POLÍTICA INTERNA DE PRIVACIDADE E PROTEÇÃO DE DADOS

1. CONTEXTUALIZAÇÃO

A privacidade e a proteção de dados pessoais são compromissos institucionais da **FUNDAÇÃO REPUBLICANA BRASILEIRA – FRB**. Em todas as nossas atividades, assumimos a responsabilidade de agir com integridade, ética e respeito aos direitos das pessoas com as quais nos relacionamos, incluindo alunos, potenciais alunos, colaboradores, gestores, administradores, voluntários, terceiros e parceiros.

Em suas operações diárias, a **FRB** realiza diversas atividades que envolvem o tratamento de dados pessoais, sujeitando-se à Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD), bem como a outras normas e boas práticas aplicáveis à privacidade.

Esta Política Interna de Privacidade e Proteção de Dados tem como finalidade estabelecer diretrizes obrigatórias que orientam todos os colaboradores, prestadores de serviço e parceiros internos sobre o tratamento adequado de dados pessoais no contexto das atividades da instituição. É um documento normativo que regula o comportamento esperado no manuseio, acesso, uso, armazenamento, compartilhamento e descarte de dados pessoais no ambiente institucional.

A presente Política foi elaborada em conformidade com a LGPD e será atualizada sempre que necessário, em decorrência de mudanças legais, regulatórias e operacionais. Seu cumprimento é obrigatório para todos os que atuam nas estruturas da instituição.

2. OBJETIVO

O objetivo desta Política Interna de Privacidade e Proteção de Dados é garantir a aplicação efetiva da Lei Geral de Proteção de Dados dentro da Instituição, padronizando as práticas internas no tratamento de dados pessoais e promovendo uma cultura organizacional baseada na ética, segurança e respeito à privacidade.

Em síntese, esta Política visa demonstrar o comprometimento da **FRB** em:

a) Orientar o comportamento e as práticas de todos os colaboradores, gestores, voluntários, prestadores de serviço e parceiros quanto à coleta, uso, armazenamento, compartilhamento e descarte de dados pessoais, tanto em meio físico quanto digital;

b) Garantir a transparência institucional quanto às práticas adotadas no tratamento de dados.

c) Assegurar a conformidade legal com a LGPD e outras normas aplicáveis.

d) Proteger os direitos dos titulares dos dados e mitigar riscos legais, reputacionais e operacionais.

e) Estimular a conscientização e o engajamento de todos os envolvidos, promovendo o uso responsável dos dados pessoais tratados pela Instituição.

3. ÂMBITO DE APLICAÇÃO

A presente Política de Privacidade se aplica a todos os colaboradores, ex-colaboradores, alunos, gestores, administradores, voluntários, terceiros e parceiros com os quais a **FRB** possui relação e que em algum momento obteve contato com os dados pessoais.

4. DEFINIÇÕES E CONCEITOS LEGAIS

ENCARREGADO - Responsável pela Proteção de Dados Pessoais na **FRB** e pela comunicação com a ANPD e com os titulares.

CONTROLADOR - Pessoa a quem compete as decisões sobre o tratamento dos dados pessoais.

OPERADOR - Pessoa que realiza o tratamento de dados pessoais.

TITULAR - Pessoa a quem os dados pessoais se referem.

DADOS PESSOAIS - Qualquer informação relativa a uma pessoa singular identificada ou identificável. Isso quer dizer que um dado é considerado pessoal quando ele permite a identificação, direta ou indireta, da pessoa natural por trás do dado, como por exemplo: nome, sobrenome, data de nascimento, documentos pessoais, endereço, telefone, e-mail, dados de localização, dentre outros elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa.

DADOS PESSOAIS SENSÍVEIS - Qualquer dado pessoal que diga respeito à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, bem como dado referente à saúde ou à vida sexual, dado genético ou biométrico.

DADO ANONIMIZADO – São dados pessoais convertidos em dados não identificáveis, cujo processo de anonimização não pode ser reversível, de forma que não poderão ser associados a nenhum indivíduo específico.

TRATAMENTO - toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

COLETA - recolhimento de dados com finalidade específica.

PRODUÇÃO - criação de bens e de serviços a partir do tratamento de dados.
RECEPÇÃO - ato de receber os dados ao final da transmissão.
CLASSIFICAÇÃO - forma de ordenar e categorizar os dados.
UTILIZAÇÃO - ato ou efeito do aproveitamento dos dados.
ACESSO - ato de ingressar, transitar, conhecer ou consultar a informação.
REPRODUÇÃO - cópia de dado preexistente obtido por meio de qualquer processo.
TRANSMISSÃO - movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos, etc.
DISTRIBUIÇÃO - ato ou efeito de dispor de dados.
PROCESSAMENTO - ato ou efeito de processar dados visando organizá-los para obtenção de um resultado determinado.
ARQUIVAMENTO - ato ou efeito de manter registrado um dado embora já tenha perdido a validade ou esgotado a sua vigência.
ARMAZENAMENTO - ação ou resultado de manter ou conservar em repositório um dado.
ELIMINAÇÃO - ato ou efeito de excluir ou destruir dado do repositório.
AVALIAÇÃO - forma de analisar o dado com o objetivo de produzir informação.
CONTROLE - ato ou poder de monitorar as ações sobre o dado.
MODIFICAÇÃO - ato ou efeito de alteração do dado.
COMUNICAÇÃO - transmitir informações referentes aos dados.
TRANSFERÊNCIA - mudança de dados de uma área de armazenamento para outra, ou para terceiro.
DIFUSÃO - ato ou efeito de divulgação, propagação, multiplicação dos dados.
EXTRAÇÃO - ato de copiar ou retirar dados do repositório em que se encontrava.
ANPD - Autoridade Nacional de Proteção de Dados.

5. PRINCÍPIOS DE PROTEÇÃO DE DADOS PESSOAIS

A **FRB** zelará para que em todas as atividades de tratamento de dados pessoais dos alunos, colaboradores, gestores, voluntários, administradores, terceiros e parceiros, respeite a boa-fé e os 10 (dez) princípios trazidos pela legislação para nortear a privacidade e proteção de dados.

5.1. Finalidade

A Instituição realizará o tratamento de dados pessoais quando a finalidade do Tratamento se enquadrar em uma das hipóteses legais permitidas ou obter o consentimento do titular dos dados.

O tratamento dos dados deve se limitar aos fins legítimos, específicos, explícitos e informados ao Titular, tendo em vista que os dados pessoais não poderão ser coletados para uma finalidade, e depois utilizados para outra.

5.2 Adequação

A Instituição efetuará a coleta dos dados pessoais adequados para alcançar as finalidades informadas ao titular dos dados, pois o uso de um dado deverá ser compatível com o motivo original da coleta.

5.3 Necessidade

A Instituição limitará a coleta de dados ao mínimo necessário para o cumprimento das finalidades pretendidas e expostas ao titular. Dessa forma, o compartilhamento de dados pessoais com outra área ou outra empresa deve considerar este princípio da minimização de dados.

5.4 Livre Acesso

A Instituição garantirá a consulta facilitada e gratuita quanto a forma e duração do tratamento e integralidade dos dados pessoais.

5.5 Qualidade dos dados

A Instituição adotará medidas razoáveis para assegurar que quaisquer dados pessoais em sua posse sejam relevantes e atualizados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento, garantindo a possibilidade ao titular do dado pessoal de requerer a exclusão ou correção de dados imprecisos ou desatualizados.

5.6 Transparência

Serão garantidas aos titulares dos dados informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento.

5.7 Segurança

A Instituição se responsabiliza em assegurar que medidas técnicas e administrativas apropriadas sejam aplicadas aos dados pessoais para protegê-los contra o tratamento não autorizado ou ilegal, bem como contra a perda acidental.

5.8 Prevenção

A Instituição adotará medidas técnicas para prevenir a ocorrência de incidentes de segurança envolvendo dados pessoais.

5.9 Não Discriminação

A Instituição garantirá que as atividades de tratamento de dados pessoais não serão com o objetivo de fins discriminatórios, ilícitos ou abusivos.

5.10 Responsabilização e Prestação de Contas

A **FRB** deverá armazenar registros de todas as atividades de tratamento de dados pessoais e as respectivas medidas tomadas para adequar tais atividades às normas relativas à privacidade e proteção de dados pessoais, comprovando a eficácia e eficiência de tais medidas.

6. COLETA DE DADOS PESSOAIS

A **FRB** utilizará os dados pessoais coletados para atender a uma finalidade específica, em conformidade com os limites da legislação vigente e obedecendo os princípios que norteiam a proteção dos dados pessoais.

6.1 JUSTIFICATIVA DA COLETA DE DADOS (Porque coletamos seus dados)

a) Execução do contrato com o titular

A **FRB** realizará o tratamento de dados pessoais em casos que estejam fundamentados em um contrato firmado (ou prestes a ser firmado) com o titular, como alunos, colaboradores, gestores, administradores, voluntários, terceiros e parceiros, e que seja essencial para que a Instituição cumpra com as obrigações estabelecidas no contrato firmado.

b) Zelar pela saúde

A **FRB** poderá tratar dados pessoais dos colaboradores, incluindo dados sensíveis relacionados à saúde, tais como histórico e prontuário médico, visando proteger a saúde pessoal, e para fins de informações de licenças legais ou justificativas de ponto mediante atestados médicos.

Dados pessoais relacionados à saúde podem ser utilizados para a realização de procedimentos de saúde, campanhas de vacinação, atendimento médico em caso de acidente ou doença ocupacional e qualquer outro procedimento vinculado à saúde.

c) Zelar pela segurança, prevenção à fraude e proteção à vida

A **FRB** poderá tratar dados pessoais dos alunos, colaboradores, gestores, administradores, voluntários, terceiros e parceiros, para zelar pela segurança destes, para o controle de acesso às suas dependências, bem como para evitar fraudes de identidade, mediante o uso de identificação biométrica.

A prevenção à fraude é aplicada com a coleta de dados sensíveis, quando utilizados em procedimentos de identificação e autenticação de cadastro em sistemas eletrônicos.

d) Cumprimento de obrigações legais e regulatórias

A **FRB** tratará dados pessoais de seus alunos, colaboradores, gestores, administradores, voluntários, terceiros e parceiros inclusive dados considerados sensíveis, tais como qualificação completa, imagem (fotografia ou vídeo), filiação partidária, documentos pessoais, dados relacionados à origem racial ou étnica, dados bancários e previdenciários, exames admissionais, arquivamento de notas fiscais, dados pessoais de menor de idade, para cumprir com obrigações dispostas por lei, por regulações de órgãos governamentais, por autoridades fiscais, pelo Poder Judiciário, pelos órgãos da Justiça Eleitoral, pelo Ministério Público a título de prestação de contas ou por qualquer outra autoridade competente.

e) Exercício regular dos direitos

A **FRB** tratará dados pessoais dos alunos, colaboradores, gestores, administradores, voluntários, terceiros e parceiros, ainda que haja o término da relação contratual, garantindo seus direitos de defesa, resposta, ou atuação junto a órgãos públicos, em processos judiciais ou administrativos.

f) Interesse legítimo da **FRB**

Poderá haver o tratamento e compartilhamento de dados pessoais de seus alunos, colaboradores, gestores, administradores, voluntários, terceiros e parceiros, para finalidades legítimas e necessárias para a operação da **FRB**, envolvendo a continuidade de suas atividades, e prevalecendo direitos e liberdades fundamentais destes titulares.

Nestes casos, o tratamento será realizado se estritamente necessário para o alcance dessas finalidades.

O legítimo interesse deve ser precedido de um teste de balanceamento que considere, de um lado, os interesses do controlador ou de terceiro e, de outro, os direitos e liberdades fundamentais dos titulares. A avaliação deve envolver a elaboração de Relatório de Impacto à Proteção de Dados, que deverá ser elaborado com o apoio do responsável pela atividade.

g) Consentimento do titular

A **FRB** coletará o consentimento do titular dos dados, o qual concede autorização mediante manifestação livre, espontânea, inequívoca e para finalidades específicas para tratamento de seus dados, inclusive dados sensíveis, para as demais atividades que não possam se enquadrar nas hipóteses acima.

O consentimento somente poderá embasar atividades de tratamento de dados pessoais em casos excepcionais. Deste modo, deverá ser avaliado quanto à exigência de consentimento para determinada atividade e a impossibilidade de seu enquadramento em outras bases legais.

No caso de crianças e adolescentes com menos de 18 anos, o consentimento de pelo menos um dos pais ou do responsável deve ser obtido. Serão fornecidas informações transparentes sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos. Esta informação será fornecida de forma acessível, escrita em linguagem clara e gratuita.

Poderão ser coletados dados pessoais de crianças sem o consentimento, quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento.

7. ATRIBUIÇÕES

O projeto será supervisionado por um Comitê de Privacidade, composto pelo Encarregado de Proteção de Dados (DPO) e Consultoria especializada em Proteção de Dados. O comitê conta com o apoio estratégico de partes interessadas (stakeholders) e será executado pelas equipes de apoio de *Privacy Governance, Privacy Champions* e Segurança da Informação.

O Comitê de Privacidade, deverá:

- Revisar e aprovar esta Política, bem como suas futuras alterações.
- Monitorar a atualização do mapeamento de Dados Pessoais.
- Gerenciar e supervisionar estratégias de proteção de Dados Pessoais para estarem em conformidade com os requisitos da legislação e da regulamentação aplicáveis de proteção de Dados Pessoais.
- Fazer o gerenciamento permanente e efetivo da implementação de iniciativas de privacidade.
- Monitorar os eventos relacionados a vazamento de Dados Pessoais e acompanhar a implementação de planos de ação para correções do projeto de privacidade.
- Gerenciar e propor treinamentos, programas de conscientização e comunicação relativos à privacidade de Dados Pessoais dentro da Instituição.
- Garantir o cumprimento dos requisitos da legislação e regulamentações relacionados à privacidade e proteção de dados pessoais.
- Monitorar o cumprimento das regras internas de privacidade.
- Monitorar as requisições dos titulares de dados pessoais, a fim de garantir que sejam respondidas dentro do prazo.
- Responsabilizar-se pelo uso adequado de Dados Pessoais;
- Revisar anualmente, ou em prazo menor quando necessário, as iniciativas de privacidade adotadas pela Instituição.
- Cooperar e se relacionar com a Autoridade Nacional de Proteção de Dados Pessoais (Brasil).
- Realizar auditorias internas periódicas para verificar a conformidade com as políticas e procedimentos de proteção de dados pessoais.
- Aprovar políticas, procedimentos e diretrizes de privacidade e proteção de dados pessoais antes de sua implementação.
- Identificar, avaliar e mitigar riscos relacionados à privacidade e proteção de dados pessoais, garantindo que medidas corretivas sejam implementadas quando necessário.
- Assegurar que todas as partes interessadas relevantes estejam informadas e alinhadas com as políticas de privacidade da Instituição.
- Supervisionar a resposta a incidentes de segurança que envolvam dados pessoais, assegurando que as notificações às autoridades competentes sejam feitas, conforme exigido por lei.

Todos os diretores, gestores e colaboradores devem:

- Responsabilizar-se pelo uso adequado de Dados Pessoais em suas atividades.

- Cumprir a legislação e regulamentação relativas à proteção de Dados Pessoais.
- Cumprir com as medidas adequadas de segurança da informação.
- Cumprir com as regras instituídas no Termo de Responsabilidade, Consentimento e Confidencialidade para proteção de dados.
- Relatar ao Comitê de Privacidade ou equipes de apoio, a ocorrência de quaisquer incidentes de Dados Pessoais ou segurança de dados, bem como as deficiências identificadas relacionadas ou possíveis riscos de privacidade.
- Participar das atividades de treinamentos relativos à privacidade de dados pessoais dentro da Instituição.
- Reservar tempo adequado em suas agendas para atender às solicitações da Equipe do Projeto (Privacy Governance) e da Equipe de Apoio (Privacy Champions), garantindo que as informações necessárias sejam fornecidas de maneira oportuna e completa.
- Cooperar ativamente com as equipes de governança e apoio, fornecendo prontamente todas as informações e dados necessários para o preenchimento dos documentos de governança de privacidade de dados da instituição.

Equipe do Projeto ou "*Privacy Governance*":

- Reunir-se com diferentes departamentos para coletar dados e informações necessárias para o preenchimento de documentos de governança de privacidade.
- Garantir que a documentação necessária seja produzida com precisão e entregue dentro dos prazos estabelecidos.
- Relatar regularmente ao Comitê de Privacidade sobre o progresso das atividades de coleta de dados e preenchimento de documentos, destacando quaisquer desafios ou necessidades de suporte adicional.
- Assegurar que as decisões e diretrizes do comitê sejam implementadas e seguidas nas atividades do projeto.
- Contribuir para a conformidade dos documentos com as políticas de privacidade e as exigências legais antes de sua aprovação e uso.
- Contribuir ativamente nas discussões, oferecendo soluções para desafios relacionados à privacidade.
- Fornecer informações e dados para avaliações e gerenciamentos, facilitando o acesso a informações precisas e atualizadas para a realização de análises de conformidade e gestão de riscos.
- Promover a conscientização sobre conformidade com a LGPD em suas áreas, implementando campanhas de conscientização e treinamento para garantir que todos os colaboradores estejam cientes de suas responsabilidades em relação à LGPD.

Equipe de Apoio ou "*Privacy Champions*":

- Reunir-se com diferentes departamentos para coletar dados e informações necessárias para o preenchimento de documentos de governança de privacidade.
- Garantir que as informações coletadas sejam completas, precisas e entregues dentro dos prazos estabelecidos.
- Relatar regularmente ao Comitê de Privacidade sobre o progresso das atividades de coleta de dados e preenchimento de documentos, destacando quaisquer desafios ou necessidades de suporte adicional.
- Auxiliar na disseminação das decisões tomadas e garantir que as áreas sob sua responsabilidade estejam alinhadas com as diretrizes do projeto.
- Colaborar na coleta de dados e fornecimento de informações essenciais para a tomada de decisões e para o cumprimento dos objetivos do projeto.
- Promover a conscientização sobre conformidade com a LGPD em suas áreas e ser um ponto de referência para questões de privacidade dentro de suas áreas, promovendo a cultura de conformidade e atuando como modelo de boas práticas em proteção de dados.

8. FERRAMENTA AVANT DATA PROTECTION

A **FRB** possui a ferramenta Avant Data Protection para assegurar a adequação integral à Lei Geral de Proteção de Dados (LGPD). Essa ferramenta permite a gestão eficaz do projeto de conformidade, incluindo:

- Gestão de Projetos: Calendário detalhado das atividades relacionadas à LGPD, com gráficos e relatórios que oferecem uma visão 360 graus do programa de adequação.
- Biblioteca de Documentos: Disponibilização de uma biblioteca com 50 modelos de documentos editáveis, essenciais para o arcabouço do programa de gestão de documentação.
- Organograma e DataFlow: Desenvolvimento e criação de organogramas e fluxos de dados.
- Gestão de Riscos: Ferramentas para identificar, avaliar e gerenciar riscos associados ao tratamento de dados pessoais.
- Mapeamento de Dados e Processos: Geração automatizada de matrizes de riscos, Relatórios de Impacto à Proteção de Dados (DPIA), Registros de Operações de Tratamento (ROPA), fluxogramas, diagramas de processos, ciclos de vida de dados e mapas de transferências internacionais de dados, exportáveis em Excel, Word e PDF.

- Gestão de Fornecedores: Checklists de conformidade, análise e relatórios sobre a adequação de prestadores de serviços às exigências da LGPD.
- Gestão de Incidentes: Estruturação de times de resposta a incidentes, gestão de comunicação de incidentes e planos estratégicos de resposta, com relatórios detalhados sobre incidentes ocorridos.
- Gestão de Ativos: Tabelas de gestão de acessos, gráficos de vulnerabilidades, expectativas de perdas e inventário de ativos com relatórios completos.
- Ciclo de Retenção e Descarte de Dados: Programas específicos para a retenção e descarte adequado de dados pessoais.
- Atendimento aos Direitos dos Titulares: Ferramenta de atendimento aos direitos dos titulares de dados por meio do portal "Minha Privacidade" no site institucional, com gestão completa de consentimentos.

Essa ferramenta garante que todos os aspectos de conformidade com a LGPD sejam tratados de maneira eficiente, integrando tecnologia de ponta na gestão de dados pessoais e proteção de privacidade.

9. PRESTADORES DE SERVIÇOS TERCEIRIZADOS

Os prestadores de serviços terceirizados que tratem dados pessoais sob as instruções da **FRB**, estão sujeitos às obrigações impostas aos Processadores de acordo com a legislação e regulamentação de proteção de Dados Pessoais aplicáveis e de acordo com as cláusulas contratuais ou Termo de Responsabilidade e Confidencialidade de dados pessoais.

Os fornecedores ou terceirizados que realizam tratamento de dados pessoais tendo esta Instituição como controladora, deverão implementar medidas de segurança, controles técnicos e administrativos apropriados para garantir a confidencialidade e segurança dos dados pessoais, conforme acordado em cláusulas contratuais ou Termo de Responsabilidade e Confidencialidade de dados pessoais.

10. GERENCIAMENTO DE VIOLAÇÃO DE DADOS

A Instituição atuará de forma justa e proporcional, considerando as ações a serem tomadas para informar as partes afetadas com relação a violações de dados pessoais. Será gerenciada a violação de dados por meio de processo de tratamento de incidentes de segurança da informação.

Em consonância com a LGPD, no caso de verificação da ocorrência de uma violação que possa resultar em um risco para os direitos e liberdades dos indivíduos, a autoridade

fiscalizadora será informada em até três dias úteis, contados da data em que o controlador confirmar que o incidente afetou dados pessoais (Resolução nº 2 da ANPD).

11. COMPARTILHAMENTO DE DADOS

No caso de transferência ou o compartilhamento de dados pessoais para terceiros ("operadores": terceiros contratados que processam os dados pessoais em nome da Instituição, conforme definido pela LGPD), para a prestação de um serviço específico, a Instituição celebrará instrumentos contratuais capazes de garantir a integridade e a confiabilidade das informações compartilhadas.

Em alguns casos, é possível que os dados dos alunos, colaboradores, gestores, administradores, voluntários, terceiros e parceiros da FRB sejam compartilhados com empresas controladas e fornecedoras de serviços, para atendimento de uma atividade específica. Assim, serão utilizados instrumentos contratuais e procedimentos técnicos com o objetivo de assegurar que esses terceiros estejam em plena conformidade com a legislação aplicável, em especial com as disposições da Lei Geral de Proteção de Dados.

É possível que alguns desses terceiros ("operadores") estejam localizados fora do território brasileiro. Nesta hipótese, as transferências de dados pessoais para fora do Brasil serão cuidadosamente revisadas, para garantir que estão dentro dos limites impostos pela LGPD.

A **FRB** somente compartilhará o que for estritamente necessário para o alcance de uma finalidade específica.

12. DIREITOS DOS TITULARES

Os alunos, colaboradores, gestores, administradores, voluntários, terceiros e parceiros poderão obter da **FRB**, durante a vigência de vínculo com a Instituição, a qualquer momento e mediante requisição, os seguintes direitos:

1. Direito à informação.
2. Direito de acesso aos dados.
3. Direito de retificação.
4. Direito de eliminação (direito de esquecer).
5. Direito a anonimização ou bloqueio no tratamento.
6. Direito a notificação de retificação ou eliminação.
7. Direito de portabilidade de dados.
8. Direito de se opor à tomada de decisão automatizada.

Esses direitos são respeitados pela **FRB** por meio de procedimentos adequados que permitem que a ação necessária seja realizada de acordo com os prazos indicados na LGPD.

Solicitação de Dados	Prazo
O direito de ser informado	Quando os dados são coletados (se fornecidos pelo titular) ou no prazo de 15 (quinze) dias (se não forem fornecidos pelo titular)
O direito de acesso	15 (quinze) dias ou Imediatamente (se formato simplificado)
O direito de retificação	15 (quinze) dias
O direito de apagar	Imediatamente, exceto se houver justificativa
O direito de restringir o tratamento	Imediatamente, exceto se houver justificativa
O direito à portabilidade de dados	15 (quinze) dias
Direitos em relação à tomada de decisões e perfis automatizados.	Não especificado

OBS Tabela – Prazos no caso de solicitações de dados.

13. ARMAZENAMENTO DE DADOS

A Instituição deixará de reter os dados pessoais de seus colaboradores ou ex-colaboradores, alunos, gestores, administradores, voluntários, terceiros e parceiros, podendo utilizar meios técnicos para deles retirar a possibilidade de associação, direta ou indireta a tais indivíduos, assim que findo o vínculo ou relação contratual, respeitando os prazos legais de guarda destas informações.

Ressalta-se também que caso seja solicitada a exclusão de informações, a Instituição se reserva o direito de preservar e divulgar todo e qualquer dado que julgue ser necessário para o cumprimento de obrigações legais ou regulatórias ou derivadas de ordem judicial.

14. SEGURANÇA DA INFORMAÇÃO

Para garantir a segurança dos dados pessoais tratados no exercício de suas atividades e evitar a ocorrência de acessos indevidos ou não autorizados, perda, destruição ou qualquer outra ação que comprometa a integridade, disponibilidade ou confidencialidade dessas informações, a Instituição se compromete com a implementação de ferramentas e padrões de Segurança da Informação e com a proteção de Dados Pessoais, com vistas a garantir o direito fundamental do indivíduo.

O Comitê de Privacidade e a área de segurança da informação deverão trabalhar em conjunto para manter todos os dados pessoais tratados sempre seguros, maximizando a prevenção a exposições, vazamentos e acesso indevido.

Todos os Integrantes com acesso a Dados Pessoais de responsabilidade da Instituição estão obrigados aos deveres de confidencialidade dos Dados Pessoais mediante a anuência nas obrigações de sigilo e confidencialidade constantes no Contrato de Trabalho.

As regras detalhadas de segurança da informação adotadas pela Instituição encontram-se descritas na **Política de Segurança da Informação**, que deve ser consultada e seguida rigorosamente por todos os colaboradores, gestores, administradores, voluntários, terceiros e parceiros.

15. PROCEDIMENTOS EM CASO DE INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

Em caso de suspeita ou confirmação de incidente de segurança envolvendo dados pessoais, os seguintes passos devem ser adotados imediatamente:

- Comunicação imediata ao Comitê de Privacidade ou ao Encarregado de Proteção de Dados pelo e-mail: dpo@fundacaorepublicana.org.br.
- Registro do incidente na ferramenta Avant Data Protection.
- Isolamento do sistema ou ambiente afetado, quando aplicável, para preservar evidências.
- Avaliação do incidente pelo Comitê de Resposta a Incidentes (CRI) e definição das medidas corretivas.
- Notificação à ANPD e aos titulares, se houver risco relevante aos direitos dos envolvidos (prazo legal de até 3 dias úteis).
- Registro e acompanhamento do caso, com ações de melhoria e prevenção de reincidência.

É dever de todos os integrantes da instituição relatar qualquer indício de violação, acesso indevido, perda ou uso indevido de dados pessoais. A omissão ou negligência na

comunicação de incidentes configura **infração grave** e poderá gerar sanções disciplinares.

As regras detalhadas de procedimentos de incidentes de segurança da informação adotadas pela Instituição encontram-se descritas no documento de *Procedimento de Incidente de Segurança da Informação e Plano de Resposta a Incidentes*, que deve ser consultado e seguido rigorosamente por todos os colaboradores, gestores, administradores, voluntários, terceiros e parceiros.

16. RESPONSABILIDADES

Os integrantes ou representantes da Instituição são responsáveis por conhecer e compreender todos os documentos internos que lhes forem aplicáveis. De forma similar, os gestores são responsáveis por garantir que todos os integrantes de sua equipe compreendam e sigam os documentos orientadores aplicáveis à Instituição.

Para garantir o cumprimento das normas de privacidade e proteção de dados pessoais, os pontos a seguir devem ser observados por todos, sem prejuízo dos demais pontos desta política:

a) Os colaboradores, gestores, administradores, terceiros e parceiros, possuem como dever primário o de garantir a integridade, sigilo e confidencialidade dos dados pessoais tratados no exercício de sua função.

b) O tratamento dos dados pessoais deverá, necessariamente, observar as finalidades propostas, não permitindo o tratamento incompatível ou excessivo ou para finalidades diversas.

c) Os colaboradores, gestores, administradores, terceiros e parceiros deverão se utilizar do mínimo de informações necessárias para o cumprimento das finalidades pretendidas e regular exercício de suas funções.

d) Os dados pessoais tratados no exercício da função deverão necessariamente ser armazenados em local seguro e oficialmente aprovados pela Instituição, sendo vedado o armazenamento não autorizado em ambientes próprios, como notebooks ou área de trabalho de computadores.

e) Os dados pessoais tratados no exercício da função não poderão ser apagados, deletados ou anonimizados, sem que haja comando direto da Instituição para tanto.

f) Os dados pessoais tratados no exercício da função, como regra, não poderão ser enviados para endereços de e-mail pessoal ou dispositivos remotos como pen drives.

g) Todos os gestores devem continuamente encorajar seus liderados a reportar violações.

h) Caso qualquer integrante da Instituição ou terceiro tenha conhecimento de potencial conduta ilegal ou antiética, incluindo potenciais violações às Políticas que regem a Instituição, devem imediatamente reportar a potencial violação ao Comitê de Privacidade ou via endereço de e-mail: dpo@fundacaorepublicana.org.br.

17. DISPOSIÇÕES FINAIS

O descumprimento das disposições desta Política Interna de Privacidade e Proteção de Dados poderá acarretar sanções disciplinares, conforme a gravidade da infração, entre elas:

a) Advertência verbal ou escrita.
b) Suspensão das atividades.
c) Desligamento por justa causa, nos termos da CLT (para colaboradores).
d) Rescisão contratual, no caso de prestadores de serviço ou terceiros.
e) Responsabilização civil, administrativa ou penal, conforme o caso.

As penalidades poderão ser aplicadas independentemente de outras medidas legais cabíveis.

A **FRB** se reserva ao direito de revisar esta Política, na periodicidade que melhor entender, sempre respeitando as atualizações legais e de procedimentos internos.

Versão: 02
Ano: 2025
Atualizada em: Janeiro de 2025.