

POLÍTICA DE GOVERNANÇA E PROTEÇÃO DE DADOS PESSOAIS

1. A **Planejar – Associação Brasileira de Planejamento Financeiro** (“Planejar”), dispendo do objetivo de estabelecer diretrizes gerais sobre Governança e Proteção de dados pessoais estabelece a Política de Governança e Proteção de Dados Pessoais (“Política”) e reforça seu compromisso em manter a privacidade dos dados pessoais obtidos no curso de suas atividades e cumprir as leis e regulamentação aplicáveis sobre o tratamento de dados pessoais.

2. A Política está dividida em 16 (dezesesseis) seções: (I) Definições; (II) Objetivo; (III) Abrangência; (IV) Vigência; (V) Compromissos Gerais; (VI) Responsabilidades; (VII) Princípios Relacionados ao Tratamento de Dados; (VIII) Tratamento de Dados Pessoais; (IX) Base Legal para Tratamento de Dados; (X) Transferência de Dados Pessoais para o Exterior; (XI) Direitos dos Titulares dos Dados; (XII) Padrões de Segurança; (XIII) Prestadores de Serviços/Fornecedores; (XIV) Incidentes de Segurança; (XV) Legislação Relacionada; e (XVI) Referências Internas.

I. DEFINIÇÕES

3. Os termos e expressões a seguir, quando escritos em letras maiúsculas, deverão ter os seguintes significados, conforme definido abaixo:

4. “**Autoridade Nacional de Proteção de Dados**” ou “**ANPD**” significa a autoridade administrativa encarregada da Proteção de Dados Pessoais, um órgão da administração pública nacional responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados Pessoais em todo o território brasileiro.

5. “**Profissionais**” significa todos os profissionais da Planejar, incluindo representantes legais, diretores, estagiários, voluntários, aprendizes, terceiros e qualquer outra pessoa que possua vínculo direto com a Planejar.

6. “**Controlador de Dados**” ou “Controlador” significa uma pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao Tratamento de Dados Pessoais.

7. “**Dados Pessoais**” significa quaisquer dados relacionados a um indivíduo (pessoa

natural) que é ou possa ser identificado a partir dos dados ou a partir dos dados em conjunto com outras informações.

8. “**Dados Pessoais Sensíveis**” significa os Dados Pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, ou outros dados específicos na forma da legislação.

9. “**DPIA**” significa Data Protection Impact Analysis ou, em português, o relatório de impacto à proteção de dados pessoais.

10. “**Encarregado de Dados**” significa a pessoa que na Planejar é a responsável por coordenar e por assegurar a conformidade com esta Política, com a Legislação de Proteção de Dados e que atuará como canal da Planejar com os Titulares de Dados e com a Autoridade Nacional de Proteção de Dados.

11. “**Legislação de Proteção de Dados**” significa toda a legislação brasileira, decretos e regulamentações, que dispõem sobre a proteção de Dados Pessoais, incluindo a LGPD.

12. “**LGPD**” significa a Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709, de 14 de agosto de 2018.

13. “**Operador de Dados**” ou “**Operador**” significa uma pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador de Dados.

14. “**Política**” significa esta Política de Governança e Proteção de Dados Pessoais.

15. “**RoPA**” significa o registro de atividades de processamento de Dados Pessoais.

16. “**Signatários**” significa pessoas jurídicas integrantes da Planejar, como grandes empresas, PMEs e organizações não empresariais que visam melhorar suas práticas e/ou fomentar o setor empresarial, representadas por pessoas naturais.

17. “**Titular(es) de Dados**” significa qualquer pessoa natural a quem se referem os Dados Pessoais que são objeto de Tratamento.

18. “**Tratamento**” significa qualquer operação realizada com Dados Pessoais, como, por exemplo, 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.

II. OBJETIVO

19. O objetivo desta Política é definir as principais responsabilidades e regras em relação à proteção de Dados Pessoais que são aplicáveis à Planejar, para garantir um nível adequado de proteção aos Dados Pessoais, incluindo as medidas adequadas para prevenção contra o Tratamento não autorizado e ilegal de Dados Pessoais e contra perda ou destruição acidental.

III. ABRANGÊNCIA

20. A presente Política aplica-se ao Tratamento de Dados Pessoais de Titulares de Dados localizados no Brasil, envolvendo dados coletados em território nacional, ou cujas atividades ocorram ou tenham por objetivo a oferta ou o fornecimento de bens ou serviços no Brasil inclusive caso parte do Tratamento, como, por exemplo, o armazenamento, ocorra no exterior.

21. A presente Política aplica-se a todas as atividades de Tratamento da Planejar.

IV. VIGÊNCIA

22. A presente Política entrará em vigor em **27/02/2025**.

V. COMPROMISSOS GERAIS

23. Nos termos da presente Política, a Planejar deverá observar os seguintes compromissos:

(i) Elaborar e manter um registro de atividades de Tratamento de Dados Pessoais de

Titulares, exceto se tal obrigação for dispensada pela regulamentação;

- (ii) Caso necessário e de acordo com os desenvolvimentos regulatórios da ANPD a respeito da aplicabilidade da LGPD a pequenas e médias empresas e entidades sem fins lucrativos, nomear um Encarregado para proteção de Dados Pessoais e manter uma estrutura adequada para as atividades relacionadas à proteção de Dados Pessoais;
- (iii) Implementar medidas necessárias para o atendimento aos direitos dos Titulares de Dados Pessoais, incluindo a divulgação de avisos de privacidade que informem, dentre outros itens, a finalidade do Tratamento, a forma e duração do Tratamento; a identificação da Planejar como controlador do Tratamento, conforme aplicável; informações de contato da Planejar; e informações sobre o uso compartilhado de Dados Pessoais pela Planejar;
- (iv) Implementar as medidas organizacionais e técnicas adequadas para a prevenção e segurança dos Dados Pessoais contra o Tratamento irregular, indevido ou ilegal;
- (v) Realizar avaliações periódicas sobre o risco que um Tratamento de Dados Pessoais pode representar a um Titular e, conforme necessário e adequado, adotar medidas para proteger o Titular de Dados Pessoais, na forma exigida pela regulamentação aplicável; e
- (vi) Aplicar treinamentos a todos os Profissionais sobre temas relacionados à segurança da informação e à proteção de dados pessoais.

VI. RESPONSABILIDADES

- 24. A estrutura de governança da Planejar para proteção de Dados Pessoais será composta pelo Encarregado de Dados e pelo Comitê de Governança.
- 25. As seguintes atribuições e responsabilidades são definidas:

Comitê de Governança

- a) Nomear o Encarregado de Dados, que será gerido pelo(a) Diretor(a) Executivo(a) da Planejar, garantida a independência funcional.
- b) Exercer funções consultivas e deliberativas em matéria de proteção de dados pessoais, com o assessoramento do Encarregado de Dados.
- c) Encarregado de Dados ou membro apontado como responsável pelas ações de Proteção de Dados (“Responsável”)
- d) Manter o registro de atividades de Tratamento de Dados Pessoais da Planejar, conforme exigido.
- e) Acompanhar e apoiar a implementação de melhorias na proteção de dados.
- f) Participar dos projetos da Planejar que envolvam Tratamento de Dados Pessoais a fim de garantir que estejam de acordo com a Legislação de Proteção de Dados.
- g) Elaborar e realizar treinamentos de proteção de Dados Pessoais para os Profissionais.
- h) Garantir que a Planejar possua e mantenha atualizada toda a documentação necessária e as evidências para atendimento à Legislação de Proteção de Dados, conforme requerido em regulamento.
- i) Monitorar o cumprimento, pelos Profissionais, desta Política e da Legislação de Proteção de Dados.
- j) Coordenar a elaboração de DPIAs, quando forem necessários.
- k) Revisar e atualizar avisos de privacidade aos Titulares.
- l) Endereçar as solicitações dos Titulares de Dados Pessoais.
- m) Responsabilizar-se pela interface com a ANPD, sempre que for necessário.
- n) Coordenar os esforços necessários em caso de incidentes de segurança.

Tecnologia da Informação (“TI”)

- a) Implementar e monitorar todas as medidas de segurança adequadas e necessárias, de acordo com a regulamentação ou, em sua ausência, de acordo com padrões

recomendáveis em vista da natureza dos Dados Pessoais Tratados pela Planejar.

- b) Assessorar o Encarregado de Dados / Responsável em todas as questões técnicas e de segurança da informação e cooperar no cumprimento desta Política e da Legislação de Proteção de Dados.
- c) Prestar suporte técnico e analisar novos sistemas no que se refere à segurança de Dados Pessoais.
- d) Prestar o suporte técnico necessário para elaboração de DPIAs.
- e) Analisar e efetuar a coleta de evidências técnicas nos casos de incidentes de segurança.

Todos os Profissionais

- a) Providenciar suporte na implementação de planos de ação aprovados pelo

Comitê de Governança e gerenciados pelo Encarregado de Dados/Responsável

- a) Responsabilizar-se pelo uso adequado de Dados Pessoais no desempenho de suas atividades.
- b) Manter a mais estrita confidencialidade, integridade e disponibilidade dos Dados Pessoais a que tiver acesso em razão do desempenho de sua função.
- c) Cumprir com seu contrato de trabalho, com a Legislação de Proteção de Dados, esta Política e todas as políticas relacionadas.
- d) Reportar todas as situações de não conformidade e os incidentes de segurança que tome conhecimento ao Encarregado de Dados/ Responsável.
- e) Participar de todos os treinamentos relacionados à proteção de Dados Pessoais.

VII. PRINCÍPIOS RELACIONADOS AO TRATAMENTO DE DADOS PESSOAIS

26. O Tratamento de Dados Pessoais executado sob o controle da Planejar será feito de acordo com a Legislação de Proteção de Dados e com as disposições desta Política e em particular com as seguintes disposições:

- Os Dados Pessoais devem ser obtidos de forma justa e legal, e o Tratamento deve ser compatível com as finalidades informadas ao Titular de Dados e, ainda, deve limitar-se ao mínimo necessário para a realização de suas finalidades.
- Os Dados Pessoais devem ser tratados apenas para propósitos específicos, explícitos e legítimos e informados ao Titular de Dados e não podem ser tratados de forma incompatível com esses propósitos. Os Dados Pessoais apenas serão disponibilizados a terceiros para os ditos propósitos ou de qualquer outra forma permitida pela Legislação de Proteção de Dados.
- Os controles e procedimentos técnicos e organizacionais apropriados devem ser implementados para garantir a segurança dos Dados Pessoais e evitar acesso ou divulgação não autorizados, que potencialmente poderiam resultar em alteração, destruição acidental ou ilegal, perda dos dados e contra todas as demais formas ilegais de Tratamento.
- Devem ser garantidas aos Titulares de Dados informações claras, precisas e facilmente acessíveis sobre a realização do Tratamento, bem como implementados procedimentos para garantir respostas às solicitações dos Titulares de Dados, nos termos da Legislação de Proteção de Dados.
- Os Dados Pessoais não podem ser tratados para fins discriminatórios, ilícitos ou abusivos.
- Os Dados Pessoais não podem ser mantidos por um período maior que o necessário para o atingimento dos objetivos para os quais foram obtidos ou se de outra forma autorizado pela Legislação de Proteção de Dados.

VIII. O TRATAMENTO DE DADOS PESSOAIS

27. A Planejar realizará o tratamento de dados pessoais nos seguintes casos:

- Coleta de informações de terceiros participantes dos projetos e iniciativas realizadas pela Planejar, conforme o Aviso de Privacidade aos Beneficiários;

- Coleta de informações dos representantes dos Signatários e potenciais Signatários, conforme o Aviso de Privacidade aos Signatários e Potenciais Signatários;
- Coleta de informações de Profissionais, conforme o Aviso de Privacidade aos Profissionais;
- Coleta de informações de fornecedores ou parceiros, conforme a Política de Tratamento de Dados Pessoais Para Fornecedores e Parceiros.

IX. BASES LEGAIS PARA TRATAMENTO DE DADOS

IX.1 PESSOAS SENSÍVEIS

28. Os Dados Pessoais podem ser tratados apenas de acordo com bases legítimas previstas da Legislação de Proteção de Dados, incluindo:

- o consentimento livre, informado e inequívoco do Titular de Dados;
- o cumprimento de uma obrigação legal ou regulatória pelo Controlador;
- a execução de um contrato entre o Controlador e o Titular de Dados, incluindo procedimento preliminares para elaboração do contrato;
- para o exercício regular de direitos em processo judicial, administrativo ou arbitral;
- para cumprir com interesses legítimos da Planejar ou de terceiro;

29. O Tratamento de Dados Pessoais Sensíveis poderá ocorrer também apenas de acordo com bases legítima, incluindo as seguintes hipóteses:

- o consentimento livre, informado, inequívoco, de forma específica e destacada e para finalidades específicas, do Titular de Dados;
- o cumprimento de uma obrigação legal ou regulatória pelo Controlador;
- para o exercício regular de direitos, inclusive em contratos e processos judicial, administrativo ou arbitral;

- (iv) para fins de autenticação e segurança em sistemas eletrônicos.

X. TRANSFERÊNCIA DE DADOS PESSOAIS PARA O EXTERIOR

30. A Planejar deve garantir que transferências de Dados Pessoais para o exterior observem o estabelecido pela LGPD.

31. Nesse sentido, Dados Pessoais poderão ser transferidos ao exterior nos seguintes casos:

- (i) para países que proporcionem grau de proteção de dados pessoais adequado, conforme será determinado pela ANPD;
- (ii) mediante cláusulas contratuais específicas para determinada transferência, cláusulas-padrão contratuais, normas corporativas globais ou selos, certificados e códigos de conduta, todos a serem aprovados pela ANPD;
- (iii) quando o Titular de Dados tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades.

32. A não ser que de outra forma comunicado ao Titular de Dados, a Planejar apenas realizará transferências de dados pessoais para o exterior para as seguintes finalidades:

- (i) armazenamento de dados em sistemas de nuvem internacionais;
- (ii) armazenamento de dados e informações no sistema da instituição certificadora internacional “FPSB” (Financial Planning Standard Boards);
- (iii) (cumprimento de contratos e parcerias com entidades internacionais para realização de ações específicas (como eventos), mediante notificação prévia no momento da inscrição.

XI. DIREITOS DOS TITULARES DE DADOS

33. A LGPD define que os Titulares de Dados devem receber informações sobre o Tratamento dos Dados Pessoais no momento de sua coleta. Os termos de uso, contratos ou avisos de privacidade devem disponibilizar as informações sobre o Tratamento de forma clara, adequada e ostensiva, incluindo:

- a) nome do Controlador e suas informações de contato, que será a Planejar, nesse caso;
- b) quais Dados Pessoais são coletados;
- c) para quais finalidades os Dados Pessoais serão usados;
- d) com quem os Dados Pessoais serão compartilhados;
- e) forma e duração do Tratamento;
- f) informações sobre os direitos dos Titulares de Dados e como exercer esses direitos.

34. No caso de um Tratamento de Dados Pessoais, os Titulares de Dados possuem os seguintes direitos dentre outros previstos na Legislação de Proteção de Dados e que também devem constar nos contratos, termos de uso e/ou políticas de privacidade:

- a) confirmação da existência de Tratamento;
- b) acesso aos Dados Pessoais;
- c) correção de Dados Pessoais que estejam incompletos, inexatos ou desatualizados;
- d) anonimização, bloqueio ou eliminação de Dados Pessoais desnecessários, excessivos ou tratados em desconformidade com a LGPD;
- e) portabilidade dos Dados Pessoais a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da ANPD;
- f) informação sobre a possibilidade de não fornecer seu consentimento para Tratamento dos Dados Pessoais e sobre as consequências da negativa;
- g) revogação do consentimento, por procedimento gratuito e facilitado, nos casos em que a base legal utilizada para Tratamento dos Dados Pessoais tenha sido o consentimento.

35. Os Titulares de Dados poderão exercer seus direitos por meio de solicitações encaminhadas ao Encarregado de Dados.

XII. PADRÕES DE SEGURANÇA

36. Todos os Profissionais da Planejar devem anuir e cumprir com esta Política e demais normativos internos e instruções comunicadas de tempos em tempos pela Planejar.

37. Ao implementar novos processos, procedimentos ou sistemas que envolvam o Tratamento de Dados Pessoais, a Planejar deve adotar todas medidas para garantir o cumprimento da Legislação de Proteção de Dados desde a fase de concepção do produto ou do serviço até a sua execução.

38. A Planejar aplicará procedimentos de segurança física e informacional adequados e em conformidade com as regulamentações aplicáveis.

39. Os Profissionais, inclusive prestadores de serviço e parceiros de negócio da Planejar serão vinculados a obrigações de confidencialidade. Apenas os Profissionais que necessitam acessar Dados Pessoais para o desenvolvimento de suas atividades terão acesso a tais Dados Pessoais.

XIII. PRESTADORES DE SERVIÇO/FORNECEDORES

40. Os prestadores de serviços/fornecedores que tratem Dados Pessoais em nome da Planejar estão sujeitos às obrigações impostas aos Operadores de acordo com a LGPD e a Política de Tratamento de Dados Pessoais Para Fornecedores e Parceiros da Planejar.

41. Os Profissionais que negociem contratos em nome da Planejar deverão assegurar que todos os contratos com prestadores de serviço/fornecedores contenham disposições sobre proteção de Dados Pessoais adequadas às circunstâncias, bem como que os Operadores implementem todas as medidas de segurança e controles técnicos e administrativos

apropriados para garantir a confidencialidade e segurança dos Dados Pessoais tratados em nome da Planejar.

XIV. INCIDENTES DE SEGURANÇA

42. Todos os incidentes de segurança devem ser reportados por meio do preenchimento do formulário de reporte de incidentes de segurança que consta no Anexo A desta Política e será incluído na intranet /Teams da Planejar, para acesso por todos os Profissionais.

43. Incidentes de segurança incluem, sem limitação, qualquer perda, exclusão, roubo ou acesso não autorizado aos Dados Pessoais que estejam em posse da Planejar.

44. São exemplos de incidentes de segurança:

- a) instalação de ferramentas não autorizadas nos sistemas da Planejar por qualquer Profissionais ou terceiro que tenha acesso a tais sistemas;
- b) tentativas não autorizadas de acesso ou acessos não autorizados aos sistemas da Planejar;
- c) vírus e outros códigos maliciosos;
- d) sequestro de dados;
- e) desrespeito a esta Política ou à Legislação de Proteção de Dados.

45. Todos os incidentes de segurança serão avaliados pelo Comitê de Governança que deverá definir quais medidas serão adotadas, incluindo a notificação à ANPD e/ou aos Titulares de Dados.

XV. LEGISLAÇÃO RELACIONADA

Constituição Federal

Lei nº 8.078/90 - Código de Defesa do Consumidor

Lei nº 12.965/2014 - Marco Civil da Internet

Decreto nº 8.771/2016 - Decreto Regulamentador do Marco Civil da Internet

Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais

XVI. REFERÊNCIA INTERNA

Política de Tratamento de Dados Para Fornecedores e Parceiros da Planejar

Aviso de Privacidade aos Signatários e Potenciais Signatários da Planejar

Aviso de Privacidade aos Profissionais da Planejar

Aviso de Privacidade aos Beneficiários da Planejar

CONSELHO DE ADMINISTRAÇÃO PLANEJAR

ANEXO

Anexo A – Formulário de reporte de incidentes de segurança

Nome:

Cargo:

Área:

Descrição do Incidente:

Data e hora que o incidente foi descoberto:

Locais e sistemas afetados:

O incidente foi solucionado? De que maneira?

Potenciais impactos do incidente: [Danos aos sistemas/perda de dados/violação da legislação/violação de políticas internas]

Há ou se desconfia que haja o envolvimento de algum Profissional no incidente de segurança? Se sim, qual o nome e qual foi a participação deste Profissional Planejar?