

DECRETO RIO Nº 49558 DE 6 DE OUTUBRO DE 2021

Estabelece os procedimentos iniciais a serem adotados pela Administração Pública Municipal visando à construção de uma cultura de proteção de dados pessoais e dá outras providências.

O PREFEITO DA CIDADE DO RIO DE JANEIRO no uso de suas atribuições legais e,

CONSIDERANDO o disposto no inciso X, do art. 5º, da Constituição da República Federativa do Brasil, o qual estabelece que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas;

CONSIDERANDO o disposto no inciso VI, do art. 107, da Lei Orgânica do Município do Rio de Janeiro;

CONSIDERANDO o disposto no art. 25, da Lei Federal nº 12.527, de 18 de novembro de 2011, que estabelece que é dever do Estado controlar o acesso e a divulgação de informações sigilosas produzidas por seus órgãos e entidades, assegurando sua proteção;

CONSIDERANDO o disposto na Lei Federal nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais - LGPD;

CONSIDERANDO que o parágrafo único, do art. 1º, da LGPD, estabelece que as normas gerais de proteção contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios;

CONSIDERANDO ser assegurado a toda pessoa natural a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos do art. 17, da LGPD;

CONSIDERANDO que a Prefeitura da Cidade do Rio de Janeiro busca construir sua própria política de proteção de dados, baseada nos princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas, nos termos do art. 6º, da LGPD;

CONSIDERANDO o disposto no Decreto Rio nº 48.349, de 1º de janeiro de 2021, que instituiu o Programa Carioca de Integridade Pública e Transparência - Rio Integridade; e

CONSIDERANDO as conclusões constantes do Relatório do Grupo de Trabalho Governo Digital, em especial o diagnóstico constante da Área 6 do Relatório, que contém as conclusões relativas à proteção de dados pessoais e sensíveis,

DECRETA:

CAPÍTULO I **DISPOSIÇÕES GERAIS**

Art. 1º O presente Decreto tem por objetivo iniciar a adequação da Prefeitura da Cidade do Rio de Janeiro - PCRJ a uma cultura de proteção de dados nos serviços e políticas executados pelo Poder Executivo Municipal, através do estabelecimento de um Programa de Proteção de Dados.

Art. 2º Para fins deste Decreto, 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 dos dados: 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, devendo fornecer elementos decisórios essenciais ao operador;

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 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;

IX - Agentes de tratamento de dados pessoais: o controlador e o operador;

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

XVI - Uso compartilhado de dados pessoais: 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 (RIPD): documentação do controlador, conforme definido no inciso VI, do art. 2º, 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;

XIX - Autoridade Nacional de Proteção de Dados - ANPD: órgão da Administração Pública Federal, cujos papéis e competências estão definidos na Lei Federal nº 13.709, de 14 de Agosto de 2018, (Lei Geral de Proteção de Dados - LGPD), entre eles: elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e fiscalizar e aplicar sanções em caso de tratamento de dados realizado

em descumprimento à legislação; e

XX - Incidente de Segurança de Dados: violação às medidas de segurança, técnicas e administrativas implementadas para 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.

Parágrafo único. As regras constantes da LGPD aplicam-se à Prefeitura da Cidade do Rio de Janeiro, assim como os regulamentos e as orientações publicadas pela Autoridade Nacional de Proteção de Dados.

CAPÍTULO II **DO PROGRAMA DE PROTEÇÃO DE DADOS PESSOAIS**

Art. 3º Fica estabelecido o Programa de Proteção de Dados, constituído por frentes de atuação divididas nos seguintes eixos, assim definidos:

I - Eixo compreender o problema: elaboração de um conjunto de diagnósticos que permita mapear os tratamentos de dados pessoais e sensíveis que são realizados pela Prefeitura, além de possibilitar a análise dos riscos envolvidos.

II - Eixo criar e revisar normativos: criação de uma Política Municipal de Proteção de Dados para o Poder Executivo Municipal, que abrangerá os atores relevantes para a implementação da política, as competências desses atores, os instrumentos, os processos de trabalho e as atividades atinentes à Política, bem como a produção de textos normativos e regulatórios.

III - Eixo gerenciar riscos: identificação dos riscos e definição das medidas para mitigá-los, estruturando-se ferramentas, instrumentos e processos de trabalho para dirimir os riscos, criar respostas a incidentes de segurança de dados e realizar as comunicações previstas na legislação e regulamentos.

IV - Eixo elaborar instrumentos: desenvolvimento de metodologias, minutas-padrão, modelos de documentação e procedimentos para que os instrumentos necessários ao atendimento dos direitos dos titulares e demais dispositivos constantes na LGPD e legislação correlata, bem como em regulamentos complementares, venham a ser implementados.

V - Eixo capacitar e sensibilizar: promoção de capacitação para os agentes públicos da PCRJ, de modo a fomentar uma cultura de proteção de dados no âmbito da Administração Pública Municipal, além da realização de workshops, seminários, rodas de conversa e demais eventos mobilizadores, que poderão contar com a participação da sociedade civil e de especialistas em temas relativos à proteção e governança de dados.

Parágrafo único. Caberá à Secretaria Municipal de Governo e Integridade Pública - SEGOVI propor as medidas de governança necessárias à implementação do Programa de Proteção de Dados no âmbito da PCRJ.

Art. 4º Ficam estabelecidas as seguintes regras de transição para a implementação do Programa de Proteção de Dados na PCRJ:

I - Compete à Procuradoria Geral do Município - PGM: propor cláusula-padrão acerca da proteção de dados pessoais que passe a ser utilizada por toda a Administração Municipal Direta e Indireta;

II - Compete à Controladoria Geral do Município - CGM: propor, em conjunto com a SEGOVI, a metodologia de análise de riscos que orientará os órgãos e entidades da Administração na identificação e tratamento dos riscos referentes à proteção de dados;

III - Compete à SEGOVI:

a) aplicação do questionário de avaliação de maturidade para todos os órgãos e entidades da Administração Pública Municipal Direta e Indireta, além da compilação dos resultados obtidos, de modo a obter informações qualificadas que permitam subsidiar a elaboração da Política Municipal de Proteção de Dados;

- b) esclarecimento de eventuais dúvidas dos órgãos e entidades da Administração Pública Municipal Direta e Indireta acerca da proteção de dados e da governança de dados até que a Política Municipal de Proteção de Dados esteja implementada; e
- c) construção das orientações para atendimento aos titulares de dados pessoais, de modo que o exercício de direito dos titulares seja plenamente garantido, providenciando as capacitações necessárias, além das adequações dos sítios eletrônicos e canais institucionais de comunicação para que os titulares possam solicitar o acesso facilitado às informações sobre o tratamento de seus dados no âmbito da Prefeitura.

§ 1º Os órgãos e entidades da Administração Pública Municipal Direta e Indireta, que realizam compartilhamento de dados com operadores, deverão identificar e mapear os dados compartilhados, a finalidade do compartilhamento, quem terá acesso a esses dados, entre outros elementos, de forma a produzir, posteriormente, orientações aos operadores, conforme modelo a ser encaminhado pela SEGOVI.

§ 2º Os órgãos e entidades da Administração Pública Municipal Direta e Indireta deverão encaminhar à SEGOVI, no prazo de 15 (quinze) dias após a publicação deste Decreto, a indicação de pelo menos 1 (um) ponto focal para a realização de capacitação e para a futura elaboração de documentos, normativos e instrumentos relativos à proteção de dados, devendo os profissionais indicados possuir o seguinte perfil mínimo:

- I - possuir conhecimento das bases de dados, digitais e não digitais, existentes no órgão ou entidade;
- II - possuir acesso ao nível estratégico do órgão ou entidade;
- III - possuir disponibilidade para participar das capacitações que serão indicadas; e
- IV - possuir perfil proativo, dinâmico e realizador.

§ 3º Os pontos focais de cada órgão e entidade da Administração Pública Municipal Direta e Indireta devem ser indicados considerando-se a possibilidade de, futuramente, serem objeto de nova indicação para atuarem como encarregados pelo tratamento de dados pessoais, de modo a exercerem as atribuições constantes do art. 41, da LGPD.

§ 4º O questionário de avaliação de maturidade a que se refere a alínea "a", do inciso III, do art. 4º, deve ser respondido por todos os órgãos e entidades da Administração Pública Direta e Indireta Municipal, contendo o máximo de informações acerca das bases de dados, digitais ou não, de sua instituição, devendo ser feito um esforço proativo de obtenção de informações realistas e descriptivas, de modo a corresponder à realidade de atuação e exercício das suas atividades.

§ 5º Os órgãos e as entidades da Administração Pública Municipal Direta e Indireta podem efetuar o uso compartilhado de dados pessoais a que se refere o inciso XVI, do art. 2º, com outros órgãos e entidades públicas para atender a finalidades específicas de execução de políticas públicas, no âmbito de suas atribuições legais, observados os princípios de proteção de dados pessoais elencados no art. 6º da LGPD.

Art. 5º Caberá à Empresa Municipal de Informática - IPLANRIO:

- I - implementar e administrar, direta ou indiretamente, métodos de desenvolvimento, implantação e gerenciamento de serviços Tecnologia da Informação e Comunicação - TIC que promovam a proteção dos dados pessoais;
- II - zelar pela conformidade dos serviços de TIC a todas as políticas e normas de Proteção de Dados Pessoais;
- III - avaliar os novos sistemas, aplicativos e bancos de dados que possam realizar tratamento dos dados pessoais a serem implementados pelos órgãos e entidades da Administração Pública Municipal Direta e Indireta, até que a Política Municipal de Proteção de Dados esteja implementada, elaborando resoluções e demais instrumentos normativos para que essa avaliação seja realizada; e
- IV - atualizar e adequar a política de segurança da informação sob sua responsabilidade para o atendimento às exigências constantes da Lei Geral de Proteção de Dados.

Art. 6º Caberá aos órgãos e entidades da Administração Pública Municipal Direta e Indireta, enquanto a Política de Proteção de Dados não tiver sido implementada:

I - gerenciar os riscos relativos ao tratamento de dados pessoais, conforme metodologia de análise de riscos a ser divulgada pela SEGOVI em conjunto com a Controladoria Geral do Município - CGM;

II - elaborar os mapeamentos e inventários de dados, conforme metodologia a ser divulgada pela SEGOVI;

III - identificar contratos, convênios, Termos de Cooperação, Acordos de Resultados, editais de licitação e demais documentos jurídicos congêneres em que se realize o tratamento de dados ou o compartilhamento de dados pessoais e que possam precisar de futuras modificações para serem adequados à LGPD;

IV - zelar para que todos os processos, sistemas e serviços que tratem dados pessoais estejam em conformidade com as políticas e normas de proteção de dados pessoais;

V - identificar quais funcionários atuam no tratamento de dados pessoais e dados sensíveis, de modo a que esses funcionários futuramente assinem Termos de Responsabilidade;

VI - identificar quais são os compartilhamentos de dados pessoais e dados sensíveis realizados com terceiros, sejam eles públicos ou privados;

VII - disseminar aos agentes públicos o conhecimento das políticas e normas de governança digital, assim como das melhores práticas de proteção de dados pessoais;

VIII - realizar a elaboração do Relatório de Impacto de Proteção de Dados, conforme exigido na LGPD, com base na metodologia a ser divulgada pela SEGOVI.

IX - designar, em até 60 (sessenta) dias após a publicação deste Decreto, pelo menos 1 (um) titular e 1 (um) suplente para a função de encarregado de dados para o órgão ou entidade, que será responsável pelas atribuições constantes do art. 41 da LGPD, devendo esta designação ser publicada por meio de portaria ou resolução e posteriormente encaminhada por Ofício para a SEGOVI.

Art. 7º Para fins deste Decreto, estão definidos como controladores de dados, com as atribuições que constam do inciso VI, do art. 2º, todos os órgãos da Administração Direta e todas as entidades da Administração Indireta do Município.

Art. 8º As entidades integrantes da Administração Indireta do Município que atuarem em regime de concorrência, sujeitas ao disposto no art. 173, da Constituição Federal, deverão observar o regime relativo às pessoas jurídicas de direito privado particulares, exceto quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, nos termos do art. 24 da LGPD.

Art. 9º Na hipótese de ocorrência de um incidente de segurança de dados, conforme definido no inciso XX, do art. 2º, os encarregados dos órgãos e entidades da Administração Pública Municipal devem comunicar à ANPD, consultando, antes do envio do incidente à Autoridade, a Coordenadoria Técnica de Proteção de Dados, da Subsecretaria de Transparência e Governo Digital - CTPD/SUBTGD, da SEGOVI.

Parágrafo único. A SEGOVI, através da CTPD/SUBTGD, irá emitir regramento específico acerca da comunicação dos incidentes de segurança de dados que eventualmente ocorram.

Art. 10. Os direitos, princípios e deveres expressos neste Decreto não excluem outros previstos no ordenamento jurídico relacionado à matéria.

Art. 11. Este Decreto entra em vigor na data de sua publicação.

Rio de Janeiro, 6 de outubro de 2021; 457º ano da fundação da Cidade.

EDUARDO PAES