



RIO GRANDE DO NORTE

INSTRUÇÃO NORMATIVA Nº 02/2023 - CONTROL, DE 12 DE JULHO DE 2023

Orienta todos os Órgãos e Entidades do Poder Executivo Estadual acerca das diretrizes referentes ao tratamento de dados pessoais.

A CONTROLADORA-GERAL DO ESTADO, no uso das atribuições que lhe confere o inciso VIII, do art. 7º, da Lei Complementar nº 638, de 28 de junho de 2018 e o Art. 22, do Decreto Estadual nº 32.815, de 12 de julho de 2023;

CONSIDERANDO o disposto na Lei Federal nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados (LGPD) e o estabelecido no Decreto Estadual nº 32.815, de 12 de julho de 2023, que regulamenta a Lei nº 13.709, de 14 de agosto de 2018, no âmbito do Poder Executivo Estadual e dá outras providências;

CONSIDERANDO que a Controladoria-Geral do Estado do Rio Grande do Norte (CONTROL/RN), Órgão central do controle interno do Poder Executivo Estadual é competente para o gerenciamento das atividades de institucionalização e fomento à Lei Geral de Proteção de Dados (LGPD), nos termos do art. 8, do Decreto Estadual nº 32.815, de 12 de julho de 2023,

RESOLVE:

CAPÍTULO I DAS DISPOSIÇÕES GERAIS

Art. 1º Os procedimentos relativos à privacidade e à proteção de dados pessoais, no âmbito da Administração Pública do Poder Executivo Estadual, deverão obedecer às disposições estabelecidas nesta Instrução Normativa.

Art. 2º A Política de Proteção de Dados Pessoais da Administração Pública Potiguar (PPDPAP/RN) tem por finalidade estabelecer o conjunto de diretrizes, normas, objetivos, decisões públicas, metas, indicadores de avaliação, sistemas de governança, programas e ações estratégicas finalísticas coordenadas para a formulação, a implementação e a avaliação do desenvolvimento e da adaptação da ação governamental, no âmbito da administração pública do Poder Executivo Estadual à Lei Federal nº 13.709, de 2018.

Art. 3º A PPDPAP/RN e suas eventuais normas complementares, metodologias, manuais e procedimentos é de observância obrigatória à todos os órgãos e entidades do Poder Executivo Estadual, abrangendo os servidores, prestadores de serviço, colaboradores, estagiários, consultores externos e quem, de alguma forma, desempenhe atividades de tratamento de dados pessoais.

Art. 4º A PPDPAP/RN tem por objetivos:

I - proporcionar a adequação das atividades desenvolvidas pela Administração Pública Potiguar à LGPD e aos regulamentos, resoluções e orientações emitidas pela Autoridade Nacional de Proteção de Dados Pessoais - ANPD;

II - produzir informações íntegras, confiáveis e completas das demandas dos titulares do dado;

III - salvaguardar o direito à proteção dos dados pessoais dos titulares;

IV - possibilitar a adequada apuração dos responsáveis, em todos os níveis, que tenham acesso inadequado aos dados pessoais, em especial, aqueles considerados sensíveis;

V - reduzir os riscos relacionados a incidentes envolvendo dados pessoais, com a implantação de medidas de controle de segurança da informação; e

VI - orientar e servir de diretriz.

Art. 5º São diretrizes da PPDPAP/RN:

I – a definição de objetivos e metas para as estratégias de adequação à LGPD e para os programas de governança em privacidade e o monitoramento dos resultados;

II - a gestão e o fortalecimento da integridade institucional com a promoção da cultura ética sob a perspectiva da preservação da privacidade;

III - o desenvolvimento contínuo do nível de maturidade dos tratamentos dos dados;

IV – o alinhamento com as políticas de segurança da informação do Estado do Rio Grande do Norte;

V – o alinhamento com as boas práticas de transparência e as regras definidas na Lei Estadual nº 9.963, de 27 de julho de 2015, no seu decreto regulamentador e na Lei Complementar nº 638, de 28 de junho de 2018, e seus substitutos normativos;

VI – a implementação de processos de gestão de risco pelos órgãos e entidades abrangidos por este Decreto para balizar a adoção de boas práticas e regras de governança associadas ao Programa de Governança em Privacidade;

VII - a manutenção da segurança jurídica dos instrumentos firmados;

VIII - a proporcionalidade das medidas acerca de proteção de dados, privacidade e segurança da informação;

IX - o atendimento tempestivo, simplificado e, preferencialmente, eletrônico às demandas do titular de dados pessoais;

X – divulgação permanente e sensibilização dos gestores e servidores sobre a relevância da conformidade do tratamento de dados pessoais; e

XI – outras diretrizes estabelecidas pela Instância de Controle e Governança e pelo Comitê Gestor de Dados e Informações

Parágrafo único. O modelo de gestão de gerenciamento de riscos deve seguir o método de priorização de processos, considerando sua relevância e impacto na estratégia da Secretaria.

Art. 6º O método de priorização de processos deverá seguir a seguinte disposição:

I – Processos prioritários: serão avaliados imediatamente e reavaliados bianualmente;

II – Processos relevantes: serão avaliados no ano subsequente e reavaliados a cada três anos;

III – Processos não-prioritários: serão avaliados em dois anos e reavaliados a cada quatro anos.

Parágrafo único. A classificação de priorização será realizada por meio de ato aprovado pela Controladoria-Geral do Estado (CONTROL-RN), e possuirá metodologia própria.

CAPÍTULO II DO TRATAMENTO DE DADOS PESSOAIS

Art. 7º As atividades de proteção de dados pessoais no âmbito do Poder Executivo Estadual, bem como seus instrumentos resultantes, deverão observar os princípios estabelecidos no Decreto Estadual nº 32.815, de 12 de julho de 2023 e, ainda, os seguintes:

I - aderência à integridade e aos valores éticos no tratamento de dados pessoais;

II - adequado suporte de tecnologia da informação para apoiar os processos de adaptação dos tratamentos de dados pessoais;

III - disseminação de informações necessárias ao fortalecimento da cultura do tratamento de dados pessoais em respeito à Lei Federal nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais – LGPD;

IV - realização de avaliações periódicas internas para verificar a eficácia da proteção de dados pessoais, comunicando o resultado aos responsáveis pela adoção de ações corretivas, inclusive à alta administração;

V - estruturação do conhecimento e das atividades em metodologias, normas, manuais e procedimentos;

VI - aderência dos métodos e modelos de tratamento de dados às exigências regulatórias da LGPD.

Art. 8º. O tratamento de dados pessoais realizados pela Administração Pública do Poder Executivo Estadual será realizado com vistas ao atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar suas competências legais e de cumprir as atribuições legais do serviço público.

Art. 9º. Os dados pessoais tratados pela Administração Pública do Poder Executivo Estadual deverão:

I - ser protegidos por procedimentos internos para registrar autorizações e utilizações;

II - mantidos disponíveis, exatos, adequados, pertinentes e atualizados, sendo retificado ou eliminado o dado pessoal mediante informação ou constatação de impropriedade ou face à solicitação de descarte, devendo a neutralização ou descarte do dado observar as condições e períodos da tabela de temporalidade de retenção de dados;

III - compartilhados somente para o exercício das funções institucionais ou para atendimento de políticas públicas aplicáveis; e

IV - revistos em periodicidade mínima bianual, sendo de imediato eliminados aqueles que já não forem necessários, por terem cumprido sua finalidade ou por ter se encerrado o seu prazo de retenção.

Art. 10 Quando do compartilhamento ou uso compartilhado de dados pessoais pelos órgãos e entidades da Administração Pública Estadual com outros órgãos e entidades públicas, para atender a finalidades específicas de execução de políticas públicas, no âmbito de suas atribuições legais, poderá o órgão ou entidade requisitado solicitar esclarecimentos ao órgão ou entidade requisitante, de modo a atender à boa-fé e aos princípios previstos na Lei Federal nº 13.709/2018.

Art. 11 Os órgãos e entidades da Administração Pública Estadual somente poderão efetuar a comunicação ou o uso compartilhado de dados pessoais a pessoa de direito privado com prévia comunicação a Controladoria-Geral do Estado - CONTROL/RN, que informará à Autoridade Nacional de Proteção de Dados (ANPD), na forma do regulamento federal correspondente, em atenção ao artigo 27, da Lei Federal nº 13.709/2018.

Art. 12 Os órgãos e entidades da Administração Pública do Poder Executivo Estadual deverão:

I – elaborar um Plano operacional de adequação (POA) que descreva todas as ações desenvolvidas e a serem desenvolvidas para a implementação do sistema normativo de proteção de dados pessoais em vigor, observadas as disposições do Decreto Estadual nº 32.815, de 12 de julho de 2023 e a presente Instrução Normativa a ser submetido à aprovação pela Controladoria-Geral do Estado;

II – certificar-se de que o compartilhamento e o uso compartilhado de dados pessoais sejam realizados apenas em locais adequados e aprovados, por meios autorizados, não sendo possível o uso de sistemas de acesso não fornecidos ou não permitidos pela Administração Pública Estadual, assim como o armazenamento de dados pessoais e informações em contas não-organizacionais ou particulares; e

III – estimular a participação em capacitações dos responsáveis ou de equipe, preferencialmente efetivos, com atribuições relativas ao tratamento de dados pessoais, especialmente sobre os riscos de compartilhamento e uso compartilhado de dados pessoais.

Parágrafo único. A Controladoria-Geral do Estado (CONTROL-RN) publicará guias orientativos que objetivem nortear a implementação das disposições gerais desta Instrução Normativa.

Art. 13 Poderá implicar em responsabilização das autoridades:

I – o descumprimento das recomendações, solicitações e ordens expedidas pela Controladoria-Geral do Estado, no prazo fixado, quando ausente justificativa;

II – o não encaminhamento de informações, no prazo por este fixado, sobre o tratamento de dados pessoais, que venham a ser solicitadas pela Autoridade Nacional de Proteção de Dados (ANPD);

III – o não encaminhamento de Relatório de Impacto à Proteção de Dados Pessoais ou de informações necessárias à sua elaboração;

IV – a não disponibilização de informações que assegurem, de forma adequada e em tempo útil, o conhecimento sobre todas as questões relacionadas com a proteção de dados pessoais no âmbito do Poder Executivo Estadual; e

V – a não disponibilização das informações sobre o fluxo de dados pessoais tratados por cada unidade, quando solicitado.

CAPÍTULO III

DO PLANO OPERACIONAL DE ADEQUAÇÃO

Art. 14. Relatórios sobre o Plano operacional de adequação (POA), previsto no artigo 12, inciso I, da presente instrução normativa, deverão ser publicados e anualmente atualizados, observados os seguintes requisitos:

I – publicidade das informações relativas ao tratamento de dados pessoais em veículos de fácil acesso, preferencialmente nas páginas dos órgãos e entidades, na Internet, bem como no Portal da Transparência;

II – atendimento das exigências que vierem a ser estabelecidas pela Autoridade Nacional de Proteção de Dados (ANPD), nos termos do artigo 23, § 1º, e do artigo 27, parágrafo único, da Lei Federal nº 13.709/2018;

III – manutenção de dados em formato interoperável e estruturado para o compartilhamento e uso compartilhado de dados pessoais 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;

IV – elaboração de Mapeamento de Dados Pessoais de cada processo realizado pelo órgão ou entidade, contendo, no mínimo, as seguintes informações:

- a) data de criação e de atualização do mapeamento de dados pessoais;
- b) identificação dos processos nos quais há o tratamento de dados pessoais;
- c) identificação dos agentes de tratamento e do Encarregado;
- d) fases do ciclo de vida do tratamento de dados pessoais;
- e) natureza e escopo do tratamento de dados pessoais;
- f) finalidade do tratamento de dados pessoais;
- g) categorias de dados pessoais tratados, inclusive com a descrição das categorias de dados pessoais sensíveis;
- h) volume das operações de tratamento e das categorias de dados pessoais tratados;
- i) categorias de titulares de dados pessoais;
- j) compartilhamento e uso compartilhado de dados pessoais, inclusive com a descrição dos agentes de tratamento com os quais os dados pessoais são compartilhados;
- k) contratos de serviços e soluções de tecnologia da informação que tratam os dados pessoais do processo mapeado;

l) transferência internacional de dados pessoais; e
m) gestão de riscos à segurança da informação, à privacidade e à proteção de dados pessoais.

V – elaboração de Relatório de Impacto à Proteção de Dados Pessoais, que contenha as seguintes informações:

a) data de criação e de atualização do Relatório de Impacto à Proteção de Dados Pessoais;

b) identificação dos agentes de tratamento e do Encarregado;

c) necessidade de sua elaboração ou atualização;

d) descrição do tratamento de dados pessoais, com base no mapeamento de dados pessoais;

e) natureza e escopo do tratamento de dados pessoais;

f) contexto e necessidade do tratamento de dados pessoais;

g) finalidade do tratamento de dados pessoais;

h) gestão de riscos à segurança da informação, à privacidade e à proteção de dados pessoais; e

i) partes consultadas durante a elaboração do Relatório de Impacto à Proteção de Dados Pessoais.

Art. 15. Os Planos operacionais de adequação (POA), a serem elaborados deverão ser encaminhados à Controladoria Geral do Estado (CONTROL) para análise e aprovação, que poderá:

I – emitir orientações de adequação aos termos desta Instrução Normativa, do Decreto Estadual nº 32.815/2022 e da Lei Federal nº 13.709/2018; e

II - solicitar informações quanto ao Plano elaborado e submetido.

Parágrafo único. A Controladoria Geral do Estado (CONTROL-RN), no que couber, auxiliará os órgãos e as entidades da Administração Pública Estadual no cumprimento das obrigações definidas nesta Instrução Normativa.

CAPÍTULO IV

DAS DISPOSIÇÕES FINAIS

Art. 16 Os órgãos da Administração Pública Estadual deverão disponibilizar, em seus sítios eletrônicos e em lugares visíveis das respectivas instalações físicas, às hipóteses de tratamento de dados pessoais, bem como fornecer instrumentos adequados para que o titular de dados pessoais manifeste o seu consentimento, quando necessário, de forma livre, informada e inequívoca, conforme o artigo 5º, inciso XII, da Lei Federal nº 13.709/2018.

Art. 17 A implementação desta Política de Proteção de Dados Pessoais da Administração Pública Potiguar (PPDPAP/RN) será realizada de forma imediata.

Art. 18 Os casos omissos ou excepcionalidades serão deliberados pelo Controlador-Geral do Estado, podendo ser consultado o Comitê Gestor de Dados e Informações do Estado do Rio Grande do Norte.

Art. 19 Esta Instrução Normativa entra em vigor na data de sua publicação.

Controladoria-Geral do Estado, Natal/RN, 12 de julho de 2023.

LUCIANA DALTRO DE CASTRO PÁDUA

Controladora-Geral do Estado