gov.br

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS

GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO

Modelo de Política de Proteção de Dados Pessoais

Programa de Privacidade e Segurança da Informação (PPSI)

Versão 1.1
Brasília, outubro de 2024

MODELO DE POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS
Esther Dweck
Ministra

SECRETARIA DE GOVERNO DIGITAL
Rogério Souza Mascarenhas
Secretário de Governo Digital

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO
Leonardo Rodrigo Ferreira
Diretor de Privacidade e Segurança da Informação

COORDENAÇÃO-GERAL DE PRIVACIDADE
Julierme Rodrigues da Silva
Coordenador-Geral de Privacidade

COORDENAÇÃO-GERAL DE SEGURANÇA DA INFORMAÇÃO
Loriza Andrade Vaz de Melo
Coordenadora-Geral de Segurança da Informação

Equipe Técnica de Elaboração
Francisco Magno Felix Nobre
Ivaldo Jeferson de Santana Castro
Leonard Keyzo Yamaoka Batista
Rafael da Silva Ribeiro

Equipe Revisora
Adriano de Andrade Moura
Julierme Rodrigues da Silva
Rogério Vinícius Matos Rocha

Equipe Técnica de Revisão - Versão 1.1
Adriano de Andrade Moura
Anderson Souza de Araújo
Bruno Pierre Rodrigues de Sousa
Ivaldo Jeferson de Santana Castro
Leonard Keyzo Yamaoka Batista
Raphael César Estevão
Rafael da Silva Ribeiro
Rogério Vinícius Matos Rocha

Histórico de versões

Data	Versão	Descrição	Autor
24/10/2023	1.0	Modelo de Política de Proteção de Dados Pessoais	Equipe Técnica de Elaboração
03/10/2024	1.1	Adequação do Modelo a Resolução CD/ANPD Nº 18, de 16 de julho de 2024.	Equipe Técnica de Revisão

Sumário

1 Aviso preliminar e agradecimentos

O presente Modelo, especialmente recomendado e dirigido aos órgãos e às entidades da Administração Pública Federal - APF, 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 Administração Pública, ao prestar diversos serviços que tratam dados pessoais à sociedade, 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 Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos - MGI e tem como referência fundamental o Guia do Framework de Privacidade e Segurança da Informação 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, tais referências, quando escritas em línguas estrangeiras, foram traduzidas para o português pela equipe técnica da Diretoria de Privacidade e Segurança da Informação (DPSI) da Secretaria de Governo Digital.

Nesse cenário, a Secretaria de Governo Digital 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 modelo; e
e) caso o leitor deseje se certificar de que atende integralmente os requisitos das publicações das instituições mencionadas, deverá consultar diretamente as fontes oficiais de informação ofertadas por elas, que foram listadas na seção “Referências Bibliográficas” deste documento.

Finalmente, um agradecimento especial deve ser registrado ao CIS, à ISO, ao NIST e aos profissionais de privacidade e segurança da informação consultados, por suas valiosas contribuições para a comunidade e para elaboração deste documento.

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

2 Introdução

Este modelo tem por finalidade apresentar orientações com o intuito de auxiliar os órgãos e entidades da Administração Pública Federal, direta, autárquica e fundacional a elaborar sua Política de Proteção de Dados Pessoais no âmbito institucional.

O Controle 22 do Guia do Framework de Privacidade e Segurança da Informação (p. 62) estabelece que:

Controle 22: Políticas, Processos e Procedimentos – Definir, desenvolver, divulgar, implementar e atualizar políticas, processos e procedimentos operacionais, internos e externos que regem as ações relativas à proteção de dados pessoais e privacidade, e controles para programas, sistemas de informação ou tecnologias que envolvam o tratamento de dados pessoais.

O presente documento serve como um modelo prático a ser utilizado na implementação do controle 22 do Guia do Framework de Privacidade e Segurança da Informação1 v1 e respectivas evoluções desta versão (1.1, 1.2 etc.) elaborado e publicado pela SGD. A medida do controle 22 que está contemplada por este modelo é a 22.2.

Cada vez mais o Governo utiliza a tecnologia para melhorar e expandir a oferta de serviços públicos para o cidadão apoiado em sistemas informatizados.

Nesse contexto, os órgãos federais, com infraestrutura própria ou contratada de terceiros, coletam, recebem, acessam, processam, modificam, produzem, extraem, validam, armazenam, distribuem e transmitem informações confidenciais e públicas para apoiar a entrega de produtos e serviços essenciais (por exemplo, fornecimento de serviços financeiros; fornecimento de serviços de emissões guias, certificados e carteiras; processamento de autorizações de segurança ou dados de saúde; fornecimento de serviços em nuvem; desenvolvendo comunicações via cabo, wireless e/ou satélites; sistemas militares de defesa). As informações federais são frequentemente fornecidas ou compartilhadas, obedecidos os requisitos legais, com entes como governos estaduais e municipais, empresas públicas e privadas, faculdades e universidades, organizações de pesquisa independentes ou públicas e organizações do terceiro setor.

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 (BRASIL, 2018).

Ressaltamos ainda, que a adoção deste modelo não dispensa as instituições da Administração Pública Federal 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.

3 Política de Proteção de Dados Pessoais

IMPORTANTE: Este modelo deve ser utilizado exclusivamente como referência, devendo o órgão ou entidade considerar as particularidades técnicas especificas do seu ambiente, bem como observar a boa aderência aos processos internos a fim de construir uma política que seja adequada a sua realidade.

Este modelo tem por foco prover diretrizes para a elaboração da política de proteção de dados pessoais.

Para usar este modelo, basta substituir o texto [com destaque amarelo] por informações personalizadas do seu órgão ou entidade. Quando estiver concluído, exclua todos os textos introdutórios ou de exemplos (em vermelho) e converta todo o texto restante em preto antes do processo de aprovação.

4 Propósito

Objetivo da Política

Levando em consideração a natureza e a finalidade do órgão ou entidade, descreva os fatores ou circunstâncias que determinam a existência da política de proteção de dados pessoais. Além disso, demonstre os objetivos básicos da política e o que ela pretende alcançar.

Exemplo: 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 [Órgão ou Entidade] 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.

[Acrescente aqui os objetivos para a Política de Proteção de Dados Pessoais que julgar necessário.]

5 Escopo

Amplitude, alcance da Política

Defina a quem e a quais sistemas esta política se aplica. Liste os agentes públicos e colaboradores necessários para cumprir ou simplesmente indique "todos" se todos devem cumprir. Também indique quaisquer exclusões ou exceções que estejam fora de escopo, ou seja, essas pessoas, elementos ou situações que não estejam cobertas por esta política ou onde uma consideração especial possa ser feita.

Exemplo:

Instituir a Política de Proteção de Dados Pessoais (PPDP), no âmbito do(a) [Órgão ou entidade], 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.

Esta Política regula a proteção de dados pessoais, que [Órgão ou entidade] 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.

[Acrescente aqui mais definições sobre o escopo da Política de Proteção de Dados Pessoais que julgue necessárias.]

6 Termos e definições

Glossário

Defina quaisquer termos-chave, siglas ou conceitos que serão utilizados na política. [Recomenda-se utilizar como referência as definições apresentadas no Art. 5 da LGPD, além da PORTARIA GSI/PRNº 93, DE 18 DE OUTUBRO DE 2021 – Glossário de Segurança da Informação do Gabinete de Segurança Institucional da PRESIDÊNCIA DA REPÚBLICA].

Exemplo:

AGENTES DE TRATAMENTO: o controlador e o operador;

CONTROLADOR: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

OPERADOR: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

ENCARREGADO: pessoa indicada pelo controlador e operador, para atuar como canal de comunicação entre o controlador, os titulares dos dados pessoais e a Autoridade Nacional de Proteção de Dados (ANPD);

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;

[Acrescente os termos-chave, siglas ou conceitos que podem ser utilizados na política.]

7 Declarações da política

Regras aplicáveis ao caso específico

Descreva as regras que compõem a política. Isso normalmente toma a forma de uma série de breves declarações prescritivas. A subdivisão desta seção em subseções pode ser necessária dependendo da complexidade da política.

Art. 1º. Fica instituída a Política de Proteção de Dados Pessoais do [Órgão ou entidade], 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.

Art. 2º. Esta Política de Proteção de Dados Pessoais aplica-se a todas as unidades organizacionais do(a) [Órgão ou entidade], e deverá ser observada por todos os usuários de informação, seja servidor ou equiparado, empregado, prestador de serviços ou pessoa habilitada pela administração, por meio da assinatura de Termo de Responsabilidade, para acessar os ativos de informação sob responsabilidade deste(a) [Órgão ou entidade].

Art. 3°. A aplicação desta Política será pautada pelo dever de boa-fé e pela observância dos princípios previstos no art. 6º da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

CAPÍTULO I - Das Disposições Gerais

Art. 4° São objetivos da Política de Proteção de Dados Pessoais:

I. estabelecer medidas eficazes para o cumprimento das normas de proteção de dados pessoais e demonstrar a eficácia das mesmas;
II. estabelecer revisões de processos com o objetivo de aferir a diminuição ou aumento de riscos que envolvem o tratamento de dados pessoais;
III. promover a administração dos dados pessoais coletados e tratados, em qualquer meio, físico ou digital, custodiados ou sob orientação direta ou indireta do [Órgão ou entidade], de acordo com as diretrizes especificadas;
IV. estabelecer a necessidade de criar e manter um registro de todas as operações de tratamento de dados pessoais realizados;
V. promover a adequada gestão do tratamento dos dados pessoais;
VI. promover a criação de programas de treinamento e conscientização para que os colaboradores entendam suas responsabilidades e procedimentos na proteção de dados pessoais;
VII. promover a formulação regras de segurança, de boas práticas e de governança com objetivo de definir procedimentos e outras ações referentes a privacidade e proteção de dados pessoais;

Art. 5º O(a) [Órgão ou entidade] registrará e gravará as preferencias e navegações realizadas nas respectivas páginas para fins estatísticos e de melhoria dos serviços ofertados, através de arquivos (cookies), respeitando o consentimento do titular.

Art. 6º São responsabilidades do [Órgão ou entidade]:

I. atender ao disposto nos normativos e publicações da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) que disciplinam o tratamento e a governança dos dados pessoais;
II. elaborar, quando couber, o Relatório de Impacto de Proteção de Dados Pessoais (RIPD) relacionados às operações de tratamento, e atualizá-lo quando necessário;
III. realizar o desenvolvimento e a atualização das políticas/avisos de privacidade, que tem por finalidade o fornecimento de informações sobre o tratamento de dados pessoais em cada ambiente físico ou virtual, bem como, especificar as medidas de proteção de dados adotadas para salvaguardar esses dados pessoais.

[Acrescente aqui as diretrizes gerais que fazem parte do escopo da organização e que devem ser consideradas para a política]

CAPÍTULO II - Tratamento de Dados Pessoais

É necessário deixar claro que o órgão adotará medidas para garantir os direitos dos titulares de dados pessoais quando houver tratamento, quais princípios deverão ser observados em todas as operações realizadas com os dados pessoais, dentre outras diretrizes que julgar pertinentes ao escopo desta política.

Art. 7°. O tratamento de dados pessoais deve ser sempre realizado para o atendimento de sua finalidade pública, conforme o interesse público, com o objetivo de executar competências legais e de cumprir as atribuições legais do serviço público.

Art. 8°. As unidades organizacionais do(a) [Órgão ou entidade] devem adotar mecanismos para que os titulares de dados pessoais usufruam dos direitos assegurados pela LGPD e normativos correlatos.

[Listar por quais canais de atendimento o órgão irá garantir esses direitos].

Art. 9°. O tratamento de dados pessoais sensíveis deve ocorrer somente nos termos da seção II do capítulo II da LGPD e são estabelecidos procedimentos de segurança no tratamento destes dados conforme orientações da LGPD e demais normativos.

Art. 10. O tratamento de dados pessoais de crianças e de adolescentes deve ser realizado nos termos da seção III do capítulo II da LGPD, bem como, pode ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da mesma lei, desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do art. 14 da Lei.

Art. 11. O uso compartilhado de dados pessoais deve ocorrer em estrita observância ao art. 26 da LGPD.

Parágrafo Único. As operações remanescentes de uso compartilhado de dados devem seguir o disposto no Art. 27 da LGPD.

Art. 12. A transferência internacional de dados pessoais deve observar o disposto no Capítulo V da LGPD.

[Liste aqui demais diretrizes a serem seguidas nas operações de tratamento dos dados pessoais].

CAPÍTULO III - Conscientização, Capacitação e Sensibilização

Essa seção tem como objetivo dispor de diretrizes sobre a conscientização, capacitação e sensibilização dos colaboradores da organização na temática de proteção de dados pessoais e privacidade conforme o que a LGPD e normativos estipulam.

Art. 13. Os servidores do [Órgão ou entidade], com acesso a dados pessoais devem participar de programas de conscientização, capacitação e sensibilização em matérias de privacidade e proteção de dados pessoais, objetivando adequar o tema aos seus papeis e responsabilidades.

[Liste aqui diretrizes que julgue necessários para a conscientização, capacitação e sensibilização]

CAPÍTULO IV - Segurança e Boas Práticas

A segurança e o conjunto de boas práticas visam prevenir violações de privacidade e segurança, cumprir normas e regulamentações, bem como proteger a privacidade e promover a confiança dos titulares de dados pessoais. O órgão deve apresentar suas abordagens, políticas e ações recomendadas que asseguram a integridade, confidencialidade e disponibilidade de dados. Nesta seção, poderá ser especificado aspectos gerais das boas práticas e segurança que o órgão adota para garantir a proteção adequada dos dados pessoais coletados. Não havendo medidas técnicas de privacidade e segurança implementadas, deverão ser listadas ações de mitigação de riscos que se destinam a privacidade e proteção dos dados pessoais.

Art. 14. Considerando a necessidade de mitigar incidentes com dados pessoais, devem ser adotadas as seguintes medidas técnicas e organizacionais de privacidade e proteção de dados:

I. o acesso aos dados pessoais deve estar limitado as pessoas que realizam o tratamento.
II. as funções e responsabilidades dos colaboradores envolvidos nos tratamentos de dados pessoais devem ser claramente estabelecidas e comunicadas;
III. devem ser estabelecidos acordos de confidencialidade, termos de responsabilidade ou termos de sigilo com operadores de dados pessoais;

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

[Liste aqui outras medidas que julgue necessárias]

Art. 15. 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. 16. As unidades organizacionais do(a) [Órgão ou entidade] devem manter uma base de conhecimento com documentos que apresentam condutas e recomendações que melhoram o gerenciamento de risco e orientam na tomada de decisões adequadas em casos de comprometimento de dados pessoais.

[Liste aqui medidas de segurança e conjunto de boas práticas que fazem parte do escopo de privacidade e proteção de dados pessoais da organização].

CAPÍTULO V - Auditoria e Conformidade

Essa seção tem por objetivo orientar como será realizada a avaliação para determinar se a organização está em conformidade com as normas que regem a política. É importante estabelecer os responsáveis pela auditoria, os instrumentos pelo qual poderá ser realizada e documentada, além da periodicidade que ela será realizada.

Art. 17. 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 das cláusulas de responsabilidade e sigilo constantes de termos de responsabilidade, contratos, convênios, acordos e instrumentos congêneres.

Art. 18. As atividades, produtos e serviços desenvolvidos no(a) [Órgão ou entidade] devem observar os requisitos de privacidade e proteção de dados pessoais constantes de leis, regulamentos, resoluções, normas, estatutos e contratos jurídicos vigentes para estarem em conformidade.

Art. 19. Os resultados de cada ação de verificação de conformidade devem ser documentados em relatório de avaliação de conformidade.

[Liste aqui procedimentos que julgue ser necessários à auditoria e conformidade].

CAPÍTULO VI - Funções e Responsabilidades

Essa seção tem o objetivo de estabelecer as funções e responsabilidades dos operadores, encarregado e controlador da organização.

Também devem ser apresentadas as responsabilidades e diretrizes para o estabelecimento do Comitê de Proteção de Dados Pessoais (CPDP) ou estrutura equivalente. O uso da denominação "Comitê de Proteção de Dados Pessoais (CPDP)" apresenta caráter meramente ilustrativo, o órgão ou entidade deve citar, caso exista, o nome do colegiado que delibera sobre privacidade e proteção de dados pessoais na instituição. O tema da Proteção de Dados Pessoais faz parte de uma disciplina mais ampla chamada Governança de Dados. Desta forma, essas responsabilidades também podem ser absorvidas por um Comitê de Governança de Dados em um contexto mais abrangente.

É uma boa prática de governança existir o Comitê de Proteção de Dados Pessoais, mas seu destaque nesse modelo não significa que está sendo indicada a obrigatoriedade de existência, ficando a cargo da instituição avaliar a definição dessa estrutura. Se a instituição não adota colegiado sobre o tema privacidade e proteção de dados pessoais, então indica-se retirar os textos relacionados com o CPDP.

Art. 20. Qualquer pessoa natural ou jurídica de direito público ou privado que tenha interação em qualquer fase do tratamento de dados pessoais deve assegurar a privacidade e a proteção de dados pessoais que trata, mesmo após o término do tratamento, observando as medidas técnicas e administrativas determinadas pelo(a) [Órgão ou entidade].

Art. 21. Compete ao [Comitê de Proteção de Dados Pessoais (CPDP) ou estrutura equivalente]:

I. promover a proteção de dados pessoais e a adequação do [Órgão ou entidade] à LGPD;
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. a responsabilidade por gerenciar a implementação da LGPD dentro da organização e a administração da Política de Proteção de Dados Pessoais
V. incentivar a conscientização, capacitação e sensibilização das pessoas que desempenham qualquer atividade de tratamento de dados pessoais dentro do(a) [Órgão ou entidade].

[Liste as demais atribuições do Comitê de Proteção de Dados Pessoais (CPDP) ou estrutura equivalente que julgue necessário.]

Art. 22. O [Comitê de Proteção de Dados Pessoais (CPDP) ou estrutura equivalente] é constituído no mínimo por:

A composição destacada abaixo é meramente ilustrativa, ficando a cargo da instituição a definição da composição que considerar adequada a sua realidade.

I. gestor de Segurança da Informação;
II. o encarregado pelo tratamento de dados pessoais;
III. um representante da Secretaria-Executiva ou estrutura equivalente;
IV. um representante do departamento de tecnologia da informação;
V. um representante do departamento jurídico;
VI. um representante da ouvidoria;
VII. um representante da unidade de controle interno ou estrutura equivalente;
VIII. um representante de cada unidade finalística.

[Liste os demais integrantes do Comitê de Proteção de Dados Pessoais (CPDP) ou estrutura equivalente que julgue necessário.]

Art. 23. A presidência do [Comitê de Proteção de Dados Pessoais (CPDP) ou estrutura equivalente] será exercida pelo titular/representante da Secretária-Executiva do(a) [Órgão ou entidade].

Art. 24. A responsabilidade pelas decisões relacionadas ao tratamento de dados pessoais é do(a) [Órgão ou entidade] 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. 25. Compete ao 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; e
VIII. requerer do titular a ciência com o termo de uso para cada serviço ofertado, informatizado ou não, que trate dados pessoais.

[Liste as demais atribuições do controlador que julgue necessário.]

§ 1º É vedado qualquer tratamento de dados pessoais para fins não relacionados com as atividades desenvolvidas pela organização ou por pessoa não autorizada formalmente pelo(a) [Órgão ou entidade].

Art. 26. 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. Quaisquer fornecedores de produtos ou serviços, que por algum motivo, realizam 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. 27. Compete ao 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;

[Liste as demais atribuições do operador que julgue necessário.]

Parágrafo único. Não é competência do operador decidir unilateralmente quanto aos meios e finalidades utilizados para o tratamento de dados pessoais.

Art. 28. Compete ao 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;
III. orientar os colaboradores da organização a respeito das práticas a serem adotadas em relação à proteção de dados pessoais; e
IV. executar as demais atribuições determinadas pelo agente de tratamento ou estabelecidas em normas complementares.

Parágrafo único: Ao receber comunicações da ANPD, o encarregado adotará as medidas necessárias para o atendimento da solicitação e para o fornecimento de informações pertinentes, adotando, dentre outras, as seguintes providências:

I. encaminhar internamente a demanda para as unidades competentes
II. fornecer orientação e a assistência necessárias ao agente de tratamento; e

III. indicar expressamente o representante do agente de tratamento perante a ANPD para fins de atuação em processos administrativos, quando esta função não for exercida pelo próprio encarregado.

[Liste as demais atribuições do encarregado que julgue necessário, conforme destacado pelo inciso IV do § 2º do art. 41 da LGPD].

Art. 29 O encarregado de proteção de dados prestará assistência e orientação ao agente de tratamento na elaboração, definição, e implementação de:

I. registro e comunicação de incidente de segurança;
II. registro das operações de tratamento de dados pessoais;
III. relatório de impacto à proteção de dados pessoais;
IV. mecanismos internos de supervisão e de mitigação de riscos relativos ao tratamento de dados pessoais;
V. medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;
VI. processos e políticas internas que assegurem o cumprimento da LGPD, e dos regulamentos e orientações da ANPD;
VII. instrumentos contratuais que disciplinem questões relacionadas ao tratamento de dados pessoais;
VIII. transferências internacionais de dados;
IX. regras de boas práticas e de governança e de programa de governança em privacidade, nos termos do art. 50 da LGPD.
X. produtos e serviços que adotem padrões de design compatíveis com os princípios previstos na LGPD, incluindo a privacidade por padrão e a limitação da coleta de dados pessoais ao mínimo necessário para a realização de suas finalidades; e
XI. outras atividades e tomada de decisões estratégicas referentes ao tratamento de dados pessoais.

Art.30 Compete ao agente de tratamento:

I. prover os meios necessários para o exercício das atribuições do encarregado, neles compreendidos, entre outros, recursos humanos, técnicos e administrativos;
II. solicitar assistência e orientação do encarregado quando da realização de atividades e tomada de decisões estratégicas referentes ao tratamento de dados pessoais;
III. garantir ao encarregado a autonomia técnica necessária para cumprir suas atividades, livre de interferências indevidas, especialmente na orientação a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
IV. assegurar aos titulares meios céleres, eficazes e adequados para viabilizar a comunicação com o encarregado e o exercício de direitos; e

V. garantir ao encarregado acesso direto às pessoas de maior nível hierárquico dentro da organização, aos responsáveis pela tomada de decisões estratégicas que afetem ou envolvam o tratamento de dados pessoais, bem como às demais áreas da organização.

CAPÍTULO VII - Contratos, Convênios, Acordos e Instrumentos Congêneres

Este item tem como finalidade assegurar que o controlador observe rigorosamente se o terceiro, por meio de contratos, convênios ou quaisquer instrumentos afins, adota as medidas definidas pelo controlador com o propósito de cumprir os requisitos de privacidade e proteção de dados. O contrato entre as partes estabelece suas atribuições e responsabilidades. Cabe ao órgão citar quaisquer outras diretrizes pertinentes ao item.

Art. 31. Os contratos, convênios, acordos e instrumentos similares atualmente em vigor, que de alguma forma envolvam o tratamento de dados pessoais, precisam incorporar cláusulas específicas em total conformidade com a presente Política de Proteção de Dados Pessoais e que contemplem minimamente:

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.

[Liste as demais diretrizes que julgarem pertinentes sobre os contratos, convênios, acordos e instrumentos congêneres que devem estar presentes nesta Política de Proteção de Dados Pessoais].

A Secretaria de Governo Digital disponibiliza em seu portal o Guia de Requisitos e Obrigações quanto à Privacidade e Segurança da Informação que orienta a adequação do processo de contratação para contemplar os requisitos mais importantes de privacidade e segurança dos dados.

Art. 32. As unidades organizacionais do(a) [Órgão ou entidade] devem adotar medidas rigorosas com o propósito de assegurar que os terceiros e processadores de dados pessoais contratados estejam plenamente em conformidade com as cláusulas contratuais estabelecidas no momento da celebração do acordo entre as partes envolvidas.

CAPÍTULO VIII - Penalidades

Estabelecer as consequências e as penalidades para os casos de violação da Política de Proteção de Dados Pessoais ou de quebra de segurança, de acordo com as normas já existentes no ordenamento jurídico vigente sobre penalidades ao servidor público federal relativas ao assunto.

Art. 33. 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. 34. Casos de descumprimento desta Política serão registrados e comunicados ao [responsável] para ciência e tomada das providências cabíveis.

[Liste, caso necessário, as penalidades que estarão sujeitos aqueles que infligirem a Política de Proteção de Dados Pessoais].

CAPÍTULO IX - Disposições Finais

Este item tem como finalidade dispor das diretrizes finais que a organização deve expor para a revisão, e melhoria contínua da Política de Proteção de Dados Pessoais.

Art. 35. Os integrantes do [Comitê de Proteção de Dados Pessoais (CPDP) ou estrutura equivalente] poderão expedir instruções complementares, no âmbito de suas competências, que detalharão suas particularidades e procedimentos relativos à Proteção de Dados Pessoais alinhados às diretrizes emanadas pelo [CPDP ou estrutura equivalente] e aos respectivos Planos Estratégicos Institucionais do(a) [Órgão ou entidade].

Art. 36. As dúvidas sobre a Política de Proteção de Dados Pessoais e seus documentos serão submetidas ao [Comitê de Proteção de Dados Pessoais ou estrutura equivalente].

Art. 37. Esta política será revisada no período de [definir o prazo para revisão da política], a partir do início de sua vigência.

Art. 38. Os casos omissos serão resolvidos pela [autoridade máxima da organização ou CPDP].

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

[Liste, caso necessário, as diretrizes finais da Política de Proteção de Dados Pessoais].

Referências Bibliográficas

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado**. Abril de 2022.<https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf> Acesso em: 24 set 2024.

BRASIL. Autoridade Nacional de Proteção de Dados. **Resolução CD/ANPD Nº 18, de 16 de julho de 2024**. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074> Acesso em: 24 set 2024.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos**. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 24 set 2024.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Portaria nº 93, de 26 de setembro de 2019. Glossário de Segurança da Informação**. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-%20219115663>. Acesso em: 24 set 2024.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Instrução Normativa nº 01, maio de 2020. Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal**. Disponível em: <https://www.gov.br/gsi/pt-br/dsic/legislacao/copy_of_IN01_consolidada.pdf>. Acesso em: 24 set 2024.

COMITÊ ESTRATÉGICO DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS - MINISTÉRIO DA ECONOMIA - Resolução CEPPDP/ME Nº 7. Fevereiro de 2022. **Política de Proteção de Dados Pessoais no Ministério da Economia**. Disponível em:<https://www.gov.br/economia/pt-br/acesso-a-informacao/acoes-e-programas/integra/governanca/comites-tematicos-de-apoio-a-governanca/comite-tematico-de-protecao-de-dados-pessoais-ceppdp/documentos-ceppdp/resolucoes-ceppdp/resolucao-no-7-ceppdp-22-02-22> Acesso em: 24 set 2024.

COMPANHIA NACIONAL DE ABASTECIMENTO. **Política de Proteção de Dados Pessoais. 2021**. Disponível em: <https://www.conab.gov.br/institucional/normativos/politicas-planos-e-cartas/item/download/37247_7d884f3edcf4e911cae38ddd842b28fb>. Acesso em 24 set 2024.

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO DA SECRETARIA DE GOVERNO DIGITAL – DPSI/SGD. **Guia do Framework de Privacidade e Segurança da**

Informação. Novembro 2022. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf>. Acesso em: 24 set 2024.

MINISTÉRIO DA ECONOMIA. **Portaria Nº 218. Maio 2020. Política de Segurança da Informação do Ministério da Economia**. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-n-218-de-19-de-maio-de-2020-257605466> Acesso em: 24 set 2024.

MINISTÉRIO DA ECONOMIA. **Portaria ME Nº 4424, Abril 2021. Institui o Comitê Estratégico de Privacidade e Proteção de Dados Pessoais no âmbito do Ministério da Economia**. Disponível em: <https://www.gov.br/economia/pt-br/acesso-a-informacao/acoes-e-programas/integra/gestao-do-conhecimento/legislacoes/portaria-no-4-424-20-04-2021>. Acesso em: 24 set 2024.

TRIBUNAL REGIONAL DO TRABALHO DA 5ª REGIÃO. ATO TRT5 N. 468, Outubro de 2022. **Política de Privacidade e Proteção de Dados Pessoais do Tribunal Regional do Trabalho da 5ª Região**. Disponível em: <https://www.trt5.jus.br/sites/default/files/cdp/0468-2022_institui_a_politica_de_privacidade_e_protecao_de_dados_pessoais.pdf>. Acesso em: 24 set 2024.

TRIBUNAL REGIONAL DO TRABALHO DA 16ª REGIÃO. **Resolução Nº 144. Agosto de 2021. Política de Privacidade e Proteção de Dados Pessoais (PPPDP) do Tribunal Regional do Trabalho da 16ª Região (TRT16)**. Disponível em: <https://www.trt16.jus.br/sites/portal/files/roles/lgpd/pol%C3%ADtica%20de%20privacidade%20de%20dados%20pessoais%20do%20trt16.pdf>. Acesso em: 24 set 2024.

TRIBUNAL REGIONAL DO TRABALHO DA 18ª REGIÃO. **Resolução Administrativa Nº 96/2021. Agosto de 2021. Regulamenta as funções do Controlador, do Encarregado, dos Operadores e da Ouvidoria no âmbito do Tribunal Regional do Trabalho da 18ª Região**. Disponível em: <https://bibliotecadigital.trt18.jus.br/bitstream/handle/bdtrt18/22825/Resolucao%20Administrativa_TRT18_96_2021.PDF?sequence=1&isAllowed=y>. Acesso em: 24 set 2024.

TRIBUNAL REGIONAL DO TRABALHO DA 18ª REGIÃO. **Resolução Administrativa Nº 130/2021. Novembro de 2021. Política de Privacidade e Proteção de Dados Pessoais no âmbito do Tribunal Regional do Trabalho da 18ª Região**. Disponível em: <https://bibliotecadigital.trt18.jus.br/bitstream/handle/bdtrt18/24405/RA_2021_00130_comp_Port_2022_00304.pdf?sequence=4&isAllowed=y>. Acesso em: 24 set 2024.

TRIBUNAL DE JUSTIÇA DE SÃO PAULO. **Portaria Nº 9923. Novembro de 2020. Política de Proteção de Dados Pessoais dos sítios eletrônicos do Poder Judiciário de São Paulo**. Disponível em <https://www.tjsp.jus.br/Download/Portal/LGPD/Portaria_LGPD_9923-2020-2.pdf?638307375346176962>. Acesso em: 24 set 2024.

TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E DOS TERRITÓRIOS. **Resolução Nº 9. Setembro de 2020. Política de Privacidade dos Dados das Pessoas Físicas no Tribunal de Justiça do Distrito Federal e dos Territórios – TJDFT**. Disponível em: <https://www.tjdft.jus.br/publicacoes/publicacoes-oficiais/resolucoes-do-pleno/2020/resolucao-9-de-02-09-2020>. Acesso em: 24 set 2024.

TRIBUNAL DE CONTAS DA UNIÃO. 2010. **Padrões de Auditoria de Conformidade**. Disponível em: <https://portal.tcu.gov.br/contas-e-fiscalizacao/controle-e-fiscalizacao/auditoria/normas-de-fiscalizacao/auditoria-de-conformidade.htm>. Acesso em: 24 set 2024.

FACULDADES INTEGRADAS DE TAQUARA. **Política de Privacidade e Proteção de Dados Pessoais**. Disponível em: <https://www2.faccat.br/portal/?q=politica_privacidade> Acesso em: 24 set 2024.

Data Protection Policy – Template. Disponivel em: <https://www.eugdpr.institute/wp-content/uploads/2019/09/Data-Protection-Template.pdf> Acesso em: 24 set 2024.

INFORMATION COOMISSIONER'S OFFICE. **Data Protection Policy 2021**. Disponível em: <https://ico.org.uk/media/about-the-ico/policies-and-procedures/4025073/data-protection-policy.pdf >Acesso em: 24 set 2024.

INTERNATIONAL GENERAL INSURANCE GROUP. **Data Protection Policy 2018**. Disponível em: <https://iginsure.com/media/2061/data-protection-policy-published.pdf>. Acesso em: 24 set 2024.

WORLD CUSTOMS ORGANIZATION. **Personal Data Protection Policy**. Disponível em: <https://www.wcoomd.org/-/media/wco/public/global/pdf/about-us/legal-instruments/policies/personal-data-protection-policy_en.pdf?la=en>. Acesso em: 24 set 2024.

ANEXO I

Este anexo tem a finalidade de fornecer os destaques das mudanças inseridas nas versões do Modelo de Política de Proteção de Dados Pessoais, em comparação com o documento originalmente publicado em outubro de 2023.

Mudanças da Versão 1.1

As mudanças inseridas nesta versão em comparação com a anterior visam a adequação do Modelo com a Resolução CD/ANPD Nº 18, de 16 de julho de 2024.

Destacam-se as seguintes alterações:

- Adição do termo “agente de tratamento” e adequação da definição do termo “encarregado” na seção Termos e Definições.
- Na seção Definições da Política foram realizadas as seguintes atualizações:
    a) Inclusão do art. 7 que estipula a observação dos dispositivos normativos da ANPD já publicados para a elaboração da PPDP;
    b) Atualização do art. 34 que descreve as atribuições do encarregado de proteção de dados;
    c) Inclusão do art. 35 que descreve as atribuições do encarregado quando for prestar assistência ao agente de tratamento; e
    d) Inclusão do art. 36 que descreve as atribuições do agente de tratamento.
- Inclusão da Resolução CD/ANPD Nº 18, de 16 de julho de 2024 nas referências bibliográficas.