POL – 0010_Política de Proteção de Dados Pessoais

Histórico de Revisão

Data	Versão	Descrição	Autor
22/01/2024	1.0	POL – 0010_Política de Proteção de Dados Pessoais	Cláudio Boros
18/03/2024	2.0	POL – 0010_Política de Proteção de Dados Pessoais	Cláudio Boros

Aviso Preliminar

O presente Documento visa a auxiliar na elaboração da Política de Proteção de Dados Pessoais, em atendimento ao previsto no art. 50 da Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), que determina que a Plano Consultoria, ao prestar diversos serviços que tratam dados pessoais à seus contratantes, deve, no âmbito de suas competências, formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. Adicionalmente, a Elaboração da Política de Proteção de Dados Pessoais visa a atender, além da LGPD, a outros normativos vigentes sobre o tema de privacidade e proteção de dados.

Este documento é de autoria exclusiva da Plano Consultoria, baseado em diversas publicações e documentos técnicos já existentes que são utilizados amplamente por profissionais da área de privacidade e segurança da informação. Destacam-se as publicações do Center for Internet Security (CIS), da International Organization for Standardization (ISO) e do National Institute of Standards and Technology (NIST), com o objetivo de facilitar a difusão de conhecimentos sobre privacidade e segurança da informação.

Nesse cenário, a Plano Consultoria enfatiza que:

a) não representa, tampouco se manifesta em nome do CIS, da ISO e do NIST;
b) não se manifesta em nome da ANPD;
c) não é coautora das publicações internacionais abordadas;
d) não assume responsabilidade administrativa, técnica ou jurídica por usos ou interpretações inadequadas, fragmentados ou parciais do presente documento; e
e) caso o leitor deseje se certificar de que atende integralmente os requisitos das publicações das instituições mencionadas, CIS, à ISO, à ABNT, ao NIST.

Este Documento será atualizado frequentemente, de acordo com as novas diretrizes determinadas pelas autoridades em privacidade e proteção de dados, ou segundo eventuais alterações que ocorram nos normativos vigentes relacionados a privacidade e proteção de dados e outras referências utilizadas neste documento.

Introdução

Este documento tem por finalidade apresentar orientações sobre a Política de Proteção de Dados Pessoais no âmbito institucional.

O Art.50. da Lei Geral de Proteção de Dados (LGPD) estabelece que os controladores e operadores devem criar e implementar regras de boas práticas de governança para o tratamento de dados pessoais:

> "Art. 50: Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais."

Ressaltamos ainda, que a adoção deste documento não dispensa a Plano Consultoria de observar e considerar as diretrizes estabelecidas pela Autoridade Nacional de Proteção de Dados (ANPD), pela Lei Geral de Proteção de Dados Pessoais (LGPD) e outras normas vigentes.
A Política de Proteção de Dados Pessoais é um normativo institucional que tem o papel de estabelecer regras e diretrizes para o tratamento e para a governança de dados pessoais dentro de uma organização. Estipular papeis e responsabilidades claras e objetivas, definir diretrizes de tratamento e estabelecer meios de monitoramento do cumprimento da política são processos muito importantes para garantir a privacidade e a proteção de dados pessoais custodiados pela organização.

Objetivo da Política

A Política de Proteção de Dados Pessoais tem por objetivo estabelecer diretrizes, princípios e conceitos a serem seguidos por todas as pessoas e entidades que se relacionam com a Plano Consultoria, que em algum momento realizam operações de tratamento de dados pessoais, visando o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD) e outras normas vigentes.

Nesse contexto, a Plano Consultoria também precisa estar em conformidade com a LGPD, uma vez que lida diariamente com informações pessoais de seus colaboradores, parceiros, representantes de fornecedores e clientes. É relevante destacar que essa lei é embasada em diversas regulamentações que visam a proteção de dados pessoais, tendo o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia como uma de suas principais referências. O GDPR é um conjunto abrangente de regras do direito europeu relacionadas à privacidade e proteção de informações pessoais.

Escopo

Instituir a Política de Proteção de Dados Pessoais (PPDP), no âmbito da Plano Consultoria, com a finalidade de estabelecer princípios e diretrizes para a implementação de ações que garantam a proteção de dados pessoais, e no que couber, no relacionamento com outras entidades públicas ou privadas que tenham acesso e/ou utilize dados institucionais, incluindo os dados pessoais.
Esta Política regula a proteção de dados pessoais, que Plano Consultoria é o agente de tratamento, bem como o meio utilizado para este tratamento, seja digital ou físico, além de qualquer pessoa que realize operações de tratamento de dados pessoais em seu nome ou em suas dependências.

Termos e Definições

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, constituída pela área de Segurança da Informação;

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, constituída pela área de Segurança da Informação;

Encarregado: pessoa indicada pelo controlador, para atuar como canal de comunicação entre o controlador, os titulares dos dados pessoais e a Autoridade Nacional de Proteção de Dados (ANPD), constituída pela área de Projetos e Processos.

Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

Dado pessoal sensível: dado pessoal 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, quando vinculado a uma pessoa natural;

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

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;

Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

CAPÍTULO I

Das Diretrizes Gerais

Art. 1º A Plano Consultoria, deverá estar apto(a) a demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, e a eficácia dessas medidas.

Art. 2º Devem ser estabelecidas revisões de processos com o objetivo de aferir a diminuição ou aumento de riscos que envolvem o tratamento de dados pessoais.

Art. 3º Os dados pessoais que forem coletados e tratados no software, site ou aplicativo mantido pela Plano Consultoria, também devem ser administrados de acordo com as diretrizes desta política. Normativos específicos devem ser elaborados para a gestão destes dados coletados a partir de sites, software e aplicativos.

Art. 4º A Plano Consultoria, poderá utilizar arquivos (cookies) para registrar e gravar no computador do usuário as preferencias e navegações realizadas nas respectivas páginas para fins estatísticos e de melhoria dos serviços ofertados, respeitando o consentimento do titular.

Art. 5º É competência dos responsáveis em administrar a Proteção de Dados Pessoais, gerenciar a implementação da LGPD dentro da organização e a administração da Política de Proteção de Dados Pessoais.

Art. 6º A Plano Consultoria deve manter registro das operações de tratamento de dados pessoais que realizarem.

Art. 7º Deve ser elaborado o Relatório de Impacto de Proteção de Dados Pessoais (RIPD) relacionados às operações de tratamento, e atualizá-lo quando necessário.

Art. 8º A Plano Consultoria deverá desenvolver e manter atualizados as políticas/avisos de privacidade, que fornecerão informações sobre o processamento de dados pessoais em cada ambiente físico ou virtual, bem como detalhar as medidas de proteção de dados adotadas para salvaguardar esses dados pessoais.

Art. 9º Será estabelecido o programa de treinamento e conscientização para que os colaboradores entendam suas responsabilidades e procedimentos na proteção de dados pessoais;

Art. 10º Serão formuladas regras de segurança, de boas práticas e de governança que definam procedimentos e outras ações referentes a privacidade e proteção de dados pessoais.

CAPÍTULO II

Tratamento de Dados Pessoais

Art. 11. A aplicação desta Política será pautada pelo dever de boa-fé e pela observância dos princípios previstos no art. 6º da LGPD.

Art. 12. O tratamento de dados pessoais deverá ser realizado para o atendimento de sua finalidade, com o objetivo de executar competências legais e de cumprir suas atribuições legais.

Art. 13. A Plano Consultoria adotará mecanismos para que o titular do dado pessoal usufrua dos direitos assegurados pela LGPD e normativos correlatos, que será tratado pela Segurança da Informação.

Art. 14. Deverá ser realizado o tratamento de dados pessoais sensíveis somente nos termos da seção II do capítulo II da LGPD e devem ser estabelecidos procedimentos de segurança no tratamento destes dados conforme a LGPD e demais normativos.

Art. 15. Deverá ser realizado o tratamento de dados pessoais de crianças e de adolescentes nos termos da seção III do capítulo II da LGPD, bem como, poderá ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da Lei Geral

de Proteção de Dados Pessoais (LGPD), desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do art. 14 da Lei.

Art. 16. O uso compartilhado de dados deverá observar o art. 26 da LGPD bem como sua comunicação estará sujeita ao que consta no art. 27 da mesma lei.

Art. 17. No caso de transferência internacional de dados pessoais deverá ser observado o que consta no Capítulo V da LGPD.

CAPÍTULO III

Conscientização, Capacitação e Sensibilização

Art. 18. As pessoas que possuem acesso aos dados pessoais na Plano Consultoria, devem fazer parte de programas de conscientização, capacitação e sensibilização em matérias de privacidade e proteção de dados pessoais.

I. A conscientização, capacitação e sensibilização em privacidade e proteção de dados pessoais deve ser adequada aos papéis e responsabilidades das pessoas.

II. Assinatura do documento do termo de ciência LGPD.

CAPÍTULO IV

Segurança e Boas Práticas

Art. 19. A Plano Consultoria, deve manter uma base de conhecimento com documentos que apresentam condutas e recomendações que melhoram o gerenciamento de risco e que orientam na tomada de ações adequadas em caso de comprometimento de dados pessoais.

Art. 20. Qualquer ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos dados pessoais dos titulares deve ser comunicada a Autoridade Nacional de Proteção de Dados (ANPD) dentro do prazo previsto pela LGPD.

Art. 21. Serão adotadas medidas técnicas e organizacionais de privacidade e proteção de dados, dispostas a seguir, com o objetivo diminuir ou mitigar a existência incidentes com os dados pessoais do titular:

I. o acesso aos dados pessoais é limitado as pessoas que realizam o tratamento.

II. as funções e responsabilidades dos colaboradores envolvidos nos tratamentos de dados pessoais são claramente estabelecidas e comunicadas;

III. são estabelecidos acordos de confidencialidade, termos de responsabilidade ou termos de sigilo com operadores de dados pessoais;

IV. todos os dados pessoais são armazenados em ambiente seguro, de modo que terceiros não autorizados não possam acessá-los.

CAPÍTULO V

Auditoria e Conformidade

Art. 22. O cumprimento desta Política, bem como dos normativos que a complementam devem ser avaliados periodicamente por meio de verificações de conformidade, buscando a certificação do cumprimento dos requisitos de privacidade e proteção de dados pessoais e da garantia de cláusula de responsabilidade e sigilo constantes de termos de responsabilidade, contratos, convênios, acordos e instrumentos congêneres.

Art. 23. As atividades, produtos e serviços desenvolvidos na Plano Consultoria, devem estar em conformidade com requisitos de privacidade e proteção de dados pessoais constantes de leis, regulamentos, resoluções, normas, estatutos e contratos jurídicos vigentes.

Art. 24. Os resultados de cada ação de verificação de conformidade devem ser documentados em relatório de avaliação de conformidade.

CAPÍTULO VI

Funções e Responsabilidades

Art. 25. Qualquer pessoa natural ou jurídica de direito público ou privado que tenha interação em qualquer fase do tratamento de dados pessoais deve garantir a privacidade e a proteção de dados pessoais, mesmo após o término do tratamento, observando as medidas técnicas e administrativas determinadas pela organização.

Art. 26. Compete a Plano Consultoria, prover orientação e o patrocínio necessários às ações de privacidade e proteção de dados pessoais, de acordo com os objetivos estratégicos e com as leis e regulamentos pertinentes.

I. assessorar a implementação da proteção de dados pessoais;

II. constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre proteção de dados pessoais;

III. participar da elaboração da Política de Proteção de Dados Pessoais e das demais normas internas de privacidade e proteção de dados pessoais, além de propor atualizações e alterações nestes dispositivos;

IV. incentivar a conscientização, capacitação e sensibilização das pessoas que desempenham qualquer atividade de tratamento de dados pessoais dentro da Plano Consultoria.

Art. 27. A responsabilidade pelas decisões relacionadas ao tratamento de dados pessoais é da Plano Consultoria, que no exercício das atribuições típicas de controlador determina as medidas necessárias para executar a Política de Proteção de Dados Pessoais dentro de sua estrutura organizacional.

Art. 28. São atribuições do controlador:

I. observar os fundamentos, princípios da privacidade e proteção de dados pessoais e os deveres impostos pela LGPD e por normativos correlatos no momento de decidir sobre um futuro tratamento ou realizá-lo;

II. considerar o preconizado pelos art. 7º, art. 11 e art. 23 antes de realizar o tratamento de dados pessoais;

III. cumprir o previsto pelos art. 46 e art. 50 da LGPD buscando à proteção de dados pessoais e sua governança;

IV. indicar um encarregado pelo tratamento de dados pessoais, divulgando a identidade e as informações de contato do encarregado de forma clara e objetiva, preferencialmente no sítio institucional.

V. elaborar o inventário de dados pessoais a fim de manter registros das operações de tratamento de dados pessoais;

VI. reter dados pessoais somente pelo período necessário para o cumprimento da hipótese legal e finalidade utilizadas como justificativa para o tratamento de dados pessoais;

VII. criar e manter atualizados os avisos ou políticas de privacidade, que informarão sobre os tratamentos de dados pessoais realizados em cada

ambiente físico ou virtual, e como os dados pessoais neles tratados são protegidos;

VIII. requerer do titular a ciência com o termo de uso para cada serviço ofertado, informatizado ou não, que trate dados pessoais.

§ 1º É vedado qualquer tratamento de dados pessoais para fins não relacionados com as atividades desenvolvidas pela organização, ou por pessoa não autorizada formalmente pela Plano Consultoria.

Art. 29. São considerados operadores de dados pessoais as pessoas naturais ou jurídicas de direito público ou privado, que realizam operações de tratamento de dados pessoais em nome do controlador.
Parágrafo único. Qualquer fornecedor de produtos ou serviços, que por algum motivo, realiza o tratamento de dados pessoais a eles confiados, são considerados operadores e devem seguir as diretrizes estabelecidas nesta política, em especial o capítulo VII.

Art. 30. São atribuições do operador:

I. observar os princípios estabelecidos no Art. 6º da LGPD, ao realizar tratamento de dados pessoais.

II. seguir as diretrizes estabelecidas pelo controlador;

III. antes de efetuar o tratamento, verificar se as diretrizes estabelecidas pelo controlador cumprem os requisitos legais presentes nos art. 7º, art. 11 e art. 23 da LGPD;

Parágrafo único. É proibida a decisão unilateral do operador quanto aos meios e finalidades utilizados para o tratamento de dados pessoais.

Art. 31. São atribuições do encarregado de proteção de dados:

I. receber reclamações e comunicações dos titulares, prestar esclarecimentos e adotar

providências;

II. receber comunicações e requisições da ANPD e adotar providências; e

III. orientar os colaboradores da organização a respeito das práticas a serem adotadas em relação à proteção de dados pessoais.

CAPÍTULO VII

Contratos, Convênios, Acordos e Instrumentos Congêneres

Art. 32. Os contratos, convênios, acordos e instrumentos similares atualmente em vigor, que de alguma forma envolvam o tratamento de dados pessoais, devem incorporar cláusulas específicas em total conformidade com a presente Política de Proteção de Dados Pessoais e que contemplem:

I. requisitos mínimos de segurança da informação.

II. determinação de que o operador não processe os dados pessoais para finalidades que divergem da finalidade principal informada pelo controlador.

III. requisitos de proteção de dados pessoais que os operadores de dados pessoais devem atender.

IV. condições sob as quais o operador deve devolver ou descartar com segurança os dados pessoais após a conclusão do serviço, rescisão de qualquer contrato ou de outra forma mediante solicitação do controlador

V. diretrizes especificas sobre o uso de subcontratados pelo operador para execução contratual que envolva tratamento de dados pessoais.

Art. 33. São adotadas medidas rigorosas com o propósito de assegurar que os terceiros e processadores de dados pessoais contratados estão plenamente em conformidade com as cláusulas contratuais estabelecidas no momento da celebração do acordo entre as partes envolvidas.

CAPÍTULO VIII

Penalidades

Art. 34. Ações que violem a Política de Proteção de Dados Pessoais poderão acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurados aos envolvidos o contraditório e a ampla defesa.

Art. 35. Casos de descumprimento desta Política deverão ser registrados e comunicados para ciência e tomada das providências cabíveis.

CAPÍTULO IX

Disposições Finais

Art. 36. As dúvidas sobre a Política de Proteção de Dados Pessoais e seus documentos devem ser submetidas aos responsáveis, através do Canal de Confiança, que foi estabelecido para tratar tais necessidades.

Art. 37. Esta política deverá ser revisada periodicamente, a partir do início de sua vigência.

Art. 38. Os casos omissos serão resolvidos pela alta direção.

Art. 39. Esta política entra em vigor na data de sua publicação.