CARTILHA DE

BOAS PRÁTICAS DE PROTEÇÃO DE DADOS E PRIVACIDADE

A Lei Geral de Proteção de Dados Pessoais (Lei Federal nº 13.709, de 14 de agosto de 2018 – LGPD) e o Decreto Municipal nº 59.767, de 15 de setembro de 2020, instituíram as regras para a proteção dos dados pessoais e da privacidade dos cidadãos na Cidade de São Paulo.

Os agentes públicos, em função dessas normas jurídicas, devem conhecer e adotar as boas práticas de proteção e privacidade em sua atividade funcional, preservando os direitos e garantias dos cidadãos e privilegiando uma atuação em conformidade com a lei.

Nessa cartilha, estabelecemos os 10 mandamentos da proteção de dados e da privacidade na Cidade de São Paulo.

1

Identificação do Propósito do Tratamento e Minimização dos Dados na Coleta

A identificação da finalidade do tratamento de dados pessoais serve, fundamentalmente, para que as operações do ciclo de vida do dado sejam realizadas em conformidade com as regras estabelecidas pela Lei Geral de Proteção de Dados Pessoais (LGPD).

Dessa maneira, o servidor municipal deve identificar o propósito de cada tratamento que pretenda realizar antes mesmo do início desse tratamento, verificando qual a base legal adequada para o desenvolvimento dessa finalidade e se os dados a serem coletados são os estritamente necessários para o cumprimento desse propósito.

Na proteção de dados e da privacidade, menos é mais, pois, conforme o princípio da necessidade, a coleta de dados deve se dar de maneira restritiva, sempre limitada, portanto, ao propósito previamente estabelecido.

2

Transparência e Lealdade no Tratamento de Dados Pessoais

O tratamento de dados pessoais deve ser realizado pelo servidor municipal sempre de forma lícita, transparente e garantindo a lealdade desse processamento para com os cidadãos cujos dados pessoais estão sendo tratados. Dessa forma, na medida em que se assegura a privacidade dos dados pessoais, se exige mais transparência quanto às atividades do tratamento, que deve ser sempre realizado em consonância com o ordenamento jurídico e em conformidade com a finalidade inicialmente comunicada aos cidadãos.

O servidor municipal não pode utilizar os dados pessoais para outras finalidades que não sejam compatíveis com o propósito original apresentado antes da coleta dos dados, devendo, igualmente, garantir aos cidadãos que seus dados pessoais sejam conservados apenas durante o tempo necessário às finalidades para as quais foram recolhidos.

Por fim, os dados pessoais não podem ser coletados senão para finalidades específicas, sendo vedada a coleta para fins indefinidos.

3

Promoção dos Direitos e Garantias dos Titulares de Dados

O servidor municipal deve sempre realizar as atividades de tratamento de dados pessoais respeitando e priorizando os direitos e garantias dos cidadãos. Dessa maneira, deve imprimir os mais variados esforços para garantir que os titulares de dados sejam corretamente atendidos quando realizarem requisições como as de retificação e de atualização de seus dados, bem como deve ser garantida aos cidadãos a possibilidade de revogação de seu consentimento nos tratamentos em que esse for solicitado.

Além disso, o servidor municipal deve garantir aos cidadãos informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, assegurando, também, a impossibilidade de realização do tratamento para fins discriminatórios, ilícitos ou abusivos.

Portanto, são direitos dos cidadãos, enquanto titulares de dados, informação sobre o tratamento, eventuais compartilhamentos, as condições do consentimento, quando for o caso, e a possibilidade de sua revogação.

4

Anonimização e Pseudonimização dos Dados Pessoais

O servidor municipal deve utilizar os meios técnicos razoáveis e disponíveis no momento do tratamento, para garantir, sempre que necessário, a manutenção da privacidade do cidadão, a anonimização ou pseudonimização dos dados pessoais, situações empregadas para que o dado perca, permanentemente ou temporariamente, a possibilidade de associação, direta ou indireta, a um indivíduo.

A pseudonimização é o tratamento de dados pessoais que garante que tais dados não possam mais ser atribuídos ao titular de dados sem o uso de informações adicionais. Na pseudonimização, os dados permanecem como dados pessoais.

Por sua vez, a anonimização é o tratamento de dados pessoais que garantem que os dados não possam mais ser atribuídos ao titular de dados de forma alguma. Os dados pessoais que passam pelo processo de anonimização se tornam dados estatísticos.

5

Consentimento

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. Nesse sentido, caso o consentimento seja coletado para o tratamento dos dados pessoais, deve-se garantir que todos seus requisitos sejam cumpridos.

Além disso, o servidor municipal deve garantir instrumentos controles para gerenciar a concessão ou revogação do consentimento pelo cidadão.

O consentimento explícito é necessário para o tratamento de dados pessoais sensíveis: origem racional ou étnica, dados genéticos ou biométricos, filiação política, religiosa ou filosófica, dado referente à saúde ou a vida sexual, opinião política, filiação sindical e convicção religiosa.

6

Avaliação do Risco

O servidor municipal deve realizar o diagnóstico dos processos de tratamento dos dados pessoais, identificando os riscos envolvidos na atividade.

Compreendendo a importância da mitigação desses riscos para evitar incidentes de segurança, o servidor municipal deve elaborar um plano de conformidade do processamento de dados, contendo: a descrição do risco (área de ocorrência, atividade afetada e evento de risco), a avaliação do risco eminente (probabilidade, impacto, nível de risco inerente), a avaliação do risco residual (controles existentes, avaliação do controle, nível de risco residual) e o plano de resposta ao risco (tipo de tratamento, medidas de tratamento, responsável pela implementação das medidas).

7

Compartilhamento dos Dados Pessoais

O compartilhamento de dados pessoais somente deve ocorrer quando consentâneo com a finalidade do tratamento desses dados.

Em algumas situações, é necessário, inclusive, o consentimento do titular de dados para que esse compartilhamento seja permitido, obedecidos os requisitos legais.

Dessa mesma forma, é obrigação do servidor municipal não compartilhar documentos com os dados pessoais dos cidadãos por e-mail, nuvens não homologadas pela PMSP e, especialmente, por aplicativos de comunicação instalados nos celulares funcionais ou pessoais.

8

Treinamento e Comunicação

O estabelecimento de uma cultura de proteção de dados e privacidade é indispensável para o desenvolvimento do tratamento de dados baseado nos princípios da Lei Geral de Proteção de Dados.

O servidor municipal deve sempre buscar o aprimoramento de sua capacidade decisória quanto as atividades envolvidas no tratamento de dados pessoais por meio de capacitações relacionadas com o tema. Além disso, deve se colocar como agente promotor das boas práticas de proteção de dados e privacidade no ambiente da sua unidade, incentivando os demais colaboradores a realizarem suas atividades também em conformidade com essas boas práticas.

9

Resposta a Incidentes de Segurança

As boas práticas de proteção de dados e privacidade também exigem do servidor municipal prontidão no atendimento a incidentes de seguranças.

Vazamentos de dados pessoais, corrompimento do banco de dados, utilização de ferramenta não autorizada, ou até mesmo documentos contendo dados pessoais esquecidos na impressora devem ser considerados incidentes de seguranças e ser tratados pelos servidores municipais de forma séria e diligente. Todos os esforços para responder ao incidente devem ser adotadas, especialmente a transparência na comunicação ao superior hierárquico, a chefia de gabinete (nos termos do art. 7º do Decreto nº 59.767) e ao titular de dados pessoais.

10

Monitoramento

O servidor municipal deve monitorar se todas as regras, políticas, processos e procedimentos estão sendo observados nas atividades de tratamento de dados pessoais, garantindo, assim o cumprimento das garantias e direitos dos titulares desses dados.

Além disso, deve sempre buscar, no monitoramento, uma forma de promoção de melhorias nas suas atividades de tratamento de dados pessoais, corrigindo erros e inconsistências que venha a detectar por meio desse monitoramento.