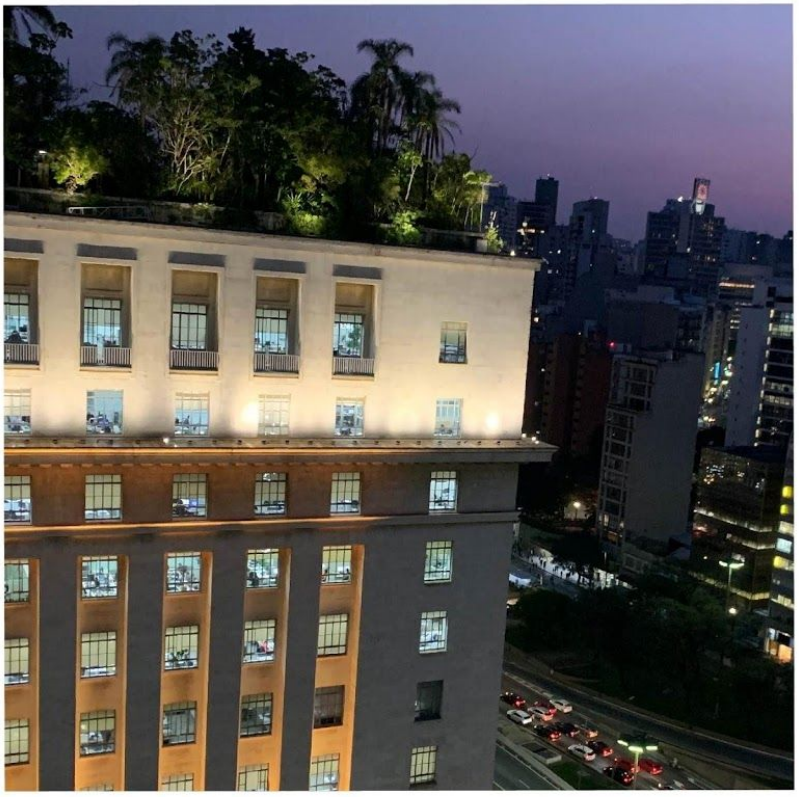

Diretrizes para o **Programa de Privacidade e Proteção de Dados** da Prefeitura Municipal de São Paulo

CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

APRESENTAÇÃO

A cartilha “Diretrizes para o Programa de Privacidade e Proteção de Dados da Prefeitura de São Paulo” tem por objetivo estabelecer o conjunto de orientações para a implementação dos processos referentes às obrigações estabelecidas na Lei 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) e no Decreto Municipal nº 59.767, de 15 de setembro de 2020.

As diretrizes estabelecidas nesta cartilha são aplicáveis a todos os processos de tratamentos de dados pessoais realizados pela PMSP ou em nome dela, assim como a todos os agentes de tratamento envolvidos nessas atividades, com o objetivo de garantir (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.

As orientações apresentadas nessa cartilha devem servir como princípios gerais para o estabelecimento dos processos de tratamento de dados pessoais na Prefeitura Municipal de São Paulo (PMSP), sendo compatibilizados, portanto, com as demais políticas e atividades em andamento, especialmente aquelas decorrentes da Lei de Acesso à Informação (LAI).

O QUE É PROTEÇÃO DE DADOS?

A proteção de dados consiste no conjunto de ações que devem ser adotadas com o objetivo de se instituir os processos necessários à adequada utilização dos dados pessoais dos cidadãos.

Dessa maneira, o tratamento dos dados pessoais deve ser desenvolvido pelos agentes públicos garantindo o respeito à privacidade e a autodeterminação informativa dos cidadãos, de modo a estabelecer uma relação de confiança entre as pessoas e as instituições municipais.

A proteção e o processamento de dados pessoais devem assegurar o tratamento justo e aberto das pessoas, reconhecendo seu direito ao controle sobre sua própria identidade e sua interação com os demais membros da sociedade, bem como devem ser realizados para atingir o equilíbrio entre os interesses públicos efetivados pela função administrativa.

As boas práticas em proteção de dados são vitais para garantir a confiança pública, o envolvimento e o apoio a usos inovadores de dados nos setores público e privado, desenvolvendo melhorias significativas na prestação dos serviços públicos.

QUAIS SÃO OS PRINCIPAIS CONCEITOS RELACIONADOS AO TRATAMENTO DE DADOS PESSOAIS?

O art. 5º da Lei Geral de Proteção de Dados (LGPD) estabelece os principais conceitos envolvendo a proteção de dados e os processos que essa proteção demanda.

Tratamento: toda operação realizada com dados pessoais, como as que se referem a acesso, armazenamento, arquivamento, avaliação, classificação, coleta, comunicação, controle, difusão, distribuição, eliminação, extração, modificação, processamento, produção, recepção, reprodução, transferência, transmissão e utilização.

Dados pessoais: informação relacionada a pessoa natural identificada ou identificável.

Dados pessoais identificados (exemplo): nome, RG, CPF, biometria, DNA, tatuagem.

Dados pessoais identificáveis (exemplo): nome, estado civil, raça, orientação sexual, identidade de gênero, IP de conexão.

Dados pessoais sensíveis: 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.

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.

QUEM SÃO OS AGENTES DE TRATAMENTO?

O art. 5º da Lei Geral de Proteção de Dados (LGPD) estabelece os agentes de tratamento responsáveis pela a proteção de dados e os processos necessários para a efetivação dessa proteção.

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Controlador: aquele a quem competem as decisões referentes ao tratamento de dados pessoais. O responsável pelo tratamento deve certificar-se de que o tratamento desses dados está em conformidade com a legislação de proteção de dados vigente.

Operador: pessoa natural ou jurídica separada, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador e de acordo com suas instruções. O operador não pode ser um funcionário

interno ou subordinado ao controlador, devendo, obrigatoriamente ser pessoa (natural ou jurídica) diversa.

QUAIS SÃO AS OBRIGAÇÕES DO CONTROLADOR PARA A MANUTENÇÃO DA QUALIDADE DOS DADOS?

1. Limitação das finalidades do tratamento

Os órgãos e entes públicos municipais, atuando na qualidade de controlador de dados, devem tratar os dados pessoais para finalidades legítimas, específicas e explícitas, respeitando as leis e regulamentos aplicáveis, bem como o dever de confidencialidade e sempre assegurando o cumprimento dos requisitos de segurança da informação.

O tratamento dos dados pessoais deve ser realizado apenas na medida em que seja essencial para o cumprimento das políticas públicas municipais, sempre respeitando as atribuições normativamente estabelecidas ao agente público.

2. Minimização e precisão dos dados

O tratamento de dados pessoais deve ser realizado limitando-se ao mínimo necessário para o atingimento de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

Os órgãos e entes públicos municipais, atuando na qualidade de controlador de dados, devem garantir que os dados pessoais dos cidadãos sejam mantidos atualizados, e que quaisquer imprecisões sejam prontamente retificadas, sendo que essas atualizações e retificações devem ser refletidas em todos os sistemas e bancos de dados internos e externos da PMSP.

3. Armazenamento dos dados

Os órgãos e entes públicos municipais, atuando na qualidade de controlador de dados, devem armazenar os dados pessoais enquanto for necessário para o cumprimento dos objetivos específicos das políticas públicas, ou conforme exigido pela legislação aplicável.

A Secretaria de Gestão (SG), conjuntamente com a Secretaria Municipal de Inovação e Tecnologia (SMIT), determinará o padrão para o gerenciamento dos documentos públicos, bem como os requisitos a serem seguidos pelos órgãos e entes públicos municipais na operação de armazenamento e descarte dos documentos contendo dados pessoais.

A Controladoria Geral do Município (CGM), por meio da Coordenadoria de Promoção da Integridade (COPI), conjuntamente com a Secretaria Municipal de Inovação e Tecnologia (SMIT), indicará os requisitos para a anonimização e pseudonimização dos dados pessoais, quando pertinente.

QUAIS SÃO AS BASES LEGAIS PARA O TRATAMENTO DE DADOS PESSOAIS?

1. Dados pessoais (art. 7°, Lei n° 13.709/18)

O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

- ✔ Mediante o fornecimento de ***consentimento*** pelo titular de dados.
- ✔ Para o ***cumprimento de obrigação legal ou regulatória*** pelo controlador.
- ✔ Para 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.
- ✔ Para a realização de ***estudos por órgão de pesquisa***.
- ✔ Para a ***execução de contrato***.
- ✔ Para o ***exercício regular de direitos*** em processo judicial, administrativo ou arbitral.

- ✔ Para a ***proteção da vida*** ou da incolumidade física do titular ou de terceiros.
- ✔ Para a ***tutela da saúde***, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.
- ✔ Para atender aos ***interesses legítimos*** do controlador.
- ✔ Para a ***proteção do crédito.***

2. Dados pessoais sensíveis (art. 11, Lei nº 13.709/18)

O tratamento de dados pessoais sensíveis somente poderá ser realizado nas seguintes hipóteses:

- ✔ Mediante o fornecimento de ***consentimento*** pelo titular de dados, de forma específica e destacada, para finalidades específicas.
- ✔ Para o ***cumprimento de obrigação legal ou regulatória*** pelo controlador.
- ✔ Para tratamento e uso compartilhado de dados necessários à ***execução de políticas públicas*** previstas em leis e regulamentos.
- ✔ Para a realização de ***estudos por órgão de pesquisa***, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis.
- ✔ Para o ***exercício regular de direitos*** em processo judicial, administrativo ou arbitral.
- ✔ Para a ***proteção da vida*** ou da incolumidade física do titular ou de terceiros.
- ✔ Para a ***tutela da saúde***, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.
- ✔ Para a garantia da ***prevenção à fraude e à segurança*** do titular.

3. Dados de crianças e de adolescentes (art. 14, Lei nº 13.709/18)

Segundo o art. 2º da Lei nº 8.069/90, crianças são as pessoas com idade entre 0 e 12 anos incompletos, enquanto adolescentes são os indivíduos com idade entre 12 anos completos e18 anos.

O tratamento de dados de crianças e de adolescentes somente poderá ser realizado nas seguintes hipóteses:

- ✔ Mediante o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.
- ✔ Sem o consentimento 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 específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

QUAIS SÃO AS CONDIÇÕES PARA O FORNECIMENTO VÁLIDO DO CONSENTIMENTO?

Conforme o art. 5º, XII da 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.

Os órgãos e entes públicos municipais, atuando na qualidade de controlador de dados, devem garantir que o consentimento tenha sido fornecido de maneira livre, específica, informada e inequívoca, por uma declaração ou ação afirmativa clara do titular dos dados, que deve, portanto, concordar com o tratamento e sua finalidade.

Além disso, os órgãos e entes públicos municipais, atuando na qualidade de controlador de dados, devem garantir que o titular de dados seja capaz de retirar seu consentimento facilmente, e tenha recebido informações dessa capacidade antes de dar consentimento ao tratamento de dados.

QUAIS SÃO OS REQUISITOS PARA A GARANTIA DA TRANSPARÊNCIA E ABERTURA DOS DADOS?

Os órgãos e entes públicos municipais, atuando na qualidade de controlador de dados, devem informar os titulares de dados, em conformidade com a legislação aplicável, no momento da coleta, de forma clara e acessível, as finalidades para as quais seus dados pessoais estão

sendo coletados, como eles serão tratados e, se aplicável, com quem serão compartilhados.

Outro ponto importante é a garantia de que os dados pessoais sejam, preferencialmente, coletados diretamente dos titulares de dados, enquanto a coleta de dados por meio de terceiros e outras fontes ocorra apenas excepcionalmente e desde que em conformidade com a legislação aplicável.

QUAIS SÃO ALGUNS DOS DEVERES DO CONTROLADOR E DO OPERADOR DE DADOS?

Os órgãos e entes públicos municipais, atuando na qualidade de controlador de dados, devem realizar avaliações de risco envolvendo os processos necessários ao tratamento dos dados pessoais, estabelecendo as salvaguardas necessárias para assegurar a segurança da informação.

O operador de dados deve, independentemente do controlador de dados, avaliar os riscos para os direitos e liberdades dos titulares inerente ao tratamento e implementação de medidas para mitigar esses riscos.

Os órgãos e entes públicos municipais, atuando na qualidade de controlador de dados, devem fiscalizar o operador de dados, com o objetivo de assegurar que esse operador esteja adotando as medidas técnicas e organizacionais e os requisitos de segurança e confidencialidade necessários para o tratamento dos dados pessoais.

Além disso, os órgãos e entes públicos municipais, atuando na qualidade de controlador de dados, devem monitorar periodicamente os operadores de dados para verificar a conformidade contínua com suas obrigações legais e contratuais.

O operador de dados deve auxiliar o controlador de dados no cumprimento das obrigações do controlador de dados de acordo com os dispositivos normativos contidos na Lei Geral de Proteção de Dados (LGPD), fornecendo ao controlador de dados informações sobre os aspectos técnicos e medidas organizacionais já implementadas

Outra questão fundamental é que o operador de dados somente poderá envolver suboperadores com a autorização prévia específica do

controlador de dados, por meio do envio de solicitação de autorização antes da contratação do suboperador.

Os órgãos e entes públicos municipais, atuando na qualidade de controlador de dados, devem cooperar com a Autoridades Nacional de Proteção de Dados (ANDP) sobre o desempenho de suas tarefas e cumprir com as determinações relacionadas com o tratamento de dados.

É NECESSÁRIO MANTER REGISTROS DO TRATAMENTO DE DADOS?

Os órgãos e entes públicos municipais, atuando na qualidade de controlador de dados, devem criar e manter um registro escrito de todas as suas atividades de tratamento de dados pessoais, sendo que os órgãos e entes públicos, atuando na qualidade de controlador de dados, devem conceder livre acesso à esses registros pelo encarregado de dados, sempre que necessário à realização de suas obrigações normativamente estabelecidas.

QUAIS SÃO ALGUMAS OBRIGAÇÕES QUANTO AOS TITULARES DE DADOS?

Os órgãos e entes públicos municipais, atuando na qualidade de controlador de dados, devem conceder aos titulares de dados a possibilidade de revisar, corrigir ou excluir seus dados pessoais, mediante solicitação e em conformidade com a legislação aplicável. Na hipótese de indeferimento do pedido do titular de dados, o controlador deve fornecer as razões que fundamentam o indeferimento, bem como os meios para a apresentação de recurso administrativo.

O titular dos dados pessoais deve, mediante acesso aos canais institucionais, identificar-se e realizar sua requisição. Nesta hipótese, o pedido será processado formalmente e respondido preferencialmente pelo mesmo canal de comunicação. Pedidos relacionados a processos já automatizados podem ser recebidos, processados e respondidos pelos canais aptos correspondentes.

Os pedidos formalmente encaminhados deverão seguir rito análogo aos pedidos com fundamento na Lei de Acesso à Informação (LAI).

O QUE FAZER EM RELAÇÃO AOS INCIDENTES DE SEGURANÇA?

Em caso de violação de dados pessoais, os órgãos e entes públicos municipais, atuando na qualidade de controlador de dados, devem, sem atrasos indevidos, notificar o encarregado de dados, para adoção das medidas normativamente determinadas.

A notificação do controlador de dados ao encarregado de dados deve, se possível, ocorrer dentro de 48 (quarenta e oito) horas após o controlador de dados ter tido conhecimento da violação de dados pessoais, para permitir que o encarregado de dados cumpra com a obrigação de notificar a violação de dados pessoais à Autoridade Nacional de Proteção de Dados (ANPD).

A resposta aos incidentes de segurança, quando detectados, deve ser tempestiva, buscando preservar os direitos dos titulares. Decisões relativas à interrupção de serviços disponibilizados ao público externo para fins de contenção de um incidente cabem exclusivamente ao Chefe de Gabinete, nos termos do art. 7º do Decreto Municipal nº 59.767, de 15 de setembro de 2020.