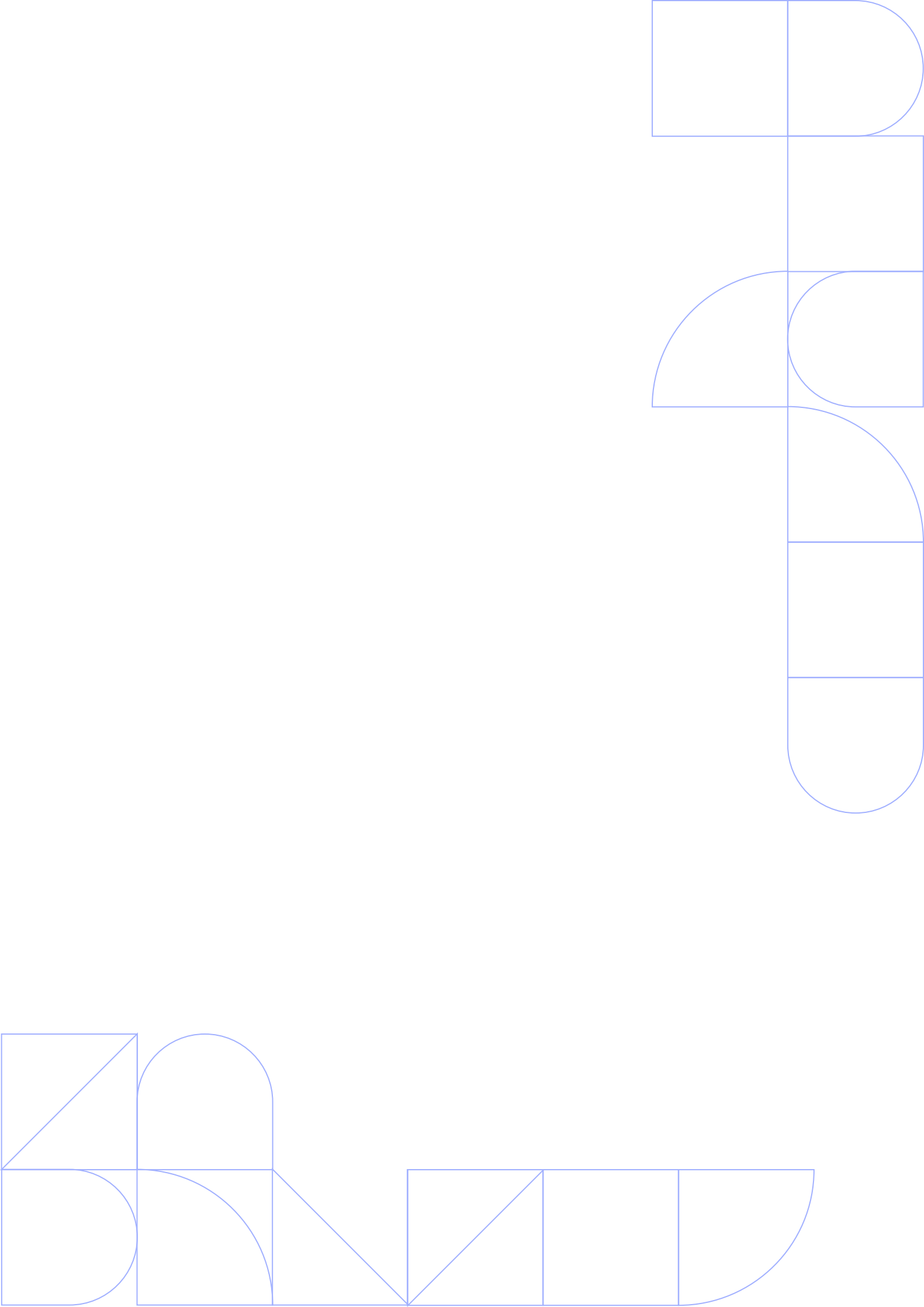


POLÍTICA DE PROTEÇÃO E DADOS PESSOAIS

MINISTÉRIO DA
GESTÃO E DA INOVAÇÃO
EM SERVIÇOS PÚBLICOS

GOVERNO DO BRASIL
DO LADO DO POVO BRASILEIRO



POLÍTICA DE PROTEÇÃO E DADOS PESSOAIS

Abril de 2026

FICHA TÉCNICA

Ministra da Gestão e da Inovação em Serviços Públicos
Esther Dweck

Secretário Executivo
Cilair Rodrigues de Abreu

Secretaria de Serviços Compartilhados
Isabela Gomes Gebrim

Diretoria de Gestão Estratégica
Rodrigo Lino de Brito

Coordenação-Geral de Proteção de Dados Pessoais
Clarissa Ferreira Lima Paes de Barros
Maria Clara Souza Caribé Frutuoso
Luiz Fernando Bastos Coura
Andreia Queiroz Correia Dummar
Julierme Rodrigues da Silva
Lucilene Ferreira da Silva Lopes
Sheila Cristina Soares Vieira
José Valter da Silva Júnior

Comitê de Privacidade e Proteção de Dados Pessoais

Titulares
Cilair Rodrigues de Abreu
Clarissa Ferreira Lima Paes de Barros
Fernanda Tsunematsu
Kimberly Coutinho Paes Leme de Castro
Hugo César de Paula Rezende
Leonardo Rodrigo Ferreira
Antonio Fiuza de Sousa Landim
Lair Maria de Oliveira
Gustavo Fernando Frohlich
Juliana Dias Viana Silva
Fabio Valotto
Domícia Gomes
Francisco Eduardo de Holanda Bessa
Ana Carolina Quintanilha dos Santos Loriato
Érica Bezerra Queiroz

Substitutos
Adauto Modesto Júnior
Maria Clara Souza Caribé Frutuoso
Luiz Fernando Bastos Coura
Miriam Barbuda Fernandes Chaves
Daniel Alves Braz dos Santos
Luís Eduardo Barreiro de Jesus
Marta Juvina de Medeiros
Rogério Mendes Meneguim
Edi Damasceno Maciel
Luciana de Almeida Toldo
João Flávio Pafume Coelho
Rudson Pereira Costa da Silva
Bruno de Freitas Tavares da Silva
Dilson Gonzaga Pereira Neto
Rildo Pereira Peixoto
Anderson Moreno Luz

SUMÁRIO

CAPÍTULO I – Das Disposições Preliminares 6

CAPÍTULO II – Das Responsabilidades 7

CAPÍTULO III – Dos Direitos dos Titulares de Dados Pessoais 9

CAPÍTULO IV – Do Tratamento de Dados Pessoais 11

Seção I – Do Termo de Uso e do Aviso de Privacidade 11

Seção II – Da Governança e das Boas Práticas 12

Seção III – Da Limitação do Tratamento 13

Seção IV – Da Gestão do Tratamento 13

Seção V – Da Qualidade dos Dados 14

Seção VI – Da Anonimização e da Pseudonimização 15

Seção VII – Do Compartilhamento 15

Seção VIII – Da Transferência Internacional de Dados 17

Seção IX – Do Término do Tratamento dos Dados 17

Seção X – Da Segurança Aplicada aos Dados Pessoais 18

Seção XI – Dos Incidentes 20

Seção XII – Da Conscientização, da Capacitação e da Sensibilização 21

Seção XIII – Dos Contratos, Convênios, Acordos e Instrumentos Congêneres 21

Seção XIV – Da Auditoria e da Conformidade 22

Seção XV – Das Penalidades 22

Seção XVI – Da Atualização 23

CAPÍTULO V – Das Disposições Finais 23

RESOLUÇÃO CPDP/MGI Nº 8, DE 17 DE ABRIL DE 2026

Dispõe sobre a Política de Proteção de Dados Pessoais no âmbito do Ministério da Gestão e da Inovação em Serviços Públicos.

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Resolução dispõe sobre a Política de Proteção de Dados Pessoais – PPDP no âmbito do Ministério da Gestão e Inovação em Serviços Públicos, que estabelece diretrizes para o tratamento de dados pessoais e tem o objetivo de garantir os direitos fundamentais de liberdade, de intimidade, de privacidade e de proteção dos dados pessoais dos titulares de dados pessoais.

§ 1º Esta Resolução aplica-se ao tratamento de dados pessoais, realizados em qualquer meio, custodiados pelo Ministério da Gestão e Inovação em Serviços Públicos ou sua sob orientação.

§ 2º Esta Resolução não se aplica ao tratamento de dados pessoais realizado para fins

exclusivos de:

I. segurança pública;

II. defesa nacional;

III. segurança do Estado; ou

IV. atividades de investigação e repressão de infrações penais.

Art. 2º Para fins desta Resolução, considera-se:

I. aviso de privacidade: documento voltado aos titulares de dados pessoais, que objetiva informar como os dados pessoais são tratados e para quais finalidades, quais os direitos dos titulares e como podem exercê-los, além de outras características que garantam ao titular a transparência em relação ao tratamento de seus dados pessoais, facilmente acessível e escrito em linguagem simples;

II. termo de uso: documento voltado aos usuários do serviço, que estabelece as regras e condições de uso de determinado serviço disponibilizado pelo Ministério da Gestão e Inovação em Serviços Públicos, facilmente acessível e escrito em linguagem clara e simples;

III. cookies: arquivos instalados no dispositivo de um usuário que permitem a coleta de determinadas informações, inclusive de dados pessoais em algumas situações, visando ao atendimento de finalidades diversas;

IV. agente público: o agente político, o servidor público e todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função no âmbito do Ministério da Gestão e Inovação em Serviços Públicos;

V. generalização: redução do nível de detalhe do dado pessoal, agrupando-o em categorias menos específicas como forma de evitar a identificação do titular dos dados; e

VI. ciclo de vida do dado: conjunto de estágios que um dado percorre desde a sua criação ou coleta até a sua eliminação ou arquivamento final.

Parágrafo único. Os demais conceitos e definições relacionados a esta PPDP poderão ser consultados na Lei nº 13.709, de 14 de agosto de 2018.

CAPÍTULO II
DAS RESPONSABILIDADES

Art. 3º São deveres do Ministério da Gestão e da Inovação em Serviços Públicos, quando em exercício das atribuições típicas do controlador:

I. observar a Lei nº 13.709, de 14 de agosto de 2018, as normas e demais publicações editadas pela Agência Nacional de Proteção de Dados — ANPD, ao decidir sobre um futuro tratamento de dados pessoais ou realizá-lo;

II. observar os requisitos legais presentes nos art. 7º, art. 11 e art. 23 da Lei nº 13.709, de 14 de agosto de 2018, antes de efetuar tratamento de dados pessoais;

III. estabelecer instrumentos legais formalizados com aqueles que, em seu nome, efetuem o tratamento de dados pessoais;

IV. adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais sob sua responsabilidade, desde a fase de concepção do produto ou do serviço até a sua execução;

V. elaborar relatórios de impacto à proteção de dados pessoais (RIPD) relativos às operações de tratamento, conforme modelo disponibilizado no Sistema Eletrônico de Informações – SEI;

VI. manter registro das operações de tratamento de dados pessoais;

VII. reter os dados pessoais pelo período estritamente necessário ao cumprimento da finalidade do tratamento de dados pessoais realizado;

VIII. realizar, no que couber, a gestão do consentimento nos termos do art. 8º da Lei nº13.709, de 14 de agosto de 2018, mantendo o respectivo histórico do consentimento fornecido e eventualmente revogado pelo titular; e

IX. observar as disposições do Programa de Privacidade e Segurança da Informação instituído pela Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025.

§ 1º É vedado o tratamento de dados pessoais pelo Ministério da Gestão e da Inovação em Serviços Públicos para finalidades incompatíveis com o objetivo de executar suas competências legais ou cumprir suas atribuições legais, bem como por pessoa não autorizada formalmente.

§ 2º O consentimento do titular é dispensado nas hipóteses de tratamento de dados pessoais fundamentadas no cumprimento de obrigação legal ou regulatória pelo controlador, ou para a execução de políticas públicas, conforme previsto nos arts. 7º e 11 da Lei nº 13.709, de 14 de agosto de 2018.

Art. 4º São deveres do Ministério da Gestão e da Inovação em Serviços Públicos, quando em exercício das atribuições típicas do operador:

I. seguir as instruções estabelecidas pelo controlador;

II. verificar, antes de efetuar o tratamento, se as instruções estabelecidas pelo controlador cumprem os requisitos legais presentes nos art. 7º, art. 11 e art. 23 da Lei nº 13.709, de 14 de agosto de 2018;

III. notificar o controlador quando as instruções por ele fornecidas não se encontrarem em perfeita consonância com a Lei nº 13.709, de 14 de agosto de 2018, as normas e demais publicações editadas pela ANPD;

IV. observar a Lei nº 13.709, de 14 de agosto de 2018 ao realizar o tratamento; e

V. manter registro das operações de tratamento de dados pessoais.

§ 1º É vedada a decisão unilateral pelo operador quanto aos meios e finalidades para o tratamento dos dados pessoais.

§ 2º Para fins de cumprimento do disposto no inciso V, o registro das operações de tratamento deverá ser realizado na ferramenta ColaboraDAP ou outro repositório oficial instituído pelo Ministério da Gestão e da Inovação em Serviços Públicos.

Art. 5º Os agentes de tratamento ou qualquer pessoa natural que intervenha em uma das fases do tratamento de dados pessoais devem garantir sua proteção, mesmo após o término do tratamento, observando as medidas técnicas e administrativas determinadas pelo Ministério da Gestão e da Inovação em Serviços Públicos.

CAPÍTULO III
DOS DIREITOS DOS TITULARES DE DADOS PESSOAIS

Art. 6º São direitos dos titulares de dados pessoais, nos termos do disposto na Lei nº 13.709, de 14 de agosto de 2018:

I. obter, em relação aos dados pessoais tratados, mediante requerimento expresso dele próprio ou por intermédio de representante legalmente constituído:

   a. a confirmação da existência do tratamento;

   b. o acesso aos seus dados pessoais, de forma simplificada e gratuita;

   c. a correção dos seus dados pessoais;

   d. anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei nº 13.709, de 14 de agosto de 2018;

   e. as informações sobre compartilhamento de seus dados pessoais; e

   f. nos casos em que o consentimento for exigido, informação sobre a possibilidade de:

      1. não fornecer consentimento e respectivas consequências da negativa;

      2. sua revogação;

II. que o Ministério da Gestão e da Inovação em Serviços Públicos, independentemente de requerimento, realize o tratamento de dados pessoais:

   a. para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

   b. em atividades compatíveis com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

   c. limitado ao mínimo necessário para a realização das finalidades, utilizando apenas os dados pertinentes, proporcionais e não excessivos em relação à finalidade do tratamento;

d. garantida a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

e. com exatidão, clareza, relevância e atualização dos dados pessoais, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

f. garantindo informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

g. por meio de medidas 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 difusão;

h. adotando medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

i. de forma a impedir tratamentos para fins discriminatórios ilícitos ou abusivos;

j. demonstrando a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas; e

k. fornecendo as informações de contato do controlador e de seus operadores, além de respectivas responsabilidades de cada tratamento.

Art. 7º São direitos dos titulares, nos termos do disposto na Lei nº 12.527, de 18 de novembro de 2011, em especial, que:

I. seus dados pessoais sejam acessados apenas por agentes públicos legalmente autorizados;

II. o acesso a seus dados pessoais por terceiros somente seja autorizado diante de previsão legal ou com o seu consentimento expresso, nos termos da lei;

III. aquele que obtiver acesso a seus dados pessoais seja responsabilizado por seu uso indevido; e

IV. observado o disposto no inciso II, quando o Ministério da Gestão e da Inovação em Serviços Públicos cumprir o dever de acesso à informação, os dados serão disponibilizados de forma anonimizada com a garantia de que o titular não possa ser identificado.

Art. 8º São direitos dos titulares, enquanto usuários da internet, nos termos do disposto na Lei nº 12.965, de 23 de abril de 2014, em especial, que:

I. a proteção dos seus dados pessoais e a indenização pelo dano material ou moral decorrente de sua violação;

II. o não fornecimento a terceiros de seus dados pessoais, salvo nas hipóteses previstas em lei; e

III. que a requisição de seus dados pessoais realizada pelo Ministério da Gestão e da Inovação em Serviços Públicos a outros órgãos e entidades públicos ou realizada por esses ao Ministério da Gestão e da Inovação em Serviços Públicos seja obrigatoriamente acompanhada da indicação do fundamento legal de competência expressa para o acesso e da motivação para o pedido de acesso aos dados cadastrais.

Parágrafo único. Na hipótese de requisição de registros de conexão ou de acesso a aplicações de internet, o atendimento deverá observar os ritos específicos estabelecidos pela Lei nº 12.965, de 23 de abril de 2014, sem prejuízo das garantias previstas na Lei nº 13.709, de 14 de agosto de 2018, com citação expressa ao fundamento legal da requisição interinstitucional.

CAPÍTULO IV
DO TRATAMENTO DE DADOS PESSOAIS

Seção I
Do Termo de Uso e Aviso de Privacidade

Art. 9º O Ministério da Gestão e da Inovação em Serviços Públicos, para cada serviço ofertado que trate dados pessoais, informatizado ou não, deverá requerer do titular a ciência do termo de uso daquele serviço.

Parágrafo único. Os termos de uso deverão:

I. adotar as diretrizes do Modelo de Acessibilidade em Governo Eletrônico – eMAG; e

II. ser editados em linguagem acessível e simples, conforme modelo disponibilizado pelo Ministério da Gestão e da Inovação em Serviços Públicos no SEI.

Art. 10. O Ministério da Gestão e da Inovação em Serviços Públicos deverá criar e manter atualizados os avisos de privacidade, que informarão sobre os tratamentos de dados pessoais realizados em cada ambiente físico ou digital, e como os dados pessoais neles tratados são protegidos.

Parágrafo único. Os avisos de privacidade deverão:

I. adotar as diretrizes do e-MAG;

II. ser editados em linguagem acessível, clara e simples;

III. ser expostos em local de fácil acesso e visualização;

IV. ser elaborados conforme modelo disponibilizado pelo Ministério da Gestão e da Inovação em Serviços Públicos no SEI;

V. obter a ciência do titular dos dados pessoais em relação ao conteúdo dos referidos avisos; e

VI. ser revistos e atualizados sempre que houver mudanças no tratamento dos dados pessoais objeto do aviso.

Art. 11. Os termos de uso e avisos de privacidade gerados em formato eletrônico por sistemas de informação ou aplicativos devem registrar:

I. a data e a hora, com precisão de minutos e segundos, bem como a versão vigente no momento da ciência do titular dos dados pessoais; e

II. a identificação da versão e a respectiva data de atualização.

Seção II
Da Governança e Boas Práticas

Art. 12 A estrutura de governança e gestão da proteção de dados pessoais no Ministério da Gestão e da Inovação em Serviços Públicos é composta por:

I. Comitê de Proteção de Dados Pessoais - CPDP, de que trata a Portaria MGI Nº 7.601, de24 de novembro de 2023;

II. Encarregado; e

III. Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos - ETIR.

§ 1º As atividades do encarregado consistem em:

I. aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II. receber comunicações da ANPD e adotar providências;

III. orientar os funcionários e os contratados do Ministério da Gestão e da Inovação em Serviços Públicos a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV. executar as demais atribuições determinadas pelo Ministério da Gestão e da Inovação em Serviços Públicos ou estabelecidas em normas complementares.

§ 2º A atuação da ETIR deve seguir as orientações previstas pelo Plano de Gestão de Incidentes com Dados Pessoais disponibilizado pelo Ministério da Gestão e da Inovação em Serviços Públicos.

Art. 13. As diretrizes, ações, metas e indicadores de proteção de dados pessoais devem ser direcionados por meio de um programa de governança em privacidade.

Parágrafo único. O programa de governança em privacidade será atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

Seção III
Da Limitação do Tratamento

Art. 14. Ao realizar operações de tratamento de dados pessoais, o Ministério da Gestão e da Inovação em Serviços Públicos adotará:

I. mecanismos para limitar a vinculação dos dados pessoais coletados, de forma a evitar que dados dispersos sejam conectados para formar um perfil ou identificar um titular dos dados pessoais para finalidade diferente do propósito original do tratamento;

II. mecanismos que busquem a generalização do dado pessoal;

III. processo de avaliação permanente no intuito de verificar se os dados pessoais tratados estão limitados somente ao necessário para alcance das finalidades específicas dos dados pessoais tratados; e

IV. medidas para reduzir a possibilidade de reidentificação de dados pessoais.

Seção IV
Da Gestão do Tratamento

Art. 15. Os sistemas de informação e aplicações utilizados no âmbito do Ministério da Gestão e da Inovação em Serviços Públicos:

I. registrarão a data em que os dados pessoais são coletados, criados, atualizados, transferidos, excluídos ou arquivados com o objetivo de acompanhar o período de retenção e viabilizar cronograma de eliminação dos dados pessoais no que for aplicável;

II. bloquearão tratamento posterior de quaisquer dados pessoais quando as finalidades declaradas tiverem expirado, mas a retenção for exigida pela legislação; e

III. limitarão o acesso dos usuários aos dados pessoais estritamente necessários para atingimento das finalidades do tratamento, de acordo com as permissões formalmente concedidas.

§1º Os sistemas de informação em desenvolvimento poderão incorporar o previsto neste artigo, conforme o estágio de implantação, garantindo o registro das ações sobre dados pessoais para controle de retenção e eliminação, em conformidade com a Lei nº 13.709, de 14 de agosto de 2018.

§ 2º Os sistemas atuais e em operação na data de publicação desta norma poderão ser dispensados do previsto neste artigo, desde que caracterizada a inviabilidade técnica de sua implementação.

§ 3º Caso a adequação dos sistemas atuais e em operação seja viável, esta deverá ocorrer de forma progressiva, priorizando as ações que tragam maior conformidade à Lei nº 13.709, de 14 de agosto de 2018 e melhor relação entre custo, risco e benefício para a administração.

Art. 16. Qualquer alteração na forma de tratamento dos dados pessoais deve ser comunicada aos titulares de maneira clara e tempestiva.

Seção V
Da Qualidade dos Dados

Art. 17. No momento da coleta de dados pessoais, deverão ser adotados, sempre que aplicável, mecanismos técnicos e procedimentais que assegurem a exatidão, a relevância e a integridade dos dados, de forma a atender aos princípios da qualidade e da prevenção previstos pela Lei 13.709, de 14 de agosto de 2018.

Art. 18. As atualizações de dados pessoais solicitadas pelo titular deverão ser executadas somente após a validação segura de sua identidade, por meio de procedimentos formais de autenticação e comprovação, de forma a prevenir alterações indevidas e garantir a integridade dos dados.

Art. 19. Os dados pessoais tratados pelo Ministério da Gestão e da Inovação em Serviços Públicos deverão ser submetidos a revisão periódica anual quanto a sua consistência, a fim de identificar e corrigir dados imprecisos ou desatualizados.

Art. 20. Os órgãos do Ministério da Gestão e da Inovação em Serviços Públicos deverão avaliar e, quando aplicável, comunicar aos agentes de tratamento e terceiros com quem os dados pessoais tenham sido compartilhados, quaisquer alterações, correções ou remoções desses dados.

Seção VI
Da Anonimização e Pseudonimização

Art. 21. Os órgãos do Ministério da Gestão e da Inovação em Serviços Públicos, sempre que possível, deverão:

I. anonimizar os dados pessoais antes de fornecê-los a órgãos de pesquisa; e

II. nos casos de fornecimento de dados pessoais para a realização de estudos em saúde pública, tais dados devem ser anonimizados ou pseudonimizados.

Art. 22. Os órgãos do Ministério da Gestão e da Inovação em Serviços Públicos realizarão tratamento de dados pessoais de forma a não identificar os titulares quando essa identificação não for necessária ou imprescindível para o cumprimento da finalidade legítima do tratamento, devidamente respaldada por base legal aplicável.

Art. 23. Os dados pessoais utilizados em ambientes de teste, desenvolvimento e homologação devem ser anonimizados ou pseudonimizados, conforme normativo interno instituído pelo Ministério da Gestão e da Inovação em Serviços Públicos.

Art. 24. Os padrões e técnicas utilizados em processos de anonimização e pseudonimização devem estar em conformidade com as diretrizes, estudos e publicações vigentes da ANPD.

Seção VII
Do Compartilhamento

Art. 25 Os compartilhamentos de dados pessoais realizados pelo Ministério da Gestão e da Inovação em Serviços Públicos devem estar alinhados com os normativos que tratam sobre governança e compartilhamento de dados no âmbito da administração pública federal, as diretrizes constantes do art. 26 da Lei nº 13.709, de 14 de agosto de 2018, as publicações da ANPD e observar, no mínimo os seguintes requisitos:

I. formalização e registro: instauração de processo administrativo, do qual constem os documentos e as informações pertinentes, incluindo análise técnica e jurídica, conforme o caso, que exponham a motivação para a realização do compartilhamento e a sua aderência à legislação em vigor;

II. ato formal: celebração de contratos, convênios ou instrumentos congêneres firmados entre as partes. O ato formal também pode ser realizado por meio de expedição de decisão administrativa pela autoridade competente, que autorize o acesso aos dados pessoais e estabeleça os requisitos definidos como condição para o compartilhamento;

III. objeto e finalidade: descrever quais dados pessoais serão compartilhados, bem como porque e para que serão compartilhados, devendo tais dados ser indicados de forma objetiva e detalhada, limitando-se ao que for estritamente necessário para as finalidades do tratamento, em conformidade com o princípio da necessidade;

IV. base legal: definição da base legal, conforme art. 7º ou, no caso de dados sensíveis, art.11 da LGPD, nos termos das orientações apresentadas pelo Guia Orientativo de Tratamento de Dados pessoais pelo Poder Público editado pela ANPD;

V. duração do tratamento: estabelecer, de forma expressa, o período de duração do uso compartilhado dos dados, além de esclarecer, conforme o caso, se há a possibilidade de conservação ou se os dados devem ser eliminados após o término do tratamento;

VI. transparência e direitos dos titulares: assegurar a disponibilização de informações claras, precisas e facilmente acessíveis aos titulares sobre a realização do compartilhamento e sobre como exercer seus direitos, conforme orientado pelo Guia Orientativo de tratamento de dados pessoais pelo poder público editado pela ANPD;

VII. prevenção e segurança: estabelecer medidas de segurança, técnicas e administrativas, que serão adotadas pelo órgão ou entidade recebedores dos dados para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; e

VIII. vedação ou permissão de novo compartilhamento: o instrumento que reger o uso compartilhado dos dados pode vedar a realização de novo compartilhamento pelo recebedor dos dados ou, ainda, autorizá-lo sob determinadas condições, observadas as normas aplicáveis.

Parágrafo único. A área responsável pelo compartilhamento deve avaliar a necessidade de atender a outros requisitos, que decorram das peculiaridades do caso concreto ou de determinações provenientes de normas específicas.

Art. 26. Os compartilhamentos de dados pessoais devem, no mínimo, ser controlados com registro no inventário de dados pessoais:

I. do órgão ou da entidade que recebe os dados;

II. da finalidade do compartilhamento;

III. das medidas de proteção adotadas e;

IV. de quais dados pessoais foram compartilhados.

Art. 27. O responsável pelo compartilhamento deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional.

Seção VIII
Da Transferência Internacional de Dados

Art. 28. A transferência internacional de dados pessoais deve ser realizada mediante finalidade legítima claramente especificada, bem como, em conformidade com o previsto pelos arts. 33 a 36 da Lei nº 13.709, de 14 de agosto de 2018 e nas resoluções editadas pela ANPD.

Parágrafo único. O armazenamento em nuvem de dados e informações produzidos ou custodiados pelo Ministério da Gestão e da Inovação em Serviços Públicos em outros países deverá seguir as diretrizes estabelecidas pelo Gabinete de Segurança Institucional da Presidência da República e o disposto na Portaria CGIGD/DTI/MGI nº 4.439, de 26 de junho de 2024, e demais normas editadas pelo Ministério da Gestão e da Inovação em Serviços Públicos.

Seção IX
Do Término do Tratamento dos Dados

Art. 29. Periodicamente, deve-se avaliar a necessidade do término do tratamento dos dados pessoais, conforme as hipóteses previstas pelo art. 15 da Lei nº 13.709, de 14 de agosto de 2018.

Art. 30. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as finalidades indicadas pelo art. 16 da Lei nº 13.709, de 14 de agosto de 2018.

Seção X
Da Segurança Aplicada aos Dados Pessoais

Art. 31. O tratamento de dados pessoais deve observar as diretrizes estabelecidas pela Política de Segurança da Informação do da Gestão e da Inovação em Serviços Públicos e adotar medidas técnicas e administrativas que assegurem:

I. a confidencialidade, integridade, disponibilidade e autenticidade das informações;

II. a proteção contra acesso, uso, modificação, destruição, divulgação ou tratamento não autorizado, acidental ou ilícito; e

III. a conformidade com a Lei nº 13.709, de 14 de agosto de 2018 e normas vigentes sobre tratamento de dados pessoais.

Parágrafo único. As medidas de que trata o *caput devem ser aplicadas em todas as fases do* ciclo de vida do dado.

Art. 32. Todos os acessos e operações realizadas sobre dados pessoais devem ser registrados em sistema de auditoria, com registro obrigatório dos seguintes campos:

I. identificador único do agente público ou processo automatizado responsável pela ação;

II. data e hora da execução;

III. identificador do titular dos dados;

IV. tipo de operação realizada (criação, leitura, modificação, exclusão, transferência, compartilhamento, entre outros); e

V. endereço de origem do acesso (Internet Protocol – IP ou identificador equivalente).

§ 1º. Os registros de auditoria devem ser armazenados por período mínimo de 24 (vinte e quatro meses), com integridade garantida por controle de hash criptográfico ou tecnologia equivalente.

§ 2º. A coleta e retenção dos registros devem observar o princípio da minimização, mantendo apenas os dados necessários à finalidade de auditoria, prestação de contas e responsabilização.

Art. 33. O gerenciamento de registros de auditoria deve:

I. seguir política de logging e monitoring (baseada na ISO/IEC 27002:2022);

II. integrar-se a mecanismo automatizado de correlação e detecção de incidentes (Security Information and Event Management - SIEM); e

III. ser submetido a revisão periódica com base na matriz de riscos e na criticidade dos sistemas.

Art. 34. O controle de acesso aos sistemas que tratam dados pessoais deve adotar, obrigatoriamente:

I. autenticação multifator (Multi-Factor Authentication - MFA) composta por, no mínimo, dois fatores distintos, conforme NIST SP 800-63B;

II. gestão centralizada de identidades e senhas (Identity and Access Management - IAM) com expiração e rotação periódica; e

III. bloqueio automático após tentativas consecutivas de autenticação malsucedida.

Art. 35. A transferência e o compartilhamento de dados pessoais devem ocorrer exclusivamente por meio de canais e mecanismos de comunicação que assegurem a confidencialidade, a integridade e a autenticidade das informações.

§ 1º O tratamento de dados pessoais em comunicações internas ou externas deve observar os mesmos requisitos de segurança aplicáveis aos sistemas e serviços institucionais, inclusive quanto à proteção contra acesso, uso ou divulgação não autorizada.

§ 2º A unidade responsável pela segurança da informação deverá definir e manter atualizados os padrões técnicos mínimos a serem observados para o compartilhamento de dados pessoais.

Art. 36. O Ministério da Gestão e da Inovação em Serviços Públicos deve implementar controles de integridade, versionamento e cópia de segurança que impeçam a modificação ou exclusão não autorizada de dados pessoais, garantindo a rastreabilidade de alterações e a restauração em caso de incidente.

Art. 37. O desenvolvimento e a aquisição de sistemas devem incorporar requisitos formais de segurança e privacidade, incluindo:

I. análise de risco e impacto à proteção de dados de processos de tratamento de dados pessoais que possam gerar riscos às liberdades civis e aos direitos fundamentais antes da implementação de novos tratamentos;

II. testes de segurança e vulnerabilidade antes da entrada em produção; e

III. aplicação dos princípios de privilégio mínimo, necessidade de conhecimento (need-to-know) e segregação de funções.

§ 1º No planejamento de novos tratamentos de dados pessoais ou mudanças no tratamento existente realizado pelos sistemas, aplicações e serviços prestados pelo Ministério da Gestão e da Inovação em Serviços Públicos, deve ser avaliada a necessidade de elaboração de um Relatório de Impacto à Proteção dos Dados Pessoais - RIPD.

§ 2º As medidas de mitigação de riscos resultantes do RIPD devem ser incorporadas ao ciclo de desenvolvimento seguro (Secure Software Development Life Cycle).

§ 3º Os requisitos previstos neste artigo aplicam-se obrigatoriamente aos sistemas novos e devem ser implementados de forma gradual nos sistemas legados, conforme avaliação técnica de viabilidade.

§ 4º Nos casos em que a adaptação de sistemas legados não for viável técnica ou economicamente, caberá ao gestor do sistema elaborar e manter atualizada a análise de riscos correspondente, indicando os controles compensatórios adotados, o impacto residual e o plano de tratamento do risco (tais como as diretrizes da ISO/IEC 27005:2022 e do NIST SP 800-30 Rev. 1).

Seção XI
Dos Incidentes

Art. 38. O agente público que, de qualquer forma, tiver ciência sobre indícios de incidentes ou incidentes que envolvam dados pessoais custodiados pelo Ministério da Gestão e da Inovação em Serviços Públicos deverão notificar o Órgão, conforme as orientações previstas na seção "Fase 2 – Detecção e análise de incidentes" do Plano de Gestão de Incidentes com Dados Pessoais do Ministério da Gestão e da Inovação em Serviços Públicos.

Seção XII
Da Conscientização, Capacitação e Sensibilização

Art. 39. O Ministério da Gestão e da Inovação em Serviços Públicos promoverá ações de desenvolvimento profissional sobre privacidade e proteção de dados pessoais destinadas aos agentes públicos que atuam no Ministério, de acordo com a disponibilidade orçamentária e financeira e o disposto pelo Plano de Desenvolvimento de Pessoas - PDP.

Seção XIII
Dos Contratos, Convênios, Acordos e Instrumentos Congêneres

Art. 40. Os contratos, convênios, acordos e instrumentos congêneres vigentes no Ministério da Gestão e da Inovação em Serviços Públicos, que envolvam o tratamento de dados pessoais, devem estar em conformidade com esta PPDP e conter cláusulas que contemplem, no mínimo:

I. a obrigação da outra parte de dar ciência desta PPDP aos seus prepostos, empregados e colaboradores, bem como a qualquer pessoa que realize o tratamento de dados pessoais em nome do Ministério da Gestão e da Inovação em Serviços Públicos no âmbito dos instrumentos citados pelo *caput;*

II. a descrição de requisitos e medidas de privacidade e segurança necessários para assegurar a proteção dos dados pessoais;

III. a determinação de que o operador não trate os dados pessoais para finalidades distintas das finalidades determinadas pelo controlador e informada ao titular de dados pessoais;

IV. as condições sob as quais o operador deverá devolver ou descartar, de forma segura, os dados pessoais após a conclusão do serviço, rescisão do contrato ou mediante solicitação do controlador;

V. as diretrizes especificas, quando aplicáveis, sobre a participação de suboperadores no tratamento de dados pessoais; e

VI. a previsão, quando aplicável, de que o Ministério da Gestão e da Inovação em Serviços Públicos, ou instituição por ele indicada, realize auditoria para avaliar o cumprimento das cláusulas relativas ao tratamento dos dados pessoais.

Parágrafo único. As cláusulas previstas devem ser inseridas nos instrumentos vigentes citados pelo caput no prazo de até 6 meses após a entrada em vigor desta PPDP ou na celebração de eventual prorrogação, o que ocorrer primeiro.

Seção XIV
Da Auditoria e Conformidade

Art. 41. O cumprimento desta PPDP e dos normativos decorrentes devem ser acompanhados por meio de verificações de conformidade anuais, com a participação da Assessoria Especial de Controle Interno, com o objetivo de evidenciar a observância dos requisitos de privacidade e proteção de dados pessoais.

Art. 42. As atividades, produtos e serviços desenvolvidos no Ministério da Gestão e da Inovação em Serviços Públicos devem observar os requisitos de privacidade e proteção de dados pessoais estabelecidos em leis, regulamentos, resoluções, normas, estatutos e nos instrumentos jurídicos vigentes tais como contratos, convênios, acordos e instrumentos congêneres.

Art. 43. Os resultados das verificações de conformidade deverão ser documentados em relatório formal de avaliação de conformidade.

Seção XV
Das Penalidades

Art. 44. As ações ou omissões que violem esta Política de Proteção de Dados Pessoais, a Lei nº 13.709, de 14 de agosto de 2018, ou demais normas correlatas, poderão acarretar responsabilização nas esferas administrativa, civil e penal, inclusive mediante aplicação das sanções previstas em regulamento da ANPD, sem prejuízo das sanções disciplinares cabíveis nos termos da Lei nº 8.112, de 11 de dezembro de 1990, e de outras legislações aplicáveis, assegurados o contraditório e a ampla defesa aos envolvidos.

§ 1º Os casos de descumprimento desta Política deverão ser registrados e comunicados ao Encarregado, para ciência e adoção das providências de sua competência, inclusive quanto à avaliação da necessidade de comunicação à ANPD e aos titulares dos dados, sem prejuízo das demais comunicações e providências cabíveis.

§ 2º Verificada, em tese, a ocorrência de descumprimento desta Política com irregularidades que possam ser consideradas disciplinares e haja envolvimento de servidor do Ministério da Gestão e da Inovação em Serviços Públicos, o fato deverá ser obrigatoriamente comunicado diretamente à Corregedoria do órgão, por meio de representação formal autuada em processo no SEI, contendo, sempre que possível:

I. descrição circunstanciada dos fatos;

II. identificação do(s) servidor(es) envolvido(s);

III. indicação dos dispositivos desta PPDP e das demais normas legais e regulamentares supostamente infringidos, inclusive os relativos à proteção de dados pessoais;

IV. especificação, em termos gerais, dos dados pessoais e, se for o caso, dos dados pessoais sensíveis afetados pelo incidente; e

V. outras informações relevantes à adequada avaliação correicional do caso.

Seção XVI
Da Atualização

Art. 45. A PPDP e os normativos dela decorrentes devem ser revisados sempre que se fizer necessário, não devendo exceder o período máximo de 3 (três anos).

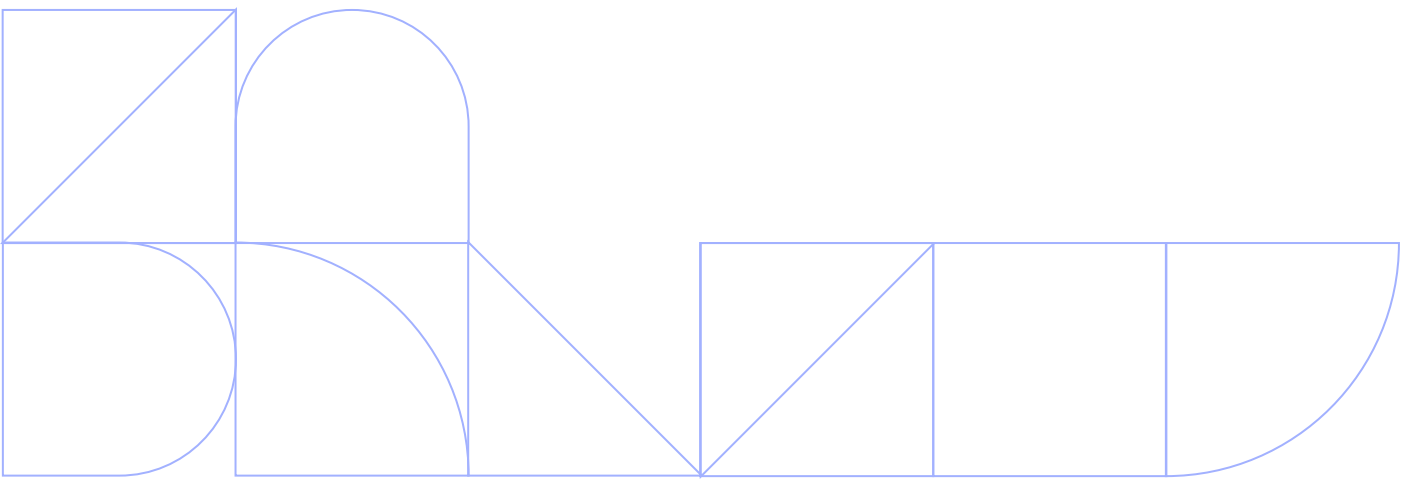
CAPÍTULO V
DAS DISPOSIÇÕES FINAIS

Art. 46 A PPDP, as publicações aprovadas pelo CPDP, bem como os normativos internos de proteção de dados pessoais e suas atualizações deverão ser amplamente divulgados a todos os agentes públicos e prestadores de serviços do Ministério da Gestão e da Inovação em Serviços Públicos.

Art. 47. Os questionamentos e casos omissos relativos à aplicação desta PPDP deverão ser submetidos ao CPDP.

Art. 48. Esta Resolução entra em vigor na data de sua publicação.

Cilair Rodrigues de Abreu
Presidente do CPDP



Este exemplar é parte do nosso compromisso com a responsabilidade ambiental.
Cada página foi impressa em papel proveniente de fontes responsáveis,
refletindo nosso cuidado em preservar os recursos naturais e minimizar
o impacto sobre o planeta. Edição limitada.

MINISTÉRIO DA
GESTÃO E DA INOVAÇÃO
EM SERVIÇOS PÚBLICOS

GOVERNO DO
BRASIL
DO LADO DO POVO BRASILEIRO