a conta do usuário permanecer ativa, permitindo personalização progressiva das recomendações e manutenção de contexto entre diferentes sessões de conversa.

Após o encerramento da conta, o histórico de conversas é mantido pelo prazo adicional de doze meses para permitir eventual reativação da conta pelo usuário com preservação de preferências e contexto histórico, bem como para análise de qualidade do serviço e aprimoramento dos algoritmos de inteligência artificial. Decorrido esse prazo, as conversas identificáveis são eliminadas, podendo ser mantidas apenas versões anonimizadas de forma irreversível para fins de pesquisa, desenvolvimento e melhoria dos modelos de processamento de linguagem natural, conforme previsto no artigo 12 da LGPD.

METAS FINANCEIRAS E PREFERÊNCIAS DO USUÁRIO

Informações sobre objetivos financeiros definidos pelo usuário, preferências declaradas, configurações personalizadas da plataforma e outros dados relacionados à experiência individualizada são mantidos exclusivamente enquanto a conta permanecer ativa, sendo eliminados imediatamente após o encerramento da conta, salvo se o usuário expressamente solicitar exportação prévia de tais informações para exercício do direito à portabilidade de dados previsto no inciso V do artigo 18 da LGPD.

DADOS DE MARKETING E COMUNICAÇÕES PROMOCIONAIS

Caso sejam implementadas no futuro funcionalidades de marketing direto ou envio de comunicações promocionais, os dados pessoais tratados com base em consentimento

específico para tais finalidades, incluindo endereços de correio eletrônico, preferências de comunicação, histórico de interações com campanhas e segmentações de interesse, serão mantidos exclusivamente enquanto o consentimento permanecer válido e ativo, sendo eliminados no prazo máximo de trinta dias após a revogação do consentimento pelo titular, salvo quando tais dados também sejam utilizados para outras finalidades amparadas em bases legais distintas, hipótese em que se aplicarão os prazos de retenção correspondentes a tais finalidades.

DADOS PARA CUMPRIMENTO DE OBRIGAÇÕES REGULATÓRIAS ESPECÍFICAS

Determinadas categorias de dados pessoais devem ser mantidas por prazos específicos em cumprimento a obrigações legais e regulatórias do setor financeiro, independentemente da revogação de consentimento ou encerramento da relação contratual. Dados relacionados a operações de crédito, identificação de clientes para fins de prevenção à lavagem de dinheiro, registros de transações financeiras e documentação comprobatória de diligências de conhecimento de cliente (know your customer) são mantidos pelo prazo mínimo de cinco anos contados da conclusão da operação ou do encerramento da conta, podendo estender-se até dez anos conforme determinações específicas do Banco Central do Brasil, do Conselho Monetário Nacional ou de outras autoridades reguladoras competentes.

A manutenção desses dados após o término da relação contratual ampara-se na base legal de cumprimento de obrigação legal prevista no inciso II do artigo 7º da LGPD, prevalecendo sobre eventual solicitação de eliminação formulada pelo titular, conforme expressamente previsto no parágrafo 3º do artigo 16 da LGPD, que estabelece a impossibilidade de eliminação quando a manutenção dos dados for necessária para o cumprimento de obrigação legal ou regulatória pelo controlador.

DADOS DE COLABORADORES E PRESTADORES DE SERVIÇO

Dados pessoais de colaboradores, incluindo informações cadastrais, documentação trabalhista, registros de ponto, avaliações de desempenho, histórico de treinamentos e demais informações relacionadas à relação de emprego, são mantidos durante todo o período de vigência do contrato de trabalho, acrescidos de período adicional que varia conforme a natureza dos dados. Dados relacionados a obrigações trabalhistas e previdenciárias são mantidos por no mínimo cinco anos após o término do vínculo empregatício, podendo estender-se por prazos superiores quando exigido por legislação específica, como no caso de documentação relacionada ao Fundo de Garantia do Tempo de Serviço ou a processos administrativos ou judiciais trabalhistas.

Dados de prestadores de serviço, incluindo informações contratuais, documentação fiscal, comprovantes de pagamento e registros de execução de serviços, são mantidos pelo prazo mínimo de cinco anos contados do término do contrato, em conformidade com prazos prescricionais aplicáveis e necessidade de comprovação de regularidade fiscal e contábil perante autoridades competentes.

DADOS DE CANDIDATOS A VAGAS DE EMPREGO

Dados pessoais de candidatos a processos seletivos, incluindo currículos, cartas de apresentação, resultados de avaliações, entrevistas e demais informações coletadas durante o processo de recrutamento e seleção, são mantidos pelo prazo máximo de doze meses contados da conclusão do processo seletivo específico para o qual o candidato se inscreveu, possibilitando consideração do candidato para outras oportunidades que surjam nesse período. Decorrido tal prazo, os dados são eliminados, salvo se o candidato expressamente autorizar manutenção por prazo superior ou se houver necessidade de preservação para defesa em reclamação trabalhista ou processo administrativo relacionado ao processo seletivo.

4. BASES LEGAIS PARA RETENÇÃO APÓS TÉRMINO DA FINALIDADE ORIGINAL

A manutenção de dados pessoais após o término da finalidade original de tratamento ou após revogação de consentimento fundamenta-se em bases legais autônomas e legítimas previstas na LGPD, conforme a categoria de dados e a natureza da obrigação que justifica a retenção estendida.

O cumprimento de obrigação legal ou regulatória pelo controlador, previsto no inciso II do artigo 7º da LGPD, constitui base legal que independe de consentimento do titular e que prevalece sobre eventuais solicitações de eliminação, conforme expressamente estabelecido no parágrafo 3º do artigo 16 da LGPD. Essa base legal justifica a retenção de dados necessários ao atendimento de exigências do Banco Central do Brasil, do Conselho de Controle de Atividades Financeiras, da Receita Federal do Brasil e demais autoridades reguladoras que estabeleçam prazos mínimos de guarda de documentação e informações.

O uso regular de dados pessoais em processo judicial, administrativo ou arbitral, previsto no inciso II do parágrafo 4º do artigo 16 da LGPD, fundamenta a manutenção de dados enquanto perdurar a necessidade de preservação para defesa de direitos ou cumprimento de determinações emanadas de autoridades competentes, cessando tal necessidade apenas com o trânsito em julgado da decisão final ou encerramento definitivo do processo.

O exercício regular de direitos em contrato e em processo judicial, administrativo ou arbitral, previsto no inciso VI do artigo 7º da LGPD, justifica a manutenção de dados durante os prazos prescricionais aplicáveis a cada tipo de pretensão, considerando-se que a eliminação prematura de dados poderia comprometer a capacidade de defesa em eventual litígio decorrente da relação contratual.

A proteção do crédito, prevista no inciso X do artigo 7º da LGPD, pode fundamentar a manutenção de determinadas informações financeiras necessárias à comprovação de histórico de relacionamento com instituições financeiras parceiras ou à demonstração de

regularidade em operações de crédito anteriormente realizadas por intermédio da plataforma.

5. PROCEDIMENTOS DE ELIMINAÇÃO SEGURA

A eliminação de dados pessoais ao término dos prazos de retenção aplicáveis é conduzida mediante procedimentos técnicos que garantem a impossibilidade de recuperação das informações, seja por meios convencionais ou por técnicas forenses avançadas, protegendo definitivamente a privacidade dos titulares e prevenindo utilizações indevidas posteriores.

Dados armazenados em backups são igualmente eliminados mediante rotinas automatizadas que identificam informações cujo prazo de retenção tenha expirado e procedem à sua remoção dos repositórios de backup, ou mediante eliminação completa de versões de backup que contenham preponderantemente dados já expirados. Sistemas de backup são configurados com políticas de retenção compatíveis com os prazos estabelecidos nesta política, garantindo que dados não permaneçam indefinidamente preservados em cópias de segurança após sua eliminação dos sistemas de produção.

Para dados armazenados em mídias físicas removíveis, como discos rígidos externos, pen drives, cartões de memória ou outras mídias magnéticas ou de estado sólido, a eliminação segura ocorre mediante destruição física das mídias por meio de trituração mecânica, desmagnetização de alta intensidade ou desintegração, conforme apropriado ao tipo de mídia. Quando a destruição física não for viável por razões operacionais, procede-se à sobrescrita completa das mídias utilizando ferramentas especializadas, seguida de teste de verificação para confirmar a impossibilidade de recuperação de dados.

Documentos físicos que contenham dados pessoais são eliminados mediante fragmentação em partículas de dimensões reduzidas utilizando equipamentos trituradores de segurança de nível adequado, conforme normas técnicas aplicáveis, ou mediante incineração supervisionada quando o volume de documentos ou a sensibilidade das informações justifiquem tal procedimento. A simples disposição de documentos em lixo comum ou reciclagem sem fragmentação prévia é absolutamente vedada, considerando-se os riscos de acesso indevido e violação de privacidade.

Registros de auditoria (logs) das operações de eliminação são mantidos pelo prazo mínimo de cinco anos, documentando a data de eliminação, a categoria de dados eliminados, o volume aproximado de registros processados, a metodologia técnica utilizada e a identificação do responsável pela execução do procedimento, permitindo comprovação de conformidade com esta política perante autoridades competentes ou titulares que questionem o tratamento de seus dados.

6. ANONIMIZAÇÃO COMO ALTERNATIVA À ELIMINAÇÃO

Em determinadas situações, a anonimização de dados pessoais constitui alternativa legítima à eliminação completa, permitindo que informações continuem sendo utilizadas para finalidades estatísticas, de pesquisa, desenvolvimento de produtos ou melhoria de serviços sem comprometer a privacidade dos titulares, considerando-se que dados efetivamente anonimizados deixam de ser considerados dados pessoais nos termos do artigo 12 da LGPD.

A anonimização é realizada mediante aplicação de técnicas reconhecidas que removem ou modificam dados identificadores diretos e indiretos de forma que a identificação do titular torne-se impossível mesmo mediante esforços razoáveis, considerando-se fatores como custo, tempo necessário, tecnologias disponíveis e possibilidade de cruzamento com outras bases de dados. Técnicas de anonimização incluem generalização de atributos, supressão de identificadores, agregação de dados em níveis que impeçam individualização, inserção de ruído estatístico e aplicação de modelos de privacidade diferencial.

A adequação da anonimização é periodicamente reavaliada considerando-se a evolução de tecnologias de reidentificação e a disponibilidade de novas bases de dados públicas ou comerciais que possam facilitar cruzamentos. Quando avaliações de risco indicarem que dados anteriormente considerados anonimizados possam ser reidentificados mediante técnicas contemporâneas, procede-se ao reforço das técnicas de anonimização ou à eliminação completa dos dados conforme apropriado.

Dados anonimizados são segregados de dados pessoais identificáveis em repositórios distintos, sendo implementados controles técnicos e organizacionais que impeçam reconexão acidental ou intencional de dados anonimizados com identificadores que permitam reidentificação dos titulares.

7. MONITORAMENTO E AUTOMAÇÃO

A execução dos prazos de retenção e dos procedimentos de eliminação é amplamente automatizada mediante implementação de rotinas sistêmicas que identificam dados cujo prazo de retenção tenha expirado e procedem automaticamente à sua eliminação ou anonimização conforme apropriado, reduzindo riscos de manutenção indevida por esquecimento ou falha humana.

Sistemas de gestão de dados são configurados com regras de retenção parametrizadas conforme as categorias e prazos estabelecidos nesta política, executando verificações periódicas, preferencialmente diárias ou semanais conforme o volume de dados tratados, para identificar registros elegíveis para eliminação. Alertas automáticos são gerados quando a execução de rotinas de eliminação falhar ou quando volumes anormalmente

elevados ou reduzidos de registros forem identificados para eliminação, permitindo investigação de possíveis problemas técnicos ou inconsistências de dados.

Relatórios gerenciais são produzidos mensalmente pelo Encarregado de Proteção de Dados, consolidando estatísticas sobre volumes de dados eliminados ou anonimizados no período, categorias de dados processadas, conformidade com cronogramas de eliminação planejados e eventuais exceções ou adiamentos de eliminação motivados por litígios em curso ou determinações de autoridades competentes.

8. EXCEÇÕES E SUSPENSÕES TEMPORÁRIAS DE ELIMINAÇÃO

A eliminação de dados pessoais pode ser temporariamente suspensa nas seguintes hipóteses excepcionais, prevalecendo a necessidade de preservação sobre os prazos ordinários de retenção estabelecidos nesta política.

Quando houver processo judicial, administrativo ou arbitral em curso no qual a Aizen figure como parte ou possa vir a ser demandada, e os dados pessoais sejam relevantes para defesa de direitos ou cumprimento de obrigações processuais, tais dados são preservados até o trânsito em julgado da decisão final ou encerramento definitivo do processo, independentemente de terem transcorrido os prazos ordinários de retenção. A suspensão de eliminação é documentada com identificação do processo que a justifica, sendo os dados segregados em repositório específico com acesso restrito e finalidade exclusiva de preservação probatória.

Determinações emanadas de autoridades judiciais, administrativas ou policiais que ordenem a preservação de dados pessoais específicos para fins de investigação criminal, processo administrativo sancionador ou outras finalidades legítimas de interesse público justificam a manutenção dos dados pelo prazo indicado na ordem ou até que seja expressamente autorizada sua eliminação. Tais determinações são rigorosamente documentadas e periodicamente revisadas para confirmar a subsistência da necessidade de preservação.

Auditorias em curso conduzidas por autoridades reguladoras, auditores externos independentes ou órgãos de controle que exijam acesso a dados históricos podem ensejar suspensão temporária de eliminação até a conclusão dos trabalhos de auditoria e emissão de relatório final, sendo a suspensão limitada às categorias de dados efetivamente relevantes para o escopo da auditoria.

Todas as exceções e suspensões temporárias de eliminação são formalmente documentadas pelo Encarregado de Proteção de Dados, incluindo justificativa detalhada, base legal aplicável, prazo estimado de duração da suspensão e aprovação por autoridade competente quando exigido. Revisões trimestrais avaliam a subsistência das razões que

motivaram cada exceção, procedendo-se à eliminação imediata dos dados tão logo cessem as circunstâncias excepcionais que justificaram sua preservação.

9. DIREITOS DOS TITULARES E SOLICITAÇÕES DE ELIMINAÇÃO

Os titulares de dados pessoais podem exercer o direito à eliminação de seus dados pessoais previsto no inciso VI do artigo 18 da LGPD mediante solicitação dirigida ao Encarregado de Proteção de Dados pelos canais de atendimento indicados na Política de Privacidade da plataforma. Tais solicitações são analisadas criteriosamente, sendo atendidas quando não houver impedimento legal ou regulatório que justifique a manutenção dos dados.

A eliminação de dados mediante solicitação do titular é processada no prazo máximo de quinze dias corridos contados do recebimento da solicitação, podendo ser prorrogado por igual período em situações excepcionais de complexidade técnica que demandem consultas a múltiplos sistemas ou validações de segurança adicionais. O titular é informado sobre o andamento de sua solicitação e sobre a conclusão do procedimento de eliminação.

Quando a eliminação solicitada pelo titular não puder ser integralmente atendida em razão de obrigação legal ou regulatória que determine a manutenção dos dados, o titular é informado de forma clara e detalhada sobre as categorias de dados que não podem ser eliminadas, as bases legais que fundamentam sua manutenção, os prazos de retenção aplicáveis e a possibilidade de recurso perante a Autoridade Nacional de Proteção de Dados caso discorde da fundamentação apresentada, em observância ao disposto no parágrafo 3º do artigo 16 da LGPD.

10. RESPONSABILIDADES E GOVERNANÇA

O Encarregado de Proteção de Dados é o responsável principal pela supervisão da execução desta política, incluindo monitoramento do cumprimento de prazos de retenção, coordenação de procedimentos de eliminação, documentação de exceções, análise de solicitações de titulares, orientação a áreas internas sobre aplicação dos critérios de retenção e reporte à alta administração sobre conformidade e eventuais desvios.

As áreas de tecnologia da informação são responsáveis pela implementação técnica de rotinas automatizadas de eliminação, configuração de sistemas conforme prazos de retenção estabelecidos, execução de procedimentos de eliminação segura, manutenção de logs de auditoria e suporte ao Encarregado de Proteção de Dados em questões técnicas relacionadas a retenção e descarte de dados.

Gestores de áreas funcionais que mantenham bases de dados ou arquivos físicos contendo dados pessoais são responsáveis por garantir que suas áreas observem os

prazos e procedimentos estabelecidos nesta política, reportando ao Encarregado de Proteção de Dados situações excepcionais que justifiquem suspensão temporária de eliminação e solicitando orientações em casos de dúvida sobre aplicação dos critérios de retenção.

A alta administração é responsável por prover recursos técnicos, humanos e financeiros adequados para implementação efetiva desta política, aprovar exceções que envolvam questões estratégicas ou riscos significativos, e garantir que a cultura organizacional valorize a proteção de dados pessoais e o cumprimento dos prazos de retenção como elemento essencial de governança de privacidade.

11. REVISÃO E ATUALIZAÇÃO DA POLÍTICA

Esta política é revisada anualmente pelo Encarregado de Proteção de Dados, com suporte jurídico e técnico, avaliando-se a adequação dos prazos de retenção estabelecidos em face de alterações legislativas, regulatórias ou jurisprudenciais, mudanças no modelo de negócio da Aizen, evolução de riscos de privacidade e segurança, e orientações emanadas da Agência Nacional de Proteção de Dados ou de autoridades reguladoras setoriais.

Alterações substanciais nos prazos de retenção ou nos procedimentos de eliminação são submetidas à aprovação da alta administração e comunicadas a todos os colaboradores e prestadores de serviço relevantes, sendo promovidos treinamentos adicionais quando necessário para garantir compreensão das modificações e adequação de práticas operacionais.

Auditorias internas periódicas, conduzidas anualmente ou com frequência superior conforme avaliação de riscos, verificam a conformidade das práticas efetivas de retenção e eliminação com as disposições desta política, identificando eventuais desvios, falhas em procedimentos automatizados ou necessidades de ajustes em processos ou sistemas.

12. DISPOSIÇÕES FINAIS

Esta política constitui instrumento fundamental do programa de governança de privacidade e proteção de dados pessoais da Aizen, integrando-se à Política de Privacidade, aos Termos e Condições de Uso da plataforma, à Política de Segurança da Informação e demais normas internas relacionadas ao tratamento de dados pessoais.

O descumprimento desta política constitui violação às obrigações de proteção de dados pessoais estabelecidas pela LGPD, sujeitando a Aizen a sanções administrativas previstas no artigo 52 da LGPD e expondo a organização a riscos de responsabilização civil perante titulares prejudicados. Colaboradores e prestadores de serviço que descumpram as disposições desta política sujeitam-se a medidas disciplinares conforme a gravidade da infração e eventual dolo ou culpa.