



**PROJETO DE RESOLUÇÃO Nº 01/2026
ATO DA MESA Nº 01/2026**

Institui as políticas de segurança, privacidade e proteção de dados pessoais na Câmara Municipal de Espigão do Oeste, em atendimento à Lei Geral de Proteção de Dados Pessoais (Lei Federal nº 13.709/2018 - LGPD).

A MESA DIRETORA DA CÂMARA MUNICIPAL DE ESPIGÃO DO OESTE, no uso das atribuições legais conferidas pelos artigos 26 e 132 do Regimento Interno, especialmente o disposto na Lei Federal nº 13.709, de 14 de agosto de 2018, propõe a aprovação da Resolução:

O PRESIDENTE DA CÂMARA MUNICIPAL DE ESPIGÃO DO OESTE- ESTADO DE RONDÔNIA, nos termos legais e conforme artigo 31, inciso XX, do Regimento Interno, FAZ SABER que a CÂMARA MUNICIPAL aprovou e ele promulga a seguinte RESOLUÇÃO:

**CAPÍTULO I
DAS DISPOSIÇÕES INICIAIS**

Art. 1º Esta Resolução dispõe sobre a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais LGPD), no âmbito da Câmara Municipal de Espigão do Oeste.

Parágrafo único. Para os fins desta Resolução, adotam-se as terminologias previstas no art. 5º da Lei nº 13.709/2018.

Art. 2º Consideram-se legítimos interesses da Câmara Municipal de Espigão do Oeste, para os fins do artigo 7º, IX, da Lei Federal nº 13.709 (LGPD), exercício das funções legislativas e administrativas, incluídas as atividades de fiscalização, controle externo, assessoramento, julgamento, representação popular, participação social e preservação histórica.

**CAPÍTULO II
DAS POLÍTICAS INSTITUCIONAIS**

Art. 3º Fica instituída a Política de Segurança da Informação (PSI) e a Política Geral de Privacidade e Proteção de Dados Pessoais (PPDP), as quais estabelecerão diretrizes, procedimentos e medidas administrativas e tecnológicas necessárias à conformidade da Câmara Municipal com a LGPD e demais normas correlatas.

§ 1º As Políticas de que trata este Capítulo deverão ser de observância obrigatória por todos os setores e agentes públicos da Câmara Municipal.

§ 2º As regras de boas práticas e de governança estabelecidas pelas Políticas devem contemplar mecanismos internos de supervisão e de mitigação de riscos, incluindo planos de resposta a incidentes de segurança.

CAPÍTULO III DO CONTROLADOR E DO OPERADOR

Art. 4º A Câmara Municipal de Espigão do Oeste é o Controlador de dados por ela tratados no cumprimento de suas funções administrativas e institucionais.

Art. 5º O Controlador manterá registro das operações de tratamento de dados pessoais que realizar, especialmente nas hipóteses previstas na LGPD.

Art. 6º O vereador será considerado controlador de dados pessoais em caráter excepcional, quando de forma autônoma e dissociada da estrutura institucional da Câmara Municipal, realizar operações de tratamento de dados pessoais:

I. mediante a utilização de meios próprios, físicos ou digitais, não integrados aos sistemas institucionais da Câmara Municipal;

II. com definição, por iniciativa própria, da finalidade e dos meios do tratamento;

III. fora do exercício de atribuições administrativas ou institucionais formalmente vinculadas à estrutura organizacional da Câmara Municipal.

§ 1º No início de cada Legislatura, os vereadores deverão firmar Termo de Ciência e Responsabilidade, conforme Anexo I, com a finalidade de comprovar ciência das disposições desta Resolução e da Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais).

§ 2º A assinatura do Termo de Ciência e Responsabilidade não configura presunção de que o vereador atue como controlador de dados pessoais, permanecendo tal condição restrita às hipóteses previstas no caput deste artigo.

§ 3º Não se caracteriza como tratamento autônomo de dados pessoais, para os fins deste artigo, aquele realizado:

I. por intermédio dos sistemas oficiais da Câmara Municipal;

II. com suporte técnico, operacional ou normativo de unidades administrativas da Câmara Municipal;

III. no estrito exercício das atribuições institucionais do mandato parlamentar.

§ 4º Na hipótese prevista no caput, o vereador responderá nos termos da Lei Federal nº 13.709/2018 (LGPD), limitadamente aos tratamentos de dados pessoais realizados de forma autônoma.

§ 5º O disposto neste artigo não afasta a responsabilidade institucional da Câmara Municipal quando o tratamento de dados pessoais ocorrer no âmbito de suas competências legais, administrativas ou regimentais.

Art. 7º Os Operadores de dados são servidores da Câmara Municipal de Espigão do Oeste e prestadores de serviços contratados que realizam o tratamento de dados pessoais em nome e por ordem do Controlador.

§ 1º Os Operadores devem realizar o tratamento de dados pessoais conforme as instruções fornecidas pelo Controlador e pela Lei nº 13.709/2018 (LGPD), verificando a observância das normas sobre a matéria.

§ 2º Qualquer empresa contratada pela Câmara Municipal que atue como operadora de dados pessoais deverá manter o registro das operações de tratamento de dados pessoais que realizar.

§ 3º Os editais de Licitações, chamamentos públicos e instrumentos contratuais devem mencionar expressamente a possibilidade de verificação da adoção das instruções e normas pela contratada no que se refere à LGPD, estando sujeitos a penalidades administrativas.

CAPÍTULO IV

DO COMITÊ DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS (CPPD)

Art. 8º Fica instituído o Comitê de Privacidade e Proteção de Dados Pessoais (CPPD), órgão técnico-consultivo responsável pela governança de privacidade e proteção de dados na Câmara Municipal de Espigão do Oeste.

§ 1º O CPPD será composto por servidores públicos em exercício na Câmara Municipal de Espigão do Oeste, designados pelo Presidente da Câmara, e atuará de forma colegiada na definição de diretrizes, na implementação de políticas e no monitoramento do cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD).

§ 2º O CPPD deverá contar, obrigatoriamente, com representantes das seguintes áreas:

I. Tecnologia da Informação;

II. Procuradoria Jurídica;

III. Controle Interno;

IV. Diretoria Geral;

V. Responsável pela Lei de Acesso à Informação.

§ 3º O Encarregado pelo Tratamento de Dados Pessoais (DPO) participará das reuniões do CPPD, com direito a voz.

Art. 9º Compete ao Comitê de Privacidade e Proteção de Dados Pessoais (CPPD):

I. formular plano de adequação à Lei Federal nº 13.709/2018 (LGPD);

II. identificar e analisar os riscos relacionados ao tratamento de dados pessoais, propondo medidas de mitigação e controle adequadas;

III. elaborar, revisar e atualizar a Política de Segurança da Informação e a Política Geral de Privacidade e Proteção de Dados Pessoais (PPDP);

IV. prover orientação e o patrocínio necessários às ações de privacidade, proteção de dados pessoais e segurança da informação na Câmara Municipal;

V. incentivar e assegurar a conscientização, capacitação e sensibilização das pessoas que realizam o tratamento de dados pessoais;

VI. expedir instruções complementares ou medidas administrativas necessárias ao cumprimento da Lei nº 13.709/2018 (LGPD) e desta Resolução;

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

CAPÍTULO V

DO ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS (DPO)

Art. 10. O Presidente da Câmara designará o Encarregado pelo Tratamento de Dados Pessoais (DPO), nos termos do art. 41 da Lei Federal nº 13.709/2018, bem como um Encarregado Substituto.

§ 1º A identidade e as informações de contato do Encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico da Câmara Municipal, em seção específica sobre tratamento de dados pessoais.

§ 2º O Encarregado deve possuir conhecimentos multidisciplinares essenciais à sua atribuição, preferencialmente, sobre privacidade e proteção de dados pessoais, segurança da

informação, análise jurídica, gestão de riscos, governança de dados e acesso à informação no setor público.

Art. 11. Além das atribuições previstas no § 2º do art. 41 da Lei Federal nº 13.709/2018, compete ao Encarregado pelo Tratamento de Dados Pessoais:

I. orientar e prestar assessoramento ao Controlador quanto à conformidade das operações de tratamento de dados pessoais com a Lei Geral de Proteção de Dados Pessoais;

II. apoiar a elaboração, a implementação e a manutenção dos procedimentos de registro, comunicação e resposta a incidentes de segurança envolvendo dados pessoais;

III. auxiliar na elaboração e atualização do Relatório de Impacto à Proteção de Dados Pessoais (RIPD);

IV. atuar como ponto de contato com a Autoridade Nacional de Proteção de Dados (ANPD), quando necessário.

Art. 12. O Encarregado comunicará ao Comitê a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, observado o disposto na Lei Federal nº 13.709/2018 (LGPD).

CAPÍTULO VI DO RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD)

Art. 13. A Câmara Municipal de Espigão do Oeste elaborará Relatório de Impacto à Proteção de Dados Pessoais (RIPD) quando o tratamento puder gerar riscos relevantes, nos termos da LGPD.

Parágrafo único. O Controlador deverá demonstrar a efetividade do seu programa de governança em privacidade e das medidas de mitigação, em especial, a pedido da Autoridade Nacional de Proteção de Dados (ANPD).

CAPÍTULO VII DO TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

Art. 14. O tratamento de dados pessoais sensíveis somente poderá ocorrer em conformidade com as hipóteses previstas no Art. 11 da LGPD, sendo indispensável quando for necessário para:

I. Cumprimento de obrigação legal ou regulatória pelo Controlador;

II. Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

III. Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

§ 1º O tratamento de dados pessoais sensíveis deve ser realizado com extremo cuidado e requer proteção extra e adequada para garantir a privacidade e a segurança das pessoas envolvidas, devendo ser implementadas medidas adicionais de proteção.

§ 2º Quando o tratamento de dados envolver as hipóteses previstas nos incisos I e II do caput, a dispensa de consentimento deverá ser publicizada, nos termos do Art. 23, I, da LGPD.

CAPÍTULO VIII DOS DIREITOS DOS TITULARES

Art. 15. O titular de dados pessoais poderá exercer os direitos previstos na Lei Federal nº 13.709/2018 e demais normas aplicáveis, mediante requisição expressa dirigida ao Encarregado, de forma facilitada e gratuita.

Art. 16. Os requerimentos formulados pelos titulares de dados pessoais serão processados pelo Encarregado, mediante comprovação de identidade compatível com a natureza do dado solicitado, observadas as medidas de prevenção à fraude e de segurança do titular.

§ 1º A comprovação de identidade poderá ser realizada por meio de documento oficial ou outro meio idôneo, conforme o caso.

§ 2º No caso de titular incapaz ou de representante legal, deverão ser apresentados os documentos que comprovem a identidade e a respectiva representação legal ou procuração com poderes específicos.

CAPÍTULO IX DAS RESPONSABILIDADES DOS AGENTES PÚBLICOS

Art. 17. Os servidores, vereadores, colaboradores, estagiários e terceirizados são responsáveis por:

I. Ler e cumprir integralmente os termos desta Resolução e as demais normas e procedimentos de proteção da privacidade e de dados pessoais aplicáveis;

II. Comunicar ao Encarregado qualquer evento que viole esta Resolução ou coloque em risco os dados pessoais tratados pelo Poder Legislativo;

III. Assegurar a rastreabilidade e a prestação de contas durante todo o tratamento de dados pessoais, inclusive daqueles compartilhados com terceiros;

IV. Gerenciar eventual violação aos dados tratados, mantendo o registro de incidentes e da resposta efetuada.

Art. 18. O descumprimento das normas e dos procedimentos referentes à proteção de dados pessoais poderá acarretar, isolada ou cumulativamente, a aplicação de sanções administrativas internas, observados os respectivos regimes jurídicos aplicáveis, sem prejuízo das responsabilidades civis e penais previstas em lei.

CAPÍTULO X DAS DISPOSIÇÕES FINAIS

Art. 19. Todas as unidades administrativas deverão prestar apoio ao Encarregado e ao CPPD no levantamento, atualização e revisão das operações de tratamento de dados pessoais.

Art. 20. Os dados pessoais serão eliminados após o término de seu tratamento, observados os prazos legais de guarda, a tabela de temporalidade documental e as normas arquivísticas aplicáveis, admitida a conservação para cumprimento de obrigação legal ou regulatória pelo Controlador ou para uso exclusivo do Controlador, desde que anonimizados, quando possível.

Art. 21. Esta Resolução deverá ser revista e atualizada periodicamente, ouvido o Comitê de Privacidade e Proteção de Dados Pessoais.

Art. 22. Casos omissos serão resolvidos pela Mesa Diretora, ouvido o Comitê de Privacidade e Proteção de Dados Pessoais (CPPD).

Art. 23. Em caso de conflito aparente de normas entre a Lei Federal nº 13.709/2018 (LGPD) e a Lei Federal nº 12.527/2011 (LAI), aplica-se o critério da especialidade, prevalecendo a norma especial sobre a geral.

Art. 24. Esta Resolução entra em vigor na data de sua publicação.

Palácio Romeu Francisco Melhorança, Espigão do Oeste - RO, 26 de fevereiro de 2026.

Justificativa

Senhores Vereadores

Encaminhamos para apreciação de Vossas Excelências o **Projeto de Resolução nº 01/2026**, proposto pela Mesa Diretora, que dispõe sobre *a instituição das Políticas de Segurança, Privacidade e Proteção de Dados Pessoais no âmbito da Câmara Municipal de Espigão do Oeste, em conformidade com a Lei Geral de Proteção de Dados Pessoais (Lei Federal nº 13.709/2018 LGPD)*.

A presente proposição também institui o Comitê de Privacidade e Proteção de Dados Pessoais, bem como estabelece diretrizes formais de governança em segurança da informação e proteção de dados, com vistas a assegurar a adequada implementação e o efetivo cumprimento da legislação vigente no âmbito deste Poder Legislativo.

Ressalte-se que esta Casa Legislativa encontra-se sob reiteração de determinações expedidas pelo Tribunal de Contas do Estado de Rondônia, conforme consignado no Acórdão APL-TC 00251/24, o qual fixou prazo improrrogável de 60 (sessenta) dias para a comprovação da adoção das seguintes providências:

1. Nomeação do Encarregado pelo Tratamento de Dados Pessoais (DPO) e de seu substituto, nos termos do art. 41 da Lei nº 13.709/2018;
2. Instituição de comitê ou grupo de trabalho responsável pela condução do processo de adequação institucional à LGPD.

A minuta de Resolução ora apresentada foi elaborada com fundamento no Guia Orientativo de Implementação da LGPD para Gestores Públicos, disponibilizado pelo Tribunal de Contas do Estado de Rondônia, bem como em materiais técnicos da Autoridade Nacional de Proteção de Dados e em atos normativos de outras Casas Legislativas que já estruturaram seus mecanismos de governança em privacidade e proteção de dados.

A aprovação da matéria revela-se medida indispensável para viabilizar as subsequentes nomeações por meio de Portaria e para possibilitar a devida comprovação do cumprimento das determinações perante o Tribunal de Contas, assegurando a regularidade institucional, a transparência administrativa e a observância dos direitos fundamentais de proteção de dados pessoais.

Palácio Romeu Francisco Melhorança, Espigão do Oeste-RO, 26 de fevereiro de 2026.

Amilton Alves de Souza

Pedro Candido Cesário Presidente da CMEO
Vice-Presidente da CMEO

Hermes Pereira Junior
1º Secretário da Mesa

Walter Gonçalves Lara
2º Secretário da Mesa

CÂMARA DE VEREADORES DO MUNICÍPIO DE ESPIGÃO DO OESTE-RO - CNPJ: 04.391.603/0001-12

Rua Vale Formoso, nº 1896 - Bairro Vista Alegre - CEP: 76.974-000 Espigão do Oeste - Rondônia



SIMPLES
ASSINATURA
ELETRÔNICA
LOGIN E SENHA

Documento assinado eletronicamente por **Hermes Pereira Junior, 1º Secretário CMEO**, em 26/02/2026 às 11:45, horário de Espigão do Oeste/RO, com fulcro no art. 17 da [Resolução nº 90 de 18/06/2021](#).



AVANÇADA
ASSINATURA
ELETRÔNICA
CERTIFICADO DIGITAL
DIGIPROG

Documento assinado eletronicamente (CD) por **Amilton Alves de Souza, Presidente da Câmara Municipal de Espigão d' Oeste**, em 26/02/2026 às 12:04, horário de Espigão do Oeste/RO, com fulcro no art. 17 da [Resolução nº 90 de 18/06/2021](#).



SIMPLES
ASSINATURA
ELETRÔNICA
LOGIN E SENHA

Documento assinado eletronicamente por **Walter Gonçalves Lara, Vereador**, em 03/03/2026 às 11:52, horário de Espigão do Oeste/RO, com fulcro no art. 17 da [Resolução nº 90 de 18/06/2021](#).



Documento assinado eletronicamente por **Pedro Candido Cesário, Vereador**, em 05/03/2026 às 09:40, horário de Espigão do Oeste/RO, com fulcro no art. 17 da [Resolução nº 90 de 18/06/2021](#).



A autenticidade deste documento pode ser conferida no site transparencia.espigaodooeste.ro.gov.br, informando o ID **1356907** e o código verificador **C5FB8AE1**.

Referência: [Processo nº 59-1/2026](#).

Docto ID: 1356907 v1



Presidência da República
Secretaria-Geral
Subchefia para Assuntos Jurídicos

LEI Nº 13.709, DE 14 DE AGOSTO DE 2018

[Texto compilado](#)

~~Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).~~

[Mensagem de veto](#)

~~Lei Geral de Proteção de Dados Pessoais (LGPD).~~
~~(Redação dada pela Lei nº 13.853, de 2019)~~ [Vigência](#)

[Vigência](#)

O PRESIDENTE DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. [\(Incluído pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

I - o respeito à privacidade;

II - a autodeterminação informativa;

III - a liberdade de expressão, de informação, de comunicação e de opinião;

IV - a inviolabilidade da intimidade, da honra e da imagem;

V - o desenvolvimento econômico e tecnológico e a inovação;

VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

I - a operação de tratamento seja realizada no território nacional;

~~II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;~~

~~II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou~~ [\(Redação dada pela Medida Provisória nº 869, de 2010\)](#)

II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou [\(Redação dada pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

§ 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:

I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

II - realizado para fins exclusivamente:

a) jornalístico e artísticos; ou

~~b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;~~

~~b) acadêmicos; (Redação dada pela Medida Provisória nº 869, de 2018)~~

b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;

III - realizado para fins exclusivos de:

a) segurança pública;

b) defesa nacional;

c) segurança do Estado; ou

d) atividades de investigação e repressão de infrações penais; ou

IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

§ 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

~~§ 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.~~

~~§ 2º O tratamento dos dados a que se refere o inciso III do caput por pessoa jurídica de direito privado só será admitido em procedimentos sob a tutela de pessoa jurídica de direito público, hipótese na qual será observada a limitação de que trata o § 3º. (Redação dada pela Medida Provisória nº 869, de 2018)~~

§ 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.

~~§ 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.~~

~~§ 3º Os dados pessoais constantes de bancos de dados constituídos para os fins de que trata o inciso III do caput não poderão ser tratados em sua totalidade por pessoas jurídicas de direito privado, não incluídas as controladas pelo Poder Público. (Redação dada pela Medida Provisória nº 869, de 2018)~~

§ 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.

~~§ 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado. (Revogado pela Medida Provisória nº 869, de 2018)~~

§ 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público. (Redação dada pela Lei nº 13.853, de 2019) Vigência

Art. 5º Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - 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;

III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

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

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



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

~~VIII - encarregado: pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional;~~

~~VIII - encarregado: pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados; (Redação dada pela Medida Provisória nº 869, de 2019)~~

~~VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); (Redação dada pela Lei nº 13.853, de 2019) Vigência~~

~~VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Agência Nacional de Proteção de Dados - ANPD; (Redação dada pela Medida Provisória nº 1.317, de 2025)~~

VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Agência Nacional de Proteção de Dados (ANPD); (Redação dada pela Lei nº 15.352, de 2026)

IX - agentes de tratamento: o controlador e o operador;

X - 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;

XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

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

XVI - 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;

XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

~~XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico;~~

~~XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e (Redação dada pela Medida Provisória nº 869, de 2019)~~

XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e (Redação dada pela Lei nº 13.853, de 2019) Vigência

~~XIX - autoridade nacional: órgão da administração pública indireta responsável por zelar, implementar e fiscalizar o cumprimento desta Lei;~~

~~XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei. (Redação dada pela Medida Provisória nº 869, de 2019)~~

~~XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. (Redação dada pela Lei nº 13.853, de 2019) Vigência~~



~~XIX - autoridade nacional: entidade da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. (Redação dada pela Medida Provisória nº 1.317, de 2025)~~

XIX - autoridade nacional: entidade da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. [\(Redação dada pela Lei nº 15.352, de 2026\)](#)

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integridade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização 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;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - responsabilização e prestação de contas: demonstração, pelo agente, da 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.

CAPÍTULO II DO TRATAMENTO DE DADOS PESSOAIS

Seção I Dos Requisitos para o Tratamento de Dados Pessoais

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular;

II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da [Lei nº 9.307, de 23 de setembro de 1996 \(Lei de Arbitragem\)](#);

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

~~VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;~~

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; [\(Redação dada pela Lei nº 13.853, de 2019\)](#) [Vigência](#)



IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

~~§ 1º Nos casos de aplicação do disposto nos incisos II e III do caput deste artigo e excetuadas as hipóteses previstas no art. 4º desta Lei, o titular será informado das hipóteses em que será admitido o tratamento de seus dados.~~ [\(Revogado pela Medida Provisória nº 869, de 2018\)](#)

§ 1º [\(Revogado\)](#). [\(Redação dada pela Lei nº 13.853, de 2019\)](#)

~~§ 2º A forma de disponibilização das informações previstas no § 1º e no inciso I do caput do art. 23 desta Lei poderá ser especificada pela autoridade nacional.~~ [\(Revogado pela Medida Provisória nº 869, de 2018\)](#)

§ 2º [\(Revogado\)](#). [\(Redação dada pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

§ 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.

§ 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

§ 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

§ 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei. [\(Incluído pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

§ 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.

§ 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.

§ 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.

§ 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.

§ 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.

§ 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.

Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

I - finalidade específica do tratamento;

II - forma e duração do tratamento, observados os segredos comercial e industrial;

III - identificação do controlador;

IV - informações de contato do controlador;

V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

VI - responsabilidades dos agentes que realizarão o tratamento; e

VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

§ 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

§ 2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.

§ 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.

Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

I - apoio e promoção de atividades do controlador; e

II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

Seção II

Do Tratamento de Dados Pessoais Sensíveis

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da [Lei nº 9.307, de 23 de setembro de 1996 \(Lei de Arbitragem\)](#);

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

~~f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou~~

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou [\(Redação dada pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

§ 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.

§ 2º Nos casos de aplicação do disposto nas alíneas “a” e “b” do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei.

§ 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.



~~§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nos casos de portabilidade de dados quando consentido pelo titular.~~

~~§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses de:~~ [\(Redação dada pela Medida Provisória nº 869, de 2018\)](#)

~~I - portabilidade de dados quando consentido pelo titular; ou~~ [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

~~II - necessidade de comunicação para a adequada prestação de serviços de saúde suplementar.~~ [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: [\(Redação dada pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

I - a portabilidade de dados quando solicitada pelo titular; ou [\(Incluído pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo. [\(Incluído pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

§ 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários. [\(Incluído pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

§ 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.

§ 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

§ 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais.

Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

§ 1º A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput deste artigo em nenhuma hipótese poderá revelar dados pessoais.

§ 2º O órgão de pesquisa será o responsável pela segurança da informação prevista no caput deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro.

§ 3º O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.

§ 4º Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

Seção III Do Tratamento de Dados Pessoais de Crianças e de Adolescentes

Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.

§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

§ 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos

a que se refere o art. 18 desta Lei.

§ 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.

§ 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.

§ 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.

§ 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

Seção IV

Do Término do Tratamento de Dados

Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;

II - fim do período de tratamento;

III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou

IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

I - cumprimento de obrigação legal ou regulatória pelo controlador;

II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou

IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

CAPÍTULO III

DOS DIREITOS DO TITULAR

Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

I - confirmação da existência de tratamento;

II - acesso aos dados;

III - correção de dados incompletos, inexatos ou desatualizados;

IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

~~V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador;~~

V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; ([Redação dada pela Lei nº 13.853, de 2019](#)) [Vigência](#)



VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

§ 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.

§ 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.

§ 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.

§ 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:

I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou

II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

§ 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.

§ 6º O responsável 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. [\(Redação dada pela Lei nº 13.853, de 2019\)](#). [Vigência](#)

§ 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.

§ 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor.

Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:

I - em formato simplificado, imediatamente; ou

II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.

§ 1º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.

§ 2º As informações e os dados poderão ser fornecidos, a critério do titular:

I - por meio eletrônico, seguro e idôneo para esse fim; ou

II - sob forma impressa.

§ 3º Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.

§ 4º A autoridade nacional poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do caput deste artigo para os setores específicos.

~~Art. 20. O titular dos dados tem direito a solicitar revisão, por pessoa natural, de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive de decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.~~

~~Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.~~ [\(Redação dada pela Medida Provisória nº 869, de 2018\)](#)

Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. ([Redação dada pela Lei nº 13.853, de 2019](#)) [Vigência](#)

§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

§ 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

§ 3º ([VETADO](#)). ([Incluído pela Lei nº 13.853, de 2019](#)) [Vigência](#)

Art. 21. Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.

Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.

CAPÍTULO IV DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

Seção I Das Regras

Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do [art. 1º da Lei nº 12.527, de 18 de novembro de 2011 \(Lei de Acesso à Informação\)](#), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;

II - ([VETADO](#)); e

~~III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei.~~

III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; e ([Redação dada pela Lei nº 13.853, de 2019](#)) [Vigência](#)

IV - ([VETADO](#)). ([Incluído pela Lei nº 13.853, de 2019](#)) [Vigência](#)

§ 1º A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento.

§ 2º O disposto nesta Lei não dispensa as pessoas jurídicas mencionadas no caput deste artigo de instituir as autoridades de que trata a [Lei nº 12.527, de 18 de novembro de 2011 \(Lei de Acesso à Informação\)](#).

§ 3º Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da [Lei nº 9.507, de 12 de novembro de 1997 \(Lei do Habeas Data\)](#), da [Lei nº 9.784, de 29 de janeiro de 1999 \(Lei Geral do Processo Administrativo\)](#), e da [Lei nº 12.527, de 18 de novembro de 2011 \(Lei de Acesso à Informação\)](#).

§ 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no caput deste artigo, nos termos desta Lei.

§ 5º Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o caput deste artigo.

Art. 24. As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no [art. 173 da Constituição Federal](#), terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei.

Parágrafo único. As empresas públicas e as sociedades de economia mista, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, nos termos deste Capítulo.

Art. 25. Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.

§ 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:

I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na [Lei nº 12.527, de 18 de novembro de 2011 \(Lei de Acesso à Informação\)](#);

II - (VETADO);

~~III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.~~

~~III - se for indicado um encarregado para as operações de tratamento de dados pessoais, nos termos do art. 39; (Redação dada pela Medida Provisória nº 869, de 2018)~~

III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.

~~IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; (Incluído pela Medida Provisória nº 869, de 2018)~~

~~V - na hipótese de a transferência dos dados objetivar a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados; ou (Incluído pela Medida Provisória nº 869, de 2018)~~

IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou [\(Incluído pela Lei nº 13.853, de 2019\)](#)

V - na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades. [\(Incluído pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

~~VI - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei. (Incluído pela Medida Provisória nº 869, de 2018)~~

§ 2º Os contratos e convênios de que trata o § 1º deste artigo deverão ser comunicados à autoridade nacional.

~~Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto:~~

~~Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa jurídica de direito privado dependerá de consentimento do titular, exceto: (Redação dada pela Medida Provisória nº 869, de 2018)~~

Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto:

I - nas hipóteses de dispensa de consentimento previstas nesta Lei;

II - nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; ou

III - nas exceções constantes do § 1º do art. 26 desta Lei.

Parágrafo único. A informação à autoridade nacional de que trata o caput deste artigo será objeto de regulamentação. [\(Incluído pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

Art. 28. (VETADO).

~~Art. 29. A autoridade nacional poderá solicitar, a qualquer momento, às entidades do Poder Público, a realização de operações de tratamento de dados pessoais, informe específico sobre o âmbito e a natureza dos dados e demais detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei.~~

~~Art. 29. A autoridade nacional poderá solicitar, a qualquer momento, aos órgãos e às entidades do Poder Público a realização de operações de tratamento de dados pessoais, as informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei. (Redação dada pela Medida Provisória nº 869, de 2018)~~

Art. 29. A autoridade nacional poderá solicitar, a qualquer momento, aos órgãos e às entidades do poder público a realização de operações de tratamento de dados pessoais, informações específicas sobre o âmbito e a natureza dos

dados e outros detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei. ([Redação dada pela Lei nº 13.853, de 2019](#)) [Vigência](#)

Art. 30. A autoridade nacional poderá estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais.

Seção II

Da Responsabilidade

Art. 31. Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação.

Art. 32. A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

CAPÍTULO V

DA TRANSFERÊNCIA INTERNACIONAL DE DADOS

Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:

I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;

II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:

a) cláusulas contratuais específicas para determinada transferência;

b) cláusulas-padrão contratuais;

c) normas corporativas globais;

d) selos, certificados e códigos de conduta regularmente emitidos;

III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;

IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

V - quando a autoridade nacional autorizar a transferência;

VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;

VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou

IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.

Parágrafo único. Para os fins do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do [art. 1º da Lei nº 12.527, de 18 de novembro de 2011 \(Lei de Acesso à Informação\)](#), no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.

Art. 34. O nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado no inciso I do caput do art. 33 desta Lei será avaliado pela autoridade nacional, que levará em consideração:

I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;

II - a natureza dos dados;

III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei;

IV - a adoção de medidas de segurança previstas em regulamento;

V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e

VI - outras circunstâncias específicas relativas à transferência.

Art. 35. A definição do conteúdo de cláusulas-padrão contratuais, bem como a verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta, a que se refere o inciso II do caput do art. 33 desta Lei, será realizada pela autoridade nacional.

§ 1º Para a verificação do disposto no caput deste artigo, deverão ser considerados os requisitos, as condições e as garantias mínimas para a transferência que observem os direitos, as garantias e os princípios desta Lei.

§ 2º Na análise de cláusulas contratuais, de documentos ou de normas corporativas globais submetidas à aprovação da autoridade nacional, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento, quando necessário.

§ 3º A autoridade nacional poderá designar organismos de certificação para a realização do previsto no caput deste artigo, que permanecerão sob sua fiscalização nos termos definidos em regulamento.

§ 4º Os atos realizados por organismo de certificação poderão ser revistos pela autoridade nacional e, caso em desconformidade com esta Lei, submetidos a revisão ou anulados.

§ 5º As garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no caput deste artigo serão também analisadas de acordo com as medidas técnicas e organizacionais adotadas pelo operador, de acordo com o previsto nos §§ 1º e 2º do art. 46 desta Lei.

Art. 36. As alterações nas garantias apresentadas como suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no inciso II do art. 33 desta Lei deverão ser comunicadas à autoridade nacional.

CAPÍTULO VI DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS

Seção I Do Controlador e do Operador

Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

Art. 40. A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência.

Seção II Do Encarregado pelo Tratamento de Dados Pessoais

Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

§ 2º As atividades do encarregado consistem em:

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

II - receber comunicações da autoridade nacional e adotar providências;

III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.



§ 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

§ 4º (VETADO). (Incluído pela Lei nº 13.853, de 2019). Vigência

Seção III

Da Responsabilidade e do Ressarcimento de Danos

Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:

I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;

II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

§ 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

§ 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.

§ 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:

I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;

II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou

III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:

I - o modo pelo qual é realizado;

II - o resultado e os riscos que razoavelmente dele se esperam;

III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.

CAPÍTULO VII

DA SEGURANÇA E DAS BOAS PRÁTICAS

Seção I

Da Segurança e do Sigilo de Dados

Art. 46. Os agentes de tratamento devem adotar 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.

§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.

Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

I - a descrição da natureza dos dados pessoais afetados;

II - as informações sobre os titulares envolvidos;

III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

IV - os riscos relacionados ao incidente;

V - os motivos da demora, no caso de a comunicação não ter sido imediata; e

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

§ 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:

I - ampla divulgação do fato em meios de comunicação; e

II - medidas para reverter ou mitigar os efeitos do incidente.

§ 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

Seção II Das Boas Práticas e da Governança

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.

§ 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:

I - implementar programa de governança em privacidade que, no mínimo:

a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;

d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;

g) conte com planos de resposta a incidentes e remediação; e

h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.

§ 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.

Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais.

CAPÍTULO VIII DA FISCALIZAÇÃO

Seção I Das Sanções Administrativas

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: [\(Vigência\)](#).

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III - multa diária, observado o limite total a que se refere o inciso II;

IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - eliminação dos dados pessoais a que se refere a infração;

VII - (VETADO);

VIII - (VETADO);

IX - (VETADO).

X - ~~(VETADO);~~ ~~(Incluído pela Lei nº 13.853, de 2019)~~ [\(Promulgação partes vetadas\)](#)

XI - ~~(VETADO);~~ ~~(Incluído pela Lei nº 13.853, de 2019)~~ [\(Promulgação partes vetadas\)](#)

XII - ~~(VETADO);~~ ~~(Incluído pela Lei nº 13.853, de 2019)~~ [\(Promulgação partes vetadas\)](#)

X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; [\(Incluído pela Lei nº 13.853, de 2019\)](#).

XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

§ 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:

I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;

II - a boa-fé do infrator;

III - a vantagem auferida ou pretendida pelo infrator;

IV - a condição econômica do infrator;

V - a reincidência;

VI - o grau do dano;

VII - a cooperação do infrator;

VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;

IX - a adoção de política de boas práticas e governança;

X - a pronta adoção de medidas corretivas; e

XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

~~§ 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas em legislação específica.~~

§ 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas na Lei nº 8.078, de 11 de setembro de 1990, e em legislação específica. [\(Redação dada pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

~~§ 3º O disposto nos incisos I, IV, V, VI, VII, VIII e IX do caput deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990 (Estatuto do Servidor Público Federal), na Lei nº 8.429, de 2 de junho de 1992 (Lei de Improbidade Administrativa), e na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).~~

§ 3º O disposto nos incisos I, IV, V, VI, X, XI e XII do **caput** deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na [Lei nº 8.112, de 11 de dezembro de 1990](#), na [Lei nº 8.429, de 2 de junho de 1992](#), e na [Lei nº 12.527, de 18 de novembro de 2011](#). [\(Redação dada pela Lei nº 13.853, de 2019\)](#)

§ 4º No cálculo do valor da multa de que trata o inciso II do caput deste artigo, a autoridade nacional poderá considerar o faturamento total da empresa ou grupo de empresas, quando não dispuser do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea.

§ 5º O produto da arrecadação das multas aplicadas pela ANPD, inscritas ou não em dívida ativa, será destinado ao Fundo de Defesa de Direitos Difusos de que tratam o art. 13 da Lei nº 7.347, de 24 de julho de 1985, e a Lei nº 9.008, de 21 de março de 1995. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

~~§ 6º (VETADO). [\(Incluído pela Lei nº 13.853, de 2019\)](#) [\(Promulgação partes vetadas\)](#)~~

§ 6º As sanções previstas nos incisos X, XI e XII do **caput** deste artigo serão aplicadas: [\(Incluído pela Lei nº 13.853, de 2019\)](#)

I - somente após já ter sido imposta ao menos 1 (uma) das sanções de que tratam os incisos II, III, IV, V e VI do **caput** deste artigo para o mesmo caso concreto; e [\(Incluído pela Lei nº 13.853, de 2019\)](#)

II - em caso de controladores submetidos a outros órgãos e entidades com competências sancionatórias, ouvidos esses órgãos. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

§ 7º Os vazamentos individuais ou os acessos não autorizados de que trata o caput do art. 46 desta Lei poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata este artigo. [\(Incluído pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

Art. 53. A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa. [\(Vigência\)](#)

§ 1º As metodologias a que se refere o caput deste artigo devem ser previamente publicadas, para ciência dos agentes de tratamento, e devem apresentar objetivamente as formas e dosimetrias para o cálculo do valor-base das sanções de multa, que deverão conter fundamentação detalhada de todos os seus elementos, demonstrando a observância dos critérios previstos nesta Lei.

§ 2º O regulamento de sanções e metodologias correspondentes deve estabelecer as circunstâncias e as condições para a adoção de multa simples ou diária.

Art. 54. O valor da sanção de multa diária aplicável às infrações a esta Lei deve observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela autoridade nacional.

Parágrafo único. A intimação da sanção de multa diária deverá conter, no mínimo, a descrição da obrigação imposta, o prazo razoável e estipulado pelo órgão para o seu cumprimento e o valor da multa diária a ser aplicada pelo seu descumprimento. [\(Vigência\)](#)

CAPÍTULO IX

DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) E DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE

Seção I

Da Autoridade Nacional de Proteção de Dados (ANPD)

CAPÍTULO IX

[\(Redação dada pela Medida Provisória nº 1.317, de 2025\)](#)

DA AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS E DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE

Seção I

Da Agência Nacional de Proteção de Dados

CAPÍTULO IX

[\(Redação dada pela Lei nº 15.352, de 2026\)](#)

DA AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS E DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE

Seção I

Da Agência Nacional de Proteção de Dados

Art. 55. (VETADO).

Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados - ANPD, órgão da administração pública federal, integrante da Presidência da República. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

Art. 55-B. É assegurada autonomia técnica à ANPD. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

Art. 55-C. ANPD é composta por: [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

I - Conselho Diretor, órgão máximo de direção; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

II - Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

III - Corregedoria; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

IV - Ouvidoria; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

V - órgão de assessoramento jurídico próprio; e [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

VI - unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei." [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

Art. 55-D. O Conselho Diretor da ANPD será composto por cinco diretores, incluído o Diretor-Presidente. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

§ 1º Os membros do Conselho Diretor da ANPD serão nomeados pelo Presidente da República e ocuparão cargo em comissão do Grupo-Direção e Assessoramento Superior - DAS de nível 5. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

§ 2º Os membros do Conselho Diretor serão escolhidos dentre brasileiros, de reputação ilibada, com nível superior de educação e elevado conceito no campo de especialidade dos cargos para os quais serão nomeados. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

§ 3º O mandato dos membros do Conselho Diretor será de quatro anos. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

§ 4º Os mandatos dos primeiros membros do Conselho Diretor nomeados serão de dois, de três, de quatro, de cinco e de seis anos, conforme estabelecido no ato de nomeação. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

§ 5º Na hipótese de vacância do cargo no curso do mandato de membro do Conselho Diretor, o prazo remanescente será completado pelo sucessor. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

Art. 55-E. Os membros do Conselho Diretor somente perderão seus cargos em virtude de renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

§ 1º Nos termos do **caput**, cabe ao Ministro de Estado Chefe da Casa Civil da Presidência da República instaurar o processo administrativo disciplinar, que será conduzido por comissão especial constituída por servidores públicos federais estáveis. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

§ 2º Compete ao Presidente da República determinar o afastamento preventivo, caso necessário, e proferir o julgamento. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

Art. 55-F. Aplica-se aos membros do Conselho Diretor, após o exercício do cargo, o disposto no [art. 6º da Lei nº 12.813, de 16 de maio de 2013](#). [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

Parágrafo único. A infração ao disposto no **caput** caracteriza ato de improbidade administrativa. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

Art. 55-G. Ato do Presidente da República disporá sobre a estrutura regimental da ANPD. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

Parágrafo único. Até a data de entrada em vigor de sua estrutura regimental, a ANPD receberá o apoio técnico e administrativo da Casa Civil da Presidência da República para o exercício de suas atividades. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

Art. 55-H. Os cargos em comissão e as funções de confiança da ANPD serão remanejados de outros órgãos e entidades do Poder Executivo federal. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

Art. 55-I. Os ocupantes dos cargos em comissão e das funções de confiança da ANPD serão indicados pelo Conselho Diretor e nomeados ou designados pelo Diretor-Presidente. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

Art. 55-J. Compete à ANPD: [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

I - zelar pela proteção dos dados pessoais; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

II - editar normas e procedimentos sobre a proteção de dados pessoais; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

III - deliberar, na esfera administrativa, sobre a interpretação desta Lei, suas competências e os casos omissos; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

IV - requisitar informações, a qualquer momento, aos controladores e operadores de dados pessoais que realizem operações de tratamento de dados pessoais; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

V - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

VI - fiscalizar e aplicar sanções na hipótese de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

VII - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

VIII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei praticado por órgãos e entidades da administração pública federal; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

IX - difundir na sociedade o conhecimento sobre as normas e as políticas públicas de proteção de dados pessoais e sobre as medidas de segurança; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

X - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle e proteção dos titulares sobre seus dados pessoais, consideradas as especificidades das atividades e o porte dos controladores; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

XI - elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

XII - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

XIII - realizar consultas públicas para colher sugestões sobre temas de relevante interesse público na área de atuação da ANPD; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

XIV - realizar, previamente à edição de resoluções, a oitiva de entidades ou órgãos da administração pública que sejam responsáveis pela regulação de setores específicos da atividade econômica; [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

XV - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

XVI - elaborar relatórios de gestão anuais acerca de suas atividades. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

§ 1º A ANPD, na edição de suas normas, deverá observar a exigência de mínima intervenção, assegurados os fundamentos e os princípios previstos nesta Lei e o disposto no art. 170 da Constituição. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

§ 2º A ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos da atividade econômica e governamental devem coordenar suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com a maior eficiência e promover o adequado funcionamento dos setores regulados, conforme legislação específica, e o tratamento de dados pessoais, na forma desta Lei. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

§ 3º A ANPD manterá fórum permanente de comunicação, inclusive por meio de cooperação técnica, com órgãos e entidades da administração pública que sejam responsáveis pela regulação de setores específicos da atividade econômica e governamental, a fim de facilitar as competências regulatória, fiscalizatória e punitiva da ANPD. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

§ 4º No exercício das competências de que trata o **caput**, a autoridade competente deverá zelar pela preservação do segredo empresarial e do sigilo das informações, nos termos da lei, sob pena de responsabilidade. [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

~~§ 5º As reclamações colhidas conforme o disposto no inciso V do caput poderão ser analisadas de forma agregada e as eventuais providências delas decorrentes poderão ser adotadas de forma padronizada. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~Art. 55-K. A aplicação das sanções previstas nesta Lei compete exclusivamente à ANPD, cujas demais competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~Parágrafo único. A ANPD articulará sua atuação com o Sistema Nacional de Defesa do Consumidor do Ministério da Justiça e com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais, e será o órgão central de interpretação desta Lei e do estabelecimento de normas e diretrizes para a sua implementação. (Incluído pela Medida Provisória nº 869, de 2018)~~

~~Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República. (Incluído pela Lei nº 13.853, de 2019)~~

~~§ 1º A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República. (Incluído pela Lei nº 13.853, de 2019) (Revogado pela Medida Provisória nº 1.124, de 2022) (Revogado pela Lei nº 14.460, de 2022)~~

~~§ 2º A avaliação quanto à transformação de que dispõe o § 1º deste artigo deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ANPD. (Incluído pela Lei nº 13.853, de 2019) (Revogado pela Medida Provisória nº 1.124, de 2022) (Revogado pela Lei nº 14.460, de 2022)~~

~~§ 3º O provimento dos cargos e das funções necessários à criação e à atuação da ANPD está condicionado à expressa autorização física e financeira na lei orçamentária anual e à permissão na lei de diretrizes orçamentárias. (Incluído pela Lei nº 13.853, de 2019) (Revogado pela Medida Provisória nº 1.124, de 2022) (Revogado pela Lei nº 14.460, de 2022)~~

~~Art. 55-A. Fica criada a Autoridade Nacional de Proteção de Dados – ANPD, autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio próprio e com sede e foro no Distrito Federal. (Redação dada pela Medida Provisória nº 1.124, de 2022)~~

~~Art. 55-A. Fica criada a Autoridade Nacional de Proteção de Dados (ANPD), autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio próprio e com sede e foro no Distrito Federal. (Redação dada pela Lei nº 14.460, de 2022)~~

~~Art. 55-A. Fica criada a Agência Nacional de Proteção de Dados – ANPD, autarquia de natureza especial vinculada ao Ministério da Justiça e Segurança Pública, dotada de autonomia funcional, técnica, decisória, administrativa e financeira, com patrimônio próprio e com sede e foro no Distrito Federal, nos termos do disposto na Lei nº 13.848, de 25 de junho de 2019. (Redação dada pela Medida Provisória nº 1.317, de 2025)~~

~~Art. 55-A. Fica criada a Agência Nacional de Proteção de Dados (ANPD), autarquia de natureza especial vinculada ao Ministério da Justiça e Segurança Pública, dotada de autonomia funcional, técnica, decisória, administrativa e financeira, com patrimônio próprio e com sede e foro no Distrito Federal, nos termos da Lei nº 13.848, de 25 de junho de 2019. (Redação dada pela Lei nº 15.452, de 2026)~~

~~Art. 55-B. É assegurada autonomia técnica e decisória à ANPD. (Incluído pela Lei nº 13.853, de 2019) (Revogado pela Medida Provisória nº 1.124, de 2022) (Revogado pela Lei nº 14.460, de 2022)~~

Art. 55-C. A ANPD é composta de: (Incluído pela Lei nº 13.853, de 2019)

I - Conselho Diretor, órgão máximo de direção; (Incluído pela Lei nº 13.853, de 2019)

II - Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019)

III - Corregedoria; (Incluído pela Lei nº 13.853, de 2019)

IV - Ouvidoria; (Incluído pela Lei nº 13.853, de 2019)

V – órgão de assessoramento jurídico próprio; e (Incluído pela Lei nº 13.853, de 2019)

V – Procuradoria; e (Redação dada pela Medida Provisória nº 1.124, de 2022)

V - (revogado); (Redação dada pela Lei nº 14.460, de 2022)

V-A – Procuradoria; e (Incluído pela Lei nº 14.460, de 2022)

V-A – Procuradoria; (Redação dada pela Medida Provisória nº 1.317, de 2025)

V-A -Procuradoria; (Redação dada pela Lei nº 15.352, de 2026)

V-B – Auditoria; e (Incluído pela Medida Provisória nº 1.317, de 2025)

V-B - Auditoria; e (Incluído pela Lei nº 15.352, de 2026)

~~VI – unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei. (Incluído pela Lei nº 13.853, de 2019)~~

~~VI - unidades administrativas e unidades especializadas. (Redação dada pela Medida Provisória nº 1.317, de 2025).~~

VI - unidades administrativas e unidades especializadas. (Redação dada pela Lei nº 15.352, de 2026)

Art. 55-D. O Conselho Diretor da ANPD será composto de 5 (cinco) diretores, incluído o Diretor-Presidente. (Incluído pela Lei nº 13.853, de 2019).

§ 1º Os membros do Conselho Diretor da ANPD serão escolhidos pelo Presidente da República e por ele nomeados, após aprovação pelo Senado Federal, nos termos da alínea 'f' do inciso III do art. 52 da Constituição Federal, e ocuparão cargo em comissão do Grupo-Direção e Assessoramento Superiores - DAS, no mínimo, de nível 5. (Incluído pela Lei nº 13.853, de 2019).

§ 2º Os membros do Conselho Diretor serão escolhidos dentre brasileiros que tenham reputação ilibada, nível superior de educação e elevado conceito no campo de especialidade dos cargos para os quais serão nomeados. (Incluído pela Lei nº 13.853, de 2019).

§ 3º O mandato dos membros do Conselho Diretor será de 4 (quatro) anos. (Incluído pela Lei nº 13.853, de 2019).

§ 4º Os mandatos dos primeiros membros do Conselho Diretor nomeados serão de 2 (dois), de 3 (três), de 4 (quatro), de 5 (cinco) e de 6 (seis) anos, conforme estabelecido no ato de nomeação. (Incluído pela Lei nº 13.853, de 2019).

§ 5º Na hipótese de vacância do cargo no curso do mandato de membro do Conselho Diretor, o prazo remanescente será completado pelo sucessor. (Incluído pela Lei nº 13.853, de 2019).

Art. 55-E. Os membros do Conselho Diretor somente perderão seus cargos em virtude de renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar. (Incluído pela Lei nº 13.853, de 2019).

§ 1º Nos termos do caput deste artigo, cabe ao Ministro de Estado Chefe da Casa Civil da Presidência da República instaurar o processo administrativo disciplinar, que será conduzido por comissão especial constituída por servidores públicos federais estáveis. (Incluído pela Lei nº 13.853, de 2019).

§ 2º Compete ao Presidente da República determinar o afastamento preventivo, somente quando assim recomendado pela comissão especial de que trata o § 1º deste artigo, e proferir o julgamento. (Incluído pela Lei nº 13.853, de 2019).

Art. 55-F. Aplica-se aos membros do Conselho Diretor, após o exercício do cargo, o disposto no art. 6º da Lei nº 12.813, de 16 de maio de 2013. (Incluído pela Lei nº 13.853, de 2019).

Parágrafo único. A infração ao disposto no caput deste artigo caracteriza ato de improbidade administrativa. (Incluído pela Lei nº 13.853, de 2019).

Art. 55-G. Ato do Presidente da República disporá sobre a estrutura regimental da ANPD. (Incluído pela Lei nº 13.853, de 2019).

§ 1º Até a data de entrada em vigor de sua estrutura regimental, a ANPD receberá o apoio técnico e administrativo da Casa Civil da Presidência da República para o exercício de suas atividades. (Incluído pela Lei nº 13.853, de 2019).

§ 2º O Conselho Diretor disporá sobre o regimento interno da ANPD. (Incluído pela Lei nº 13.853, de 2019).

Art. 55-H. Os cargos em comissão e as funções de confiança da ANPD serão remanejados de outros órgãos e entidades do Poder Executivo federal. (Incluído pela Lei nº 13.853, de 2019).

Art. 55-I. Os ocupantes dos cargos em comissão e das funções de confiança da ANPD serão indicados pelo Conselho Diretor e nomeados ou designados pelo Diretor-Presidente. (Incluído pela Lei nº 13.853, de 2019).

Art. 55-J. Compete à ANPD: (Incluído pela Lei nº 13.853, de 2019).

I - zelar pela proteção dos dados pessoais, nos termos da legislação; (Incluído pela Lei nº 13.853, de 2019).

II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei; (Incluído pela Lei nº 13.853, de 2019).

III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019).

IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; [\(Incluído pela Lei nº 13.853, de 2019\)](#).

V - apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação; [\(Incluído pela Lei nº 13.853, de 2019\)](#).

VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; [\(Incluído pela Lei nº 13.853, de 2019\)](#).

VII - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; [\(Incluído pela Lei nº 13.853, de 2019\)](#).

VIII - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis; [\(Incluído pela Lei nº 13.853, de 2019\)](#).

IX - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; [\(Incluído pela Lei nº 13.853, de 2019\)](#).

X - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial; [\(Incluído pela Lei nº 13.853, de 2019\)](#).

XI - solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei; [\(Incluído pela Lei nº 13.853, de 2019\)](#).

XII - elaborar relatórios de gestão anuais acerca de suas atividades; [\(Incluído pela Lei nº 13.853, de 2019\)](#).

XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei; [\(Incluído pela Lei nº 13.853, de 2019\)](#).

XIV - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento; [\(Incluído pela Lei nº 13.853, de 2019\)](#).

XV - arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas; [\(Incluído pela Lei nº 13.853, de 2019\)](#).

XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público; [\(Incluído pela Lei nº 13.853, de 2019\)](#).

XVII - celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942; [\(Incluído pela Lei nº 13.853, de 2019\)](#).

XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei; [\(Incluído pela Lei nº 13.853, de 2019\)](#).

XIX - garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da [Lei nº 10.741, de 1º de outubro de 2003 \(Estatuto do Idoso\)](#); [\(Incluído pela Lei nº 13.853, de 2019\)](#).

XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos; [\(Incluído pela Lei nº 13.853, de 2019\)](#).

XXI - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento; [\(Incluído pela Lei nº 13.853, de 2019\)](#).

XXII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal; [\(Incluído pela Lei nº 13.853, de 2019\)](#).

XXIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e [\(Incluído pela Lei nº 13.853, de 2019\)](#).

[de 2019\)](#)

XXIV - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

§ 1º Ao impor condicionantes administrativas ao tratamento de dados pessoais por agente de tratamento privado, sejam eles limites, encargos ou sujeições, a ANPD deve observar a exigência de mínima intervenção, assegurados os fundamentos, os princípios e os direitos dos titulares previstos no [art. 170 da Constituição Federal](#) e nesta Lei. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

§ 2º Os regulamentos e as normas editados pela ANPD devem ser precedidos de consulta e audiência públicas, bem como de análises de impacto regulatório. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

§ 3º A ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos da atividade econômica e governamental devem coordenar suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com a maior eficiência e promover o adequado funcionamento dos setores regulados, conforme legislação específica, e o tratamento de dados pessoais, na forma desta Lei. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

§ 4º A ANPD manterá fórum permanente de comunicação, inclusive por meio de cooperação técnica, com órgãos e entidades da administração pública responsáveis pela regulação de setores específicos da atividade econômica e governamental, a fim de facilitar as competências regulatória, fiscalizatória e punitiva da ANPD. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

§ 5º No exercício das competências de que trata o caput deste artigo, a autoridade competente deverá zelar pela preservação do segredo empresarial e do sigilo das informações, nos termos da lei. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

§ 6º As reclamações colhidas conforme o disposto no inciso V do caput deste artigo poderão ser analisadas de forma agregada, e as eventuais providências delas decorrentes poderão ser adotadas de forma padronizada. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

Art. 55-K. A aplicação das sanções previstas nesta Lei compete exclusivamente à ANPD, e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

Parágrafo único. A ANPD articulará sua atuação com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais e será o órgão central de interpretação desta Lei e do estabelecimento de normas e diretrizes para a sua implementação. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

Art. 55-L. Constituem receitas da ANPD: [\(Incluído pela Lei nº 13.853, de 2019\)](#)

I - as dotações, consignadas no orçamento geral da União, os créditos especiais, os créditos adicionais, as transferências e os repasses que lhe forem conferidos; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

II - as doações, os legados, as subvenções e outros recursos que lhe forem destinados; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

III - os valores apurados na venda ou aluguel de bens móveis e imóveis de sua propriedade; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

IV - os valores apurados em aplicações no mercado financeiro das receitas previstas neste artigo; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

V - (VETADO); [\(Incluído pela Lei nº 13.853, de 2019\)](#)

VI - os recursos provenientes de acordos, convênios ou contratos celebrados com entidades, organismos ou empresas, públicos ou privados, nacionais ou internacionais; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

VII - o produto da venda de publicações, material técnico, dados e informações, inclusive para fins de licitação pública. [\(Incluído pela Lei nº 13.853, de 2019\)](#)

~~Art. 55-M. Constituem o patrimônio da ANPD os bens e os direitos: [\(Incluído pela Medida Provisória nº 1.124, de 2022\)](#)~~

~~I - que lhe forem transferidos pelos órgãos da Presidência da República; e [\(Incluído pela Medida Provisória nº 1.124, de 2022\)](#)~~

~~II - que venha a adquirir ou a incorporar. [\(Incluído pela Medida Provisória nº 1.124, de 2022\)](#)~~



Art. 55-M. Constituem o patrimônio da ANPD os bens e os direitos: [\(Incluído pela Lei nº 14.460, de 2022\)](#)

I - que lhe forem transferidos pelos órgãos da Presidência da República; e [\(Incluído pela Lei nº 14.460, de 2022\)](#)

II - que venha a adquirir ou a incorporar. [\(Incluído pela Lei nº 14.460, de 2022\)](#)

Art. 56. (VETADO).

Art. 57. (VETADO).

Seção II Do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

Art. 58. (VETADO).

~~Art. 58-A. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto por vinte e três representantes, titulares suplentes, dos seguintes órgãos:~~ [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

~~I - seis do Poder Executivo federal;~~ [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

~~II - um do Senado Federal;~~ [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

~~III - um da Câmara dos Deputados;~~ [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

~~IV - um do Conselho Nacional de Justiça;~~ [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

~~V - um do Conselho Nacional do Ministério Público;~~ [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

~~VI - um do Comitê Gestor da Internet no Brasil;~~ [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

~~VII - quatro de entidades da sociedade civil com atuação comprovada em proteção de dados pessoais;~~ [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

~~VIII - quatro de instituições científicas, tecnológicas e de inovação; e~~ [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

~~IX - quatro de entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais.~~ [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

~~§ 1º Os representantes serão designados pelo Presidente da República.~~ [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

~~§ 2º Os representantes de que tratam os incisos I a VI do caput e seus suplentes serão indicados pelos titulares dos respectivos órgãos e entidades da administração pública.~~ [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

~~§ 3º Os representantes de que tratam os incisos VII, VIII e IX do caput e seus suplentes:~~ [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

~~I - serão indicados na forma de regulamento;~~ [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

~~II - terão mandato de dois anos, permitida uma recondução; e~~ [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

~~III - não poderão ser membros do Comitê Gestor da Internet no Brasil.~~ [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

~~§ 4º A participação no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será considerada prestação de serviço público relevante, não remunerada.~~ [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

~~Art. 58-B. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade:~~ [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

~~I - propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD;~~ [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

~~II - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade;~~ [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

~~III - sugerir ações a serem realizadas pela ANPD;~~ [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

~~IV - elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade;~~ [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

~~e~~ [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)
~~V - disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população em geral.~~ [\(Incluído pela Medida Provisória nº 869, de 2018\)](#)

Art. 58-A. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto de 23 (vinte e três) representantes, titulares e suplentes, dos seguintes órgãos: [\(Incluído pela Lei nº 13.853, de 2019\)](#)

I - 5 (cinco) do Poder Executivo federal; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

II - 1 (um) do Senado Federal; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

III - 1 (um) da Câmara dos Deputados; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

IV - 1 (um) do Conselho Nacional de Justiça; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

V - 1 (um) do Conselho Nacional do Ministério Público; [\(Incluído pela Lei nº 13.853, de 2019\)](#)

VI - 1 (um) do Comitê Gestor da Internet no Brasil; [\(Incluído pela Lei nº 13.853, de 2019\)](#)



VII - 3 (três) de entidades da sociedade civil com atuação relacionada a proteção de dados pessoais;
(Incluído pela Lei nº 13.853, de 2019).

VIII - 3 (três) de instituições científicas, tecnológicas e de inovação;
(Incluído pela Lei nº 13.853, de 2019).

IX - 3 (três) de confederações sindicais representativas das categorias econômicas do setor produtivo;
(Incluído pela Lei nº 13.853, de 2019).

X - 2 (dois) de entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais; e
(Incluído pela Lei nº 13.853, de 2019).

XI - 2 (dois) de entidades representativas do setor laboral.
(Incluído pela Lei nº 13.853, de 2019).

§ 1º Os representantes serão designados por ato do Presidente da República, permitida a delegação.
(Incluído pela Lei nº 13.853, de 2019).

§ 2º Os representantes de que tratam os incisos I, II, III, IV, V e VI do caput deste artigo e seus suplentes serão indicados pelos titulares dos respectivos órgãos e entidades da administração pública.
(Incluído pela Lei nº 13.853, de 2019).

§ 3º Os representantes de que tratam os incisos VII, VIII, IX, X e XI do caput deste artigo e seus suplentes:
(Incluído pela Lei nº 13.853, de 2019).

I - serão indicados na forma de regulamento;
(Incluído pela Lei nº 13.853, de 2019).

II - não poderão ser membros do Comitê Gestor da Internet no Brasil;
(Incluído pela Lei nº 13.853, de 2019).

III - terão mandato de 2 (dois) anos, permitida 1 (uma) recondução.
(Incluído pela Lei nº 13.853, de 2019).

§ 4º A participação no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será considerada prestação de serviço público relevante, não remunerada.
(Incluído pela Lei nº 13.853, de 2019).

Art. 58-B. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade:
(Incluído pela Lei nº 13.853, de 2019).

I - propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD;
(Incluído pela Lei nº 13.853, de 2019).

II - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade;
(Incluído pela Lei nº 13.853, de 2019).

III - sugerir ações a serem realizadas pela ANPD;
(Incluído pela Lei nº 13.853, de 2019).

IV - elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade; e
(Incluído pela Lei nº 13.853, de 2019).

V - disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população.
(Incluído pela Lei nº 13.853, de 2019).

Art. 59. (VETADO).

CAPÍTULO X DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 60. A [Lei nº 12.965, de 23 de abril de 2014 \(Marco Civil da Internet\)](#), passa a vigorar com as seguintes alterações: [Vigência](#)

“Art. 7º

[X](#) - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais;

.....” (NR)

“Art. 16.

.....

II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular, exceto nas hipóteses previstas na Lei que dispõe sobre a proteção de dados pessoais.” (NR)

Art. 61. A empresa estrangeira será notificada e intimada de todos os atos processuais previstos nesta Lei, independentemente de procuração ou de disposição contratual ou estatutária, na pessoa do agente ou representante ou pessoa responsável por sua filial, agência, sucursal, estabelecimento ou escritório instalado no Brasil.

~~Art. 62. A autoridade nacional e o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep), no âmbito de suas competências, editarão regulamentos específicos para o acesso a dados tratados pela União para o cumprimento do disposto no § 2º do art. 9º da Lei nº 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação Nacional), e aos referentes ao Sistema Nacional de Avaliação da Educação Superior (Sinaes), de que trata a Lei nº 10.861, de 14 de abril de 2004. (Revogado pela Medida Provisória nº 869, de 2018)~~

Art. 62. A autoridade nacional e o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep), no âmbito de suas competências, editarão regulamentos específicos para o acesso a dados tratados pela União para o cumprimento do disposto no § 2º do art. 9º da Lei nº 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação Nacional), e aos referentes ao Sistema Nacional de Avaliação da Educação Superior (Sinaes), de que trata a Lei nº 10.861, de 14 de abril de 2004.

Art. 63. A autoridade nacional estabelecerá normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, consideradas a complexidade das operações de tratamento e a natureza dos dados.

Art. 64. Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

~~Art. 65. Esta Lei entra em vigor após decorridos 18 (dezoito) meses de sua publicação oficial.~~

~~Art. 65. Esta Lei entra em vigor: (Redação dada pela Medida Provisória nº 869, de 2018)~~

~~I - quanto aos art. 55-A, art. 55-B, art. 55-C, art. 55-D, art. 55-E, art. 55-F, art. 55-G, art. 55-H, art. 55-I, art. 55-J, art. 55-K, art. 58-A e art. 58-B, no dia 28 de dezembro de 2018; e (Incluído pela Medida Provisória nº 869, de 2018)~~

~~II - vinte e quatro meses após a data de sua publicação quanto aos demais artigos. (Incluído pela Medida Provisória nº 869, de 2018)~~

Art. 65. Esta Lei entra em vigor: (Redação dada pela Lei nº 13.853, de 2019)

I - dia 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; e (Incluído pela Lei nº 13.853, de 2019)

I-A - dia 1º de agosto de 2021, quanto aos arts. 52, 53 e 54; (Incluído pela Lei nº 14.010, de 2020)

~~II - 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos. (Incluído pela Lei nº 13.853, de 2019)~~

~~II - em 3 de maio de 2021, quanto aos demais artigos. (Redação dada pela Medida Provisória nº 959, de 2020). (Convertida na Lei nº 14.058, de 2020)~~

II - 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos. (Incluído pela Lei nº 13.853, de 2019)

Brasília, 14 de agosto de 2018; 197º da Independência e 130º da República.

MICHEL TEMER

Torquato Jardim

Aloysio Nunes Ferreira Filho

Eduardo Refinetti Guardia

Esteves Pedro Colnago Junior

Gilberto Magalhães Occhi

Gilberto Kassab

Wagner de Campos Rosário

Gustavo do Vale Rocha

Ilán Goldfajn

Raul Jungmann

Eliseu Padilha

Este texto não substitui o publicado no DOU de 15.8.2018, e republicado parcialmente em 15.8.2018 - Edição extra

*



Município de Espigão do Oeste

04.695.284/0001-39

Rua Rio Grande do Sul, 2800 - Vista Alegre

www.espigaodoeste.ro.gov.br

FICHA CADASTRAL DO DOCUMENTO ELETRÔNICO

Tipo do Documento	Identificação/Número	Data
Lei	Federal n.13.709/2018	05/03/2026

ID: 1363447	Processo	Documento
CRC: 8263501B		
Processo: 59-1/2026		
Usuário: Ilza Lima do Carmo		
Criação: 05/03/2026 09:46:17	Finalização: 05/03/2026 09:47:27	

MD5: 4E7C24E29F40BE8D6627C42BDF9004A8
SHA256: D49513C2556A97615F1AABF0EB32DE7CB72699564FDB3D0C013D4E93E81EAD6E

Súmula/Objeto:

Lei Geral de Proteção de Dados Pessoais (LGPD).

INTERESSADOS

CAMARA MUNICIPAL DE ESPIGAO DO OESTE	ESPIGAO DO OESTE	RO	05/03/2026 09:46:17
--------------------------------------	------------------	----	---------------------

ASSUNTOS

PROJETO DE RESOLUÇÃO	05/03/2026 09:46:17
----------------------	---------------------

ASSINATURAS ELETRÔNICAS

SIMPLES ASSINATURA ELETRÔNICA	Ilza Lima do Carmo	Diretor Legislativo adjunto	05/03/2026 09:48:16
-------------------------------	--------------------	-----------------------------	---------------------

Assinado na forma do Resolução Municipal nº 90/2021.

A autenticidade deste documento pode ser conferida através do QRCode acima ou ainda através do site transparencia.espigaodoeste.ro.gov.br informando o ID 1363447 e o CRC 8263501B.

PROCESSO: 02341/24/TCE-RO

CATEGORIA: Auditoria e Inspeção

SUBCATEGORIA: Levantamento

ASSUNTO: Verificação do cumprimento do Acórdão APL-TC 00251/24, prolatado em processo de Levantamento para avaliar a governança e proteção de dados pessoais no âmbito das prefeituras, câmaras legislativas e institutos de previdência dos servidores dos municípios do Estado de Rondônia.

JURISDICIONADOS: Prefeituras, Câmaras Municipais e Institutos de Previdência dos servidores públicos municipais

RESPONSÁVEIS: GIOVAN DAMO, Prefeito do Município de Alta Floresta do Oeste, CPF n. ***.452.012-**;

NATÃ SOARES DA CRUZ, Presidente da Câmara Municipal de Alta Floresta do Oeste, CPF n. ***.844.182-**;

DENAIR PEDRO DA SILVA, Prefeito do Município de Alto Alegre dos Parecis, CPF n. ***.926.712-**;

VALMIRO GOMES DA SILVA, Presidente da Câmara Municipal de Alto Alegre dos Parecis, CPF n. ***.019.632-**;

JOÃO PAVAN, Prefeito do Município de Alto Paraíso, CPF n. ***.567.499-**;

VALMIR DOS SANTOS, Presidente da Câmara Municipal de Alto Paraíso, CPF n. ***.650.592-**;

JAIR LUIZ, Prefeito do Município de Alvorada do Oeste, CPF n. ***.547.982-**;

DIEGO UESLLEI DE SOUZA, Presidente da Câmara Municipal de Alvorada do Oeste, CPF n. ***.882.092-**;

ISRAEL FERREIRA DE MIRANDA, Diretor Executivo do Instituto de Previdência Social dos Servidores Públicos de Alvorada do Oeste, CPF n. ***.563.182-**;

CARLA GONÇALVES REZENDE, Prefeita do Município de Ariquemes, CPF n. ***.071.572-**;

FILIPPE RASSEN ROZIQUE, Presidente da Câmara Municipal de Ariquemes, CPF n. ***.092.141-**;



PAULO BELEGANTE, Presidente do Instituto de Previdência do Município de Ariquemes – IPAMARI, CPF n. ***.134.569-**,

VALTAIR FRITZ DOS REIS, Prefeito do Município de Buritis, CPF n. **.477.909-**;

IVAN CARLOS DUTRA, Presidente da Câmara Municipal de Buritis, CPF n. ***.216.532-**;

DARCI FERREIRA COELHO, Diretor Executivo do Instituto de Previdência Social de Buritis, CPF n. ***.804112-**;

SILVANO ASCARI DE ALMEIDA, Prefeito do Município de Cabixi, CPF n. ***.740.352-**;

MILTON ANTUNES DA SILVA, Presidente da Câmara Municipal de Cabixi, CPF n. ***.723.170-**;

DANIEL MARCELINO DA SILVA, Prefeito do Município de Cacaulândia, CPF n. ***.722.466-**;

DORAILDES DA SILVA OLIVEIRA, Presidente da Câmara Municipal de Cacaulândia, CPF n. ***.235.942-**;

JEFERSON DA SILVA OLIVEIRA, Superintendente do Instituto de Previdência dos Servidores Públicos do Município de Cacaulândia, CPF n. ***.566.522-**;

ADAILTON ANTUNES FERREIRA, Prefeito do Município de Cacoal, CPF n. ***.452.772-**;

GIMENEZ FRITZ, Presidente da Câmara Municipal de Cacoal, CPF n. ***.779.042-**;

ALEXANDRE JOSÉ SILVESTRE DIAS, Prefeito do Município de Campo Novo de Rondônia, CPF n. ***.468.749-**,

THIAGO ONOFRE, Presidente da Câmara Municipal de Campo Novo de Rondônia, CPF n. ***.598.479-**;

IZOLDA MADELLA, Superintendente do Instituto de Previdência Social dos Servidores Públicos do Município de Campo Novo de Rondônia, CPF n. ***.733.860-**;

LINDOMAR BARBOSA ALVES, Prefeito do Município de Candeias do Jamari, CPF n. ***.506.852-**;



JUCILENE MARQUES MORAES, Presidente da Câmara Municipal de Candeias do Jamari, CPF n. ***.422.882-**;

CÍCERO APARECIDO GODOI, Prefeito do Município de Castanheiras, CPF n. ***.469.632-**;

ANDRÉ DE OLIVEIRA, Presidente da Câmara Municipal de Castanheiras, CPF n. ***.835.612-**;

ELENI DE SOUZA SOLIMAN LOVISON, Superintendente do Instituto de Previdência Social dos Servidores Públicos Municipais de Castanheiras – IPC, CPF n. ***.042.301-**;

SINESIO JOSÉ DE SOUZA, Prefeito do Município de Cerejeiras, CPF n. ***.143.472-**;

SELSON LOPES DE SOUZA, Presidente da Câmara Municipal de Cerejeiras, CPF n. ***.310.332-**;

WESLEY WANDERLEY DA COSTA GONCALVES, Prefeito do Município de Chupinguaia, CPF n. ***.856.642-**;

GARDELL VINICIUS LIMA DOS SANTOS, Presidente da Câmara Municipal de Chupinguaia, CPF n. ***.837.817-**;

EDMILSON RODRIGUES DE ALMEIDA, Prefeito do Município de Colorado do Oeste, CPF n. ***.888.592-**;

MICHELLY DOS SANTOS MARTINS, Presidente da Câmara Municipal de Colorado do Oeste, CPF n. ***.645.192-**;

LEANDRO TEIXEIRA VIEIRA, Prefeito do Município de Corumbiara, CPF n. ***.849.642-**;

OLON PEREIRA DE SOUZA, Presidente da Câmara Municipal de Corumbiara, CPF n. ***.465.802-**;

FABIOMAR AGOSTINI BENTO, Prefeito do Município de Costa Marques, CPF n. ***.251.662-**;

JULIANE DUARTE SENA DAS NEVES, Presidente da Câmara Municipal de Costa Marques, CPF n. ***.436.042-**;

JOÃO BECKER, Prefeito do Município de Cujubim, CPF n. ***.096.432-**;

HAROLDO RODRIGUES FIGUEREDO, Presidente da Câmara Municipal de Cujubim, CPF n. ***.523.542-**;



ELIAS CRUZ SANTOS, Superintendente do Instituto de Previdência Social dos Servidores Públicos de Cujubim – INPREC, CPF n. ***.789.912-**;

WELITON PEREIRA CAMPOS, Prefeito do Município de Espigão do Oeste, CPF n. ***.646.905-**;

AMILTON ALVES DE SOUZA, Presidente da Câmara Municipal de Espigão do Oeste, CPF n. ***.992.702-**;

VALDINEIA VAZ LARA, Presidente do Instituto de Previdência Municipal de Espigão do Oeste, CPF n. ***.065.892-**;

GILMAR TOMAZ DE SOUZA, Prefeito do Município de Governador Jorge Teixeira, CPF n. ***.115.662-**;

LEOMARCOS SOUZA DA SILVA, Presidente da Câmara Municipal de Governador Jorge Teixeira, CPF n. ***.373.132-**;

ROSALINA MARIA DE JESUS DOMICIANO LEITE, Presidente do Instituto de Previdência Municipal de Governador Jorge Teixeira, CPF n. ***.808.558-**;

FÁBIO GARCIA DE OLIVEIRA, Prefeito do Município de Guajará-Mirim, CPF n. ***.254.478-**;

ELIEL NUNES SILVINO, Presidente da Câmara Municipal de Guajará-Mirim, CPF n. ***.201.162-**;

ALEIDE FERNANDES DA SILVA, Diretor Executivo do Instituto de Previdência Social de Guajará-Mirim, CPF n. ***.016.742-**;

IDIZNEI CASTRO MARTINS, Prefeito do Município de Itapuã do Oeste, CPF n. ***.131.922-**;

RONILVANE ALVES SANTOS, Presidente da Câmara Municipal de Itapuã do Oeste, CPF n. ***.351.732-**;

JEVERSON LUIZ DE LIMA, Prefeito do Município de Jaru, CPF n. ***.900.472-**;

TATIANE DE ALMEIDA DOMINGUES, Presidente da Câmara Municipal de Jaru, CPF n. ***.585.582-**;



GEZIEL SOARES, Superintendente do Instituto de Previdência dos Servidores Públicos do Município de Jaru, CPF n. ***.089.662-**;

AFFONSO ANTONIO CANDIDO, Prefeito do Município de Ji-Paraná, CPF n. ***.003.112-**;

MARCELO JOSÉ DE LEMOS, Presidente da Câmara Municipal de Ji-Paraná, CPF n. ***.442.942-**;

EDISIO GOMES BARROSO, Presidente do Instituto de Previdência dos Servidores de Ji-Paraná – IPREJI, CPF n. ***.907.902-**;

PAULO HENRIQUE DOS SANTOS, Prefeito do Município de Machadinho do Oeste, CPF n. ***.574.309-**;

JOSÉ FERREIRA ALVES, Presidente da Câmara Municipal de Machadinho do Oeste, CPF n. ***.914.222-**;

KERLES FERNANDES DUARTE, Presidente do Instituto Municipal de Previdência de Machadinho do Oeste, CPF n. ***.867.222-**;

JOSÉ ALVES PEREIRA, Prefeito do Município de Ministro Andreazza, CPF n. ***.096.582-**;

JUCILEIA ALVES DA SILVA, Presidente da Câmara Municipal de Ministro Andreazza, CPF n. ***.506.692-**;

JOSÉ CARLOS PEREIRA DE ANDRADE, Prefeito do Município de Mirante da Serra, CPF n. ***.849.072-**;

JOSIVALDO LOUZADA DE OLIVEIRA, Presidente da Câmara Municipal de Mirante da Serra, CPF n. ***.249.036-**;

CELSO MARTINS DOS SANTOS, Superintendente do Instituto de Previdência Social dos Servidores Públicos do Município de Mirante da Serra, CPF n. ***.536.872-**;

IVAIR JOSÉ FERNANDES, Prefeito do Município de Monte Negro, CPF n. ***.527.309-**;

JOEL RODRIGUES MATEUS, Presidente da Câmara Municipal de Monte Negro, CPF n. ***.321.762-**;

JULIANO SOUSA GUEDES, Gestor do Instituto de Previdência dos Servidores Públicos Municipais de Monte Negro, CPF n. ***.811.502-**;



CLODOALDO ALVES PEDROSO, Prefeito do Município de Nova Brasilândia do Oeste, CPF n. ***.297.462-**;

JHONATAN SOUZA ANDRADE, Presidente da Câmara Municipal de Nova Brasilândia do Oeste, CPF n. ***.109.102-**;

MARCÉLIO RODRIGUES UCHOA, Prefeito do Município de Nova Mamoré, CPF n. ***.943.052-**;

ADALTO FERREIRA DA SILVA, Presidente da Câmara Municipal de Nova Mamoré, CPF n. ***.833.752-**;

RENI PARENTE DA SILVA TELES, Presidente do Instituto de Previdência Social dos Servidores Públicos Municipais de Nova Mamoré, CPF n. ***.027.772-**;

JOÃO JOSÉ DE OLIVEIRA, Prefeito do Município de Nova União, CPF n. ***.133.851-**;

MARCOS RAMON RIBEIRO, Presidente da Câmara Municipal de Nova União, CPF n. ***.578.622-**;

OSVALDO SOARES DE OLIVEIRA, Superintendente do Instituto de Previdência dos Servidores Públicos do Município de Nova União, CPF n. ***.514.872-**;

RONALDO DELAZARI, Prefeito do Município de Novo Horizonte do Oeste, CPF n. ***.553.382-**;

DIOGO FARIAS PADILHA, Presidente da Câmara Municipal de Novo Horizonte do Oeste, CPF n. ***.289.922-**;

ANDRESSA RAASCH FELTZ, Presidente do Instituto de Previdência Social de Novo Horizonte do Oeste, CPF n. ***.330.562-**;

JUAN ALEX TESTONI, Prefeito do Município de Ouro Preto do Oeste, CPF n. ***.400.012-**;

GILVANE FERNANDES DA SILVA, Presidente da Câmara Municipal de Ouro Preto do Oeste, CPF n. ***.475.602-**;

SEBASTIÃO PEREIRA DA SILVA, Diretor-Presidente do Instituto de Previdência dos Servidores do Município de Ouro Preto do Oeste, CPF n. ***.183.342-**;

MARCONDES DE CARVALHO, Prefeito do Município de Parecis, CPF n. ***.258.262-**;



DONIZETE VITOR ALVES, Presidente da Câmara Municipal de Parecis, CPF n. ***.694.972-**;

MARCILENE RODRIGUES DA SILVA SOUZA, Prefeita do Município de Pimenta Bueno, CPF n. ***.947.732-**;

LUCAS SAMPAIO CABRAL MACIEL, Presidente da Câmara Municipal de Pimenta Bueno, CPF n. ***.814.252-**;

VALÉRIA APARECIDA MARCELINO GARCIA, Prefeita do Município de Pimenteiras do Oeste, CPF n. ***.937.928-**;

ARMINDO LEITE RIBEIRO, Presidente da Câmara Municipal de Pimenteiras do Oeste, CPF n. ***.232.182-**;

LEONARDO BARRETO DE MORAES, Prefeito do Município de Porto Velho, CPF n. ***.330.739-**;

FRANCISCO GEDEÃO BESSA HOLANDA DE NEGREIROS, Presidente da Câmara Municipal de Porto Velho, CPF n. ***.322.762-**;

CLAUDINEIA ARAUJO DE OLIVEIRA BORTOLETE, Presidente do Instituto de Previdência e Assistência Médica dos Servidores do Município de Porto Velho, CPF n. ***.967.302-**;

SÉRGIO PEDRO DA SILVA, Prefeito do Município de Presidente Médici, CPF n. ***.381.602-**;

EDIRLEI CASSIMIRO DE OLIVEIRA, Presidente da Câmara Municipal de Presidente Médici, CPF n. ***.890.802-**;

LUCAS NUNES DA SILVA, Prefeito do Município de Primavera de Rondônia, CPF n. ***.486.692-**;

ROGÉRIO BARBOSA RODRIGUES, Presidente da Câmara Municipal de Primavera de Rondônia, CPF n. ***.267.532-**;

ÉDER DA SILVA, Prefeito do Município de Rio Crespo, CPF n. ***.164.002-**;

ODAIR JOSÉ RODRIGUES, Presidente da Câmara Municipal de Rio Crespo, CPF n. ***.786.422-**;

ALDAIR JÚLIO PEREIRA, Prefeito do Município de Rolim de Moura, CPF n. ***.990.452-**;

IVAN FERREIRA DE VASCONCELOS, Presidente da Câmara Municipal de Rolim de Moura, CPF n. ***.265.982-**;



JOSÉ LUIZ ALVES FELIPIN, Presidente do Instituto de Previdência Social dos Servidores Públicos do Município de Rolim de Moura, CPF n. ***.414.512-**;

JURANDIR DE OLIVEIRA ARAÚJO, Prefeito do Município de Santa Luzia do Oeste, CPF n. ***.662.192-**;

ALDAIR LEITE RODRIGUES, Presidente da Câmara Municipal de Santa Luzia do Oeste, CPF n. ***.881.922-**;

SIDNEY BORGES DE OLIVEIRA, Prefeito do Município de São Felipe do Oeste, CPF n. ***.774.697-**;

LEIZA MARIA SOARES, Presidente da Câmara Municipal de São Felipe do Oeste, CPF n. ***.263.872-**;

JOSÉ WELLINGTON DRUMOND GOUVEA, Prefeito do Município de São Francisco do Guaporé, CPF n. ***.811.682-**;

GEFERSON DOS SANTOS, Presidente da Câmara Municipal de São Francisco do Guaporé, CPF n. ***.654.282-**;

FLÁVIA ALVES DE ALMEIDA, Superintendente do Instituto Municipal de Previdência dos Servidores de São Francisco do Guaporé – IMPES, CPF n. ***.769.312-**;

EDILSON CRISPIN DIAS, Prefeito do Município de São Miguel do Guaporé, CPF n. ***.380.172-**;

JAIR SILVA GOMES, Presidente da Câmara Municipal de São Miguel do Guaporé, CPF n. ***.509.962-**;

GILBERTO BARBOSA SILVA, Presidente do Instituto de Previdência Social dos Servidores Públicos de São Miguel do Guaporé, CPF n. ***.728.842-**;

ARMANDO BERNARDO DA SILVA, Prefeito do Município de Seringueiras, CPF n. ***.857.728-**;

JULIANE CRESTANI, Presidente da Câmara Municipal de Seringueiras, CPF n. ***.625.902-**;

ANDRIELE APARECIDA GUEDES, Diretora Executiva do Instituto de Previdência Social dos Servidores Públicos de Seringueiras, CPF n. ***.960.242-**;

OSMY TOLEDO DE SOUZA, Prefeito do Município de Teixeiraópolis, CPF n. ***.006.472-**;



ELIZEU RODRIGUES, Presidente da Câmara Municipal de
Teixeirópolis, CPF n. ***.118.002-**;

GILLIARD DOS SANTOS GOMES, Prefeito do Município de
Theobroma, CPF n. ***.740.002-**;

ADELSON VALTER CORREIA, Presidente da Câmara
Municipal de Theobroma, CPF n. ***.560.392-**;

RICARDO LUIZ RIFFEL, Superintendente do Instituto de
Previdência Social dos Servidores Públicos de Theobroma –
IPT, CPF n. ***.657.762-**;

EZEQUIEL SALDANHA, Prefeito do Município de Urupá,
CPF n. ***.487.722-**;

JARBAS LUÍS DE ALMEIDA, Presidente da Câmara
Municipal de Urupá, CPF n. ***.656.602-**;

CLEONE LIMA RIBEIRO, Prefeito do Município de Vale do
Anari, CPF n. ***.407.462-**;

ROMILDO LEMOS DE MEIRA, Presidente da Câmara
Municipal de Vale do Anari, CPF n. ***.445.982-**;

MICHELY CRISTIANE ANTUNES DA SILVA,
Superintendente do Instituto de Previdência dos Servidores
Públicos Municipais de Vale do Anari, CPF n. ***.623.502-**;

CHARLES LUIS PINHEIRO GOMES, Prefeito do Município
de Vale do Paraíso, CPF n. ***.785.025-**;

BRUNO JOSÉ CAMATA, Presidente da Câmara Municipal de
Vale do Paraíso, CPF n. ***.740.072-**;

MARCELO JURACI DA SILVA, Presidente do Instituto de
Previdência do Município de Vale do Paraíso, CPF n.
***.817.728-**;

FLORI CORDEIRO DE MIRANDA JÚNIOR, Prefeito do
Município de Vilhena, CPF n. ***.160.068-**;

CELSON EDUARDO MACHADO, Presidente da Câmara
Municipal de Vilhena, CPF n. ***.511.701-**;

BRUNO CRISTIANO NEVES STEDILE, Presidente do
Instituto de Previdência Municipal de Vilhena, CPF n.
***.728.703-**.

RELATOR: Conselheiro Paulo Curi Neto



DM 0226/2025-GPCPN

LEVANTAMENTO. ENTES MUNICIPAIS.
PROTEÇÃO DE DADOS E SEGURANÇA
INFORMACIONAL. IMPLEMENTAÇÃO.
VERIFICAÇÃO DE CUMPRIMENTO DE
ACÓRDÃO. DETERMINAÇÕES NÃO CUMPRIDAS.
MUDANÇA DE GESTÃO. REITERAÇÃO DE
DETERMINAÇÕES.

1. O baixo índice de cumprimento das determinações pelos gestores responsáveis prejudica a eficiência do desenvolvimento de programa de capacitação dos agentes públicos para a efetiva implementação da política de proteção de dados e segurança informacional nas suas respectivas unidades jurisdicionadas e, por consequência, a afeta utilidade da inclusão de ações de controle na programação anual de fiscalizações, destinadas à avaliação dessa política e à conformidade dos atos de gestão à legislação correspondente.

2. Em que pese ser possível desde logo o sancionamento dos gestores que não comprovaram o cumprimento das determinações, considerando as dificuldades habituais relacionadas ao início de gestão nos entes públicos, afigura-se apropriado reiterar as determinações feitas, concedendo novo e improrrogável prazo para que os responsáveis comprovem nos autos seu integral cumprimento, sob pena de multa, nos termos do art. 55, inciso IV da Lei Complementar Estadual n. 154/1996, c/c. art. 103, inciso IV, do Regimento Interno desta Corte.

1. Cuidam os autos de Levantamento realizado para avaliar a implementação da Lei Federal n. 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados (LGPD), nas prefeituras, câmaras municipais e institutos de previdência dos servidores municipais do Estado de Rondônia. O objetivo principal da fiscalização foi identificar vulnerabilidades e propor medidas corretivas para garantir a proteção dos dados pessoais.

2. Efetuado o Levantamento pela Secretaria Geral de Controle Externo, com metodologia de autoavaliação de controles internos, por meio de questionários respondidos pelos gestores das entidades, o relatório técnico produzido (ID=1554276) revelou um quadro preocupante de fragilidades na implementação da LGPD, com a maioria das entidades encontrando-se em estágios iniciais de adequação, o que coloca em risco os dados pessoais dos cidadãos e expõe as entidades a possíveis sanções.

3. O Ministério Público de Contas corroborou as conclusões da peça técnica, nos termos do Parecer n. 0249/2024-GPEPSO (ID=1664144).



4. Na sequência, o egrégio Tribunal Pleno, acolhendo por unanimidade o voto deste relator, prolatou o Acórdão APL-TC 00251/24 (ID=1687216),¹ exarando, dentre outros comandos, determinações para que os gestores municipais adotassem providências para sanar as irregularidades, com prazo de 60 dias para comprovação do cumprimento.

5. A parte dispositiva do acórdão em comento consignou os seguintes comandos (destaques no original):

ACORDAM os Senhores Conselheiros do Pleno do Tribunal de Contas do Estado de Rondônia, em consonância com o Voto do Relator, Conselheiro Paulo Curi Neto, por unanimidade de votos, em:

I – Determinar aos prefeitos municipais e aos gestores dos institutos de previdência municipais, de forma integrada – ou isoladamente, mediante justificativa –, bem como aos vereadores-presidentes das câmaras municipais, todos listados no cabeçalho deste acórdão, ou a quem vier a substituí-los ou sucedê-los nos respectivos cargos, que adotem as providências necessárias para:

a) **nomear**, nos termos do art. 41 da Lei 13.709/2018, um agente público **encarregado pela proteção e tratamento de dados pessoais** (*Data Protection Officer* – DPO) e um **encarregado substituto**;

b) **instituir** um comitê ou **grupo de trabalho** para adequação da estrutura e funcionamento da instituição às exigências da LGPD;

II – Fixar o prazo de **60 (sessenta) dias**, a contar do recebimento da notificação desta Corte, via ofício, para que os gestores responsáveis **comproven nestes autos o cumprimento da determinação contida no item I**, sob pena de multa nos termos do art. 55, inciso IV, da Lei Complementar estadual n. 154/1996, c/c. o art. 103, inciso IV, do Regimento Interno desta Corte, devendo, para tanto, juntar cópias dos atos de nomeação do DPO e do comitê ou grupo de trabalho, bem como as justificativas, no caso dos gestores de institutos de previdência que optarem por fazer a nomeação em separado do Poder Executivo correspondente;

III – Ordenar, com supedâneo no art. 15-E, incisos II e III, e no art. 50, incisos I e II, ambos da Lei Complementar estadual n. 1.024, de 6 de junho de 2019, c/c. art. 246-B do Regimento Interno, que a **Secretaria-Geral de Controle Externo**, com o apoio da Secretaria Especial de Projetos Especiais em Políticas Públicas e em articulação com a Escola Superior de Contas, desenvolva **programa de capacitação** voltado à qualificação necessária e suficiente dos agentes públicos que forem designados, nos termos dos itens I e II supra, para a efetiva implementação da política de proteção de dados e segurança informacional no âmbito das unidades jurisdicionadas ora fiscalizadas;

¹ Acórdão disponibilizado no Diário Oficial do Tribunal de Contas do Estado de Rondônia nº 3225 de 19/12/2024, considerando-se como data de publicação o dia 07/01/2025, conforme certidão lançada nos autos (ID=1692901).



IV – Autorizar a Secretaria-Geral de Controle Externo a promover, **após a execução das ações de capacitação assim desenhadas**, a inclusão na programação anual de fiscalizações deste Tribunal, nos termos do art. 72, §1º, do Regimento Interno c/c. o art. 11, inciso I e §4º, da Resolução n. 268/2018/TCE-RO, as ações de controle que entender pertinentes;

V – Dar ciência aos gestores listados no cabeçalho deste decisum do aludido Guia Orientativo de Implementação da LGPD para Gestores Públicos (ID=1684961), elaborado e atualizado por este Tribunal, notificando-lhes quanto ao uso de suas balizas, em conjunto com demais documentos técnicos produzidos no país e com a legislação de regência, para a ulterior aferição da conformidade e do desempenho de suas unidades na proteção de dados pessoais;

VI – Ordenar ao Departamento do Pleno – DP-SPJ que adote as seguintes providências:

a) **notificar**, por meio eletrônico, nos termos do art. 30, caput e §2º, do RITCERO, os responsáveis designados nos itens I, II e V supra, para ciência e cumprimento de seu teor, instruindo o documento de notificação com cópia do relatório técnico (ID=1554276), deste acórdão e do Guia Orientativo de Implementação da LGPD para Gestores Públicos;

b) **dar ciência** desta decisão à Secretaria-Geral de Controle Externo, à Secretaria Especial de Projetos Especiais em Políticas Públicas e à Escola Superior de Contas, para cumprimento do item III supra;

c) **dar ciência** desta decisão ao Ministério Público de Contas, nos termos do art. 30, §10, do RITCERO;

d) promover a publicação deste acórdão no Diário Oficial Eletrônico deste Tribunal, ficando cientes os responsáveis indicados no cabeçalho de que data de publicação deve ser observada como marco inicial para possível interposição de recurso, com supedâneo no art. 22, inciso IV, c/c. o art. 29, inciso IV, da Lei Complementar n. 154/1996, bem como que o voto, o relatório técnico e o parecer ministerial, em seu inteiro teor, estão disponíveis para consulta no endereço eletrônico www.tce.ro.gov.br; e

VII – Uma vez cumpridos todos os itens acima, **arquivar** os presentes autos, após os trâmites regimentais.

6. Os prefeitos municipais, presidentes das câmaras municipais e titulares dos institutos de previdência dos servidores municipais foram devidamente notificados, tendo início o prazo para cumprimento das determinações constantes do item I (letras “a” e “b”) em 08/04/2025 e findando-se em 06/06/2025, consoante certidão de ID=1745997.

7. Vários responsáveis solicitaram prorrogação de prazo, muito embora tenham posteriormente encaminhado documentos, conforme atestado pela certidão de ID=1787573, datada de 15/07/2025. Após essa data, ainda, novos documentos foram colacionados aos autos por responsáveis, os quais foram objeto de análise pelo Corpo



Técnico, para fins de verificação do cumprimento das determinações exaradas no aludido acórdão.

8. A Unidade Técnica juntou aos autos o Relatório de Cumprimento de Decisão (ID=1828209), a 24/09/2025, com as conclusões dessa análise. Não obstante, após essa data, foi protocolizado o Documento n. 06174/25, contendo o Ofício n. 0146/GP/25/CMETOPO/RO (ID=1827677), encaminhado pelo Presidente da Câmara Municipal de Ouro Preto do Oeste, Vereador Gilvane Fernandes da Silva, com cópia da “Resolução Legislativa n. 151/2025 referente a Regulamentação da Lei de Proteção de Dados Pessoais (LGPD)” da referida Casa de Leis (ID=1827678), em a título de complemento de informação.

9. Em despacho deste relator (ID=1828047), determinou-se a juntada do documento a estes autos pela SGCE, que após cumprida a ordem, devolveu-os conclusos a este gabinete, sem análise complementar relativa ao novo documento.

10. Em todo caso, a peça técnica coligida (ID=1828209) concluiu por um baixo índice de cumprimento das determinações deste Tribunal constantes das letras “a” e “b” do item I do Acórdão APL-TC 00251/24 – erroneamente indicadas como alíneas “c” e “d” no Relatório Técnico –, pelas entidades jurisdicionadas, representando os resultados em dois gráficos, reproduzidos a seguir:

Gráfico 1 - Cumprimento de determinação, APL-TC nº 00251/24, item I, alínea c)

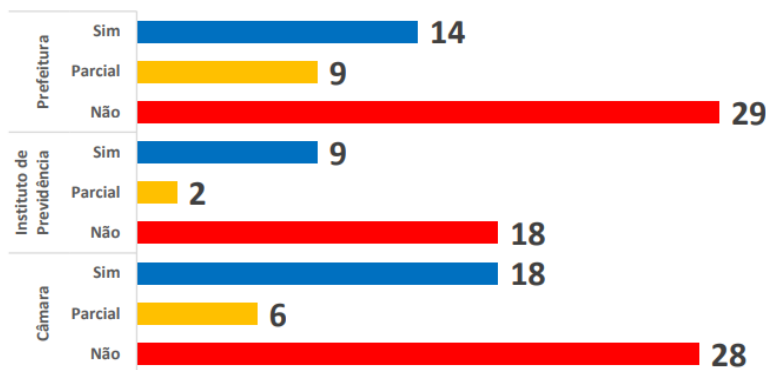
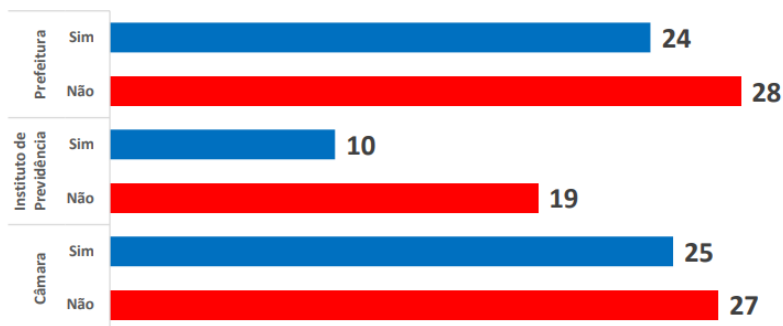


Gráfico 2 - Cumprimento de determinação, APL-TC nº 00251/24, item I, alínea d)



11. Os gráficos acima foram seguidos de listas das unidades jurisdicionadas, agrupadas conforme o cumprimento, o parcial cumprimento e o descumprimento da letra “a” do item I, consistente na nomeação de um DPO titular e de seu substituto (subitens 3.1.1, 3.1.2 e 3.1.3), e de listas conforme o cumprimento e o descumprimento da letra “b”, consistente na nomeação de comitês ou grupos de trabalho para adequação da Administração à LGPD (subitens 3.2.1 e 3.2.2). Essas mesmas listas foram reproduzidas nos anexos I a V do Relatório Técnico.
12. A par disso, de acordo com o Corpo Técnico, o descumprimento das determinações inviabiliza o cumprimento do comando expresso no item III do *decisum* em comento, destinado à própria SGCE, para desenvolvimento de programa de capacitação dos agentes públicos para a efetiva implementação da política de proteção de dados e segurança informacional nas suas respectivas unidades jurisdicionadas.
13. Por consequência, malgrado não tenha sido afirmado na peça técnica, segundo essa linha de raciocínio, estaria também inviabilizado o cumprimento da ordem expedida no item IV do acórdão supratranscrito, para inclusão de ações de controle na programação anual de fiscalizações, destinadas à avaliação dessa política e à conformidade dos atos de gestão à legislação correspondente.
14. Assim concluiu a Unidade Técnica, com subsequente proposta de encaminhamento (destaques no original):

4. CONCLUSÃO

17. A análise realizada demonstra que, embora algumas entidades tenham avançado na implementação das medidas determinadas pelo Acórdão APL-TC nº 00251/24, a maioria dos entes avaliados não cumpriram a determinação de nomeação de DPO's e instituição de comitês ou grupos de trabalho para adequação à LGPD, o que inviabiliza o cumprimento da determinação contida no Acórdão APL-TC nº 00251/24, item III, a saber:

***III – Ordenar**, com supedâneo no art. 15-E, incisos II e III, e no art. 50, incisos I e II, ambos da Lei Complementar estadual n. 1.024, de 6 de junho de 2019, c/c. art. 246-B do Regimento Interno, que a **Secretaria-Geral de Controle Externo**, com o apoio da Secretaria Especial de Projetos Especiais em Políticas Públicas e em articulação com a Escola Superior de Contas, desenvolva **programa de capacitação** voltado à qualificação necessária e suficiente dos agentes públicos que forem designados, nos termos dos itens I e II supra, para a efetiva implementação da política de proteção de dados e segurança informacional no âmbito das unidades jurisdicionadas ora fiscalizadas;*

18. Isso porque, ainda não foram designados os agentes públicos, pela maior parte dos entes avaliados, que comporão o público alvo do programa de capacitação a ser ofertado pela Escola Superior de Contas.



19. Ademais, a ausência de nomeação de DPO's e de comitês ou grupos de trabalho para adequação à LGPD compromete a conformidade legal das entidades e aumenta os riscos de vazamento de dados e responsabilização jurídica.

20. Diante do exposto, é essencial que o Tribunal intensifique as ações de controle para assegurar o cumprimento integral das determinações.

5. PROPOSTA DE ENCAMINHAMENTO

21. Diante do exposto, submetem-se os autos ao Gabinete do Excelentíssimo Senhor Conselheiro Relator Paulo Curi Neto, com base no art. 25 da Resolução nº 268/2018/TCERO, propondo:

I. Considerar cumprida a determinação **item I, alínea c) do Acórdão APL-TC nº 00251/24**, quanto a nomeação, nos termos do art. 41 da Lei nº 13.709/2018, um agente público encarregado pela proteção e tratamento de dados pessoais (DPO) e um encarregado substituto, pelas unidades jurisdicionadas listadas, conforme Anexo I deste relatório;

II. Considerar cumprida parcialmente a determinação **item I, alínea c) do Acórdão APL-TC nº 00251/24**, quanto a nomeação, nos termos do art. 41 da Lei nº 13.709/2018, um agente público encarregado pela proteção e tratamento de dados pessoais (DPO) e um encarregado substituto, pelas unidades jurisdicionadas listadas, conforme Anexo II deste relatório;

III. Considerar não cumprida a determinação **item I, alínea c) do Acórdão APL-TC nº 00251/24**, quanto a nomeação, nos termos do art. 41 da Lei nº 13.709/2018, um agente público encarregado pela proteção e tratamento de dados pessoais (DPO) e um encarregado substituto, pelas unidades jurisdicionadas listadas, conforme Anexo III deste relatório;

IV. Considerar cumprida a determinação **item I, alínea d) do Acórdão APL-TC nº 00251/24**, quanto a instituição de comitê ou grupo de trabalho para adequação da estrutura e funcionamento da instituição às exigências da LGPD, pelas unidades jurisdicionadas listadas, conforme Anexo IV deste relatório;

V. Considerar não cumprida a determinação **item I, alínea d) do Acórdão APL-TC nº 00251/24**, quanto a instituição de comitê ou grupo de trabalho para adequação da estrutura e funcionamento da instituição às exigências da LGPD, pelas unidades jurisdicionadas listadas, conforme Anexo V deste relatório;

VI. Alertar, aos gestores das unidades listados nos anexos II, III e V que a não nomeação de Encarregado de Proteção de Dados Pessoais (art. 41, caput, da Lei nº 13.709/2018 – LGPD) e a não adoção de medidas técnicas e administrativas voltadas à implementação da LGPD (arts. 6º, 46 e 50) poderão caracterizar conduta deliberada de descumprimento das normas de proteção de dados pessoais podendo ser considerada infração sujeita à aplicação de sanções pelo TCERO, nos termos do seu Regimento Interno.



VII. Dar ciência às prefeituras municipais, câmaras municipais e institutos de previdência municipais, listados nos Anexo I e IV, quanto ao cumprimento das determinações **item I, alíneas c) e d) do Acórdão APL-TC nº 00251/24**, encaminhando-lhes cópia do Relatório Técnico;

VIII. Determinar às prefeituras municipais e câmaras municipais para que no prazo de 60 (sessenta) dias após a notificação via ofício desta Corte:

a) Nomear encarregado e encarregado substituto de proteção de dados pessoais (DPO, *Data Protection Officer*), conforme unidades gestoras listadas nos anexos II, III;

b) Instituir comitê ou grupo de trabalho para adequação à LGPD, conforme unidades gestoras listadas no anexo V;

IX. Recomendar aos institutos de previdência que integrem as ações de adequação à LGPD conjuntamente com o poder executivo municipal;

15. Pois bem. À vista da análise empreendida pelo Corpo Técnico, considerando que, **de um total de 133 (cento e trinta e três) unidades jurisdicionadas**, entre prefeituras, câmaras municipais e institutos de previdência, **apenas 41 (quarenta e uma) cumpriram integralmente a determinação contida na letra “a”** do item I do Acórdão APL-TC 00251/24, **e apenas 59 (cinquenta e nove) cumpriram a determinação constante da letra “b”** do mesmo item I, forçoso é convergir com a conclusão de baixo cumprimento das determinações.

16. Conquanto não se considere inviabilizada a elaboração de programa de capacitação, pela constatação do pleno atendimento das ordens emitidas por este Tribunal por algumas dezenas de unidades jurisdicionadas, é de se convir que a deflagração de semelhante ação educacional apenas para parcela do público-alvo diminuiria a eficiência da medida, ante a necessidade de repeti-la com novos agentes públicos, à medida que fossem devidamente nomeados. Tal linha de ação, caso adotada, concorreria igualmente para ampliar a diferença entre essas unidades, relativamente à sua plena adequação aos ditames da LGPD, com a efetiva implementação da política de proteção de dados e segurança informacional.

17. Em adendo, convém ressaltar que o acórdão em comento foi prolatado ainda em dezembro de 2024, com publicação em janeiro de 2025,² de modo que coincidiu com a mudança das gestões municipais, após o pleito eleitoral realizado no ano findo.

18. **Isso em nada prejudicou a cientificação dos novos gestores**, é bom frisar, dado que as notificações foram todas cumpridas já no corrente ano de 2025,³ e tendo em vista

² Vide supra, nota 01.

³ O Ofício Circular n. 0002/25-DP-SPJ (ID=1702700), dirigido às prefeituras, foi expedido em 23/01/2025. Sobrevieram, então, diversos ofícios de notificação direcionados às câmaras municipais e institutos de previdência. Cf. IDs 1703970 a 1718402. No ensejo, os nomes dos atuais dos gestores públicos já constam do cabeçalho desta decisão.



que os comandos exarados já vinculavam eventuais substitutos e sucessores dos titulares das unidades jurisdicionadas, como visto linhas acima, sem olvido de que o **item II** da parte dispositiva do *decisum* também alertava para **cominação de multa por descumprimento**.

19. Mesmo assim, em que pese ser possível desde logo o sancionamento dos gestores que não comprovaram o cumprimento das determinações, considerando as dificuldades habituais relacionadas ao início de gestão nos entes públicos, afigura-se apropriado **reiterar as determinações feitas, concedendo novo e improrrogável prazo** para que os responsáveis comprovem nos autos seu integral cumprimento, **sob pena de multa**, nos termos do art. 55, inciso IV da Lei Complementar Estadual n. 154/1996, c/c. art. 103, inciso IV, do Regimento Interno desta Corte.

20. Desta feita, acolhendo as propostas do Corpo Técnico, **DECIDO**:

I – Considerar cumprida a determinação constante do item I, letra “a”, do Acórdão APL-TC 00251/24, quanto à nomeação de um agente público encarregado pela proteção e tratamento de dados pessoais (DPO) e de um encarregado substituto, nos termos do art. 41 da Lei n. 13.709/2018, **pelas unidades jurisdicionadas listadas no Anexo I** do Relatório de Cumprimento de Decisão (ID=1828209);

II – Considerar parcialmente cumprida a determinação constante do item I, letra “a”, do Acórdão APL-TC 00251/24, quanto à nomeação de um agente público encarregado pela proteção e tratamento de dados pessoais (DPO) e de um encarregado substituto, nos termos do art. 41 da Lei n. 13.709/2018, **pelas unidades jurisdicionadas listadas no Anexo II** do Relatório de Cumprimento de Decisão (ID=1828209);

III – Considerar não cumprida a determinação constante do item I, letra “a”, do Acórdão APL-TC 00251/24, quanto à nomeação de um agente público encarregado pela proteção e tratamento de dados pessoais (DPO) e de um encarregado substituto, nos termos do art. 41 da Lei n. 13.709/2018, **pelas unidades jurisdicionadas listadas no Anexo III** do Relatório de Cumprimento de Decisão (ID=1828209);

IV – Considerar cumprida a determinação constante do item I, letra “b”, do Acórdão APL-TC 00251/24, quanto à instituição de comitê ou grupo de trabalho para adequação da estrutura e funcionamento da instituição às exigências da LGPD, pelas unidades jurisdicionadas listadas no Anexo IV do Relatório de Cumprimento de Decisão (ID=1828209);

V – Considerar não cumprida a determinação constante do item I, letra “b”, do Acórdão APL-TC 00251/24, quanto à instituição de comitê ou grupo de trabalho para adequação da estrutura e funcionamento da instituição às exigências da LGPD, **pelas unidades jurisdicionadas listadas no Anexo V** do Relatório de Cumprimento de Decisão (ID=1828209);



VI – Reiterar as determinações contidas no item I da parte dispositiva do Acórdão APL-TC 00251/24, para que os gestores das unidades jurisdicionadas listadas nos anexos II, III e V do Relatório de Cumprimento de Decisão (ID=1828209), no prazo improrrogável de 60 (sessenta) dias após a notificação, sob pena de multa nos termos do art. 55, inciso IV, da Lei Complementar Estadual n. 154/1996, c/c. art. 103, inciso IV, do Regimento Interno deste Tribunal, comprovem nestes autos a adoção das providências a seguir, porventura não comprovadas anteriormente:

a) Nomeação de um agente público encarregado de proteção de dados pessoais (DPO, *Data Protection Officer*) e encarregado substituto, nos termos do art. 41 da Lei 13.709/2018;

b) Instituição de um comitê ou grupo de trabalho para adequação da estrutura e funcionamento da instituição às exigências da LGPD;

VII – Ordenar ao Departamento do Pleno – DP-SPJ que adote as seguintes providências:

a) notificar, por meio eletrônico, nos termos do art. 30, *caput* e §2º, do RITCERO, **os responsáveis designados no item VI supra, para ciência e cumprimento de seu teor**, instruindo o documento de notificação com cópia desta decisão e do Relatório de Cumprimento de Decisão (ID=1828209);

b) dar ciência desta decisão aos gestores das unidades jurisdicionadas listadas nos Anexos I e IV do Relatório de Cumprimento de Decisão (ID=1828209), quanto ao cumprimento das determinações item I, letras “a” e “b”, do Acórdão APL-TC 00251/24, encaminhando-lhes cópia da mencionada peça técnica;

c) dar ciência desta decisão à Secretaria-Geral de Controle Externo e ao Ministério Público de Contas, na forma regimental;

d) publicar esta decisão no Diário Oficial Eletrônico deste Tribunal, nos termos do art. 20 do RITCERO;

e) sobrestar os presentes autos no Departamento pelo prazo consignado no item VI desta decisão, ou até o envio da documentação pelos gestores nele designados, remetendo o feito, com ou sem manifestação dos responsáveis, à Secretaria-Geral de Controle Externo para análise quanto ao seu devido cumprimento.

Porto Velho/RO, datado e assinado eletronicamente.

PAULO CURI NETO
Conselheiro Relator
Matrícula n. 450





Município de Espigão do Oeste

04.695.284/0001-39

Rua Rio Grande do Sul, 2800 - Vista Alegre

www.espigaodoeste.ro.gov.br

FICHA CADASTRAL DO DOCUMENTO ELETRÔNICO

Tipo do Documento	Identificação/Número	Data
Acórdão	TCE-RO LGPD	24/11/2025

ID: 1271289	Processo	Documento
CRC: 9DF5056F		
Processo: 65-5/2025		
Usuário: Alisson Ludtke Schwanz		
Criação: 24/11/2025 10:34:08	Finalização: 24/11/2025 10:34:32	

MD5: AE4141F32E619C142B973778B0EB202E
SHA256: C11A0C6DD362879A8C6C21C1FC89E1F731AAB6A6A3D403B320CF090EE9AB10D4

Súmula/Objeto:

Solicitação de abertura imediata de processo interno para análise e implementação da resolução que institui o Comitê e as Políticas de Proteção de Dados, em atendimento ao Acórdão do TCE-RO.

INTERESSADOS

Amilton Alves de Souza	Espigão dOeste	RO	24/11/2025 10:34:08
------------------------	----------------	----	---------------------

ASSUNTOS

Abertura de processo administrativo	24/11/2025 10:34:08
-------------------------------------	---------------------

DOCUMENTOS RELACIONADOS

Ofício 6	24/11/2025	1271130
----------	------------	---------

ASSINATURAS ELETRÔNICAS

 Alisson Ludtke Schwanz	Técnico em Informática	06/02/2026 10:43:55
---	------------------------	---------------------

Assinado na forma do Resolução Municipal nº 90/2021.

A autenticidade deste documento pode ser conferida através do QRCode acima ou ainda através do site transparencia.espigaodoeste.ro.gov.br informando o ID 1271289 e o CRC 9DF5056F.



G U I A
ORIENTATIVO DE
IMPLEMENTAÇÃO
DA LGPD PARA
GESTORES PÚBLICOS

VERSÃO 1.0 - 2024



G U I A ORIENTATIVO DE IMPLEMENTAÇÃO DA LGPD PARA GESTORES PÚBLICOS

VERSÃO 1.0 - 2024



G U I A

ORIENTATIVO DE IMPLEMENTAÇÃO DA LGPD PARA GESTORES PÚBLICOS

Dados Internacionais de Catalogação na Publicação - CIP

V331g

Vasconcelos, Charles Rogério.

Guia orientativo de implementação da LGPD para
gestores públicos / Charles Rogério Vasconcelos. – Porto
Velho: TCE-RO, 2024.
189p.

ISBN 978-85-64505-18-6

1. Lei Geral de Proteção de Dados Pessoais 2. Gestão
Pública 3. Dados Pessoais 4. Direito Digital I. Título II.
Tribunal de Contas do Estado de Rondônia.

CDDir: 340

Ficha Catalográfica elaborada pela Diretoria Setorial de Biblioteca / ESCon / TCE-RO





Presidente do Tribunal de Contas do Estado de Rondônia
Wilber Carlos dos Santos Coimbra

Presidente do Comitê de Segurança da Informação e Comunicação
Francisco Junior Ferreira da Silva

Secretário-Geral de Controle Externo
Marcus César Santos Pinto Filho

Encarregado pelo Tratamento de Dados Pessoais (DPO)
Charles Rogério Vasconcelos

Elaboração
Charles Rogério Vasconcelos

Colaboração
Francisco Régis Ximenes de Almeida

Revisão
Lorena Reis Miranda

Concepção Visual, Projeto Gráfico e Editorial
Assessoria de Comunicação Social

Tribunal de Contas do Estado de Rondônia – TCERO
Assessoria de Privacidade e Proteção de Dados Pessoais – ASPPROD
Av. Presidente Dutra, 4229, Bairro Olaria – Porto Velho – RO
CEP.: 76.801-326



SUMÁRIO

Palavra do Presidente do TCERO	8
1. Apresentação	11
2. Conceitos Básicos da LGPD	14
2.1 O que é a Lei Geral de Proteção de Dados Pessoais?	15
2.2 Por que a LGPD é importante?	17
2.3 Conceitos-chave da LGPD	18
2.4 Princípios fundamentais da LGPD	21
3. Responsabilidades dos Gestores Públicos	25
3.1 Conhecimento da legislação	26
3.2 Implementação de medidas de segurança da informação	27
3.3 Designação do Encarregado pelo Tratamento de Dados Pessoais (DPO)	28
3.4 Sensibilização e capacitação dos agentes públicos	29
4. Abrangência da LGPD	31
4.1 Tipos de dados abrangidos pela LGPD	31
4.2 Instituições afetadas pela LGPD	31
4.3 Como isso se aplica aos órgãos públicos?	32
5. Tratamento de Dados Pessoais pelo Poder Público	34
5.1 Harmonização entre LGPD e LAI	34
6. O Tratamento Especial de Dados Pessoais Sensíveis	37
6.1 A natureza especial dos dados pessoais sensíveis	38
6.2 Princípios aplicáveis ao tratamento de dados pessoais sensíveis	38
6.3 Medidas adicionais de proteção aos dados pessoais sensíveis	39
7. Titulares de Dados Pessoais e seus Direitos	41



SUMÁRIO

7.1 Identificação dos titulares de dados pessoais	41
7.2 Direitos garantidos aos titulares de dados pessoais	42
8. O Papel do Encarregado pelo Tratamento de Dados Pessoais (DPO)	46
8.1 O Encarregado de Dados Pessoais (DPO)	47
8.2 Qualificação necessária do Encarregado	48
8.3 Responsabilidades do Encarregado	49
8.4 Coordenação das atividades de conformidade à LGPD	50
8.5 Independência e autonomia do Encarregado	51
9. Ouvidoria como Canal Oficial de Comunicação para a LGPD	54
9.1 Canal específico para demandas da LGPD	55
10. Mapeamento de Dados Pessoais	57
10.1 Identificação dos dados pessoais	57
10.2 Análise do fluxo de dados	59
10.3 Identificando a finalidade do tratamento	60
11. Avaliação de Riscos	62
11.1 Importância da avaliação de riscos	62
11.2 Como realizar a avaliação de riscos de forma eficaz	63
12. Relatório de Impacto à Proteção de Dados Pessoais (RIPD)	66
12.1 O Relatório de Impacto à Proteção de Dados Pessoais (RIPD)	66
12.2 Quando é necessário realizar o RIPD?	67
12.3 Etapas da Elaboração de um RIPD	68
12.4 Benefícios da realização do RIPD	69



SUMÁRIO

13. A Importância da Transparência no Tratamento dos Dados Pessoais	71
13.1 Transparência na proteção de dados pessoais e seus benefícios	73
13.2 A transparência e os benefícios para os titulares dos dados	74
14. Hipóteses Legais para o Tratamento de Dados Pessoais	77
14.1 As bases legais frequentemente utilizadas pelo poder público	78
14.2 Condições para obtenção do consentimento	81
14.3 Limitações ao uso das bases legais	83
15. Implementação de Medidas de Segurança	86
15.1 Medidas técnicas de segurança	87
15.2 Medidas organizacionais de segurança	89
15.3 Boas práticas na proteção de dados pessoais e segurança da informação nos órgãos públicos	95
16. Política de Privacidade e Cookies	98
16.1 Aviso de Privacidade ou Política de Privacidade?	98
17. Política de Proteção de Dados Pessoais (PPDP)	102
18. Política de Segurança da Informação (PSI)	105
19. Normas ABNT ISO/IEC para Apoiar a Implementação da LGPD	108
20. Modelos, Cartilhas e Guias de Boas Práticas	113
21. Programa de Governança em Privacidade (PGP)	116
22. Auditorias Internas e Monitoramento da Conformidade à LGPD	119
22.1 Importância das auditorias internas	120



121	22.2 Monitoramento contínuo da conformidade
123	22.3 Identificação de áreas de melhoria
125	23. Capacitação e Treinamento
127	23.1 Capacitação técnica para o Encarregado
127	23.2 Capacitação em LGPD e segurança da informação
129	23.3 Conscientização sobre boas práticas de proteção de dados
131	24. Cuidados com o Compartilhamento de Dados entre Órgãos Públicos
132	24.1 Importância do compartilhamento de dados entre órgãos públicos
132	24.2 Cuidados necessários no compartilhamento de dados pessoais
134	24.3 Proteção dos direitos fundamentais
136	25. Gestão de Incidente de Segurança
138	25.1 Identificação de incidentes de segurança
138	25.2 Resposta imediata e mitigação de danos
140	25.3 Notificação às autoridades e aos titulares de dados afetados
142	26. Sanções Previstas pela LGPD aos Órgãos Públicos
142	26.1 Importância do cumprimento das obrigações legais da LGPD
143	26.2 Sanções administrativas previstas pela LGPD
145	26.3 Responsabilidades individuais
147	27. A LGPD no Tribunal de Contas de Rondônia
153	28. 20 Passos Práticos para Implementação da LGPD
181	29. Glossário de Proteção de Dados Pessoais da ANPD
188	ANEXO I - Categorias e Tipos de Dados Pessoais e Sensíveis



Caro Gestor Público,



WILBER COIMBRA
Presidente do TCERO

Em um mundo cada vez mais conectado, onde a informação é um dos ativos mais valiosos, a proteção dos dados pessoais se tornou, inegavelmente, uma preocupação central para governos, empresas e cidadãos. Nesse contexto fático, a Lei Federal n. 13.709, de 14 de agosto de 2018 - **Lei Geral de Proteção de Dados Pessoais (LGPD)** surge como um marco regulatório fundamental para garantir a privacidade e a segurança das informações dos indivíduos.

À luz dessa inteligência silogístico-jurídica, traz-se a lume que a Emenda Constitucional n. 115, promulgada em 10 de fevereiro de 2022, conferiu tal proteção e acrescentou o inciso LXXIX ao artigo 5º da Constituição da República, além de garantir a proteção dos dados pessoais em nível constitucional, conferiu o status de **direito fundamental (cláusula pétrea)**.

Todo agente público tem a responsabilidade de zelar pelos dados confiados ao seu órgão, garantindo não apenas o cumprimento da legislação, mas também a preservação dos direitos fundamentais dos cidadãos. O Tribunal de Contas do Estado de Rondônia elaborou, cuidadosamente, este **Guia Orientativo de Implementação da LGPD para Gestores Públicos**, a fim de orientar nessa jornada de adequação à lei e na promoção de uma cultura de privacidade e proteção de dados nas instituições públicas.



Neste Guia, foram abordados desde os fundamentos da LGPD e sua aplicação, até as melhores práticas para a implementação de medidas de segurança da informação e mitigação de riscos de sanções. No aludido guia, encontraremos orientações extremamente úteis, exemplos ilustrativos, além de **20 passos práticos para auxiliar a conduzir os órgãos públicos rumo à conformidade legal**, resguardando a confiança dos cidadãos e evitando sanções pelos órgãos reguladores e de controle.

O **Tribunal de Contas do Estado de Rondônia** entende os desafios que a mencionada Lei Geral de Proteção de Dados Pessoais traz para toda a administração pública e reconhece as oportunidades que surgem ao priorizar o direito fundamental à proteção de dados pessoais, porque quando o gestor público investe na conformidade com a LGPD, não apenas cumpre uma obrigação legal, mas também fortalece a reputação de sua instituição, promove a transparência e estabelece uma relação de confiança com os cidadãos.

Estamos juntos nessa jornada e vamos orientá-lo na busca por transformar desafios em oportunidades, garantindo não apenas a conformidade legal, mas também a excelência na proteção dos dados pessoais sob sua responsabilidade.

Vamos começar!



1

APRESENTAÇÃO





1 APRESENTAÇÃO

O presente **Guia Orientativo de Implementação da LGPD para Gestores Públicos** tem o objetivo de delinear parâmetros que possam auxiliar os jurisdicionados - no âmbito municipal e estadual - nas atividades de adequação e de implementação da Lei Federal n. 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) nos órgãos e entidades da administração direta e indireta do Estado de Rondônia, em seus cinquenta e dois municípios. Tais orientações são fundamentais não só para garantir a correta aplicabilidade da lei, mas também para evitar a violação dos direitos do titular de dados em relação ao tratamento de dados pessoais efetuados pelo Poder Público.

As recomendações para a implementação da LGPD estão baseadas no conjunto de normas legais relacionadas com o tema, bem como com os materiais disponibilizados pelo Governo Federal.

O tratamento de dados pessoais pelo Poder Público possui muitas peculiaridades, que decorrem, em geral, da necessidade de compatibilização entre o exercício de prerrogativas estatais típicas e os princípios, regras e direitos estabelecidos na LGPD.

Diante desse cenário, o desafio posto é o de estabelecer parâmetros objetivos, capazes de conferir segurança jurídica às operações com dados pessoais realizadas pelos jurisdicionados, assegurando a celeridade e a eficiência necessárias à execução de políticas e à prestação de serviços públicos com respeito aos direitos à proteção de dados pessoais e à privacidade.





O Guia Orientativo inicia com uma breve explanação sobre os conceitos básicos, a importância e os princípios da LGPD. Na sequência, são apresentadas algumas responsabilidades dos gestores públicos frente à lei de proteção de dados pessoais, a abrangência da LGPD, os direitos dos titulares de dados, o papel do encarregado de proteção de dados pessoais (DPO), a Ouvidoria como canal de comunicação oficial, o mapeamento de dados e a avaliação de riscos, a elaboração do relatório de impacto à proteção de dados pessoais (RIPD), a importância da transparência e da identificação de bases legais para o tratamento de dados pessoais, a implementação de medidas de segurança e a criação de políticas internas, o uso de normas ISO para apoiar na implementação da LGPD, o Programa de Governança em Privacidade (PGP), a importância das auditorias internas, o processo de capacitação e treinamento dos agentes públicos.

Na parte final, são abordados os cuidados com o compartilhamento de dados pessoais entre órgãos públicos, o tratamento especial de dados pessoais sensíveis, o processo de gestão de incidentes de segurança, as sanções previstas para a administração pública, alguns marcos da LGPD no Tribunal de Contas de Rondônia. E para concluir, apresentamos 20 passos práticos para a implementação da LGPD. O Anexos I fornece alguns exemplos de categorias de dados pessoais e sensíveis, e tipos de atributos que podem ser considerados dados pessoais e sensíveis, dependendo do contexto. Os exemplos apresentados são informativos e estão pautados na LGPD, na norma ABNT NBR ISO/IEC 29100:2020 e no Guia de Inventário de Dados Pessoais do Governo Federal.





2

CONCEITOS BÁSICOS DA LGPD





2 | CONCEITOS BÁSICOS DA LGPD

Neste capítulo, iremos explorar os conceitos fundamentais da Lei Federal 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), e como eles se aplicam aos gestores públicos, com o objetivo de fornecer uma visão clara e detalhada sobre a importância da conformidade legal com a LGPD.





2.1 O que é a Lei Geral de Proteção de Dados Pessoais?

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei Federal 13.709/2018, é uma legislação brasileira que estabelece regras e diretrizes para o tratamento de dados pessoais por organizações públicas e privadas. Promulgada em agosto de 2018 e em vigor desde setembro de 2020, a LGPD visa proteger a privacidade dos cidadãos e garantir a proteção e transparência sobre o tratamento de seus dados pessoais em um mundo cada vez mais digitalizado e conectado, estabelecendo regras claras sobre como as organizações devem coletar, armazenar, utilizar e compartilhar informações pessoais que estão sob sua responsabilidade.

Baseada na GDPR (sigla em inglês de Regulamento Geral Sobre a Proteção de Dados) da União Europeia, a Lei nº 13.709/18 regulamenta todo o tratamento de dados pessoais dos cidadãos brasileiros dentro e fora do Brasil e visa proteger direitos fundamentais (art. 1º). A LGPD contempla 65 artigos, distribuídos em 10 capítulos, com normas gerais de interesse nacional, devendo ser observadas pela União, Estados, Distrito Federal e Municípios (art. 1º, parágrafo único), sob pena de aplicação de penalidades que podem variar da advertência à proibição do exercício de atividades relacionadas a tratamento de dados pessoais (art. 52 a 54).

A LGPD traz várias obrigações legais para organizações públicas e privadas que realizam o tratamento de dados pessoais, como garantir a segurança da informação, de forma clara e transparente sobre o tratamento dos dados, adotar medidas de segurança e administrativas para garantir a privacidade desde a concepção de produtos e serviços, obter o consentimento dos titulares se aplicável,





e nomear um Encarregado de Dados Pessoais (DPO) responsável por conduzir e monitorar a conformidade da instituição com a LGPD.

O termo “Poder Público” é definido pela LGPD de forma ampla e inclui órgãos ou entidades dos entes federativos (União, Estados, Distrito Federal e Municípios) e dos três Poderes (Executivo, Legislativo e Judiciário), inclusive das Cortes de Contas e do Ministério Público. Assim, os tratamentos de dados pessoais realizados por essas entidades e órgãos públicos devem observar as disposições da LGPD, ressalvadas as exceções previstas no art. 4º da lei.





2.2 Por que a LGPD é importante?

A implementação da Lei Federal 13.709/2018 (LGPD) é de extrema relevância para a administração pública em um contexto em que os dados pessoais se tornaram um recurso muito valioso. Em um mundo digitalizado, os órgãos governamentais têm acesso a uma grande quantidade de informações sensíveis dos cidadãos, como dados de saúde, raça, religião e opinião política, além de informações pessoais como nome, endereço, CPF, RG, CNH, dados de localização, entre outros. Ao garantir o cumprimento da LGPD por meio de governança, a administração pública assegura a proteção desses dados contra usos indevidos e abusivos, preservando assim a privacidade e os direitos individuais dos cidadãos.

A não conformidade com a LGPD pode ter uma série de consequências negativas para os órgãos públicos, tanto do ponto de vista operacional quanto reputacional. Além disso, o respeito à LGPD fortalece a confiança dos cidadãos nas instituições governamentais, promovendo uma relação transparente e ética entre o Estado e a sociedade. Portanto, a adoção de medidas que estejam em conformidade com a LGPD não só protege os direitos dos indivíduos, mas também reforça a legitimidade e eficácia das ações do poder público, contribuindo para uma gestão mais responsável e democrática, garantindo a privacidade e aos direitos fundamentais de liberdade e o livre desenvolvimento da personalidade dos indivíduos. Portanto, o agente público tem papel fundamental nesse processo.





2.3 Conceitos-chave da LGPD

Dados Pessoais: São informações relacionadas a uma pessoa natural identificada ou identificável.

Dado Pessoal Sensível: É o 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.

Tratamento de Dados: Compreende todas as operações realizadas com os dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Titular de Dados: É a pessoa física a quem os dados se referem, ou seja, nos termos da LGPD é qualquer pessoa natural, protegida pelo princípio da autodeterminação informativa (inciso II do art. 2º da Lei Geral de Proteção de Dados Pessoais).





Controlador: Conforme o art. 5º, IX, LGPD, o controlador recebeu a nomeação de **“agente de tratamento”**. Ele é o responsável pelas decisões referentes ao tratamento dos dados. Nos termos da LGPD é uma pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (inciso VI do art. 5º da Lei Geral de Proteção de Dados Pessoais). O controlador pode exercer diretamente o tratamento dos dados. Mas pode, também, designar um operador.

Operador: Assim como o controlador, também recebeu a nomeação de **“agentes de tratamento”** (art. 5º, IX, LGPD). O operador é aquele que realiza o tratamento em nome do controlador. Nos termos da LGPD é pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (inciso VII do art. 5º da Lei Geral de Proteção de Dados Pessoais). Ambos, controlador e operador, recebem a nomeação de **“agentes de tratamento”** (inciso IX do art. 5º da LGPD).

OBS: Para efeito de esclarecimento, segundo a Autoridade Nacional de Proteção de Dados (ANPD), servidores de um órgão público ou funcionários de uma empresa atuam em nome e sob a autoridade do controlador dos dados, ou seja, eles desempenham funções essenciais para o tratamento dos dados, mas **não são classificados como operadores**.





Encarregado: Corresponde a uma pessoa natural ou uma pessoa jurídica inequivocamente investida nessa função (que, na legislação europeia, corresponde ao Data Protection Officer - DPO). Sua incumbência é de fazer a intermediação entre o titular de dados pessoais e os agentes de tratamento, mas também entre estes agentes e a Autoridade Nacional de Proteção de Dados - ANPD - (inciso VIII do art. 5º da LGPD). A obrigatoriedade de indicação de Encarregado está prevista no art. 41 da LGPD.

O agente de tratamento é o responsável pela conformidade do tratamento dos dados pessoais, nos termos da Lei n. 13.709/2018, de 14 de agosto de 2018. (Art. 11 - Resolução CD/ANPD n. 18/2024).

Autoridade Nacional de Proteção de Dados (ANPD): A ANPD tem a missão de regular o setor de tratamento de dados pessoais. Está autorizada, portanto, a agir em proteção aos princípios e fundamentos da Lei Geral de Proteção de Dados Pessoais.





2.4 Princípios fundamentais da LGPD

A LGPD estabelece uma série de princípios fundamentais que **devem nortear o tratamento de dados pessoais e dados pessoais sensíveis**, que devem ser seguidos por todas as organizações, públicas ou privadas, que realizam o tratamento de dados pessoais e dados pessoais sensíveis. Destacam-se os seguintes princípios:

Finalidade: Os dados pessoais só podem ser coletados para propósitos específicos, legítimos e informados ao titular no momento da coleta. É vedado o tratamento posterior de forma incompatível com essas finalidades.

Necessidade: O tratamento deve ser limitado ao mínimo necessário para atingir a finalidade pretendida. O tratamento de dados deve ser realizado apenas quando necessário para o cumprimento de uma das finalidades previstas na LGPD. Isso implica em evitar a obtenção de informações excessivas ou irrelevantes em relação à finalidade do tratamento.

Adequação: A coleta de dados deve ser limitada ao mínimo necessário para a realização de suas finalidades. Os dados coletados devem ser pertinentes, proporcionais e não excessivos em relação à finalidade do tratamento.

Livre acesso: O titular dos dados tem o direito de obter do controlador a confirmação de que seus dados pessoais estão sendo tratados e, em caso positivo, obter informações de como ocorre o tratamento.





Qualidade dos dados: Os dados pessoais devem ser exatos, atualizados e completos. O controlador deve tomar medidas para garantir a qualidade dos dados pessoais.

Transparência: O controlador deve fornecer ao titular informações claras, precisas e completas sobre o tratamento de seus dados pessoais. Isso inclui fornecer detalhes sobre quais dados estão sendo coletados, como serão utilizados, por quanto tempo serão armazenados e se serão compartilhados com terceiros. As informações devem ser acessíveis e de fácil compreensão.

Segurança: Devem ser adotadas medidas técnicas e organizacionais para proteger os dados pessoais contra acessos não autorizados, destruição acidental ou ilícita, perda, alteração, comunicação ou difusão não autorizada.

Prevenção: Devem ser adotadas medidas para prevenir a ocorrência de danos aos titulares, como a perda, o uso indevido ou o acesso não autorizado aos seus dados pessoais.

Não discriminação: O tratamento de dados pessoais não pode ser realizado com o objetivo de discriminar o titular.

Responsabilização e prestação de contas: É preciso demonstrar 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.





Exemplo

Vamos considerar um exemplo real para ilustrar como os conceitos da LGPD se aplicam na prática. Imagine um órgão público que coleta informações pessoais durante um **processo seletivo** para contratação de servidores temporários. Nesse caso:

- Os candidatos são os **titulares dos dados pessoais**;
- O órgão público é o **controlador desses dados**; e
- Os servidores responsáveis pela análise das candidaturas fazem o **tratamento de dados** em nome do órgão (controlador), mas segundo a ANPD, esses servidores não são classificados como operadores.

Neste exemplo, para estar em conformidade com as diretrizes da LGPD, o órgão deve solicitar apenas as informações necessárias para avaliar as candidaturas, informar a finalidade do tratamento, obter consentimento explícito dos candidatos antes do tratamento desses dados e garantir sua segurança por meio de medidas técnicas adequadas.





3

RESPONSABILIDADES DOS GESTORES PÚBLICOS





3 | RESPONSABILIDADES DOS GESTORES PÚBLICOS

Os gestores públicos têm um papel fundamental na proteção dos dados pessoais sob sua responsabilidade. É primordial que estejam engajados na busca por conformidade com as exigências da LGPD. Isso inclui promover a implementação de medidas técnicas e administrativas aptas a proteger os dados pessoais, para assim garantir a confiança dos cidadãos em relação ao tratamento de seus dados pelo poder público, e ainda, evitar sanções.

O descumprimento da LGPD pode levar a uma série de consequências para o gestor público, incluindo sanções administrativas, processos criminais e ações de responsabilidade civil. É fundamental que os gestores públicos estejam cientes das suas obrigações em relação à proteção de dados pessoais e adotem medidas adequadas para garantir o cumprimento da legislação.

Neste contexto o gestor público está sujeito a diferentes tipos de responsabilização em caso de descumprimento da LGPD, como a responsabilização administrativa por órgãos de controle, responsabilização penal em casos graves de violação da Lei, e ainda, pode ser responsabilizado civilmente por danos causados a terceiros tendo a obrigação de indenizar por danos morais e materiais decorrentes da violação de seus direitos à privacidade e proteção de dados pessoais, entre outros.



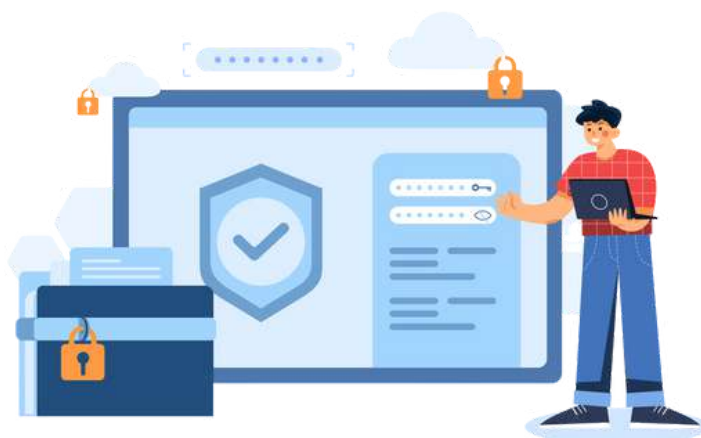


Em suma, as responsabilidades dos gestores públicos na proteção de dados são fundamentais para garantir a conformidade legal com a LGPD e a proteção da privacidade dos cidadãos. Ao implementar medidas de segurança da informação, nomear um DPO e promover a conscientização dos servidores, os gestores públicos contribuem para criar um ambiente seguro e transparente para o tratamento de dados pessoais dentro das instituições públicas.

A seguir, vamos detalhar algumas das principais responsabilidades específicas que recaem sobre os gestores públicos e como elas contribuem para a proteção da privacidade e dos direitos dos cidadãos.

3.1 Conhecimento da legislação

Os gestores públicos devem ter conhecimento das disposições e requisitos basilares da LGPD para poderem promover a implementação de políticas e procedimentos adequados no órgão público. Eles devem estar cientes das obrigações legais relacionadas ao tratamento de dados pessoais (coleta, armazenamento, uso, compartilhamento etc.).





3.2 Implementação de medidas de segurança da informação

Uma das principais responsabilidades dos gestores públicos é promover e garantir a implementação de medidas adequadas de segurança da informação para proteger os dados pessoais sob sua responsabilidade contra acessos não autorizados ou uso indevido. Isso envolve, de forma transversal, a adoção de boas práticas em termos de infraestrutura tecnológica, políticas internas, treinamentos e conscientização dos colaboradores, como por exemplo o uso de tecnologias de criptografia e autenticação, o controle de acesso aos dados, a implementação de rotinas de *backup* para restaurar informações em caso de incidentes de segurança, a realização de auditorias e monitoramento regular dos sistemas e infraestrutura de rede, entre outras medidas aplicáveis.

Exemplo

Considere um gestor público que está responsável pelo departamento financeiro em uma autarquia estadual. Ele deve **garantir que sejam adotadas medidas técnicas adequadas para proteger os dados financeiros sensíveis** dos contribuintes contra possíveis ataques cibernéticos.





3.3 Designação do Encarregado pelo Tratamento de Dados Pessoais (DPO)

De acordo com a LGPD, os órgãos públicos devem designar um Encarregado de Dados Pessoais (DPO) responsável por monitorar a conformidade com a legislação, fornecer orientações internas sobre boas práticas e atuar como ponto de contato entre a instituição, os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD). É importante que o DPO possua conhecimentos especializados sobre proteção de dados, sobre a legislação pertinente e tenha autonomia para exercer suas funções de forma eficaz e independente se reportando diretamente à alta gestão do órgão. Maiores detalhes sobre o Encarregado, como o perfil e a qualificação desejada serão abordados nos próximos capítulos.

Exemplo

Suponha que um gestor público nomeie um servidor específico como Encarregado de Dados Pessoais (DPO) em uma secretaria estadual. Essa pessoa, além de ter as competências necessárias para desempenhar a função, será **responsável por orientar e garantir que todas as atividades relacionadas ao tratamento de dados pessoais estejam em conformidade com a LGPD.**



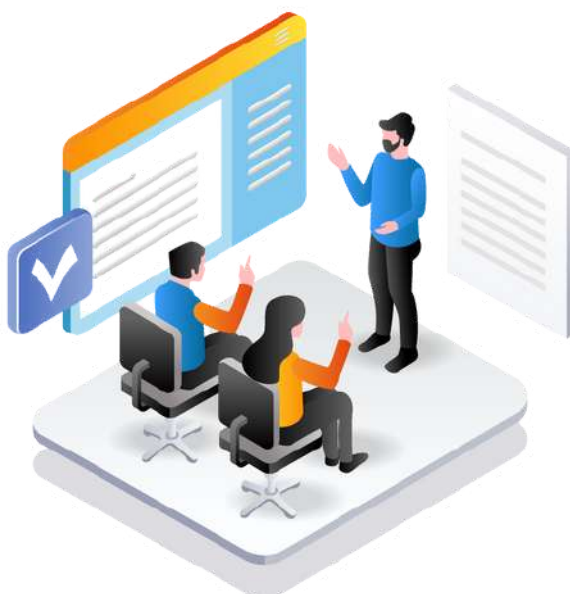


3.4 Sensibilização e capacitação dos agentes públicos

Os gestores públicos também têm a responsabilidade de promover a sensibilização e capacitação dos agentes públicos (servidores, estagiários, bolsistas etc.) sobre a importância da proteção de dados, e ainda, da necessidade de aplicação de boas práticas e medidas necessárias para garantir a conformidade com a LGPD. Isso inclui a realização de treinamentos periódicos de forma continuada, a divulgação de políticas e diretrizes internas, e o estímulo à cultura de proteção de dados dentro da instituição.

Exemplo

Um exemplo prático para evidenciar a observância dessa responsabilidade pelo gestor público é a realização de palestras, webinários, workshops, treinamentos e seminários sobre LGPD e segurança da informação para os agentes públicos do órgão.





4

ABRANGÊNCIA DA LGPD





4 | ABRANGÊNCIA DA LGPD

A Lei Geral de Proteção de Dados Pessoais tem uma abrangência significativa, aplicando-se a diversos tipos de dados pessoais e instituições, tanto do setor público quanto do setor privado. Neste capítulo, vamos explorar quais são esses tipos de dados e instituições afetadas pela LGPD e como essa legislação se aplica especificamente aos órgãos públicos.

4.1 Tipos de dados abrangidos pela LGPD

A LGPD se aplica a qualquer tipo de dado que possa identificar uma pessoa física, direta ou indiretamente. Isso inclui dados pessoais como nome, CPF, RG, endereço, telefone, e-mail, entre outros. Além disso, a LGPD também abrange dados sensíveis, que são aqueles que dizem respeito à origem racial ou étnica, convicções religiosas, opiniões políticas, filiação a sindicatos, dados genéticos, dados biométricos, entre outros, que necessitam de um cuidado especial em sua utilização.

4.2 Instituições afetadas pela LGPD

A LGPD se aplica a todas as instituições, sejam elas públicas ou privadas, que realizem o tratamento de dados pessoais. Isso inclui empresas de todos os portes, órgãos públicos dos três poderes (Executivo, Legislativo e Judiciário), autarquias, fundações públicas, empresas estatais e demais entidades governamentais, nas esferas federal, estadual e municipal.





4.3 Como isso se aplica aos órgãos públicos?

Os órgãos públicos lidam diariamente com uma grande quantidade de dados pessoais, desde informações cadastrais básicas até dados sensíveis, como informações de saúde e dados biométricos. Portanto, a LGPD se aplica integralmente aos órgãos públicos, impondo uma série de obrigações e responsabilidades aos agentes públicos para garantir a proteção da privacidade e dos direitos dos cidadãos.

Exemplo

Imagine um órgão público responsável pela emissão de documentos de identidade. Este órgão coleta uma série de informações pessoais dos cidadãos, como nome, data de nascimento, CPF, foto e impressões digitais. Com a LGPD, esse órgão **deve garantir que esses dados sejam tratados de forma segura e transparente, informando aos cidadãos sobre como suas informações serão utilizadas e protegidas.**

Exemplo

Hospitais públicos e particulares também estão sujeitos à LGPD, pois lidam com uma grande quantidade de dados pessoais de pacientes, incluindo informações médicas sensíveis. Portanto, é fundamental que, no **registro de pacientes, essas instituições implementem medidas de segurança e privacidade para proteger esses dados contra acessos não autorizados e uso indevido.**





5

TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO





5 | TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

A Lei Geral de Proteção de Dados Pessoais (LGPD), dedicou todo um capítulo (IV) ao tratamento de dados pessoais pelo Poder Público, e é neste capítulo que se buscou estabelecer o equilíbrio e harmonia entre acesso à informação e a proteção dos dados pessoais dos cidadãos sob tutela da administração pública.

5.1 Harmonização entre LGPD e LAI

A transparência dos dados sob guarda do Poder Público, possui previsão constitucional com regulação através da Lei nº 12.527/2011 (Lei de Acesso à Informação – LAI) possuindo limites na vedação de fornecimento de dados pessoais pela Administração Pública. Assim, se faz necessário **harmonizar os princípios da proteção da privacidade** (inclui-se aqui os dados pessoais e sensíveis) **e da transparência**, que estão intrinsecamente conectados e possuem limitações.

O art. 23 da LGPD, entre outros, nos traz que, o tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:





- Sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos; e
- Seja indicado um Encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 41 da LGPD.

Portanto, é imprescindível que o Poder Público esteja atento e em conformidade com os requisitos estabelecidos para o tratamento de dados pessoais. A busca pelo equilíbrio entre o acesso à informação e a proteção dos dados dos cidadãos demanda uma abordagem cuidadosa e transparente por parte das instituições públicas. É crucial que os órgãos públicos informem claramente sobre as hipóteses e finalidades do tratamento de dados, garantindo o acesso às informações de maneira clara e simplificada. Além disso, a nomeação de um Encarregado para supervisionar as operações de tratamento de dados é uma medida obrigatória para assegurar o cumprimento das disposições legais. Assim, é fundamental que o Poder Público esteja plenamente consciente de suas responsabilidades e cumpra rigorosamente os requisitos estabelecidos pela legislação, garantindo assim a proteção dos direitos dos cidadãos e o cumprimento de sua finalidade pública.





6

O TRATAMENTO ESPECIAL DE DADOS PESSOAIS SENSÍVEIS





6 | O TRATAMENTO ESPECIAL DE DADOS PESSOAIS SENSÍVEIS

A sensibilidade se estende a todos os dados pessoais dos quais dados pessoais sensíveis podem ser derivados. Por exemplo, as prescrições médicas podem revelar informações detalhadas sobre a saúde do titular de dado pessoal. Mesmo que os dados pessoais não contenham informações diretas sobre a orientação sexual ou saúde do titular, se eles puderem ser usados para inferir nessas informações, os dados pessoais poderiam ser considerados sensíveis. Para os efeitos da norma ABNT NBR ISO/IEC 29100:2020, os dados pessoais devem ser tratados como sensíveis onde tal inferência e conhecimento da identidade do titular for razoavelmente possível.

Neste capítulo, vamos explorar o tratamento especial dos dados sensíveis no contexto da administração pública, considerando as diretrizes estabelecidas pela Lei Geral de Proteção de Dados Pessoais (LGPD).

O **Anexo I deste Guia**, apresenta rol exemplificativo, e não exaustivo, de categorias e tipos de atributos que, a depender do contexto, são considerados dados pessoais e dados pessoais sensíveis em consonância com a Lei Federal 13.709/2018, a norma ABNT NBR ISO/IEC 29100:2020 e o Guia de Inventário de Dados Pessoais do Governo Federal.





6.1 A natureza especial dos dados pessoais sensíveis

Os dados pessoais sensíveis são informações que exigem um cuidado adicional devido à sua natureza particularmente sensível. Eles podem revelar aspectos como origem racial ou étnica, convicções religiosas, opiniões políticas, filiação sindical, orientação sexual, entre outros (artigo 5º, inciso II da LGPD). O tratamento desses dados requer proteção extra e adequada para garantir a privacidade e a segurança das pessoas envolvidas.

Exemplo

Um órgão público realiza pesquisas sobre saúde mental da população. Durante essas pesquisas, são coletadas informações sobre diagnósticos psicológicos e histórico de tratamentos das pessoas entrevistadas. Esses dados são considerados sensíveis por sua relação com a saúde individual e devem ser tratados com extrema cautela.

6.2 Princípios aplicáveis ao tratamento de dados pessoais sensíveis

No contexto da administração pública, o tratamento de dados pessoais sensíveis deve seguir os mesmos princípios gerais estabelecidos pela LGPD para todos os tipos de dados pessoais. Isso inclui princípios como finalidade específica, necessidade do tratamento, base legal válida para o processamento dos dados, ou o consentimento do titular quando necessário.





6.3 Medidas adicionais de proteção aos dados pessoais sensíveis

Além dos princípios gerais da LGPD, medidas adicionais devem ser implementadas no tratamento dos dados pessoais sensíveis no âmbito do órgão público. Essas medidas visam garantir uma proteção adequada às informações pessoais mais delicadas.

Ao tratar os dados pessoais sensíveis no contexto da administração pública em conformidade com as diretrizes estabelecidas pela LGPD, é possível promover um ambiente seguro onde os indivíduos se sintam protegidos em relação às suas informações mais íntimas.

Exemplo

Um órgão público cria uma política interna específica que detalha as medidas técnicas e organizacionais necessárias para proteger os dados pessoais sensíveis sob sua responsabilidade. Isso pode incluir **restrições rígidas de acesso a esses dados por parte dos servidores e a utilização de tecnologias avançadas de criptografia para garantir sua confidencialidade.**





7

TITULARES DE DADOS PESSOAIS E SEUS DIREITOS





7 | TITULARES DE DADOS PESSOAIS E SEUS DIREITOS

Segundo o artigo 17 da LGPD, toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos da Lei. A seguir veremos como identificar os titulares, bem como alguns de seus direitos previstos na LGPD.

7.1 Identificação dos titulares de dados pessoais

Os titulares de dados são as pessoas físicas às quais os dados pessoais se referem. Eles são os indivíduos sobre os quais as informações estão relacionadas, seja em âmbito pessoal ou profissional. Esses titulares podem ser usuários, funcionários, pacientes, clientes ou qualquer outra pessoa cujos dados estejam sendo tratados por uma organização pública ou privada.

A Lei Geral de Proteção de Dados Pessoais (LGPD) confere aos titulares de dados uma série de direitos que visam garantir o controle sobre suas informações pessoais e proteger sua privacidade. Neste capítulo, vamos explicar quais são esses direitos e como os gestores públicos podem assegurá-los no contexto da administração pública.





7.2 Direitos garantidos aos titulares de dados pessoais

Os direitos assegurados aos titulares de dados pela LGPD são fundamentais para garantir a privacidade e a proteção das informações pessoais dos cidadãos. Os gestores públicos têm o dever de assegurar esses direitos, implementando políticas e procedimentos adequados para garantir que os titulares de dados possam exercê-los de forma eficaz e transparente. A seguir descrevemos alguns dos direitos dos titulares previstos na LGPD.

Direito à informação: O titular tem o direito de receber informações claras sobre como seus dados pessoais serão tratados, incluindo a finalidade do tratamento, a base legal utilizada e, em caso de compartilhamento, os eventuais destinatários desses dados.

Direito ao acesso: O titular pode solicitar o acesso aos seus dados pessoais que estão sob posse da organização. Isso permite verificar a precisão das informações e saber como elas estão sendo utilizadas. Os gestores públicos devem garantir que os titulares de dados possam exercer esse direito de forma fácil e transparente, fornecendo meios específicos e adequados para solicitar acesso às suas informações.

Direito à retificação: É garantido aos titulares de dados o direito de corrigir informações incompletas, inexatas ou desatualizadas que estejam sendo processadas sobre eles. Os gestores públicos devem estabelecer procedimentos claros e eficazes para que os titulares de dados possam solicitar a retificação de suas informações pessoais quando necessário.





Direito à portabilidade: O titular pode solicitar que seus dados sejam transferidos para outra organização em um formato estruturado e legível por máquina.

Direito à não discriminação: É vedada qualquer forma de discriminação baseada nos dados pessoais do titular.

Direito à exclusão: O titular tem o direito de solicitar a exclusão dos seus dados pessoais quando não forem mais necessários para a finalidade original ou quando houver revogação do consentimento.

OBS: O Poder Público pode, em algumas situações, negar a exclusão de dados do titular, mesmo quando não mais necessários para a finalidade original do tratamento. Isso ocorre quando os dados são necessários para cumprir obrigações legais, executar políticas públicas, garantir a transparência, proteger o crédito, prevenir fraudes, garantir a segurança pública, prestar contas, preservar a memória nacional, atender ao interesse público ou para fins de pesquisa. A negativa será sempre fundamentada e o titular dos dados poderá contestá-la.

Ao conhecerem esses direitos garantidos pela LGPD, os titulares dos dados têm maior controle sobre suas informações pessoais e podem exercer um papel ativo na proteção da sua privacidade.





Exemplo 1

Uma câmara de vereadores disponibiliza uma política de privacidade em seu site oficial. Essa política deve conter **informações claras** sobre quais dados são coletados dos usuários do site, como serão utilizados (por exemplo, para responder a consultas), por quanto tempo serão armazenados e se serão compartilhados com outras entidades públicas.

Exemplo 2

Suponha que um cidadão identifique um erro em seu registro de identidade emitido por um órgão público, como a data de nascimento incorreta. Nesse caso, o gestor público deve fornecer um **canal de comunicação** para que o cidadão possa solicitar a retificação da informação e garantir que o registro seja corrigido de acordo com as disposições da LGPD.





8

O PAPEL DO ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS (DPO)





8 | O PAPEL DO ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS

Com a entrada em vigor da Lei Geral de Proteção de Dados Pessoais (LGPD), em setembro de 2020, os órgãos públicos estão obrigados a designar um Encarregado pelo Tratamento de Dados Pessoais (que, na legislação europeia, corresponde ao Data Protection Officer - DPO) para garantir o cumprimento da legislação e proteger a privacidade dos cidadãos.

A Autoridade Nacional de Proteção de Dados (ANPD) regulamentou o a atuação do Encarregado, por meio da **Resolução CD/ANPD n. 18, de 16 de julho de 2024**, que estabelece normas complementares sobre a indicação, a definição, as atribuições e a atuação do encarregado, de que trata a Lei n. 13.709/2018.

A **Norma do Encarregado** traz, entre outras, a obrigatoriedade do controlador indicar formalmente o Encarregado (e um substituto, que atuará em situações de ausência, impedimento e vacância do Encarregado); de disponibilizar em seu sítio eletrônico, de forma clara, precisa e em local de destaque e fácil acesso, a identidade e informações de contato do Encarregado; a vedação para que o Encarregado ocupe posição que acarrete conflito de interesses; que o DPO tenha 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; que seja capaz de se comunicar com os titulares e com a ANPD em língua portuguesa, e ainda, que o Encarregado não é responsável, perante a ANPD, pela conformidade do tratamento dos dados pessoais realizado pelo controlador.





Neste capítulo, vamos explorar o papel fundamental do Encarregado no processo de adequação do órgão público à LGPD, além de traçar o perfil e qualificações desejadas para exercer essa função, bem como suas responsabilidades, entre outras.

8.1 O Encarregado de Dados Pessoais (DPO)

O Encarregado pelo Tratamento de Dados Pessoais (DPO) poderá ser uma pessoa natural, integrante do quadro organizacional do agente de tratamento ou externo a esse, ou uma pessoa jurídica. Deve atuar na intermediação entre o titular e os agentes de tratamento, mas também entre estes agentes e a Autoridade Nacional de Proteção de Dados - ANPD - (inciso VIII do art. 5º da LGPD).

A indicação formal de um DPO é necessária para garantir o cumprimento da LGPD e proteger os direitos dos titulares de dados. O Encarregado é um profissional designado pelo órgão público para atuar como ponto focal na implementação e monitoramento da conformidade com a LGPD. Ele é responsável por garantir que as atividades relacionadas ao tratamento dos dados pessoais estejam adequadas à legislação.

No Tribunal de Contas do Estado de Rondônia, o Encarregado de Dados (DPO) titular é o servidor **Charles Rogério Vasconcelos**, designado por meio da Portaria n. 189/2020/TCERO, o qual possui competências em proteção e privacidade de dados, segurança da informação, e ainda conhecimento jurídico-regulatório para atuar nas frentes de implementação da LGPD na Corte de Contas.

Quem desempenha a função de Encarregada de Dados Substituta na Corte de Contas é a servidora **Karllini Porphirio Rodrigues dos Santos**, designada por meio da Portaria n. 258/2024/TCERO.





O Encarregado de Dados do TCERO também é coordenador do Programa Corporativo de Gestão da Segurança da Informação e Privacidade de Dados (PCGSIPD), membro do Comitê de Segurança da Informação e Comunicação, e do Núcleo de Governança para uso da Inteligência Artificial no Tribunal.

Já a Encarregada (DPO) substituta, atua como Gestora de Segurança da Informação e Privacidade, nos termos da Res. n. 330/2020/TCERO, e integra a Equipe de Tratamento de Resposta a Incidentes (ETIR).

Importante destacar que, é fundamental que o Encarregado e seu substituto contem com o apoio irrestrito dos gestores públicos para desempenharem adequadamente suas funções, assegurando uma efetiva governança da privacidade no órgão ao qual representam.

8.2 Qualificação necessária do Encarregado

Segundo a ANPD, cabe ao agente de tratamento estabelecer as qualificações profissionais necessárias para o desempenho das atribuições do Encarregado, considerando seus conhecimentos sobre a legislação de proteção de dados pessoais, bem como o contexto, o volume e o risco das operações de tratamento realizadas.

É desejável que um DPO tenha conhecimentos sólidos sobre a LGPD e outras leis aplicáveis, inclusive em gestão de riscos e segurança da informação. Ele deve se manter atualizado sobre as melhores práticas e possuir habilidades técnicas adequadas para realizar suas funções, interagindo diretamente com a alta gestão e com as áreas da organização, em especial junto ao jurídico e à TI.

O Encarregado é fundamental no processo de conformidade à LGPD. Executando funções de alta criticidade, ele ajuda a promover uma cultura organizacional voltada a garantir a privacidade dos cidadãos e assegurar que os direitos dos titulares sejam respeitados.





8.3 Responsabilidades do Encarregado

Durante todo o ciclo do processo de implementação e manutenção da LGPD no órgão, o Encarregado desempenha diversas funções, e elas são primordiais para o sucesso do projeto, tais como:

Assessoria: O Encarregado fornece orientações e conselhos internos sobre aplicação de boas práticas relacionadas à proteção dos dados pessoais.

Monitoramento: Ele acompanha continuamente as atividades relacionadas aos dados pessoais dentro do órgão público para garantir a conformidade com a LGPD e outras leis de proteção de dados.

Ponto focal: O DPO atua como ponto central de comunicação entre o órgão público, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), e ainda, recebe e responde a solicitações de titulares de dados relacionadas aos seus direitos previstos na LGPD.

Orientação interna: Ele deve orientar e aconselhar os agentes públicos da organização sobre as obrigações de conformidade com a LGPD, contribuindo para promover internamente uma cultura de proteção de dados.





Coordenação do Programa de Governança em Privacidade: O Encarregado deve coordenar o pleno funcionamento do Programa de Governança em Privacidade e acompanhar as atividades de proteção de dados pessoais e promover avaliações de impacto à privacidade e gestão de incidentes de segurança.

Treinamentos: Ele deve promover treinamentos internos sobre a proteção dos dados pessoais, sensibilizando a alta gestão e os colaboradores sobre suas responsabilidades e deveres.

Avaliação de conformidade: O Encarregado deve realizar avaliações regulares para verificar se os procedimentos e as políticas de segurança e de proteção de dados pessoais estão sendo aplicadas e seguidas corretamente.

O Encarregado pode executar outras atribuições definidas em atos normativos próprios do órgão ou em normas complementares.

8.4 Coordenação das atividades de conformidade à LGPD

Convém que o Encarregado coordene a implementação e o pleno funcionamento do Programa de Governança em Privacidade (PGP) do órgão, incluindo a gestão das políticas de proteção de dados pessoais e de privacidade, promovendo a aplicação das diretrizes da Lei n. 13.709/2018 (LGPD) no dia a dia da instituição.





8.5 Independência e autonomia do Encarregado

O Encarregado (DPO) deve agir com independência e autonomia para reportar diretamente à alta administração do órgão, as intercorrências ou os fatos relevantes que entender necessários, ocorridos durante a execução de suas atribuições, para assegurar uma efetiva gestão de riscos de privacidade em relação ao órgão público, sem sofrer influências indevidas ou ser penalizado por cumprir suas obrigações relacionadas à proteção dos dados pessoais. Isso garante que ele possa exercer suas funções com imparcialidade e boa-fé, em prol de preservar os direitos dos titulares.

O Encarregado deve atuar de forma que não haja conflito de interesses. O conflito de interesse pode se configurar entre as atribuições exercidas internamente em um agente de tratamento ou no exercício da atividade de Encarregado em agentes de tratamento distintos, ou com o acúmulo das atividades de Encarregado com outras que envolvam a tomada de decisões estratégicas sobre o tratamento de dados pessoais pelo controlador, ressalvadas as operações com dados pessoais inerentes às atribuições do Encarregado.

Exemplo 1

Imagine que o DPO identifique uma possível violação da LGPD dentro do órgão público. Ele deve ter liberdade para relatar essa situação à alta administração e propor soluções para mitigar a violação, independentemente das possíveis consequências negativas que isso possa acarretar.





Exemplo 2

Uma situação de conflito de interesses é quando o Encarregado acumula funções com competência para decisões referentes ao tratamento de dados pessoais. Portanto, o agente de tratamento deve atentar para que, neste contexto, o Encarregado não esteja ocupando ou venha a ocupar posição que acarrete conflito de interesses.





PROTEÇÃO DE DADOS PESSOAIS



Encarregado Titular
Charles Rogério Vasconcelos



Encarregada Substituta
Karllini Porphirio R. dos Santos



Telefone: 0800 645 8750



E-mail: encarregado.lgpd@tcero.tc.br



Endereço: Tribunal de Contas do Estado de Rondônia
Av. Presidente Dutra, 4229, Bairro Olaria
Porto Velho – RO – CEP.: 76.801-326



9

OUVIDORIA COMO CANAL OFICIAL DE COMUNICAÇÃO PARA A LGPD





9 | OUVIDORIA COMO CANAL OFICIAL DE COMUNICAÇÃO PARA A LGPD

Ter um único canal oficial para receber demandas relacionadas à LGPD é de suma importância por vários motivos. A centralização das demandas em um único canal simplifica o processo de gestão e resposta, garantindo que todas as solicitações sejam registradas, monitoradas e tratadas de forma adequada e eficiente, inclusive no controle dos prazos legais. Isso evita a dispersão de informações e a possibilidade de solicitações serem perdidas ou negligenciadas em diferentes canais de comunicação.

O Tribunal de Contas do Estado de Rondônia definiu sua Ouvidoria como canal de comunicação oficial entre o Encarregado pelo Tratamento de Dados Pessoais (DPO) do Tribunal de Contas do Estado de Rondônia, os titulares dos dados pessoais e a Autoridade Nacional de Proteção de Dados (ANPD).

Nos termos da LGPD, a Ouvidoria do TCERO atua para receber e controlar as requisições dos titulares de dados pessoais, solicitações da ANPD ou quaisquer outros expedientes que lhe sejam encaminhados sobre a Lei Geral de Proteção de Dados Pessoais, objetivando adotar providências para encaminhamento imediato ao Encarregado (DPO) do Tribunal.





9.1 Canal específico para demandas da LGPD

A criação de um canal de Ouvidoria específico para a LGPD é muito positiva, uma vez que a Ouvidoria atua de forma independente e imparcial. Isso proporciona maior confiança e garantia de tratamento adequado das demandas relacionadas à LGPD, promovendo a proteção dos direitos dos titulares de dados e fortalecendo a credibilidade do órgão público perante a sociedade.

Quando o órgão público opta por criar um canal de comunicação específico para as demandas da LGPD ele toma uma medida essencial para garantir a eficácia, transparência e legitimidade do processo de tratamento de demandas relacionadas à proteção de dados pessoais sob sua responsabilidade.

Para entrar em contato com a Ouvidoria do TCERO para tratar da LGPD, utilize os canais mencionados a seguir:



Sítio Eletrônico: <http://ouvidoria.tce.ro.gov.br>



Telefone: 0800 645 8750



E-mail: ouvidoria@tce.ro.gov.br



Endereço: Tribunal de Contas do Estado de Rondônia. Av. Presidente Dutra, 4229, Bairro Olaria – Porto Velho – RO – CEP.: 76.801-326.





10

MAPEAMENTO DE DADOS PESSOAIS





10 | MAPEAMENTO DE DADOS PESSOAIS

A etapa de mapeamento dos dados, também conhecida como de inventário de dados pessoais (IDP), serve para identificar os tipos de dados pessoais que são tratados pelo órgão. É essencial realizar um mapeamento detalhado dos fluxos de dados pessoais. Isso envolve identificar quais dados pessoais são coletados, como são utilizados, onde são armazenados, como são compartilhados e qual é a finalidade e a necessidade desse tratamento. Esse mapeamento permite ter uma visão clara do ciclo de vida dos dados pessoais na instituição.

O mapeamento de dados é uma etapa crucial no processo de conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), pois permite aos gestores públicos entenderem quais dados pessoais estão sendo tratados, de onde eles vêm, como são utilizados e para qual finalidade.

10.1 Identificação dos dados pessoais

O primeiro passo para realizar o mapeamento de dados é identificar quais tipos de dados pessoais estão sendo tratados pelo órgão público. Isso inclui dados como nome, CPF, RG, endereço, telefone, e-mail, entre outros. Os gestores públicos devem promover a realização de um levantamento completo de todos os sistemas, bancos de dados e documentos (eletrônicos e físicos) que contenham dados pessoais, identificando quais informações estão sendo coletadas, armazenadas, processadas e compartilhadas.





Objetivando auxiliar no entendimento e identificação dos dados pessoais e dados pessoais sensíveis, apresentamos no Anexo I deste Guia, rol exemplificativo, e não exaustivo, de categorias e tipos de atributos que, a depender do contexto, são considerados dados pessoais e dados pessoais sensíveis em consonância com a Lei Federal 13.709/2018, a norma ABNT NBR ISO/IEC 29100:2020 e o Guia de Inventário de Dados Pessoais do Governo Federal. O artigo 5º, inciso II da LGPD é taxativo no que se refere aos tipos de dados pessoais considerados sensíveis.

Exemplo

Um exemplo prático de identificação de dados pessoais é o mapeamento dos registros de atendimento em unidades de saúde de um órgão público. Nesse caso, os gestores públicos devem identificar quais informações pessoais são coletadas dos pacientes, como nome, idade, sexo, histórico médico, dados biométricos, entre outros.





10.2 Análise do fluxo de dados

Após identificar os dados pessoais, será preciso analisar o fluxo desses dados dentro da instituição, ou seja, como eles são tratados (coletados, armazenados, transmitidos, compartilhados e utilizados ao longo do tempo). Isso inclui identificar os pontos de entrada e saída dos dados, os sistemas e processos envolvidos em seu tratamento, e as pessoas ou setores responsáveis por seu tratamento.

Exemplo 1

Um exemplo de análise do fluxo de dados é o mapeamento do processo de solicitação e emissão de documentos em um órgão público, como carteira de identidade. Nesse caso, os gestores públicos devem identificar como os dados dos cidadãos são coletados, armazenados, processados ou compartilhados desde a solicitação do documento até a sua emissão.

Exemplo 2

Imagine que uma prefeitura realiza um inventário de dados pessoais (IDP) que lista todas as atividades relacionadas ao tratamento dos dados em seus diferentes departamentos. Esse inventário é fundamental para identificar potenciais riscos à privacidade e adotar medidas adequadas para mitigá-los de forma contínua.





10.3 Identificando a finalidade do tratamento

Por fim, será necessário documentar a finalidade para a qual os dados pessoais estão sendo tratados pelo órgão, ou seja, o motivo pelo qual estão sendo coletados, armazenados, compartilhados, utilizados etc. Isso inclui especificar se os dados estão sendo utilizados para cumprir uma obrigação legal, executar políticas públicas, realizar atividades administrativas, execução de contrato, entre outros. Essa documentação é essencial para assegurar a transparência e a conformidade com a LGPD.

Exemplo

Um exemplo de identificação da finalidade do tratamento é a especificação dos motivos pelos quais os dados pessoais dos agentes públicos são coletados e utilizados em um sistema de gestão de recursos humanos de um órgão público, como pagamento de salários, concessão de benefícios, entre outros.





11

AVALIAÇÃO DE RISCOS



11 AVALIAÇÃO DE RISCOS

A avaliação de riscos é uma etapa fundamental no processo de conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), pois permite identificar e mitigar potenciais ameaças à privacidade e segurança dos dados pessoais sob responsabilidade do órgão público. Neste capítulo, vamos discutir a importância da avaliação de riscos e como realizar essa avaliação de forma eficaz.

11.1 Importância da avaliação de riscos

Na etapa de avaliação de riscos será possível identificar ameaças internas e externas, vulnerabilidades nos sistemas e processos, e impactos potenciais em caso de incidentes de segurança ou violações de dados. Com base nessa análise, os gestores públicos devem tomar medidas proativas para mitigar os riscos e proteger os dados dos cidadãos que estão sob sua guarda.





11.2 Como realizar a avaliação de riscos de forma eficaz

Para realizar a avaliação de riscos de forma eficaz, os órgãos públicos devem seguir algumas etapas-chave, como:

- **Identificação dos ativos de dados:** Identificar todos os ativos de dados pessoais sob responsabilidade do órgão público, incluindo sistemas, bancos de dados, documentos e dispositivos;
- **Análise das ameaças e vulnerabilidades:** Identificar as ameaças potenciais à privacidade e segurança dos dados, tanto internas quanto externas, e as vulnerabilidades nos sistemas e processos que podem ser exploradas por essas ameaças;
- **Avaliação dos impactos potenciais:** Avaliar os impactos potenciais em caso de ocorrência de incidentes de segurança ou violações de dados, incluindo danos à privacidade dos cidadãos, perdas financeiras e danos à reputação da instituição; e
- **Priorização e mitigação dos riscos:** Priorizar os riscos identificados com base em sua gravidade e probabilidade de ocorrência, e tomar medidas proativas para mitigar esses riscos, como implementar controles de segurança adicionais, atualizar políticas e procedimentos internos e fornecer treinamento para os funcionários.





Exemplo 1

Um exemplo da importância da avaliação de riscos é o caso envolvendo um órgão público que sofreu um vazamento de dados devido a uma falha de segurança em seu sistema. Provavelmente, se essa instituição tivesse realizado uma avaliação de riscos prévia, poderia ter identificado a vulnerabilidade no sistema e tomado medidas para corrigi-la antes que ocorresse o incidente.

Exemplo 2

Um exemplo de realização de avaliação de riscos é o processo adotado por uma prefeitura ao implantar um sistema de gestão de documentos digitalizados. Antes de implementar o sistema, a prefeitura realizou uma avaliação de riscos para identificar potenciais ameaças à segurança dos dados e tomar medidas para mitigar esses riscos, como criptografar os arquivos digitalizados e implementar controles de acesso restrito.





12

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD)





12 | RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD)

Neste capítulo, vamos explorar o tema do Relatório de Impacto à Proteção de Dados Pessoais (RIPD) e quando é necessário realizá-lo, conforme estabelecido pela Lei Geral de Proteção de Dados Pessoais (LGPD).

12.1 O Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

O RIPD é utilizado para demonstrar os riscos identificados e associados ao tratamento dos dados pessoais. Ele tem por objetivo analisar as possíveis consequências do tratamento desses dados, especialmente aquelas que podem afetar os direitos e liberdades dos titulares.





12.2 Quando é necessário realizar o RIPD?

De acordo com a LGPD, o RIPD deve ser realizado sempre que o tratamento dos dados pessoais representar um alto risco às liberdades civis e aos direitos fundamentais dos titulares. Alguns cenários nos quais o RIPD pode ser exigido incluem:

- **Tratamento sistemático e/ou abrangente de dados sensíveis;**
- **Monitoramento em larga escala;**
- **Decisões automatizadas com base em perfis individuais;**
- **Transferência internacional de dados.**

Exemplo

Um órgão público decide utilizar um sistema automatizado para tomar decisões sobre concessão ou negação de benefícios sociais com base nos dados pessoais dos cidadãos. Nesse caso, um RIPD seria necessário para avaliar os possíveis impactos dessas decisões automatizadas sobre os direitos e liberdades dos cidadãos afetados.





12.3 Etapas da Elaboração de um RIPD

A elaboração de um RIPD deve contemplar, no mínimo, as seguintes etapas:

- **Identificar os agentes de tratamento de dados: Controlador, Operador, Encarregado (DPO);**
- **Reconhecer a necessidade de elaborar o relatório:**
 - a) Para tratamento de dados pessoais realizados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (exceções previstas pelo inciso III do art. 4º);
 - b) Quando houver infração da LGPD em decorrência do tratamento de dados pessoais por órgãos públicos (arts. 31 e 32 combinados); e
 - c) A qualquer momento sob determinação da ANPD (art. 38).
- **Descrever o tratamento: especificação da natureza, escopo, contexto e finalidade do tratamento que podem gerar riscos às liberdades civis e aos direitos fundamentais.**

É importante que o RIPD seja revisto e atualizado anualmente ou quando houver mudança que atinja o tratamento dos dados pessoais realizados pela instituição.





12.4 Benefícios da realização do RIPD

Ao considerar as circunstâncias específicas do tratamento dos dados pessoais, é fundamental determinar se a realização do Relatório de Impacto à Proteção de Dados Pessoais (RIPD) é necessário. Essa análise contribui para promover uma cultura organizacional voltada à privacidade e demonstra o compromisso da organização em garantir a proteção adequada das informações pessoais.

Ao realizar o RIPD, as organizações obtêm diversos benefícios:

- **Identificação antecipada de riscos:** A análise detalhada permite identificar potenciais riscos relacionados ao tratamento dos dados pessoais antes que eles se concretizem.
- **Implementação adequada das medidas protetivas:** Com base na avaliação realizada no RIPD, as organizações podem implementar medidas adequadas para mitigar os riscos identificados.
- **Conformidade com a LGPD:** Ao realizar o RIPD quando exigido pela lei, as organizações demonstram seu comprometimento com o cumprimento das obrigações legais estabelecidas pela LGPD.





13

A IMPORTÂNCIA DA TRANSPARÊNCIA NO TRATAMENTO DOS DADOS PESSOAIS





13 | A IMPORTÂNCIA DA TRANSPARÊNCIA NO TRATAMENTO DOS DADOS PESSOAIS

Em se tratando da Lei Geral de Proteção de Dados Pessoais (LGPD) é importante que a administração pública encontre formas adequadas para dar transparência à sociedade e aos órgãos de controle sobre suas ações advindas da LGPD.

Neste sentido, o Tribunal de Contas do Estado de Rondônia, reconhecendo a importância do tema, criou seu Portal da LGPD. O portal representa compromisso com a transparência e a conformidade com a legislação de proteção de dados pessoais. Ao disponibilizar informações detalhadas sobre as políticas, procedimentos e práticas relacionadas à LGPD, o Tribunal demonstra sua responsabilidade na gestão dos dados pessoais sob sua responsabilidade.

Além disso, o Portal da LGPD do TCERO oferece acesso facilitado servindo como um recurso valioso para consulta dos jurisdicionados e cidadãos, fornecendo informações e documentos relevantes como a política de privacidade, política de proteção de dados pessoais, política de segurança da informação, meios de contato com o Encarregado de Proteção de Dados Pessoais (DPO), orientações sobre a LGPD, bem como sobre as etapas do processo de adequação do Tribunal à Lei Geral de Proteção de Dados Pessoais, e ainda o rol de direitos dos titulares sobre a proteção de seus dados e como exercê-los perante o TCERO.



O Portal da LGPD do TCERO pode ser acessado por meio do link:

 [Portal LGPD](#)



Portanto, seguindo essas premissas, é necessário que o órgão desenvolva, entre outras, políticas de privacidade e proteção de dados transparentes e acessíveis, que detalhem o tratamento dos dados pessoais realizado pela instituição e garanta a conformidade com os requisitos da LGPD. Essas políticas devem ser elaboradas de forma a serem compreensíveis para os cidadãos e podem incluir informações sobre os tipos de dados coletados, as bases legais para o tratamento, os direitos dos titulares de dados, as medidas de segurança adotadas, os meios de contato com o Encarregado de Proteção de Dados Pessoais (DPO), entre outros.

A adoção da transparência no tratamento dos dados pessoais é crucial para garantir que os titulares estejam informados e tenham controle sobre suas informações. Ao promover essa cultura organizacional voltada à privacidade, os órgãos públicos fortalecem sua relação com os cidadãos e cumprem suas obrigações legais estabelecidas pela LGPD.

Neste capítulo, vamos explorar a importância da transparência no tratamento dos dados pessoais, conforme estabelecido pela LGPD.





13.1 Transparência na proteção de dados pessoais e seus benefícios

A transparência significa fornecer informações claras e acessíveis aos titulares dos dados sobre como seus dados pessoais estão sendo tratados (coletados, utilizados, armazenados, transmitidos, compartilhados etc.). Isso envolve garantir que os titulares tenham conhecimento das práticas adotadas pelo órgão público relacionadas ao tratamento de seus dados pessoais.

Ao adotar uma abordagem transparente no tratamento dos dados pessoais, as organizações obtêm diversos benefícios:

- **Confiança:** A transparência ajuda a construir uma relação sólida baseada na confiança entre as organizações e os titulares dos dados.
- **Cumprimento legal:** A LGPD exige que as organizações sejam transparentes no tratamento dos dados pessoais, cumprindo assim suas obrigações legais.
- **Reputação:** Uma postura transparente em relação à proteção dos dados certamente melhora a reputação organizacional perante os cidadãos.
- **Responsabilidade:** Através da transparência, as organizações demonstram sua responsabilidade quanto à proteção adequada dos direitos dos titulares.





13.2 A transparência e os benefícios para os titulares dos dados

A transparência é fundamental para promover a confiança dos titulares em relação ao tratamento de seus dados pessoais. Ela permite que os titulares estejam cientes dos propósitos do tratamento, das entidades envolvidas e das possíveis consequências desse tratamento.

Na gestão pública, a transparência pode ser assegurada por meio da disponibilização de políticas internas e externas claras sobre proteção de dados, e por meio da publicação de informações relevantes nos sites oficiais dos órgãos públicos.

Exemplo 1

Uma prefeitura desenvolveu uma política de privacidade abrangente e a disponibilizou em seu site eletrônico para os cidadãos. A política detalha como os dados pessoais são coletados, armazenados, utilizados, compartilhados e protegidos pelo órgão público, proporcionando transparência e confiança aos usuários. Essa iniciativa promove a transparência ao permitir que os cidadãos tenham acesso fácil às informações pertinentes ao tratamento de dados pessoais pela prefeitura.





Exemplo 2

Um órgão público criou um portal específico sobre a LGPD contendo informações e documentos relevantes, como sua política de privacidade, política de proteção de dados pessoais, política de segurança da informação, orientações sobre a Lei Geral de Proteção de Dados Pessoais e sobre como os cidadãos podem exercer seus direitos de proteção de dados, contato do Encarregado pelo Tratamento de Dados Pessoais (DPO), notícias e atualizações sobre o tema, assegurando transparência às ações e atividades realizadas pelo órgão na busca por conformidade legal.





14

HIPÓTESES LEGAIS PARA O TRATAMENTO DE DADOS PESSOAIS



14 | HIPÓTESES LEGAIS PARA O TRATAMENTO DE DADOS PESSOAIS

O tratamento de dados pessoais pelos órgãos públicos está sujeito a diversas hipóteses ou bases legais previstas na Lei Geral de Proteção de Dados Pessoais (LGPD), que determinam as condições em que os dados podem ser processados.

Uma das principais providências a serem tomadas antes de realizar o tratamento de dados pessoais é a de identificar a base legal aplicável. O tratamento de dados pessoais pelo Poder Público deve se amparar em uma das hipóteses previstas no art. 7º ou, no caso de dados sensíveis, no art. 11 da LGPD. Esses dispositivos devem ser interpretados em conjunto e de forma sistemática com os critérios adicionais previstos no art. 23, que complementam e auxiliam a interpretação e a aplicação prática das bases legais no âmbito do Poder Público, conforme será demonstrado.

As bases legais e as condições para obtenção do consentimento são fundamentais para garantir a conformidade com a LGPD e proteger a privacidade dos cidadãos. Ao seguir as disposições da legislação e garantir que o tratamento de dados seja realizado de acordo com as bases legais adequadas, os órgãos públicos promovem a confiança dos cidadãos na administração pública e garantem o respeito aos direitos de privacidade e proteção de dados.

Neste capítulo, vamos explorar as bases legais mais comuns no poder público e as condições para obtenção do consentimento quando necessário.





14.1 As bases legais frequentemente utilizadas pelo poder público

A LGPD estabelece diversas bases legais que permitem o tratamento de dados pessoais pelos órgãos públicos, considerando as peculiaridades do Poder Público, nos limitaremos a descrever apenas as seguintes bases legais:

- **Cumprimento de obrigação legal ou regulatória:** O tratamento é necessário para o cumprimento de uma obrigação legal ou regulatória pelo órgão público. Vale destacar que essa interpretação do conceito de obrigação legal, conforme previsto no art. 7º, II, e no art. 11, II, a, da LGPD, é reforçada pelo disposto no art. 23 da mesma lei, segundo o qual o tratamento de dados pessoais no setor público deverá ser realizado “com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público”, observando-se o interesse público e o atendimento da finalidade pública do controlador.
- **Execução de políticas públicas:** O inciso III do art. 7º da LGPD estabelece que a “administração pública” pode realizar “o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres”. Por sua vez, em relação aos dados sensíveis, o art. 11, II, b, refere-se ao “tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos”.





- **Legítimo Interesse:** A base legal do legítimo interesse autoriza o tratamento de dados pessoais de natureza não sensível quando necessário ao atendimento de interesses legítimos do controlador ou de terceiros, “exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais” (art. 7º, IX). Trata-se, portanto, de base legal não aplicável ao tratamento de dados pessoais sensíveis.

Por ser uma base legal mais flexível, sua adoção deve ser precedida de uma avaliação em que seja demonstrada a proporcionalidade entre, de um lado, os interesses do controlador ou de terceiro para a utilização do dado pessoal e, de outro, os direitos e as legítimas expectativas do titular. Além disso, deve-se considerar que, conforme o art. 18, § 2º, o titular tem o direito de se opor ao tratamento realizado com base no legítimo interesse, em caso de descumprimento dos requisitos previstos na LGPD.

- **Consentimento:** Conforme a definição legal (art. 5º, XII, LGPD), o consentimento é a “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”. Adicionalmente, no caso de dados sensíveis, o consentimento deve ser fornecido “de forma específica e destacada, para finalidades específicas” (art. 11, I, LGPD).

Assim, a autorização do titular deve ser intencional e ele deve saber exatamente para que fim seus dados serão tratados, sendo vedada a autorização tácita e para finalidades genéricas. Além disso, o consentimento pressupõe uma escolha efetiva entre autorizar e recusar o tratamento dos dados pessoais, incluindo a possibilidade de revogar o consentimento a qualquer momento.





Diante dessas características, em muitas ocasiões, o consentimento não será a base legal mais apropriada para o tratamento de dados pessoais pelo Poder Público, notadamente quando o tratamento for necessário para o cumprimento de obrigações e atribuições legais. Nesses casos, o órgão ou a entidade exerce prerrogativas estatais típicas, que se impõem sobre os titulares em uma relação de desbalanceamento de forças, na qual o cidadão não possui condições efetivas de se manifestar livremente sobre o uso de seus dados pessoais.

Exemplo

Quando um órgão público coleta informações sobre os cidadãos para a emissão de documentos de identidade. Nesse caso, o tratamento dos dados é justificado pelo cumprimento de uma obrigação legal, já que o órgão público é responsável por emitir documentos de identificação conforme a legislação vigente.





14.2 Condições para obtenção do consentimento

O consentimento é uma das bases legais para o tratamento de dados pessoais. Em alguns casos, o tratamento pelos órgãos públicos pode exigir o consentimento do titular dos dados. Para que o consentimento seja válido, deve ser fornecido de forma livre, informada e inequívoca, mediante manifestação específica do titular. Além disso, o consentimento deve ser obtido para finalidades específicas e destacadas, não podendo ser considerado como consentimento tácito.

Desta forma, o consentimento representa a manifestação livre, informada e inequívoca do titular dos dados concordando com a utilização de suas informações pessoais por parte da organização para finalidade específica.

Exemplo 1

Um órgão público de educação realiza uma pesquisa social para avaliar o acesso à educação em uma determinada região. Os resultados da pesquisa serão utilizados para identificar barreiras ao acesso à educação e propor políticas públicas mais eficazes.

Para coletar dados socioeconômicos dos cidadãos, como renda, nível de escolaridade e condições de moradia, o consentimento livre e informado é necessário para garantir a proteção da privacidade e o uso responsável das informações.

Ao participar da pesquisa, os cidadãos devem ser informados sobre os objetivos da pesquisa, como os dados serão coletados, armazenados e utilizados, além de ter o direito de negar o consentimento ou retirá-lo posteriormente.



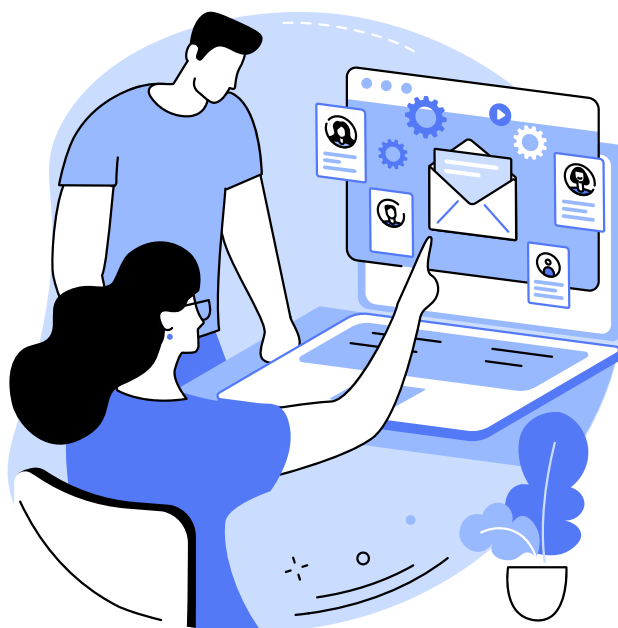


Exemplo 2

Um órgão público realiza um estudo de opinião para avaliar a percepção dos cidadãos sobre políticas públicas específicas. Os resultados da pesquisa serão utilizados para aprimorar as políticas públicas e atender às necessidades da população.

Para coletar dados de opinião dos cidadãos, como satisfação com serviços públicos, confiança em instituições e expectativas para o futuro, o consentimento livre e informado é fundamental para garantir a proteção da privacidade e o uso imparcial das informações.

Ao participar do estudo, os cidadãos devem ser informados sobre os objetivos da pesquisa, como os dados serão coletados, armazenados e utilizados, além de ter o direito de negar o consentimento ou retirá-lo posteriormente.





14.3 Limitações ao uso das bases legais

É importante destacar que tanto o consentimento quanto as outras bases legais têm limitações específicas:

- **Princípio da necessidade:** Mesmo quando há base legal válida, apenas os dados estritamente necessários devem ser coletados e utilizados.
- **Proteção especial:** A LGPD exige proteção especial para determinadas categorias sensíveis de dados pessoais (por exemplo, saúde ou origem racial) independentemente da base legal utilizada.
- **Consentimento informado:** Nos casos em que o poder público necessite utilizar a base legal do consentimento, ele deve ser livre e informado ao titular dos dados pessoais. No entanto, para que seja válido, é crucial que os titulares recebam informações claras e completas sobre como seus dados serão utilizados. Isso significa:
 - a) **Propósito:** Detalhar os objetivos específicos do tratamento de dados.
 - b) **Consequências:** Esclarecer as implicações e os impactos do tratamento para o titular.
 - c) **Uso:** Especificar como os dados serão utilizados, por quem e para quais finalidades.
 - d) **Direitos:** Informar o titular sobre seus direitos em relação aos dados, como acesso, correção, exclusão e portabilidade.





Ao considerar as diferentes bases legais no setor público, é fundamental garantir que todas as atividades relacionadas ao tratamento dos dados pessoais estejam em conformidade com a LGPD e respeitem os direitos fundamentais dos titulares.

Exemplo

Um hospital público precisa coletar informações médicas detalhadas sobre seus pacientes. Mesmo que haja uma base legal válida (cumprimento de obrigação legal), ele deve garantir que apenas os profissionais autorizados tenham acesso a essas informações e que elas sejam protegidas adequadamente contra acessos indevidos.





15

IMPLEMENTAÇÃO DE MEDIDAS DE SEGURANÇA





15 | IMPLEMENTAÇÃO DE MEDIDAS DE SEGURANÇA

A implementação de medidas técnicas e organizacionais adequadas é fundamental para garantir a segurança da informação e proteger os dados pessoais contra acessos não autorizados ou uso indevido. Isso envolve a adoção de controles físicos e lógicos, políticas internas claras, procedimentos operacionais padronizados, além da criação de Comitê de Privacidade e Proteção de Dados Pessoais, e a nomeação de Encarregado pelo Tratamento de Dados Pessoais (DPO).

Neste contexto, a segurança da informação desempenha um papel crucial na proteção das informações sob guarda dos órgãos públicos, especialmente à luz da Lei Geral de Proteção de Dados Pessoais (LGPD).

Neste capítulo, destacamos algumas medidas técnicas e organizacionais, mínimas, que os gestores públicos devem implementar para aprimorar a segurança da informação e a proteção dos dados pessoais sob sua responsabilidade, para assim mitigar riscos e proteger a privacidade dos cidadãos, promovendo a confiança na administração pública e o cumprimento da LGPD.





15.1 Medidas técnicas de segurança

As medidas técnicas de segurança visam proteger os sistemas de informação e os dados pessoais contra acessos não autorizados, ataques cibernéticos e outros riscos de segurança. Algumas das principais medidas técnicas que os órgãos públicos devem implementar incluem:

- **Criptografia de dados:** Utilizar técnicas de criptografia para proteger os dados pessoais durante sua transmissão e armazenamento, garantindo que apenas pessoas autorizadas possam acessá-los.
- **Controles de acesso:** Implementar controles físicos e lógicos é essencial para proteger os dados pessoais contra acessos não autorizados ou uso indevido. Isso envolve a adoção de medidas como controle de acesso às instalações físicas por meio de identificação biométrica ou cartões eletrônicos, além da utilização de senhas fortes, autenticação multifatorial e políticas de acesso baseadas em funções, criptografia e firewalls para proteger os sistemas computacionais.
- **Atualizações de segurança:** Manter os sistemas e aplicativos atualizados com as últimas correções de segurança e patches de software para proteger contra vulnerabilidades conhecidas.





Exemplo 1

Um exemplo de medida técnica de segurança é a implementação de um sistema de firewall em rede para monitorar e controlar o tráfego de dados entre a rede interna de um órgão público e a internet, ajudando a proteger o ambiente organizacional do órgão contra ataques cibernéticos.

Exemplo 2

Imagine que um órgão público, como forma de implementar medidas de segurança, adota técnicas de criptografia para proteger os dados em trânsito ou em repouso nos sistemas internos. Além disso, estabelece políticas claras sobre o acesso às informações confidenciais apenas por pessoas autorizadas.

Exemplo 3

Outro exemplo de aplicação de medidas técnicas de segurança é quando uma autarquia estadual investe na instalação de câmeras com monitoramento em suas dependências físicas para controlar o acesso aos locais onde são armazenados os documentos contendo dados pessoais sensíveis. Além disso, implementa controles lógicos avançados nos servidores que processam esses dados.





15.2 Medidas organizacionais de segurança

Além das medidas técnicas, os órgãos públicos também devem implementar medidas organizacionais de segurança para promover uma cultura de segurança da informação e garantir a conformidade com a LGPD. Algumas dessas medidas incluem:

- **Criação de Comitê de Privacidade e Proteção de Dados Pessoais:** Instituir um Comitê de Privacidade e Proteção de Dados Pessoais é fundamental para a governança de dados no órgão público. Sua criação permite centralizar as decisões estratégicas sobre proteção de dados pessoais, promover uma cultura de compliance e fortalecer a transparência nas ações do órgão

É importante que seja composto por membros de diferentes áreas da organização. O Comitê atua de forma colegiada para definir diretrizes, implementar políticas e monitorar o cumprimento da LGPD. Entre suas funções estratégicas, podemos destacar:

- a) **Integração com o Encarregado (DPO):** O Comitê deve atuar de forma integrada com o Encarregado pelo Tratamento de Dados Pessoais (DPO) para que de forma conjunta, promovam no órgão ações inerentes à LGPD na busca por conformidade legal, inclusive, apoiando e fiscalizando a atuação do DPO.
- b) **Análise e avaliação de riscos:** O Comitê identifica e avalia os riscos relacionados ao tratamento de dados pessoais, propondo medidas de mitigação e controle adequadas.





- c) **Orientação e assessoria:** O Comitê, em consonância com o Encarregado (DPO), deve orientar e assessorar os agentes públicos sobre a aplicação da LGPD, esclarecendo dúvidas e fornecendo suporte técnico necessário.
- d) **Promoção da cultura de privacidade:** O Comitê promove a cultura de privacidade dentro da organização, sensibilizando servidores e colaboradores para a importância da proteção dos dados pessoais sob responsabilidade do órgão.
- e) **Gestão de incidentes:** O Comitê atua na gestão de incidentes de segurança da informação e violações de dados, definindo a adoção de medidas de resposta e contenção adequadas.
- f) **Conformidade:** O Comitê deve promover avaliações internas de conformidade do órgão com leis e regulamentos de segurança da informação, privacidade e proteção de dados pessoais buscando identificar lacunas e áreas de melhoria.

Ao instituir um Comitê de Privacidade e Proteção de Dados Pessoais, a Administração Pública demonstra seu compromisso com a proteção dos dados dos cidadãos e com a construção de uma cultura de compliance em toda a organização. O Comitê assume um papel fundamental na governança de dados, contribuindo para a efetividade da LGPD e para a construção de uma relação de confiança com a sociedade.





- **Nomeação do Encarregado pelo Tratamento de Dados Pessoais (DPO):** Designar um DPO é essencial para o cumprimento das obrigações legais e o fortalecimento da confiança dos cidadãos no tratamento de seus dados pelo Estado. A LGPD instituiu o Encarregado como figura crucial para a construção de uma cultura de proteção de dados nas organizações.

O DPO assume um papel estratégico na criação de um ambiente seguro e transparente para o tratamento de dados pessoais. Sua atuação garante a implementação de medidas eficazes de segurança da informação, a realização de treinamentos para os agentes públicos e a promoção da sensibilização sobre a LGPD em todo o órgão. Além disso, atua como canal de comunicação entre o órgão e a Autoridade Nacional de Proteção de Dados (ANPD), facilitando a resolução de dúvidas e a investigação de eventuais violações.

- **Criação de Grupos de Trabalho:** Estabelecer grupos de trabalho permite a criação de uma equipe multidisciplinar, reunindo profissionais de diferentes áreas com conhecimentos e experiências diversas, o que enriquece o processo de implementação e contribui para a identificação de soluções mais abrangentes para o enfrentamento dos desafios inerentes à LGPD. Isso facilita a divisão de tarefas e responsabilidades, permitindo uma abordagem mais ágil e eficiente na execução das atividades relacionadas à implementação da lei, além de promover a colaboração e o alinhamento transversal entre as diversas áreas do órgão público, possibilitando a integração de políticas, processos e sistemas de forma mais coordenada e coesa.





Certamente a criação de grupos de trabalho auxiliará na troca de conhecimentos, experiências e boas práticas entre os membros, promovendo o aprendizado contínuo e a melhoria constante dos processos de privacidade e proteção de dados pessoais na instituição.

- **Registro de evidências das ações realizadas:** Registrar com evidências as ações realizadas pelos grupos de trabalho durante a implementação da LGPD no órgão público é fundamental. Pois, com o registro detalhado das atividades é possível acompanhar o progresso das iniciativas, identificar eventuais desafios e tomar medidas corretivas ou preventivas conforme necessário. Além disso, o registro fornece uma documentação robusta que pode ser utilizada para prestar contas às partes interessadas, como a alta administração, os órgãos reguladores e a sociedade em geral, demonstrando transparência e comprometimento com a conformidade legal. Essas evidências também são importantes para fins de auditoria interna e externa, possibilitando a verificação da eficácia dos processos implementados e a identificação de áreas de melhoria.

O registro das ações também permite criar um histórico que pode ser utilizado para fins de aprendizado e capacitação, permitindo a disseminação de boas práticas e lições aprendidas para futuros projetos ou iniciativas relacionadas ao tema no âmbito da organização.





- **Políticas internas claras:** Estabelecer políticas internas claras é fundamental para orientar as práticas relacionadas à segurança da informação, privacidade e proteção de dados pessoais nos órgãos públicos. Essas políticas devem abordar questões como o tratamento dos dados pessoais, uso adequado dos recursos tecnológicos, proteção contra ameaças cibernéticas, gestão de incidentes de segurança e descarte seguro das informações. Propondo diretrizes para o tratamento seguro dos dados e informações, promovendo a conscientização dos agentes públicos do órgão sobre as melhores práticas de segurança a serem adotadas no ambiente organizacional.
- **Treinamento e sensibilização:** Promover a sensibilização dos agentes públicos sobre as práticas adequadas relacionadas à segurança da informação é um aspecto crucial na garantia da privacidade e proteção dos dados pessoais. Treinamentos periódicos devem ser realizados para fornecer informações atualizadas sobre ameaças cibernéticas, phishing, engenharia social, entre outros temas relevantes. Os agentes também devem ser orientados sobre suas responsabilidades individuais no tratamento e na proteção dos dados pessoais.

É importante orientar sobre como reconhecer e relatar ameaças de segurança, criar e proteger senhas fortes e dados confidenciais, e agir de acordo com as diretrizes das políticas internas.

- **Gestão de incidentes de segurança:** Desenvolver e implementar um plano de resposta a incidentes de segurança que estabeleça procedimentos claros para detectar, relatar e responder a incidentes de segurança, incluindo a notificação adequada às autoridades competentes e aos titulares de dados afetados.





Exemplo

Como forma de demonstrar a implementação de medidas técnicas organizacionais, um órgão público atualiza sua política interna de segurança da informação para incluir diretrizes específicas relacionadas à proteção dos dados pessoais. Essa política estabelece procedimentos claros em relação ao acesso aos sistemas computacionais que processam esses dados, bem como orientações sobre requisitos legais para o tratamento e uso seguro das informações pessoais que estão sendo tratadas.

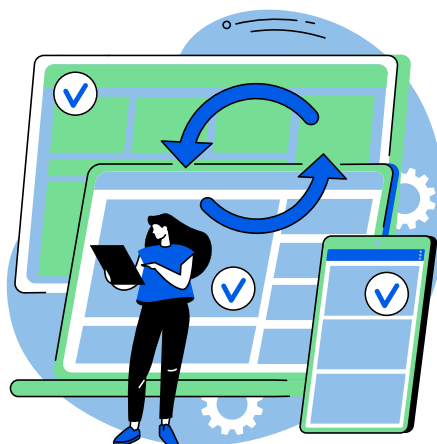




15.3 Boas práticas na proteção de dados pessoais e segurança da informação nos órgãos públicos

A aplicação de boas práticas na conformidade com a LGPD e os exemplos de casos de sucesso na proteção de dados e segurança da informação demonstram o compromisso dos órgãos públicos com a proteção da privacidade dos cidadãos e o cumprimento da legislação de proteção de dados pessoais. Ao seguir esses exemplos e implementar medidas eficazes de proteção de dados, os órgãos públicos podem promover a confiança dos cidadãos na administração pública e garantir a integridade e confidencialidade das informações pessoais. Abaixo temos alguns exemplos da aplicação de boas práticas, diante do contexto:

- Um órgão estadual implementou um programa de treinamento contínuo para sensibilização de seus agentes públicos em segurança da informação, privacidade e proteção de dados pessoais, que inclui treinamentos regulares com especialistas sobre práticas seguras de tratamento de dados pessoais, prevenção a ameaças de engenharia social, phishing e procedimentos para relatar incidentes de segurança.





- Uma câmara de vereadores de um município implementou um sistema de gestão de incidentes de segurança da informação, que permite o registro e acompanhamento de incidentes relacionados à proteção de dados. Isso permitiu à Câmara identificar e responder rapidamente a potenciais violações de segurança, protegendo assim a privacidade dos cidadãos.
- Uma secretaria estadual implementou medidas de segurança robustas em seus sistemas de arrecadação tributária, incluindo criptografia de dados, controles de acesso baseados em função e monitoramento contínuo para identificar atividades suspeitas. Isso garantiu a integridade e confidencialidade dos dados, protegendo assim os direitos dos cidadãos.
- Uma prefeitura promoveu ação de sensibilização entre seus agentes públicos sobre os riscos de phishing e forneceu treinamento sobre como identificar e evitar esse tipo de ataque. Isso ajudou a reduzir o número de incidentes de segurança relacionados a phishing, ampliando a proteção dos dados pessoais e das informações confidenciais da prefeitura.





16

AVISO DE PRIVACIDADE OU POLÍTICA DE PRIVACIDADE?





16 | AVISO DE PRIVACIDADE OU POLÍTICA DE PRIVACIDADE?

A Política de Privacidade e Cookies cumpre, fundamentalmente, o dever de transparência disposto como princípio na LGPD, tendo como objetivo descrever ao titular dos dados pessoais, os procedimentos e processos adotados no tratamento de dados pessoais realizado pelo serviço, bem como informá-lo sobre as medidas de proteção de dados pessoais adotadas.

16.1 Aviso de Privacidade ou Política de Privacidade?

A Norma **ABNT NBR/ISO 29100:2020** discorre que o termo “política de privacidade” é frequentemente usado para se referir a políticas de privacidade internas e externas. Uma **política de privacidade interna** documenta os objetivos, regras, obrigações, restrições e/ou controles adotados por uma organização para atender aos requisitos de proteção de privacidade pertinentes para o tratamento de dados pessoais. Uma **política de privacidade externa** fornece às pessoas de fora da organização um aviso das práticas de privacidade da organização, bem como outras informações pertinentes, como identidade e endereço oficial do controlador de dados pessoais, pontos de contato dos quais os titulares de DP podem obter informações adicionais etc.





Neste Guia, utiliza-se o termo “**política de privacidade**” para se referir à política externa, voltada ao titular dos dados pessoais. Porém, caso julgue mais adequado, o órgão ou entidade pode utilizar o termo “**aviso de privacidade**”, nos termos da **ABNT NBR/ISO 29184:2021** para a política externa, principalmente quando já possui uma política de privacidade interna ou a esteja elaborando.

É importante notar que ambos os termos não estão presentes na LGPD mas são frequentemente utilizados de forma intercambiável pelas organizações.

O sítio eletrônico do Tribunal de Contas do Estado de Rondônia e seus portais possuem política de privacidade, que foi regulamentada por meio da Resolução Administrativa nº 352/2021/TCERO, estando disponível no seguinte link:



[Política de Privacidade](#)



A referida Resolução Administrativa instituiu também a política de cookies do TCERO.





Em observância aos princípios da publicidade e da transparência, e a fim de garantir aos cidadãos amplo acesso às informações dos dados pessoais, a política de privacidade deve:

- Ser editada em linguagem acessível, clara e simples;
- Apresentar informações precisas sobre a realização do tratamento dos dados pessoais do cidadão;
- Ser exposta em local de fácil acesso e visualização;
- Deixar de forma clara como o usuário pode apresentar eventual manifestação sobre as finalidades de coleta, uso, armazenamento, tratamento e proteção dos dados pessoais dos usuários; e
- Ser constantemente atualizada.

Exemplo

Um exemplo da importância da política de privacidade é o caso de um órgão público que coleta informações pessoais de seus cidadãos para fornecer serviços online, como agendamento de consultas médicas. Uma política de privacidade clara e acessível seria essencial para informar aos cidadãos como seus dados serão utilizados e protegidos durante o processo de agendamento.





17

POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS (PPDP)





17 | POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS (PPDP)

Uma Política de Proteção de Dados Pessoais (PPDP) 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 papéis 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 pelo órgão.

O Governo Federal disponibilizou por meio da Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos, um Modelo editável que visa 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.





O modelo disponibilizado pelo Governo Federal deve ser utilizado exclusivamente como referência, devendo o órgão ou entidade considerar as particularidades técnicas específicas do seu ambiente, bem como observar a boa aderência aos processos internos a fim de construir uma política que seja adequada a sua realidade.

Link do modelo:



[Governo Digital - Política de Privacidade](#)



Exemplo

Imagine que um órgão público desenvolve uma política interna que define os procedimentos específicos para o manuseio e armazenamento dos documentos contendo dados pessoais sensíveis. Essa política inclui diretrizes claras sobre como esses documentos devem ser tratados durante todo o ciclo de vida, desde sua criação até seu descarte final.





18

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)





18 | POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

A criação de uma Política de Segurança da Informação (PSI) possibilita ao órgão público estabelecer e fortalecer diretrizes para apoiar no processo de identificação e avaliação de riscos, considerando a estratégia e os objetivos globais de negócios; os requisitos legais, estatutários, regulamentares e contratuais que as partes interessadas (parceiros comerciais, prestadores de serviços etc.) têm que cumprir, e o conjunto de princípios, objetivos e requisitos de negócios para todas as etapas do ciclo de vida das informações objetivando apoiar suas operações, assegurando a confidencialidade, a integridade e a disponibilidade dos dados, das redes e dos sistemas de informação utilizados pelo órgão.

É importante destacar que uma “Política de Segurança da Informação” deve extrapolar o escopo abrangido pelas áreas de sistemas de informação e recursos computacionais, ou seja, como previsto nas normas ISO da família 27000, **a PSI não deve ficar restrita à área de informática**, ao contrário, ela deve estar integrada à visão, à missão, ao negócio e às metas institucionais, bem como ao plano estratégico de informática e às políticas da instituição concernentes à segurança em geral.

A norma **ABNT NBR ISO/IEC 27002:2022** nos traz que a segurança da informação é obtida pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware, complementando que esses controles precisam ser estabelecidos, implementados, monitorados, revisados e melhorados quando necessário, para assegurar que a segurança e os objetivos específicos do negócio sejam atendidos.





Neste sentido, o Tribunal de Contas da União (TCU), no item 9.1.3 do Acórdão nº 1.603/2008, recomendou a vários órgãos federais que orientem sobre a importância do gerenciamento da segurança da informação, promovendo, inclusive mediante normatização, ações que visem estabelecer e/ou aperfeiçoar a gestão da continuidade do negócio, a gestão de mudanças, a gestão de capacidade, a classificação da informação, a gerência de incidentes, a análise de riscos, a área específica para gerenciamento da segurança da informação, a política de segurança da informação e os procedimentos de controle de acesso.

Assim, o principal objetivo de uma Política de Segurança da Informação é estabelecer regras e estratégias para mitigar vulnerabilidades e ameaças de segurança da informação em todo o ambiente organizacional, fornecendo orientações e diretrizes a serem seguidas pelos agentes públicos do órgão.





19

NORMAS ABNT NBR ISO/IEC PARA APOIAR A IMPLEMENTAÇÃO DA LGPD





19 | **NORMAS ABNT NBR ISO/IEC PARA APOIAR A IMPLEMENTAÇÃO DA LGPD**

Para dar suporte ao desenvolvimento das ações e atividades de adequação do órgão público à Lei Geral de Proteção de Dados Pessoais (LGPD), convém utilizar normas técnicas para subsidiar o estabelecimento de processos claros e eficazes para identificar, avaliar e mitigar os riscos de segurança da informação, garantindo assim a proteção adequada dos dados pessoais conforme exigido pela LGPD.

A adoção das normas ABNT NBR ISO/IEC da família 27000 traz diversas vantagens para o órgão público na adequação à LGPD e na implementação de Políticas de Segurança da Informação. Essas normas fornecem diretrizes internacionalmente reconhecidas, estabelecendo um padrão robusto e confiável para a gestão da privacidade dos dados, a proteção de dados pessoais e a segurança da informação.

Além disso, a adoção das normas da família 27000 promove a interoperabilidade e a compatibilidade com outras instituições públicas, facilitando a colaboração e a troca segura de informações entre elas. Isso ajuda a construir uma cultura de privacidade e segurança da informação dentro do órgão público e promove a confiança dos cidadãos e das partes interessadas na capacidade da organização em proteger seus dados pessoais de forma adequada e eficaz, fortalecendo assim o cumprimento da LGPD e a reputação do órgão público perante a sociedade.





A seguir apresentamos as principais Normas ABNT ISO/IEC que podem ser utilizadas durante todo o processo de adequação à LGPD, de acordo com a necessidade do órgão:

ABNT NBR ISO/IEC 27701:2020

Extensão da ABNT 27001 e 27002 para gestão da privacidade da informação – Requisitos e diretrizes

ABNT NBR ISO/IEC 29100:2020

Tecnologia da informação – Técnicas de segurança – Estrutura de privacidade

ABNT NBR ISO/IEC 29134:2020

Tecnologia da informação – Técnicas de segurança – Avaliação de impacto de privacidade - Diretrizes

ABNT NBR ISO/IEC 29151:2020

Tecnologia da informação — Técnicas de segurança — Código de prática para proteção de dados pessoais





ABNT NBR ISO/IEC 29184:2021

Tecnologia da informação — Avisos de privacidade on-line e consentimento



ABNT NBR ISO/IEC 27001:2023

Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos



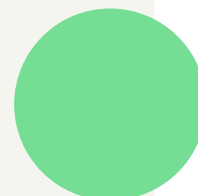
ABNT NBR ISO/IEC 27002:2022

Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação



ABNT NBR ISO/IEC 27005:2023

Segurança da informação, segurança cibernética e proteção à privacidade — Orientações para gestão de riscos de segurança da informação





ABNT NBR ISO/IEC 27014:2021

Segurança da informação, segurança cibernética e proteção da privacidade — Governança da segurança da informação



ABNT NBR ISO/IEC 27035:2023

Tecnologia da informação — Gestão de incidentes de segurança da informação - Parte 1: Princípios e processo



ABNT NBR ISO/IEC 27032:2015

Tecnologia da informação – Técnicas de segurança – Diretrizes para segurança cibernética





20

MODELOS, CARTILHAS E GUIAS DE BOAS PRÁTICAS





20 | MODELOS, CARTILHAS E GUIAS DE BOAS PRÁTICAS

O Governo Federal, por meio do Ministério da Gestão e da Inovação em Serviços Públicos tem empreendido esforços para fortalecer a privacidade e a segurança da informação no Governo Digital. Para tanto, desenvolveu um Programa de Privacidade e Segurança da Informação (PPSI), o qual envolve um conjunto de ações de adequação na temática, voltadas para melhoria no grau de maturidade e de resiliência dos órgãos e das entidades da Administração Pública Federal.

A partir do sítio eletrônico do Governo Digital, é possível acessar publicações no âmbito do Programa de Privacidade e Segurança da Informação (PPSI) voltadas para a efetiva implementação das melhores práticas de privacidade, segurança da informação e proteção de dados, objetivando promover as boas práticas por meio de disponibilização de guias e modelos para Publicações de apoio voltadas para elevar a maturidade e a resiliência dos órgãos e entidades, em termos de privacidade e segurança da informação.

No portal do Governo Digital que trata de privacidade e segurança, são disponibilizados materiais como:

- **Modelo de Política de Proteção de Dados Pessoais;**
- **Modelo de Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação;**
- **Modelo de Política de Backup;**





- **Modelo de Política de Gestão de Ativos;**
- **Modelo de Política de Controle de Acesso;**
- **Modelo de Política de Gestão de Registros (Logs) de Auditoria;**
- **Guia de Boas Práticas – LGPD;**
- **Guia de Inventário de Dados Pessoais;**
- **Guia de Termo de Uso e Política de Privacidade;**
- **Guia de Gerenciamento de Vulnerabilidades e Modelo de Política de Gerenciamento de Vulnerabilidades;**
- **Guia de Resposta a Incidentes de Segurança;**
- **Cartilha do Programa de Privacidade e Segurança da Informação (PPSI); e**
- **Cartilha sobre Finalidades e Hipóteses Legais.**

O acesso aos Guias e Modelos disponibilizados pelo Governo Digital pode ser feito por meio do link:



[Governo Digital - Guias e Modelos](#)



Importante destacar que o fortalecimento da privacidade e segurança da informação na administração pública aumenta o grau de confiança do cidadão no uso dos serviços públicos digitais.





21

PROGRAMA DE GOVERNANÇA EM PRIVACIDADE (PGP)





21 | PROGRAMA DE GOVERNANÇA EM PRIVACIDADE (PGP)

A elaboração de um Programa de Governança em Privacidade (PGP) é fundamental para atendimento ao previsto no art. 50 da Lei Federal nº 13.709/2018 - 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 de um Programa de Governança em Privacidade visa a atender, além da LGPD, a outros normativos vigentes sobre o tema de privacidade e segurança da informação.

Na administração pública, a governança em privacidade deve incluir as estratégias, habilidades, pessoas, processos e ferramentas que o órgão precisa prover para conquistar a confiança dos seus agentes públicos, dos cidadãos e, ao mesmo tempo, cumprir com exigências apresentadas nos normativos de privacidade.





Um PGP captura e consolida os requisitos de privacidade com o intuito de ditar e influenciar como os dados pessoais são tratados (manuseados) em todo seu ciclo de vida. Ele é essencial para que o órgão público alcance a maturidade necessária na gestão de riscos aos dados pessoais e garanta a efetividade da conformidade com a LGPD.

Em resumo, a implementação de um Programa de Governança em Privacidade (PGP) em um órgão público traz diversos benefícios que impactam positivamente a organização e a sociedade. Através do PGP, o órgão público pode garantir a conformidade com a LGPD, proteger os dados pessoais dos cidadãos, aumentar a transparência, melhorar a eficiência, fortalecer a imagem e a reputação, e construir uma cultura de proteção de dados no seu ambiente organizacional.

É importante destacar que, a elaboração de um Programa de Governança em Privacidade deve ser feita de forma personalizada, considerando as características e necessidades específicas de cada órgão público.





22

AUDITORIAS INTERNAS E MONITORAMENTO DA CONFORMIDADE À LGPD





22 | AUDITORIAS INTERNAS E MONITORAMENTO DA CONFORMIDADE À LGPD

A Lei Geral de Proteção de Dados Pessoais (LGPD) exige que os órgãos públicos adotem medidas eficazes para garantir a proteção dos dados pessoais dos cidadãos. Nesse contexto, auditorias internas regulares e o monitoramento contínuo dos processos de tratamento de dados se configuram como ferramentas essenciais para o cumprimento da legislação e a construção de uma cultura de conformidade.

Ao conduzir auditorias internas regulares focadas na verificação da conformidade com a LGPD, o órgão público demonstra seu comprometimento em atender às obrigações legais relativas à proteção dos dados pessoais. Essas auditorias ajudam a garantir que políticas adequadas estejam inseridas no contexto organizacional, fortalecendo uma cultura voltada à temática.

Neste capítulo, vamos explorar o papel das auditorias internas e do monitoramento continuado no contexto da LGPD e como elas podem auxiliar o gestor público na verificação da conformidade com as obrigações legais relacionadas à proteção dos dados pessoais.





22.1 Importância das auditorias internas

Realizar auditorias internas regulares é fundamental para avaliação da conformidade das organizações com leis e regulamentos aplicáveis, incluindo a LGPD. Elas são responsáveis por verificar se as políticas, procedimentos e controles implementados estão em conformidade com os requisitos legais e identificar possíveis lacunas ou áreas de melhoria.

Essas auditorias permitem identificar falhas, implementar medidas corretivas e aprimorar os processos de tratamento de dados, garantir a eficácia das medidas de segurança implementadas e a prevenir violações de dados, protegendo assim a privacidade dos cidadãos e mantendo a conformidade com a legislação.

Exemplo

Um órgão público designa os membros de seu Comitê de Privacidade e Proteção de Dados Pessoais para realizarem verificações periódicas em todas as áreas relacionadas ao tratamento de dados pessoais. Essa equipe revisa os processos internos, entrevista colaboradores-chave e analisa a documentação pertinente para garantir que o órgão esteja cumprindo suas obrigações legais





22.2 Monitoramento contínuo da conformidade

Como vimos, no contexto da LGPD, as auditorias internas podem ter como objetivo verificar se a organização está adotando medidas adequadas para proteger os dados pessoais sob sua responsabilidade. Isso inclui avaliar se foram implementados controles técnicos e organizacionais suficientes para garantir a segurança dos dados, verificar se há políticas claras de privacidade, proteção de dados e segurança da informação em vigor, e atualizadas, e se os agentes públicos estão cientes das suas responsabilidades individuais.

O monitoramento contínuo dos processos de tratamento de dados complementa as auditorias e garante que as medidas de segurança e proteção da privacidade estejam sendo implementadas de forma eficaz no dia a dia do órgão público. Isso inclui o monitoramento do acesso aos dados, a detecção de atividades suspeitas e a resposta imediata a incidentes de segurança.

Um processo de auditoria e monitoramento geralmente envolve as seguintes etapas:

- **Identificação de áreas de risco:** Identificar os processos e sistemas de tratamento de dados pessoais que apresentam maior risco de violações de segurança ou não conformidade com a LGPD.
- **Coleta de evidências:** Coletar evidências relevantes, como registros de acesso, diretrizes de políticas de segurança e relatórios de incidentes, para avaliar a conformidade e a eficácia das medidas de proteção de dados.



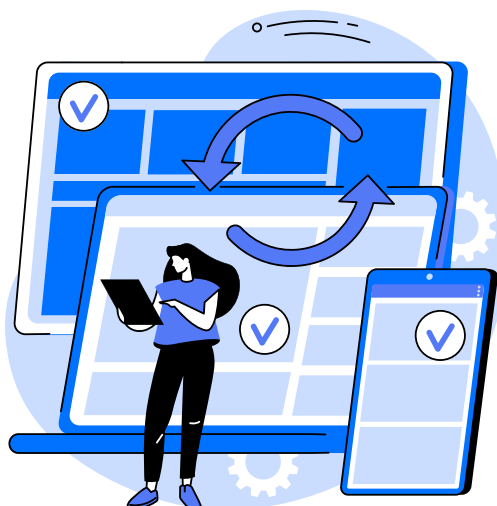


- **Análise e avaliação:** Analisar as evidências coletadas e avaliar o grau de conformidade com os requisitos da LGPD, identificando áreas de não conformidade e propondo medidas corretivas, se necessário.

Ao implementar uma cultura de auditoria e monitoramento, o órgão público demonstra sua maturidade em relação à proteção de dados e constrói uma relação de confiança com os cidadãos. Essa cultura garante que os dados pessoais sejam tratados de forma ética, responsável e segura, em consonância com os princípios da LGPD.

Exemplo

Um órgão público realiza uma auditoria interna focada na área de tecnologia da informação para verificar se os sistemas utilizados estão em conformidade com as diretrizes estabelecidas pela LGPD. Essa auditoria envolve testes técnicos nos sistemas, revisão dos registros de acesso aos dados pessoais e entrevistas com os responsáveis pela segurança da informação e cibernética.





22.3 Identificação de áreas de melhoria

Além de verificar a conformidade com a LGPD, as auditorias internas também têm como objetivo identificar áreas de melhoria nas práticas relacionadas à proteção dos dados pessoais. Ao analisar os resultados das auditorias, os órgãos públicos podem tomar medidas corretivas necessárias para fortalecer sua postura em relação à privacidade dos dados.

Exemplo

Um órgão público realiza uma auditoria interna abrangente que revela que determinados departamentos não estão seguindo adequadamente as diretrizes estabelecidas pela LGPD. Com base nessas descobertas, são desenvolvidos planos de melhoria específicos para cada departamento, incluindo treinamentos adicionais sobre privacidade, proteção de dados e segurança da informação.





23

CAPACITAÇÃO E TREINAMENTO





23 | CAPACITAÇÃO E TREINAMENTO

É importante que o órgão público invista em programas de capacitação e sensibilização para seus agentes públicos, com o objetivo de garantir que compreendam os requisitos da Lei Geral de Proteção de Dados Pessoais (LGPD), reconheçam os riscos de segurança relacionados ao tratamento de dados pessoais e saibam como agir de acordo com as melhores práticas de proteção de dados.

Instituir um **“Programa de Conscientização e Treinamento”** que contemple a promoção continuada de cursos e eventos de formação, capacitação, aperfeiçoamento sobre privacidade, para assim treinar os agentes públicos para desempenhar suas funções e responsabilidades relacionadas à privacidade de acordo com as políticas, processos, procedimentos, acordos e valores de privacidade da organização, bem como para influenciar e conscientizar o comportamento dos agentes, tornando-os devidamente qualificados e assim atingir o objetivo de reduzir riscos de segurança da informação e cibernética do órgão.

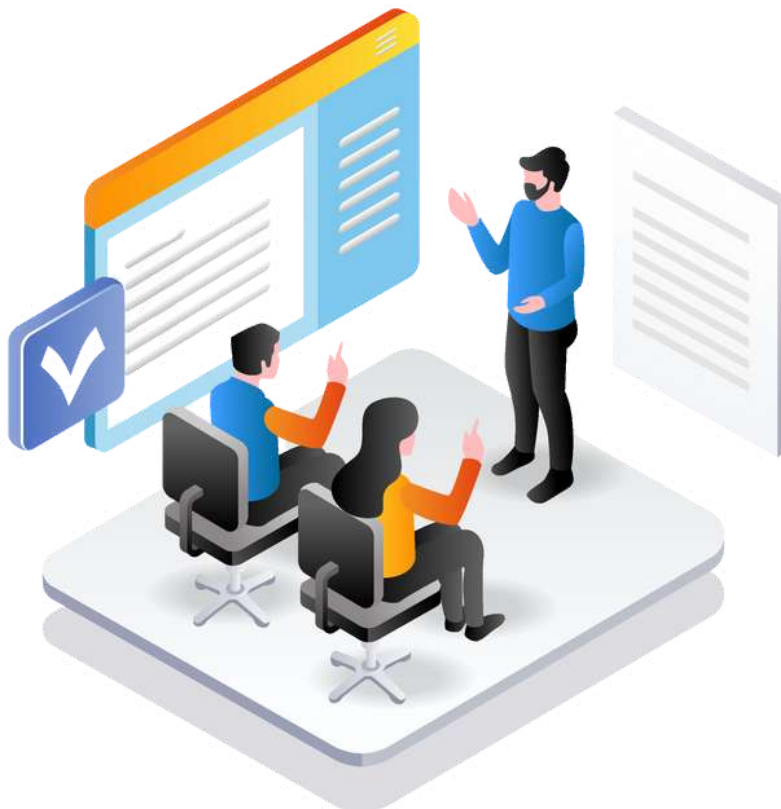
Para capacitar seus agentes públicos, o órgão pode recorrer a diversas formas e fontes de treinamento, tais como cursos EAD ou presenciais, palestras e seminários conduzidos por especialistas em privacidade, proteção de dados e segurança da informação, além de utilizar recursos disponibilizados por órgãos reguladores e entidades especializadas, como a Autoridade Nacional de Proteção de Dados (ANPD) e associações do setor.





Com a implementação de um Programa de Conscientização e Treinamento, o órgão cria um cenário educacional adaptado às necessidades específicas de seus agentes, utilizando livros, materiais educativos, palestras e simulações de situações práticas para reforçar a importância da proteção de dados e promover uma cultura de privacidade.

Ao investir na capacitação e na conscientização dos agentes públicos, a instituição fortalece sua postura em relação à proteção de dados, reduz o risco de violações de segurança e promove a confiança dos cidadãos na administração pública.





23.1 Capacitação técnica para o Encarregado

É recomendado que o DPO, durante o exercício da sua função e de outras relacionadas ao tema, participe de cursos periódicos de capacitação que contemplem conteúdo de caráter multidisciplinar, tais como:

- **Aspectos jurídicos da proteção de dados pessoais;**
- **Gestão e governança de dados pessoais; e**
- **Tecnologias da informação e comunicação e segurança da informação e cibernética.**

23.2 Capacitação em LGPD e segurança da informação

A capacitação dos agentes públicos em relação à LGPD e segurança da informação é essencial para garantir que eles compreendam as disposições da legislação, reconheçam os riscos de segurança relacionados ao tratamento de dados pessoais e saibam como agir de acordo com as melhores práticas de proteção de dados. Os treinamentos devem abordar temas como os princípios da LGPD, os direitos dos titulares de dados, as bases legais para o tratamento de dados e as medidas de segurança necessárias para proteger as informações.





Exemplo 1

Um exemplo de capacitação em LGPD e segurança da informação é a realização de eventos como workshops e palestras para os agentes de um órgão público, ministrados por especialistas na área. Durante esses eventos, os agentes públicos podem aprender sobre os requisitos da LGPD, os riscos de segurança cibernética e as melhores práticas para proteger, das ameaças existentes, os dados pessoais dos cidadãos com os quais lidam durante suas atividades laborais, e ainda como notificar e responder a incidentes de segurança.

Exemplo 2

Imagine que uma secretaria estadual realiza treinamentos regulares com seus servidores, estagiários, bolsistas e prestadores de serviço terceirizado sobre as melhores práticas em relação à segurança da informação e proteção de dados. Esses treinamentos abordam tópicos como identificação de e-mails fraudulentos, cuidados ao lidar com informações confidenciais, com dados pessoais e sensíveis, e ainda, sobre como aplicar boas práticas no uso dos dispositivos móveis.





23.3 Conscientização sobre boas práticas de proteção de dados

Além da capacitação formal, é importante promover a conscientização contínua sobre boas práticas de proteção de dados entre os servidores públicos. Isso inclui incentivar a adoção de medidas simples, como o uso de senhas fortes, a atualização regular de software e a proteção adequada de dispositivos e arquivos. A conscientização também pode envolver a disseminação de informações sobre incidentes de segurança e exemplos de boas práticas em proteção de dados.

Exemplo 1

Um exemplo de conscientização sobre boas práticas de proteção de dados é a distribuição de materiais educativos, como cartilhas, boletins, vídeos e folders, em locais visíveis nas unidades do órgão público, destacando dicas e recomendações para proteger os dados pessoais. Esses materiais podem incluir orientações sobre como identificar e relatar phishing, como proteger dispositivos móveis e como lidar com informações sensíveis e confidenciais, como aplicar técnicas para criar senhas fortes, entre outros.

Exemplo 2

Um órgão público realiza treinamentos internos sobre a proteção dos dados pessoais, fornecendo informações detalhadas sobre como os agentes devem lidar com esses dados em suas atividades diárias. Esses treinamentos podem incluir exemplos reais para demonstrar situações práticas.





24

CUIDADOS COM O COMPARTILHAMENTO DE DADOS ENTRE ÓRGÃOS PÚBLICOS





24 | CUIDADOS COM O COMPARTILHAMENTO DE DADOS ENTRE ÓRGÃOS PÚBLICOS

O compartilhamento de dados pessoais é a operação de tratamento pela qual órgãos e entidades públicos conferem permissão de acesso ou transferem uma base de dados pessoais a outro ente público ou a entidades privadas visando ao atendimento de uma finalidade pública. De forma mais específica, a LGPD utiliza o termo “uso compartilhado de dados”, que é definido como a “comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicas 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.”

O uso compartilhado de dados é um mecanismo relevante para a execução de atividades típicas e rotineiras do Poder Público, a exemplo de pagamento de servidores e prestação de serviços públicos. A LGPD reconhece essa relevância ao estabelecer, em seu art. 25, que os dados devem ser mantidos “em formato interoperável e estruturado para o uso compartilhado”, visando, entre outras finalidades, “à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral”.

Neste capítulo, vamos explorar os cuidados necessários que o gestor público deve ter ao promover o compartilhamento de dados com outros órgãos públicos.





24.1 Importância do compartilhamento de dados entre órgãos públicos

O compartilhamento de dados entre órgãos públicos é fundamental para promover a eficiência na prestação dos serviços públicos e evitar a duplicidade de informações. Isso permite uma melhor tomada de decisões e uma maior integração entre as diferentes esferas governamentais.

Exemplo

Um município precisa acessar informações sobre a renda dos seus cidadãos para conceder benefícios sociais adequados. O compartilhamento desses dados com o órgão responsável pela arrecadação dos impostos permite uma análise mais precisa da situação financeira dos beneficiários.

24.2 Cuidados necessários no compartilhamento de dados pessoais

No entanto, é importante tomar alguns cuidados para garantir que o compartilhamento de dados seja realizado de forma segura e em conformidade com as leis aplicáveis:

- **Base legal:** Verificar se existe base legal válida que autorize o compartilhamento dos dados pessoais entre os órgãos públicos.





- **Princípio da finalidade:** Assegurar que os dados sejam utilizados exclusivamente para as finalidades específicas acordadas entre os órgãos envolvidos.
- **Segurança da informação:** Adotar medidas técnicas e administrativas adequadas para proteger os dados durante todo o processo de compartilhamento.

Exemplo

Dois órgãos públicos decidem estabelecer um acordo formal para o compartilhamento das informações fiscais dos contribuintes. Nesse acordo, são definidas as finalidades específicas desse compartilhamento (por exemplo, identificar possíveis fraudes fiscais) e são estabelecidas as medidas técnicas necessárias para garantir a segurança dos dados compartilhados durante toda a operação.





24.3 Proteção dos direitos fundamentais

Ao realizar o compartilhamento de dados pessoais entre órgãos públicos, é fundamental proteger os direitos fundamentais dos titulares desses dados. Isso inclui garantir a confidencialidade, integridade e disponibilidade das informações pessoais, bem como respeitar os princípios da finalidade, necessidade, proporcionalidade e minimização do tratamento.

Exemplo

Uma secretaria estadual é instada a fornecer determinadas informações pessoais de seus servidores à um órgão de controle para fins de auditoria. Nesse caso, ambas as instituições devem garantir que apenas as informações estritamente necessárias para a finalidade sejam fornecidas, e que essas informações sejam tratadas sob as diretrizes da LGPD durante todo o processo.

Ao tomar os cuidados necessários no compartilhamento de dados entre órgãos públicos, é possível promover uma maior eficiência na gestão pública enquanto respeita-se a privacidade dos cidadãos e protege-se seus direitos fundamentais.





25

GESTÃO DE INCIDENTE DE SEGURANÇA





25 | GESTÃO DE INCIDENTE DE SEGURANÇA

A Autoridade Nacional de Proteção de Dados (ANPD) aprovou, por meio da Resolução CD/ANPD nº 15, de 24 de abril de 2024, o Regulamento de Comunicação de Incidente de Segurança. O Regulamento tem por objetivo estabelecer os procedimentos para Comunicação de Incidente de Segurança, que possa acarretar risco ou dano relevante aos titulares, nos termos do art. 48 da Lei Federal nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).

O Regulamento procura assegurar a proteção dos direitos dos titulares; a adoção das medidas necessárias para mitigar ou reverter os efeitos dos prejuízos gerados; a efetividade do princípio da responsabilização e da prestação de contas pelos agentes de tratamento; a atuação transparente dos agentes de tratamento e o estabelecimento de confiança com o titular. Além de promover a adoção de regras de boas práticas, de governança, de medidas de prevenção e segurança adequadas; estimular a promoção da cultura de proteção de dados pessoais; e por fim, fornecer subsídios para as atividades regulatória, fiscalizatória e sancionatória da Autoridade Nacional de Proteção de Dados (ANPD).

O Regulamento de Comunicação de Incidente de Segurança está disponível neste link:

 [Regulamento de Comunicação de Incidente de Segurança](#)





Neste contexto, a gestão eficaz de incidente de segurança é uma parte crítica e fundamental para proteger os dados pessoais nos órgãos públicos e garantir a conformidade com a LGPD. Ao seguir os procedimentos corretos de identificação, resposta e notificação, o órgão público pode mitigar os danos causados por um incidente de segurança e manter a confiança dos cidadãos na proteção de seus dados pessoais.

É recomendável que o órgão institua uma Equipe de Tratamento e Resposta a Incidentes (ETIR), e estabeleça os fluxos e as responsabilidades para receber, analisar e responder às notificações e atividades relacionadas à incidentes de segurança no âmbito da instituição. A ETIR deve ser composta, preferencialmente, por agentes com conhecimentos em proteção de dados, sistemas de informação, segurança da informação e cibernética, infraestrutura de redes e banco de dados.

Neste capítulo, vamos abordar como o órgão público pode agir em caso de incidente de segurança ou violações de dados, incluindo os procedimentos de notificação às autoridades e aos titulares de dados afetado, nos termos da Resolução CD/ANPD nº 15/2024 e demais frameworks de segurança.





25.1 Identificação de incidentes de segurança

O primeiro passo na gestão de incidentes é a identificação rápida e precisa de qualquer incidente de segurança ou violação de dados. Isso pode incluir atividades suspeitas, como acessos não autorizados a sistemas, vazamento de informações, falhas de segurança relatadas por agentes públicos ou usuários de serviços, entre outras.

Exemplo

Um exemplo de identificação de incidente de segurança é o caso de um servidor público que percebe atividades incomuns em sua conta de e-mail, como envio de mensagens não autorizadas para destinatários desconhecidos. Isso pode ser um sinal de que a conta foi comprometida e que um incidente de segurança está ocorrendo.

25.2 Resposta imediata e mitigação de danos

Após a identificação do incidente, é essencial agir rapidamente para conter o problema e minimizar os danos. Isso pode envolver medidas como comunicar o incidente a uma Equipe de Tratamento e Resposta a Incidentes (ETIR) e ao Encarregado pelo Tratamento de Dados Pessoais (DPO) para que avalie os danos que podem ser causados aos titulares, desconectar sistemas comprometidos da rede, restringir o acesso a dados sensíveis, e tomar medidas para impedir que o incidente se espalhe para outros sistemas ou usuários.





Exemplo

Um exemplo de resposta imediata é o caso de uma prefeitura que identifica um ataque de **ransomware** em sua rede de computadores. A ETIR age rapidamente para isolar os sistemas afetados, interromper a propagação do malware e iniciar os procedimentos de recuperação de dados para reestabelecer o ambiente enquanto o Encarregado (DPO) toma as providências para avaliar os riscos que o incidente pode trazer aos titulares dos dados e, se for o caso, comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares afetados.





25.3 Notificação às autoridades e aos titulares de dados afetados

De acordo com a LGPD, os órgãos públicos são obrigados a notificar as autoridades competentes e os titulares de dados afetados em caso de incidentes de segurança que possam resultar em riscos ou danos significativos aos direitos e liberdades dos titulares.

Exemplo

Um exemplo de notificação é o caso de uma prefeitura que sofre uma violação de dados em seu sistema de cadastro de beneficiários de programas sociais que possa ocasionar risco ou dano relevante. A prefeitura **é obrigada a notificar, no prazo de três dias úteis**, a Autoridade Nacional de Proteção de Dados (ANPD) e os titulares de dados afetados pelo o incidente, fornecendo informações sobre a natureza da violação e as medidas tomadas para reverter ou mitigar seus efeitos sobre os titulares.





26

SANÇÕES PREVISTAS PELA LGPD AOS ÓRGÃOS PÚBLICOS



26 | SANÇÕES PREVISTAS PELA LGPD AOS ÓRGÃO PÚBLICOS

Neste capítulo, vamos explorar algumas das sanções previstas pela Lei Geral de Proteção de Dados Pessoais (LGPD) em caso de descumprimento das obrigações legais relacionadas à proteção dos dados pessoais.

26.1 Importância do cumprimento das obrigações legais da LGPD

O cumprimento das obrigações legais estabelecidas pela LGPD é fundamental para garantir a proteção adequada dos dados pessoais e preservar os direitos dos titulares desses dados. O não cumprimento dessas obrigações pode resultar em riscos à privacidade dos indivíduos e prejudicar a confiança nas organizações que tratam essas informações.

Exemplo

Uma prefeitura decide coletar dados pessoais de seus contribuintes para uma campanha de marketing direcionada sem obter o consentimento necessário ou sem implementar medidas adequadas de segurança da informação. Esse descumprimento das obrigações legais pode expor os contribuintes a riscos como roubo de identidade ou invasões à privacidade.





26.2 Sanções administrativas previstas pela LGPD

O art. 52, § 3º, estabelece quais sanções podem ser aplicadas às entidades e aos órgãos públicos, com expressa exclusão das penalidades de multa simples ou diária previstas na LGPD.

Porém, apesar da administração pública estar isenta de sanções pecuniárias, como multas, o descumprimento da lei por órgãos públicos não significa ausência de consequências. Na prática, diversas medidas podem ser tomadas, pela ANPD ou pelos demais órgãos de controle, para garantir os direitos dos titulares de dados e a conformidade com a LGPD. Portanto, os impactos pelo descumprimento legal podem ser significativos para o órgão e seus gestores públicos.

Abrangência das Sanções:

- Nos termos da LGPD a administração pública está sujeita a sanções administrativas como advertência, bloqueio e suspensão de dados, publicização da infração e até mesmo a proibição de atividades relacionadas ao tratamento de dados.

Impactos na Administração Pública:

- O descumprimento da LGPD pode gerar impactos negativos para a administração pública em diversos aspectos, como:
 - a) **Prejuízos à imagem e reputação:** A publicização de infrações pode afetar a confiança da sociedade no órgão, prejudicando sua imagem e reputação.





- b) **Dificuldades na prestação de serviços:** O bloqueio ou suspensão de dados pode impedir o funcionamento de sistemas e serviços essenciais, dificultando a prestação de serviços à população.
- c) **Riscos de judicialização:** A LGPD abre caminho para ações civis públicas e individuais, aumentando os riscos de processos e condenações contra o órgão.
- d) **Responsabilidade dos gestores:** Gestores públicos podem ser responsabilizados por danos causados pelo descumprimento da LGPD, inclusive com sanções administrativas e até mesmo civis e criminais.
- e) **Advertência:** A organização infratora pode receber uma advertência formal sobre o descumprimento da lei.





26.3 Responsabilidades individuais

Além das sanções às organizações, a LGPD também prevê responsabilidades individuais no tratamento dos dados pessoais. Os agentes públicos que atuam no tratamento desses dados devem cumprir as disposições legais e tomar as medidas necessárias para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

O cumprimento das obrigações legais estabelecidas pela LGPD é essencial para promover uma cultura organizacional voltada à privacidade e proteger os direitos fundamentais dos titulares dos dados pessoais.

A LGPD não é apenas uma lei que impõe sanções, mas uma oportunidade para a administração pública aprimorar a gestão de dados, aumentar a transparência e fortalecer a confiança da sociedade. A adequação à LGPD é um investimento em um futuro mais transparente, seguro e eficiente para a gestão pública brasileira.

Exemplo

Um servidor público divulga indevidamente informações pessoais sobre um cidadão sem justificativa legal ou consentimento prévio. Nesse caso, além das sanções aplicáveis ao órgão público envolvido, o servidor também poderia enfrentar consequências disciplinares individuais por seu comportamento inadequado.





27

A LGPD NO TRIBUNAL DE CONTAS DE RONDÔNIA





27 | A LGPD NO TRIBUNAL DE CONTAS DE RONDÔNIA

Neste capítulo, apresentamos os principais marcos e ações realizadas pelo TCERO na busca por conformidade legal em consonância com as diretrizes da Lei Geral de Proteção de Dados Pessoais (LGPD), tais como:

2024

- **Criada a Assessoria de Privacidade e Proteção de Dados Pessoais (ASPPROD).** Vinculada à Presidência do Tribunal, tem por finalidade: Coordenar, orientar e acompanhar, em consonância com o Encarregado pelo Tratamento de Dados Pessoais, a implementação da LGPD no TCERO. (Lei Complementar nº 1.218/2024).

- **Criada a Coordenadoria de Segurança Cibernética (COSEC).** Vinculada à Secretaria de Tecnologia da Informação e Comunicação, tem por finalidade: Gerir a segurança cibernética no TCERO, para assegurar a proteção dos ativos contra riscos e ameaças, garantindo a aplicação dos controles adequados. (Lei Complementar nº 1.218/2024).





2023

- **Instituída a Política de Proteção de Dados Pessoais (PPDP).** Regulamenta a Lei Federal nº 13.709/2018 (LGPD) no TCERO. (Res. Adm. 407/2023/TCERO).
- **Encarregado (DPO) conclui curso de formação de professores facilitadores - Praticando a LGPD,** pela Escola Nacional de Administração Pública (ENAP).
- **Instituída a Política de Controle de Acesso (PCA).** Define as diretrizes para limitar o acesso à informação e aos recursos de tecnologia da informação no TCERO. (Res. Adm. 392/2023/TCERO).

2022

- **Instituída norma sobre descaracterização de dados pessoais e sensíveis** no âmbito do TCERO. (Res. Adm. 378/2022/TCERO).
- **Instituída a Política Corporativa de Segurança da Informação (PCSI) e o Programa Corporativo de Gestão da Segurança da Informação e Privacidade de Dados (PCGSIPD).** (Res. Adm. 377/2022/TCERO).
- **Elaboradas cláusulas de proteção de dados pessoais e sensíveis** para serem inseridas em contratos, acordos e termos de cooperação técnica.
- **Encarregado (DPO) aplica treinamento interno** sobre a LGPD e segurança da informação para os agentes públicos do Tribunal.
- **Encarregado conclui pós-graduação lato sensu em Direito Digital e Proteção de Dados.**





2021

- Encarregado ministra **webinário externo para os jurisdicionados do TCERO** com o tema: LGPD - Desafios para a Administração Pública.
- **Encarregado é certificado pela ABNT** como Lead Implementer para a Gestão da Privacidade da Informação (baseado na ABNT NBR ISO/IEC 27701:2019).
- **Encarregado é selecionado pela ANPD** para participar dos debates para elaboração da norma nacional sobre o Encarregado de Proteção de Dados Pessoais.
- **Encarregado aplica treinamento interno sobre a LGPD** e segurança da informação para os agentes públicos do TCERO.
- **O Tribunal lança seu Portal da LGPD** para demonstrar compromisso com a transparência, provendo acesso facilitado aos titulares de dados e servindo como um recurso valioso para consulta dos jurisdicionados e demais cidadãos sobre o tema.
- Encarregado conclui curso de **Bacharelado em Direito**.
- Encarregado obtém **certificação internacional como DPO EXIN**: Information Security Management based on ISO IEC 27001 (ISFS), Privacy and Data Protection Foundation (PDPF) e Privacy and Data Protection Practitioner (PDPP).





2020

- **Encarregado aplica treinamento interno** sobre a LGPD e segurança da informação para os agentes públicos do TCERO.
- **O TCERO adquire Normas ABNT ISO/IEC da família 27000** que tratam de segurança da informação, privacidade e proteção de dados.
- **Aprovado o Programa Corporativo de Gestão da Segurança da Informação e Privacidade de Dados (PCGSIPD).** (DM 0435/2020/TCERO).
- **Criada a figura dos Gestores de Segurança da Informação e Privacidade** que representam áreas críticas do Tribunal, e atuam sob coordenação do Encarregado (DPO). (Res. Adm. 330/2020/TCERO).
- **Designado o Encarregado pelo Tratamento de Dados Pessoais (DPO)** do Tribunal, que além das responsabilidades previstas na LGPD atua na coordenação das ações necessárias para adequação do TCERO à LGPD. (Portaria 189/2020/TCERO).





2019

- Criado o **Comitê de Segurança da Informação e Comunicação (COSIC)**. Tem por finalidade: Estabelecer diretrizes e propor políticas, normas e procedimentos gerais relacionados à gestão informacional e do conhecimento no âmbito do Tribunal. (Res. Adm. 287/2019/TCERO).

2018

- Aplicado o **1º treinamento interno sobre segurança da informação** para os agentes públicos do Tribunal.

2015

- Servidores da Corte participam de treinamento sobre os conceitos e aplicações das **Normas ABNT ISO/IEC 27001, 27002, 27005 e 31000** (Escola Superior de Redes - RNP).





28

20 PASSOS PRÁTICOS PARA IMPLEMENTAÇÃO DA LGPD





28 | 20 PASSOS PRÁTICOS PARA IMPLEMENTAÇÃO DA LGPD

Neste capítulo, vamos explorar 20 passos práticos essenciais para auxiliar um órgão público na implementação da Lei Geral de Proteção de Dados Pessoais (LGPD).

PASSO 1

Instituir Comitê de Privacidade e Proteção de Dados Pessoais

Instituir um Comitê de Privacidade e Proteção de Dados Pessoais multisetorial é fundamental para a governança de dados no órgão público. Sua criação permite centralizar as decisões estratégicas sobre proteção de dados pessoais, identificar e avaliar os riscos relacionados ao tratamento de dados pessoais, e ainda propor medidas de mitigação e controle adequadas para promover uma cultura de conformidade e fortalecer a transparência nas ações do órgão.

É importante que o Comitê seja composto por membros de diferentes áreas da organização, e que atue de forma colegiada para definir diretrizes, implementar políticas e monitorar o cumprimento da LGPD.

Estratégia:

Definir e estabelecer o escopo e os objetivos do Comitê de forma clara e abrangente. Compor o Comitê com representantes de diferentes áreas da organização, com expertise em proteção de dados, tecnologia da informação, área jurídica, gestão de riscos, entre outras áreas relevantes.





Designar, por meio de portaria, ou outro instrumento adequado, os membros do Comitê de forma transparente e criteriosa, considerando suas qualificações e proposta de atuação, e ainda, definir as atribuições e funções do Comitê em um regimento interno, incluindo responsabilidades, processo de tomada de decisões, periodicidade das reuniões e mecanismos de comunicação.

Também é de suma importância capacitar e treinar os membros do Comitê de forma contínua sobre a LGPD, as melhores práticas em proteção de dados e as ferramentas de gestão de riscos para que haja nivelamento do conhecimento normativo entre os integrantes do Comitê.

PASSO 2

Designar Encarregado pelo Tratamento de Dados Pessoais (DPO)

A designação de um Encarregado pelo Tratamento de Dados Pessoais (na legislação europeia, corresponde ao Data Protection Officer - DPO) é uma obrigação legal para garantir o cumprimento da LGPD (artigo 41/LGPD). O Encarregado (DPO) deve ser indicado pelo órgão público para atuar como ponto focal a fim de promover e orientar o processo de implementação e monitoramento da LGPD no órgão. Ele é responsável por garantir que as atividades relacionadas ao tratamento dos dados pessoais estejam em conformidade legal.

A Autoridade Nacional de Proteção de Dados (ANPD) por meio da **Resolução CD/ANPD n. 18, de 16 de julho de 2024**, aprovou o Regulamento sobre a atuação do Encarregado, estabelecendo norma complementar sobre a indicação, a definição, as atribuições e a atuação do Encarregado, de que trata a LGPD.





Neste contexto, é desejável que o DPO possua qualificação adequada e conhecimentos sólidos sobre a LGPD e outras leis aplicáveis à proteção dos dados pessoais. Além disso, ele deve estar atualizado quanto às melhores práticas nesse campo e possuir habilidades técnicas adequadas para realizar suas funções, interagindo diretamente com todas as áreas da organização, em especial com o jurídico, tecnologia da informação e segurança cibernética.

Estratégia:

A indicação do Encarregado deve ser realizada por ato formal do agente de tratamento, do qual constem as formas de atuação e as atividades a serem desempenhadas. Entende-se por ato formal o documento escrito, datado e assinado, que, de maneira clara e inequívoca, demonstre a intenção do órgão em designar como Encarregado uma pessoa natural ou uma pessoa jurídica.

Convém que a alta administração siga um processo criterioso para escolha do perfil do Encarregado, avaliando as necessidades do órgão e as qualificações profissionais necessárias para o desempenho das atribuições, considerando conhecimentos sobre a legislação de proteção de dados pessoais, bem como o contexto, o volume e o risco das operações de tratamento realizadas pela instituição.

Independência, imparcialidade e autonomia para reportar diretamente à alta gestão são características fundamentais para o DPO exercer suas funções com ética e profissionalismo junto ao órgão. Para tanto, é importante que a instituição evidencie formalmente as medidas administrativas adotadas para garantir tais premissas à atividade de DPO. Uma estratégia seria consolidar essas diretrizes em políticas internas, fortalecendo todo o processo de transparência da atuação do Encarregado no órgão.





PASSO 3

Capacitar o Encarregado (DPO)

É recomendado que o DPO, previamente e durante o exercício da sua função, participe de cursos periódicos de capacitação que contemplem conteúdo de caráter multidisciplinar tais como:

- **Aspectos jurídicos da proteção de dados pessoais.**
- **Gestão e governança de dados.**
- **Segurança da informação.**
- **Segurança Cibernética.**

É importante que o órgão público invista em programas de capacitação e sensibilização para seus agentes públicos, com o objetivo de garantir que compreendam os requisitos da Lei Geral de Proteção de Dados Pessoais (LGPD), reconheçam os riscos de segurança relacionados ao tratamento de dados pessoais e saibam como agir de acordo com as melhores práticas de proteção de dados.

A sensibilização e o treinamento dos agentes em relação à LGPD e segurança da informação são essenciais para garantir o cumprimento da legislação e proteger os dados pessoais dos cidadãos.

Ao investir na capacitação e na conscientização dos agentes públicos, as instituições fortalecem sua postura em relação à proteção de dados, reduz o risco de violações de segurança e promove a confiança dos cidadãos na administração pública.





PASSO 4

Realizar diagnóstico de maturidade do órgão

A etapa de diagnóstico de maturidade de privacidade é de extrema importância para que o órgão público se adeque à LGPD e garanta a proteção dos dados dos cidadãos sob sua responsabilidade. Através dessa avaliação, o órgão obtém um panorama organizacional completo em relação à proteção de dados, identificando pontos fortes, fracos e oportunidades de aprimoramento.

Ao realizar essa avaliação, o órgão obtém uma visão holística da sua atual situação, identifica riscos e oportunidades, possibilitando definir um plano de ação estratégico na busca por conformidade legal, demonstrando seu compromisso com a privacidade e proteção dos dados.

Estratégia:

O Encarregado (DPO) pode utilizar uma ferramenta que auxilia no diagnóstico de maturidade do órgão, disponibilizada pela Secretaria de Governo Digital (SGD), por meio do “Manual do Usuário da Ferramenta do Framework de Privacidade e Segurança da Informação - Programa de Privacidade e Segurança da Informação (PPSI)” disponível no link:



[Governo Digital - Programa de Privacidade e Segurança \(PPSI\)](#)

A ferramenta auxilia tanto no diagnóstico de maturidade do órgão quanto na adoção dos controles de privacidade e segurança da informação, trazendo subsídios para a formalização e cálculo de um índice de maturidade, que possibilitará ao órgão direcionar esforços e priorizar as ações necessárias para conformidade em relação à LGPD.





O documento é especialmente recomendado e dirigido aos órgãos e às entidades da Administração Pública Federal - APF para orientar a aplicabilidade da ferramenta, auxiliando no preenchimento das respostas aos diagnósticos, mas **não há impedimento de ser utilizado por outras instituições** que busquem orientações sobre o tema.

PASSO 5

Firmar parcerias para intercâmbio de conhecimento

A adequação à Lei Geral de Proteção de Dados Pessoais (LGPD) representa um desafio significativo para os órgãos públicos brasileiros. A complexa natureza da legislação, a necessidade de mudanças estruturais e a escassez de recursos especializados exigem soluções inovadoras e colaborativas. Nesse contexto, as parcerias entre órgãos públicos se configuram como uma estratégia promissora para otimizar recursos, compartilhar conhecimentos e superar os desafios inerentes à implementação da LGPD.

O intercâmbio de conhecimento permite que os órgãos compartilhem boas práticas, lições aprendidas e desafios enfrentados ao longo do processo de adequação permitindo a troca de experiências e conhecimentos entre equipes multidisciplinares. Isso pode acelerar significativamente o aprendizado e a implementação de medidas eficazes, economizando tempo e recursos financeiros que seriam gastos na tentativa e erro.





A criação de parcerias entre órgãos públicos certamente aumenta a legitimidade e credibilidade das ações de adequação à LGPD perante a sociedade, demonstrando transparência e compromisso com a proteção dos direitos dos titulares de dados. Além disso, ao unir esforços com outros órgãos públicos, é possível aproveitar economias de escala e otimizar o uso de recursos financeiros, humanos e tecnológicos.

Estratégia:

Os órgãos públicos podem compartilhar custos de treinamentos, consultorias especializadas, ferramentas e tecnologias que apoiam o processo de implementação da LGPD, reduzindo o impacto financeiro em cada organização e otimizando o tempo do projeto.

PASSO 6

Criar estrutura administrativa para governança e proteção de dados pessoais

É importante, como suporte para a estrutura de coordenação do Programa de Governança em Privacidade, assim como para a realização das atividades do Encarregado (DPO) provenientes de sua atuação como canal de comunicação entre o Controlador, os Titulares dos dados e a ANPD, o estabelecimento de estrutura administrativa, de acordo com o porte do órgão público, com equipes suficientes e adequadas para gerenciar, implementar, coordenar, manter e acompanhar de forma continuada as ações para governança e proteção de dados pessoais.





Como referência e sugestão de estruturação inicial, a Lei Complementar n. 1.218, de 18 de janeiro de 2024 apresenta, entre outras informações, as competências da Assessoria em Privacidade e Proteção de Dados Pessoais – ASPPROD do Tribunal de Contas do Estado de Rondônia, que instituiu, com êxito, a estrutura mínima proposta.

Estratégia:

A alta gestão pode criar estrutura administrativa e designar agentes públicos com habilidades e conhecimento da legislação, regulação e prática de privacidade e proteção de dados pessoais, a fim de auxiliar o Encarregado (DPO) a garantir o pleno funcionamento do Programa de Governança em Privacidade (PGP), com foco no aprimoramento das ações para o cumprimento da LGPD e na proteção dos dados pessoais dos cidadãos sob responsabilidade do órgão.

Convém que a estrutura administrativa em questão seja supervisionada por um Comitê de Privacidade e Proteção de Dados Pessoais, o qual deve acompanhar suas atividades, e ainda que a estrutura possua competências e recursos adequados para o seu pleno funcionamento.

PASSO 7

Conscientizar e sensibilizar os agentes internos sobre a LGPD

Com a designação de um Encarregado pelo Tratamento de Dados Pessoais (DPO) pelo órgão, o DPO deve promover a conscientização e sensibilização interna sobre a LGPD e suas implicações. Isso envolve, no mínimo, informar os agentes públicos sobre os princípios da proteção de dados pessoais, os direitos dos titulares dos dados, as obrigações do órgão e as responsabilidades dos seus agentes em relação ao tratamento de dados pessoais.





A alta administração deve ser sensibilizada a apoiar a priorização das ações de maior criticidade e urgência, para assim fortalecer o estabelecimento da cultura de proteção de dados na instituição.

Estratégia:

Como visto, uma boa estratégia é realizar palestras, workshops, seminários e treinamentos internos com a alta administração e demais agentes públicos do órgão, abordando temas como a importância do apoio da alta gestão, de assegurar a privacidade, a proteção dos dados pessoais e a segurança da informação, apresentar as principais mudanças trazidas pela LGPD, os riscos e as responsabilidades individuais dos agentes públicos no cumprimento dessa Lei Federal.

PASSO 8

Utilizar normas ISO para apoiar as ações de adequação à LGPD

Para dar suporte ao desenvolvimento das ações e atividades de adequação do órgão público à Lei Geral de Proteção de Dados Pessoais (LGPD), convém utilizar normas técnicas para subsidiar a gestão da privacidade, proteção de dados e segurança da informação, descrevendo as diretrizes e práticas a serem adotadas durante o processo.

Como vimos, a utilização de normas ABNT NBR ISO/IEC da família 27000 oferece diversas vantagens para o órgão público ao enfrentar os desafios de adequação à LGPD e implementação de Políticas de Segurança da Informação. Essas normas fornecem um conjunto de diretrizes reconhecidas internacionalmente, oferecendo um padrão robusto e confiável para a gestão da privacidade, proteção de dados pessoais e segurança da informação. **O capítulo 19** deste Guia apresenta as principais normas utilizadas pelo TCERO.





PASSO 9

Elaborar Programa de Governança em Privacidade (PGP)

A LGPD (Lei 13.709/2018), em sua Seção II, Das Boas Práticas e da Governança, informa, no art. 50 § 2º sobre as características mínimas de um Programa de Governança em Privacidade (PGP).

Um PGP captura e consolida os requisitos de privacidade com o intuito de ditar e influenciar como os dados pessoais são tratados (manuseados) em todo seu ciclo de vida. Ele é essencial para que o órgão público alcance a maturidade necessária na gestão de riscos aos dados pessoais e garanta a efetividade da conformidade com a LGPD.

É importante destacar que, a elaboração de um Programa de Governança em Privacidade deve ser feita de forma personalizada, considerando as características e necessidades específicas de cada órgão público.

Estratégia:

Na elaboração do PGP, o órgão público pode utilizar o “Guia de Elaboração de Programa de Governança em Privacidade”, da Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos, por meio do link:



[Governo Digital - Guia de Elaboração de Programa de Governança](#)

O Guia de Elaboração de Programa de Governança em Privacidade do Governo Federal 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.





PASSO 10

Elaborar um Plano de Comunicação sobre a LGPD

Comunicar interna e externamente sobre as ações e atividades realizadas para implementação da LGPD no órgão é fundamental para dar transparência à sociedade e aos órgãos de controle.

Estratégia:

Elabore um Plano de Comunicação para promover, de forma continuada e sistematizada, a divulgação das ações realizadas pelo órgão. Utilize cartilhas, banners, matérias jornalísticas, vídeos, boletins informativos, workshops entre outros, para informar sobre as ações do Programa de Governança em Privacidade a fim de criar uma cultura de proteção de dados, segurança da informação e privacidade, conscientizando e engajando servidores, estagiários, bolsistas e prestadores de serviços terceirizados sobre suas responsabilidades e obrigações diante da LGPD e demais normativos de segurança e proteção de dados do órgão.

PASSO 11

Realizar o Inventário de Dados Pessoais (IDP)

O processo de mapeamento dos dados, é conhecido também como de inventário de dados pessoais (IDP), que serve para identificar os tipos de dados pessoais que são tratados pelo órgão. É necessário realizar um mapeamento detalhado dos fluxos de dados pessoais. Isso envolve identificar quais dados pessoais são coletados, como são utilizados, onde são armazenados, como são compartilhados e qual é a finalidade e a necessidade desse tratamento. Esse mapeamento permite ter uma visão clara do ciclo de vida dos dados pessoais na instituição.





O mapeamento de dados pessoais é uma etapa que demanda muito esforço, sendo crucial no processo de conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), pois permite aos gestores públicos entenderem quais dados pessoais estão sendo tratados, de onde eles vêm, como são utilizados, para qual finalidade, com quem são compartilhados, entre outros.

Estratégia:

A etapa de inventário de dados pessoais (IDP) demanda muito esforço e atenção. Como estratégia para realizar um IDP fidedigno sobre o fluxo de dados pessoais no órgão, o DPO pode se reunir previamente com representantes das áreas a serem inventariadas para explicar a importância de todo o processo de mapeamento.

Para realizar as atividades e inventariar os dados pessoais, sugerimos utilizar o “Guia de Elaboração de Inventário de Dados Pessoais - LGPD” da Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos, disponível no link:

 [Guia de Elaboração de Inventário de Dados Pessoais - LGPD](#)

O documento é de autoria exclusiva da Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos 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.

Realizar o IDP é estar em conformidade com o previsto no art. 37 da LGPD, que determina que a Administração Pública, ao prestar diversos serviços que tratam dados pessoais à sociedade, deve manter registro das operações de tratamento realizadas sobre os dados que estão sob sua custódia.





Adicionalmente, a elaboração de um inventário de dados pessoais (IDP) visa a atender, além da LGPD, a outros normativos vigentes sobre o tema de privacidade e segurança da informação.

PASSO 12

Realizar a identificação e revisão de contratos relacionados a dados pessoais

O levantamento e a identificação dos contratos e acordos de cooperação que envolvem o tratamento de dados pessoais contribuem para as possíveis e necessárias adequações contratuais, tanto nos contratos e acordos existentes quanto nos futuros, por meio de aditivos de cláusulas específicas voltadas às obrigações de proteção de dados pessoais e sensíveis.

Estratégia:

O Encarregado (DPO) pode promover, junto à alta administração, a criação de um Grupo de Trabalho (GT) composto por agentes públicos que lidam diretamente com contratos e acordos de cooperação firmados pelo órgão, para atuar na identificação e catalogação dos instrumentos contratuais que envolvem o tratamento de dados pessoais, com o objetivo de incluir, por meio de aditivos, cláusulas e obrigações específicas sobre a proteção de dados pessoais.





PASSO 13

Elaborar Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

Como vimos, de acordo com a LGPD, o RIPD deve ser realizado sempre que o tratamento dos dados pessoais representar um alto risco às liberdades civis e aos direitos fundamentais dos titulares. Ele tem por objetivo analisar as possíveis consequências do tratamento desses dados, especialmente aquelas que podem afetar os direitos e liberdades dos titulares. Ao considerar as circunstâncias específicas do tratamento dos dados pessoais, é fundamental determinar se é necessário elaborar o Relatório de Impacto à Proteção de Dados Pessoais.

Estratégia:

Para realizar o RIPD, uma boa estratégia é seguir as orientações da Autoridade Nacional de Proteção de Dados (ANPD) que, dentre outras, disponibiliza uma página web com perguntas e respostas objetivando orientar e esclarecer a sociedade sobre o sobre o Relatório de Impacto à Proteção de Dados Pessoais.

O órgão público também pode utilizar o “Guia/Modelo de Relatório de Impacto à Proteção de Dados Pessoais (RIPD)” disponibilizado pela Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos, que tem como objetivo principal orientar a elaboração do RIPD que, em suma, é um documento de comunicação e transparência que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos, bem como propõe medidas, salvaguardas e mecanismos de mitigação.





O Guia/Modelo para elaboração do RIPD pode ser acessado por meio do link:

 [Governo Digital - Guia/Modelo de Relatório de Impacto à Proteção de Dados Pessoais \(RIPD\).](#)

Ao seguir esta estratégia, o órgão público pode garantir a elaboração e implementação eficaz do RIPD, demonstrando seu compromisso com a proteção de dados pessoais e a conformidade com a LGPD.

PASSO 14

Comunicar incidente de segurança

A Lei Geral de Proteção de Dados Pessoais (LGPD) determina aos agentes de tratamento de dados pessoais (controladores e operadores) a adoção de medidas para prevenir a ocorrência de danos aos titulares em virtude de suas atividades.

Na eventualidade de um incidente de segurança, uma importante medida de mitigação de danos é a comunicação da ocorrência aos titulares dos dados pessoais violados. Dessa forma, eles poderão tomar conhecimento do ocorrido e adotar medidas de precaução para mitigar os riscos a que foram expostos em razão do incidente.

A LGPD impõe aos controladores, em seu art. 48, o dever de comunicar aos titulares e à ANPD a ocorrência de incidentes que possam causar riscos ou danos relevantes aos titulares. O cumprimento dessa obrigação junto à ANPD e aos titulares afetados, se dá no processo de Comunicação de Incidente de Segurança (CIS).





Para obter orientações e reportar um incidente de segurança à ANPD basta acessar o seguinte link:

 [Governo Digital - Comunicação de Incidente de Segurança \(CIS\)](#)

OBS:

A Comunicação de Incidente de Segurança se destina exclusivamente aos controladores de dados pessoais. O titular para noticiar a ocorrência de um incidente com seus dados pessoais ou de terceiros, deve utilizar o canal de denúncia da ANPD disposto no seguinte link:

 [Canais de Atendimento - Denúncia de Descumprimento da LGPD](#)

Estratégia:

É desejável que o órgão institua uma Equipe de Tratamento e Resposta a Incidentes (ETIR), estabelecendo o fluxo e as responsabilidades para receber, analisar e responder às notificações e atividades relacionadas aos incidentes cibernéticos em sistemas computacionais e redes de dados no âmbito do órgão. A ETIR deve ser composta, preferencialmente, por agentes públicos com, no mínimo, conhecimentos em sistemas de informação, segurança cibernética, infraestrutura de redes, banco de dados e na LGPD.

Também é uma boa prática o órgão público criar um canal interno de comunicação para que em caso de ocorrência de incidente de segurança, o agente público que tiver conhecimento do fato possa reportar adequadamente para que a ETIR realize a triagem, análise, notificação e resposta ao incidente de segurança.





O Governo Federal disponibilizou por meio da Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos, o “Guia de Resposta a Incidentes de Segurança” que apresenta orientações e boas práticas para que as instituições e os profissionais de segurança da informação realizem o tratamento de incidentes cibernéticos, com enfoque em incidentes que envolvam dados pessoais.

Link do Guia:

 [Governo Digital - Guia de Resposta a Incidentes de Segurança](#)

PASSO 15

Aplicar capacitação em LGPD e segurança da informação

A capacitação dos agentes públicos em relação à LGPD e à segurança da informação e cibernética é essencial para garantir que eles compreendam as disposições da legislação, reconheçam os riscos de segurança relacionados ao tratamento de dados pessoais e saibam como agir de acordo com as melhores práticas de proteção de dados. Os treinamentos devem abordar, no mínimo, os seguintes temas: princípios da LGPD, direitos dos titulares de dados, bases legais para o tratamento de dados, os riscos e ameaças, e as medidas de segurança necessárias para proteger as informações sob responsabilidade do órgão público.





Estratégia:

Como visto, é importante promover palestras, treinamentos, workshops e seminários para os agentes de um órgão público, ministrados por especialistas nas áreas de privacidade e segurança da informação. Durante esses eventos, os agentes podem aprender sobre os requisitos da LGPD, os riscos de segurança cibernética e as melhores práticas para proteger os dados pessoais dos cidadãos com os quais lidam em suas atividades laborais no órgão.

PASSO 16

Realizar conscientização sobre boas práticas de proteção de dados

Além da capacitação formal, é importante promover a conscientização contínua sobre boas práticas de proteção de dados entre os agentes públicos. Isso inclui incentivar a adoção de medidas básicas, como o uso de senhas fortes, a atualização regular de software e a proteção adequada de dispositivos e arquivos. A conscientização também pode envolver a disseminação de informações sobre incidentes de segurança e exemplos de boas práticas em proteção de dados.

Exemplo:

Um exemplo de conscientização sobre boas práticas de proteção de dados é a distribuição de materiais educativos, como cartilhas, boletins, vídeos e folders, em locais visíveis nas unidades do órgão público, destacando dicas e recomendações para proteger os dados pessoais. Esses materiais podem incluir orientações sobre como identificar e relatar phishing, como proteger dispositivos móveis e como lidar com informações sensíveis e confidenciais, como aplicar técnicas para criar senhas fortes, entre outros.





PASSO 17

Usar plataformas gratuitas para capacitação continuada em LGPD

Uma boa estratégia para capacitar os agentes públicos é por meio dos cursos gratuitos ofertados pela Escola Virtual de Governo que desenvolveu um projeto que consiste em um conjunto de serviços disponibilizados em um Portal Único de Governo. Para o servidor ou cidadão que busca capacitação no serviço público, o Portal oferece um catálogo de cursos unificados das principais escolas de governo e centros de capacitação da Administração Pública Federal, incluindo cursos sobre a LGPD, governança de dados, segurança da informação, inteligência artificial, entre outros.

Os cursos da Escola Virtual de Governo podem ser acessados por meio do link:

 [Escola Virtual](#)

O Tribunal de Contas do Estado de Rondônia, por meio da Escola Superior de Contas (ESCon) elaborou “Portfolio de Atividades a Distância” abordando a Lei Geral de Proteção de Dados Pessoais (LGPD). Em razão da relevância do assunto, a ESCon reuniu uma coletânea de artigos informativos científicos, e-books, eventos (cursos), podcasts e vídeos, todos com a finalidade de propiciar o entendimento e contribuir para a disseminação de reflexões doutrinárias sobre a temática, incentivando a qualificação e aprimoramento dos agentes públicos do TCERO e dos órgãos jurisdicionados, assim como da própria sociedade civil organizada.

O Portfólio de Atividades a Distância – LGPD do TCERO pode ser acessado por meio do link:

 [Portfólio de Atividades a Distância – LGPD do TCERO](#)





PASSO 18

Elaborar Projeto para Implantar Programa de Governança em Privacidade (PGP)

Elaborar um projeto para adequação à LGPD em um órgão público é fundamental por várias razões. Em primeiro lugar, a LGPD impõe uma série de requisitos e responsabilidades para a proteção de dados pessoais, e um projeto bem estruturado é essencial para garantir a conformidade legal. Isso inclui a necessidade de criar, revisar e atualizar políticas internas, procedimentos operacionais e sistemas de informação para garantir que estejam alinhados com os princípios e requisitos da LGPD.

Com a elaboração de um projeto, será possível que o órgão público identifique e avalie os riscos associados ao tratamento de dados pessoais e implemente medidas adequadas de segurança e proteção. Isso ajuda a mitigar os riscos de violações de dados e protege a privacidade e os direitos dos cidadãos.

Um projeto estruturado e bem planejado facilita a gestão eficaz do processo de implementação da LGPD, garantindo a alocação adequada de recursos, o envolvimento de todas as partes interessadas e o cumprimento dos prazos e metas estabelecidos. Isso resulta em uma execução mais suave e eficiente, promovendo a confiança da sociedade e evitando possíveis sanções e penalidades por descumprimento da lei.





Neste contexto, convém que o órgão público se oriente pelas diretrizes das normas **NBR ISO/IEC da família 27000**, ou dos frameworks de segurança da informação disponíveis no mercado. Desta forma, é possível maximizar o nível de confidencialidade, integridade e disponibilidade das informações e processos críticos do órgão, além de adequar-se à Lei Federal 13.709/2018 (LGPD), por meio de ações voltadas à aplicação de diretrizes, de forma a potencializar o desempenho da organização pública nos aspectos de segurança da informação, privacidade e proteção de dados pessoais.

O projeto do PGP deve propor, no mínimo, um **conjunto básico de ações estruturantes** que fortaleçam e amparem a gestão da privacidade, a proteção dos dados pessoais e a segurança da informação na instituição a partir da utilização e aplicação de controles mais elevados e estruturados para conformidade à LGPD.

PASSO 19

Criar e executar plano de ação para implantação do Programa de Governança em Privacidade (PGP)

A implementação de um Programa de Governança em Privacidade (PGP) em um órgão público é um passo fundamental para garantir a conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) e proteger os dados pessoais sob sua guarda. No entanto, para que o PGP seja bem-sucedido e atinja seus objetivos, é crucial criar e executar um plano de ação estruturado e bem definido.

Um **plano de ação para gestão da implantação do PGP** em um órgão público oferece diversos benefícios, como:





- **Planejamento Estruturado:**

Um plano de ação bem elaborado define os objetivos, as metas, as atividades, os prazos, os recursos e os responsáveis pela implantação do PGP, proporcionando uma visão clara e organizada de todo o processo.

Essa clareza facilita a coordenação das ações, a alocação eficiente dos recursos e a comunicação entre os envolvidos, desde os gestores até os servidores públicos, garantindo um processo de implantação coeso, eficiente e transparente.

- **Implementação Sistemática e Gradual:**

O plano de ação define um cronograma detalhado para a implantação do PGP, dividindo o processo em etapas organizadas e sequenciais.

Essa abordagem gradual permite que o órgão público concentre seus esforços em cada etapa, garantindo a qualidade da implementação e evitando sobrecarga de trabalho.

Além disso, o plano de ação facilita a identificação de dependências entre as etapas, permitindo que sejam tomadas medidas para minimizar atrasos e garantir o cumprimento dos prazos.





- **Monitoramento e Avaliação Continuada:**

O plano de ação define indicadores de desempenho para acompanhar o progresso da implantação do PGP e avaliar sua efetividade.

Através de relatórios periódicos, é possível identificar desvios do cronograma, gargalos e oportunidades de melhoria, permitindo que sejam tomadas medidas corretivas quando necessário.

Esse monitoramento contínuo garante que o PGP esteja sendo implantado de acordo com o planejado e atendendo aos seus objetivos.

- **Comunicação Eficaz e Transparente:**

O plano de ação define uma estratégia de comunicação para informar e conscientizar os agentes públicos e os cidadãos sobre o PGP e sua importância.

Essa comunicação deve ser clara, transparente e acessível, utilizando diversos canais de comunicação, como boletins informativos, matérias jornalísticas, cartilhas, guias orientativos e campanhas de conscientização.

Uma comunicação eficaz promove o engajamento dos envolvidos, reduz resistências à mudança e garante o sucesso da implantação do PGP.





- **Gestão de Riscos:**

O plano de ação deve identificar e avaliar os riscos relacionados à implantação do PGP, como falta de conhecimento, resistência à mudança, falhas técnicas e violações de dados.

Para cada risco identificado, o plano de ação deve definir medidas de mitigação para minimizar seu impacto e garantir o sucesso da implantação.

A gestão eficaz dos riscos protege o órgão público de percalços e garante a segurança das informações.

PASSO 20

Monitoramento e acompanhamento contínuo do PGP

O Programa de Governança em Privacidade (PGP), instituído pelo Art. 50 da LGPD, exige um monitoramento e acompanhamento contínuos para garantir sua efetividade e o cumprimento das suas metas. Para tanto, o modelo **PDCA (Planejar, Fazer, Checar e Agir)** se apresenta como uma ferramenta fundamental para essa tarefa, permitindo um ciclo de melhoria contínua na gestão da privacidade dentro do órgão público.

Ao aplicar o ciclo PDCA de forma sistemática e diligente, o órgão garante:

- **Monitoramento contínuo do PGP:**

Acompanhamento constante do desempenho do programa, permitindo a identificação de falhas e oportunidades de melhoria em tempo hábil.





- **Melhoria contínua da gestão da privacidade:**

Implementação de medidas corretivas e ajustes no PGP com base nos resultados do monitoramento, garantindo a efetividade do programa e o cumprimento das metas.

- **Conformidade com a LGPD:**

Assegura que o tratamento de dados pessoais esteja em conformidade com as exigências da legislação, minimizando o risco de danos ao órgão, aos titulares de dados, sanções, entre outros.

- **Proteção dos dados pessoais:**

Garante a segurança da informação e a proteção dos dados pessoais dos cidadãos, construindo confiança e fortalecendo a imagem do órgão público.

- **Cultura de proteção de dados:**

Promove a cultura de proteção de dados entre os seus agentes públicos, conscientizando-os sobre a importância de assegurar a privacidade e o tratamento adequado dos dados pessoais sob sua responsabilidade.

Diversos elementos comprovam essa necessidade do monitoramento e acompanhamento contínuo do PGP, como:

- **Natureza Dinâmica do Ambiente:**

O ambiente em que o PGP é implementado está em constante mudança, com novas tecnologias, ameaças à segurança da informação e alterações na legislação surgindo frequentemente.





O monitoramento contínuo permite que o PGP seja adaptado a essas mudanças, garantindo que ele continue a ser eficaz na proteção dos dados pessoais.

- **Necessidade de Aprimoramento Contínuo:**

O PGP é um processo cíclico que requer melhoria contínua para garantir sua efetividade a longo prazo.

O monitoramento contínuo fornece informações valiosas para identificar áreas que podem ser aprimoradas e implementar as medidas necessárias.

- **Garantia de Conformidade com a LGPD:**

A LGPD exige que os órgãos públicos implementem medidas adequadas para proteger os dados pessoais dos cidadãos.

O monitoramento contínuo do PGP permite que o órgão público demonstre que está cumprindo suas obrigações legais, evitando sanções, danos aos titulares de dados, entre outros.

- **Prevenção de Falhas e Violações de Dados:**

O monitoramento contínuo permite que o órgão público identifique falhas e vulnerabilidades no PGP antes que elas causem danos.

Isso ajuda a prevenir violações de dados, que podem ter consequências graves para o órgão e para os cidadãos.





- **Promoção da Cultura de Proteção de Dados:**

O monitoramento contínuo do PGP demonstra o compromisso do órgão público com a proteção de dados e ajuda a promover uma cultura sobre o tema entre seus agentes públicos.

Isso aumenta a conscientização sobre a importância da privacidade e contribui para um ambiente mais seguro para o tratamento de dados pessoais, nos termos da LGPD.

- **Melhoria da Tomada de Decisões:**

As informações coletadas durante o monitoramento contínuo do PGP podem ser utilizadas para tomar decisões mais informadas sobre a gestão da privacidade.

Isso ajuda o órgão público a alocar recursos de forma mais eficiente e a implementar medidas de proteção de dados mais eficazes.

- **Fortalecimento da Transparência e da Confiança:**

O monitoramento contínuo do PGP demonstra para a sociedade e para os órgãos de controle, a transparência da instituição em relação ao tratamento de dados pessoais.

Isso fortalece a confiança dos cidadãos e contribui para uma relação mais positiva entre o órgão público e a sociedade.





29

GLOSSÁRIO DE PROTEÇÃO DE DADOS PESSOAIS DA ANPD





29 | GLOSSÁRIO DE PROTEÇÃO DE DADOS PESSOAIS DA ANPD

A Autoridade Nacional de Proteção de Dados (ANPD) lançou, seu Glossário de Proteção de Dados Pessoais. O documento contém o posicionamento oficial da Autoridade sobre o significado dos principais conceitos, termos e expressões usados na legislação de proteção de dados pessoais e nos documentos da Autarquia.

O Glossário oferece uma fonte de pesquisa vasta e confiável. O documento reúne informações até então dispersas em diversos documentos e indica as fontes das definições apresentadas, facilitando o acesso tanto a cidadãos quanto a profissionais da área.

Segundo a ANPD, o Glossário ficará permanentemente aberto a comentários e a contribuições. As sugestões podem ser enviadas para a Ouvidoria da ANPD, por meio da Plataforma Fala.BR do Governo Federal.

O Glossário de Proteção de Dados Pessoais da ANPD pode ser acessado neste link:

 [Glossário de Proteção de Dados Pessoais da ANPD](#)





REFERÊNCIAS BIBLIOGRÁFICAS





REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001:2023. Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27002:2022. Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27005:2023. Segurança da informação, segurança cibernética e proteção à privacidade — Orientações para gestão de riscos de segurança da informação.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27014:2021. Segurança da informação, segurança cibernética e proteção da privacidade — Governança da segurança da informação.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27032:2015. Tecnologia da informação – Técnicas de segurança – Diretrizes para segurança cibernética.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27035:2023. Tecnologia da informação — Gestão de incidentes de segurança da informação - Parte 1: Princípios e processo.





ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27701:2020. Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação-Requisitos e diretrizes.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 29100:2020. Tecnologia da informação – Técnicas de segurança – Estrutura de privacidade.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 29134:2020. Tecnologia da informação – Técnicas de segurança – Avaliação de impacto de privacidade - Diretrizes.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 29151:2020. Tecnologia da informação — Técnicas de segurança — Código de prática para proteção de dados pessoais.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 29184:2021. Tecnologia da informação — Avisos de privacidade on-line e consentimento.

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA/AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS/CONSELHO DIRETOR. 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: 01 ago. 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: 26 abr. 2024.





SECRETARIA DE GOVERNO DIGITAL (SGD). Guia de Elaboração de Termo de Uso e Política de Privacidade. Disponível em: <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_termo_uso_politica_privacidade.pdf>. Acesso em: 15 mar. 2024.

SECRETARIA DE GOVERNO DIGITAL (SGD). Guia Orientativo - Tratamento de Dados Pessoais pelo Poder Público. Disponível em: <<https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf>>. Acesso em: 15 mar. 2024.

SECRETARIA DE GOVERNO DIGITAL (SGD). Guia de Inventário de Dados Pessoais. Disponível em: <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_inventario_dados_pessoais.pdf>. Acesso em: 19 mar. 2024.

SECRETARIA DE GOVERNO DIGITAL (SGD). Modelo de Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação. Disponível em: <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/modelo_politica_desenvolvimento_pessoas.pdf>. Acesso em: 19 mar. 2024.

SECRETARIA DE GOVERNO DIGITAL (SGD). Guia de Elaboração de Programa de Governança em Privacidade. Disponível em: <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_programa_governanca_privacidade.pdf>. Acesso em: 21 mar. 2024.

SECRETARIA DE GOVERNO DIGITAL (SGD). Cartilha sobre Finalidade e Hipóteses Legais. Disponível em: <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/cartilha_finalidade_hipoteses_legais.pdf>. Acesso em: 12 fev. 2024.





SECRETARIA DE GOVERNO DIGITAL (SGD). Manual de Implementação da LGPD. Disponível em: <https://www.cge.pr.gov.br/sites/default/arquivos_restritos/files/documento/2021-06/manual_implementacao_lgpd.pdf>. Acesso em: 12 fev. 2024.

SECRETARIA DE GOVERNO DIGITAL (SGD). Guias e Modelos do Programa de Privacidade e Segurança da Informação (PPSI). Disponível em: <<https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias-e-modelos>>. Acesso em: 12 fev. 2024.

PROCURADORIA GERAL DO ESTADO DE RONDÔNIA. Guia LGPD - Boas Práticas da Lei Geral de Proteção de Dados. Disponível em: <<https://pge.ro.gov.br/wp-content/uploads/2024/04/GUIA-DE-BOAS-PRATICAS-LEI-GERAL-DE-PROTECAO-DE-DADOS-LGPD.pdf>>. Acesso em: 16 fev. 2024.

SECRETARIA DE ESTADO DE FINANÇAS DO ESTADO DE RONDÔNIA. Você sabe o que é LGPD?. Disponível em: <<https://www.sefin.ro.gov.br/portalsefin/userfiles/Cartilha-LGPD-SEFIN.pdf>>. Acesso em: 16 abr. 2024.

SECRETARIA DE GOVERNO DIGITAL - Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_r etificada.pdf>. Acessado em: 16 abr. 2024.

CONTROLADORIA GERAL DO ESTADO DO PARANÁ. Manual de implementação da LGPD. Disponível em: <https://www.cge.pr.gov.br/sites/default/arquivos_restritos/files/documento/2021-06/manual_implementacao_lgpd.pdf>. Acesso em: 17 abr. 2024.





ANEXO





ANEXO

CATEGORIAS E TIPOS DE DADOS PESSOAIS E SENSÍVEIS

CATEGORIAS DE DADOS	
DADOS PESSOAIS	DADOS PESSOAIS SENSÍVEIS
• Dados de Identificação Pessoal • Dados Financeiros • Características Pessoais • Hábitos Pessoais • Características Psicológicas • Composição Familiar • Interesse de Lazer • Associações • Processo Judicial/Administrativo/Criminal • Hábitos de Consumo • Dados Residenciais • Educação e Treinamento • Profissão e Emprego • Registro/Gravações de vídeo, imagem e voz	• Dados que revelam origem racial ou étnica • Dados que revelam convicção religiosa • Dados que revelam opinião política • Dados que revelam filiação a sindicato • Dados que revelam filiação a organização de caráter religioso • Dados que revelam filiação ou crença filosófica • Dados que revelam filiação ou preferências política • Dados referentes à saúde ou à vida sexual • Dados genéticos • Dados biométricos





TIPOS DE DADOS

DADOS PESSOAIS	DADOS PESSOAIS SENSÍVEIS
• Nome • Data de nascimento • Endereço residencial • Identificadores nacionais (por exemplo, CPF, RG, nº de passaporte) • Endereço de e-mail pessoal • Número do telefone pessoal • Fotografia ou vídeo identificado a uma pessoa natural • Contas de serviços públicos • Salários dos empregados e arquivos dos recursos humanos • Perfil financeiro • Extratos de cartão de crédito • Número do cliente • Conta bancária ou número de cartão de crédito • Localização fornecida por sistemas de telecomunicação • Trajetória no GPS • Posição no GPS • Endereço IP • Condenações criminais ou delitos cometidos • Alegações de conduta criminosa • Relatórios de investigação criminal • Número de identificação pessoal (PIN) ou senha • Perfil pessoal ou comportamental • Preferências de produtos ou serviços • Interesses pessoais derivados do rastreamento do uso	• Origem racial ou étnica • Crenças religiosas ou filosóficas • Orientação sexual • Filiação sindical • Histórico médico • Gênero • Contas médicas • Informação de diagnóstico de saúde • Deficiências • Identificador biométrico • Qualquer informação coletada durante serviços de saúde • Idade ou necessidades especiais de pessoas naturais vulneráveis

Fontes: Lei nº 13.709/2018; Norma ABNT NBR ISO/IEC 29100:2020; Guia de Inventário de Dados Pessoais - Governo Federal.





ISBN: 978-85-64505-18-6

CRL



9 788564 505186



ID: 1271292 e CRC: FF5ACBFA



Município de Espigão do Oeste

04.695.284/0001-39

Rua Rio Grande do Sul, 2800 - Vista Alegre

www.espigaodooeste.ro.gov.br

FICHA CADASTRAL DO DOCUMENTO ELETRÔNICO

Tipo do Documento		Identificação/Número		Data
Guia		LGPD - TCERO		24/11/2025
ID:	1271292		Processo	Documento
CRC:	FF5ACBFA			
Processo:	65-5/2025			
Usuário:	Alisson Ludtke Schwanz			
Criação:	24/11/2025 10:35:12	Finalização:	24/11/2025 10:35:29	
MD5:	9E99AE2824C4EFCB2D755A088B220A1E			
SHA256:	37905BA45ED61CC6FA4641D92B3BEB24ACBB2D4075B5FAB5564CCC6FDFDFD06B			

Súmula/Objeto:

Solicitação de abertura imediata de processo interno para análise e implementação da resolução que institui o Comitê e as Políticas de Proteção de Dados, em atendimento ao Acórdão do TCE-RO.

INTERESSADOS

Amilton Alves de Souza	Espigão dOeste	RO	24/11/2025 10:35:12
------------------------	----------------	----	---------------------

ASSUNTOS

Abertura de processo administrativo	24/11/2025 10:35:12
-------------------------------------	---------------------

DOCUMENTOS RELACIONADOS

Ofício 6	24/11/2025	1271130
----------	------------	---------

ASSINATURAS ELETRÔNICAS



Alisson Ludtke Schwanz

Técnico em Informática

06/02/2026 10:44:06

Assinado na forma do Resolução Municipal nº 90/2021.

A autenticidade deste documento pode ser conferida através do QRCode acima ou ainda através do site transparencia.espigaodooeste.ro.gov.br informando o ID 1271292 e o CRC FF5ACBFA.