PARECER Nº 1023/2022 DA COMISSÃO DE FINANÇAS E ORÇAMENTO SOBRE O PROJETO DE LEI N° 807/2017

O presente projeto de lei, de autoria dos nobres Vereadores Toninho Vespoli, Eduardo Matarazzo Suplicy, José Police Neto, Juliana Cardoso, Patrícia Bezerra, Sâmia Bonfim, Eduardo Tuma e Natalini, visa dispor sobre a Política Municipal de proteção de dados pessoais e da privacidade, que se aplica a qualquer operação de tratamento de dados pessoais por pessoa jurídica de direito público ou privado no âmbito da Administração Pública Municipal direta e indireta no Município de São Paulo, independentemente do país onde estejam localizados os dados. A propositura estabelece que o tratamento de dados pessoais somente poderá ser realizado após o consentimento livre, específico e inequívoco do titular e também veda o tratamento de dados pessoais sensíveis (dados pessoais sobre raça ou etnia, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, bem como dados genéticos ou biométricos), dispondo sobre as exceções e as condições que se dará o consentimento ou sua dispensa. Considera dados anonimizados como dados pessoais, quando o processo de anonimização ao qual foram submetidos for revertido ou quando, com esforços razoáveis, puder ser revertido. Ainda trata, entre outros, da transparência e do término do tratamento dos dados, dos direitos do titular, do uso compartilhado dos dados, da segurança e sigilo, da responsabilização dos agentes públicos e pessoas jurídicas. Estabelece que as Ouvidorias do Poder Executivo e Legislativo do Município de São Paulo terão, entre suas atribuições, a função de zelar pela proteção dos dados pessoais, nos termos da legislação, garantir a difusão para a população sobre direitos e deveres, medidas de segurança e informações sobre as políticas públicas de proteção de dados pessoais, coordenar ações e promover acordos com instituições competentes do sistema de justiça visando encaminhar, de forma intersetorial, as demandas, irregularidades ou ilegalidades decorrentes de violações de proteção aos dados pessoais, sob pena de responsabilidade solidária. Cria o Conselho Municipal de Proteção de Dados Pessoais e da Privacidade, um órgão consultivo, deliberativo e normativo, com atividade não remunerada.

Quanto ao aspecto financeiro, nada há a opor à propositura, visto que as despesas de sua execução serão cobertas por dotações orçamentárias próprias, suplementadas se necessário.

Favorável, portanto, é o parecer, no entanto, apresentamos o seguinte substitutivo que visa adequar o texto à técnica legislativa da Lei Complementar nº 95/98, que dispõe sobre a elaboração, a redação, a alteração e a consolidação das leis, e a alguns conceitos e disposições da Lei Federal nº 13.709, de 14 de agosto de 2018 Lei Geral de Proteção de Dados Pessoais (LGPD).

SUBSTITUTIVO Nº AO PROJETO DE LEI Nº 807/2017

Dispõe sobre a Política Municipal de Proteção de Dados Pessoais e da Privacidade no âmbito da Administração Pública direta e indireta no Município de São Paulo e dá outras providências.

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Seção I

Escopo de Aplicação da Lei

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 no âmbito da Administração Pública Municipal direta e indireta, com o objetivo de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Art. 2º A disciplina da proteção de dados pessoais é condição para o pleno exercício da cidadania e 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;

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

VIII a igualdade;

IX - o reconhecimento da condição de vulnerável de crianças e adolescentes e sua proteção integral.

Art. 3º Esta Lei aplica-se a qualquer operação de tratamento de dados pessoais no âmbito da Administração Pública Municipal direta e indireta, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, subordinando-se ao regime desta lei:

I - Os órgãos da administração direta e indireta, como autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades vinculadas ou que venham a ser vinculadas, direta ou indiretamente ao Município;

II - Pessoa natural ou jurídica de direito privado quanto contratada ou conveniada, direta ou indiretamente, pela administração pública municipal, considerando-se para os fins de aplicação desta lei:

a) todo e qualquer ajuste entre órgãos ou entidades da Administração Pública e particulares em que haja um acordo de vontades para a formação de vínculo e a estipulação de obrigações recíprocas, seja qual for a denominação utilizada;

b) editais, contratos administrativos e convênios, na forma Lei Federal 8.666, de 21 de junho de 1993, da Lei Federal 14.133, de 1º de abril de 2021, bem como da Lei Federal 11.079, de 30 de dezembro de 2004 e da Lei Federal 13.019, de 31 de julho de 2014;

c) procedimentos que visem a apresentação de projetos, levantamentos, investigações ou estudos, por pessoa física ou jurídica de direito privado, com a finalidade de subsidiar a administração pública na estruturação de empreendimentos objeto de alienação, concessão ou permissão de serviços públicos, de parceria público-privada, de arrendamento de bens públicos ou de concessão de direito de uso.

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

I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos, fora do âmbito da administração pública municipal direta ou indireta;

II - realizado para fins exclusivamente jornalísticos, artísticos, literários ou acadêmicos;

III - realizado para o fim de garantir o acesso à Informação, nos termos da Lei 12.527/2011.

Seção II

Definições

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

I - dado pessoal: dado relacionado à pessoa natural, identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos;

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 um 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: a 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 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: 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 específica;

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

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

XV - 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;

XVI - perfil comportamental: qualquer forma de tratamento automatizado de dados pessoais destinada a avaliar aspectos ou a segmentação de uma pessoa natural, ainda que não identificada ou identificável, tais como para analisar ou prever características socioeconômicas, estado de saúde, localização, deslocamento; e

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.

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé, a moralidade, impessoalidade, legalidade, publicidade e a probidade administrativa 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 integralidade 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 após o consentimento livre, específico e inequívoco do titular, salvo nas seguintes hipóteses:

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

II - pela administração pública para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas e prestação de serviços públicos previstos em leis ou regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;

III - para a realização de pesquisa histórica, científica ou estatística, garantida, sempre que possível, a anonimização dos dados pessoais;

IV - 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);

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

VI - para a tutela da saúde, com procedimento realizado por profissionais da área da saúde, serviços de saúde ou autoridades sanitárias;

§ 1º Nos casos de aplicação do disposto nos incisos I e II, o controlador deverá informar ao titular as hipóteses em que será admitido o tratamento de seus dados, nos termos do artigo 12 e seguintes.

§ 2º A forma de disponibilização das informações previstas no parágrafo anterior deverá levar em consideração as recomendações da Ouvidoria, consideradas as diretrizes do Conselho Municipal de Proteção de Dados e da Privacidade.

Art. 8º O consentimento previsto no art. 7º, caput, deverá ser livre, específico, inequívoco e fornecido por escrito ou por qualquer outro meio que demonstre a manifestação de vontade do titular.

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

§ 2º Caso o consentimento seja obtido por outro meio, este deverá ser fornecido de forma clara, adequada e ostensiva, bem como com a adoção de padrões técnicos que facilitem o controle dos titulares sobre seus dados pessoais.

§ 3º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.

§ 4º É vedado o tratamento de dados pessoais quando o consentimento tenha sido obtido mediante erro, dolo, coação, estado de perigo ou simulação.

§5º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.

§ 6º O consentimento pode ser revogado a qualquer momento, mediante manifestação expressa do titular.

§ 7º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 13, o controlador deverá obter novo consentimento do titular, após destacar de forma específica o teor das alterações.

§ 8º O titular deverá ser informado da possibilidade de não fornecer o consentimento, na hipótese em que o consentimento é requerido, mediante o fornecimento de informações sobre as consequências da negativa.

a) o consentimento 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.

b) quando o consentimento para o tratamento de dados pessoais for condição para o fornecimento de produto ou serviço ou para o exercício de direito, o titular será informado com destaque sobre tal fato e sobre os meios pelos quais poderá exercer controle sobre o tratamento de seus dados.

Art. 9º. É vedado o tratamento de dados pessoais sensíveis, salvo:

I - com fornecimento de consentimento inequívoco, expresso e específico pelo titular:

a) mediante manifestação própria, distinta da manifestação de consentimento relativa a outros dados pessoais; e

b) com informação prévia e específica sobre a natureza sensível dos dados a serem tratados, com alerta quanto aos riscos envolvidos no seu tratamento.

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 e uso compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de pesquisa histórica, científica ou estatística, 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; ou

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

§ 1º O disposto neste artigo aplica-se a qualquer tratamento de dados pessoais capaz de revelar dados pessoais sensíveis.

§ 2º O tratamento de dados pessoais sensíveis não poderá ser realizado em detrimento do titular, ressalvado o disposto em legislação específica.

§ 3º O disposto na alínea 'c' do inciso II não se aplica caso as atividades de pesquisa estejam vinculadas a qualquer das seguintes atividades:

I - comercial;

II - de administração pública, quando a pesquisa não for a atividade principal ou legalmente estabelecida do órgão; ou

III - relativa à investigação criminal ou inteligência.

§ 4º O disposto nas hipóteses do parágrafo anterior garantirá, sempre que possível, a anonimização dos dados pessoais.

§ 5º Nos casos de aplicação do disposto nas alíneas 'a' e 'b' do inciso II pelos órgãos e entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos seção III deste Capítulo.

§ 6º Medidas adicionais de segurança e de proteção aos dados pessoais sensíveis deverão ser adotadas pelo controlador ou por outros agentes do tratamento, mediante a elaboração de relatório de impacto à privacidade.

Art. 10. Nas hipóteses de dispensa do consentimento para o tratamento de dados pessoais, o controlador deverá, respeitado os direitos e liberdades fundamentais do titular, observar:

§ 1º os princípios gerais e da garantia dos direitos do titular, em particular:

I - as legítimas expectativas do titular de acordo com o contexto do tratamento, nos termos do art. 6º, I;

II - a finalidade e adequação pelo qual o tratamento dos dados é realizado para uma finalidade específica, informadas e com as legítimas expectativas do titular, de acordo com o art. 6º, II;

III - a necessidade pela qual o tratamento dos dados pessoais limita-se ao estritamente necessários para a finalidade pretendida, abrangendo dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados, o que envolve:

a) anonimização sempre que compatível com a finalidade do tratamento.

§ 2º A adoção de medidas para garantir a transparência do tratamento de dados, devendo fornecer aos titulares mecanismos eficazes para que possam manifestar sua oposição ao tratamento, de acordo com o disposto no artigo 17, §1°;

§ 3º A emissão de relatório de impacto à privacidade.

Seção II

Dados Anonimizados

Art. 11 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 o tempo necessário para reverter o processo de anonimização, de acordo com as tecnologias disponíveis;

§ 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 Consideradas as diretrizes do Conselho Municipal de Proteção de Dados e da Privacidade, a Ouvidoria poderá emitir diretrizes sobre padrões e técnicas utilizadas em processos de anonimização;

§ 4º O compartilhamento e o uso que se faz de dados anonimizados deve ser objeto de publicidade e de transparência, bem como antecedida por relatório de impacto à privacidade referente aos riscos de reversão do processo de anonimização e demais aspectos de seu tratamento;

§ 5º A reversão do processo de anonimização é proibida, salvo mediante consentimento expresso dos próprios titulares dos dados pessoais;

Seção III

Da Transparência no Tratamento dos Dados

Art. 12. Cabe aos entes sujeitos ao regime desta lei adotar procedimentos e medidas de transparência das suas atividades de tratamento de dados pessoais e que devem ser executados em conformidade com os princípios básicos da administração pública e com a seguintes diretrizes:

I - observância da publicidade como preceito geral e sigilo como exceção;

II - divulgação de informações, independentemente de solicitações, em locais e veículos de fácil acesso;

III - utilização de meios de comunicação viabilizados pela tecnologia da informação;

IV - fomento ao desenvolvimento da cultura de transparência no tratamento dos dados pessoais;

§ 1º Deverão informar de forma clara e atualizada em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos:

I - as hipóteses em que realizam o tratamento de dados pessoais;

II - as políticas organizacionais para garantir que o tratamento de dados pessoais está em conformidade com os princípios estabelecidos pelo artigo 6º desta Lei;

III - o uso compartilhado de dados;

IV - os relatórios de impacto à privacidade;

V - os critérios, procedimentos e instruções utilizados para decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem interesses do titular, inclusive as decisões destinadas a definir o seu perfil comportamental.

§ 2º Considerada as diretrizes do Conselho Municipal de Proteção de Dados e da Privacidade, o Ouvidor emitirá recomendações para o cumprimento do disposto neste artigo.

§ 3º Aplicam-se as normas e os procedimentos previstos na Lei 12.527, de 18 de novembro de 2011, para se assegurar uma gestão transparente dos dados pessoais.

Art. 13. O titular deverá ter acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva sobre, entre outros:

I - finalidade específica do tratamento;

II - forma e duração do tratamento;

III - identificação do controlador;

IV - informações de contato do controlador;

V - sujeitos ou categorias de sujeitos para os quais os dados podem ser comunicados, bem como âmbito de difusão;

VI - responsabilidades dos agentes que realizarão o tratamento, e

VII - direitos do titular, com menção explícita a:

a) possibilidade de acessar os dados, retificá-los ou revogar o consentimento, por procedimento gratuito e facilitado;

§ 1º Em caso de alteração de informação referida no inciso IV do caput, o controlador deverá comunicar ao titular as informações de contato atualizadas.

§ 2º Nas atividades que importem em coleta continuada de dados pessoais, o titular deverá ser informado periodicamente sobre as principais características do tratamento, observando-se as diretrizes definidas pelo Conselho Municipal de Proteção de Dados e da Privacidade.

Seção IV

Do Término do Tratamento de Dados

Art. 14. 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 para o alcance da finalidade específica almejada;

II - fim do período de tratamento;

III - comunicação do titular, inclusive no exercício do seu direito de revogação do consentimento conforme disposto no art. 8º, § 6º.

Art. 15. Os dados pessoais serão eliminados após o término de seu tratamento, autorizada a conservação para as seguintes finalidades:

I - cumprimento de obrigação legal do controlador;

II - pesquisa histórica, científica ou estatística, garantida, quando possível, a anonimização dos dados pessoais.

CAPÍTULO III

DOS DIREITOS DO TITULAR

Art. 16. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais, garantidos os direitos fundamentais de liberdade, intimidade e privacidade, nos termos desta Lei.

Art. 17. O titular dos dados pessoais tem direito a obter, em relação aos seus dados:

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;

V - eliminação, a qualquer momento, de dados pessoais com cujo tratamento o titular tenha consentido; e

§ 1º 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.

§ 2º Os direitos previstos neste artigo serão exercidos mediante requerimento do titular a um dos agentes de tratamento, que adotará imediata providência para seu atendimento.

§ 3º Em caso de impossibilidade de adoção imediata da providência de que trata o § 2º, o controlador enviará ao titular, em até sete dias a partir da data do recebimento do requerimento, resposta em que poderá:

I - comunicar que não é agente de tratamento dos dados, indicando, sempre que possível, quem o seja; ou

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

§ 4º A providência de que trata o § 2º será realizada sem custos para o titular.

§ 5º O controlador deverá informar aos terceiros a quem os dados tenham sido comunicados sobre a realização de correção, eliminação, anonimização ou bloqueio dos dados, para que repitam idêntico procedimento.

Art. 18. A confirmação de existência ou o acesso a dados pessoais serão providenciados, a critério do titular:

I - em formato simplificado, imediatamente; ou

II - por meio de declaração clara e completa, que indique a origem dos dados, data de registro, critérios utilizados e finalidade do tratamento, fornecida no prazo de até sete dias, a contar 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 dados poderão ser fornecidos, a critério do titular:

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

II - sob forma impressa, situação em que poderá ser cobrado exclusivamente o valor necessário ao ressarcimento do custo dos serviços e dos materiais utilizados.

§ 3º Quando o tratamento tiver origem no consentimento do titular ou em um contrato, o titular poderá solicitar cópia eletrônica integral dos seus dados pessoais em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.

§ 4º Consideradas as diretrizes do Conselho Municipal de Proteção de Dados e da Privacidade, o Ouvidor emitirá recomendações sobre os formatos em que serão fornecidas as informações e os dados ao titular.

Art. 19. O titular dos dados tem direito a solicitar revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive as decisões destinadas a definir o seu perfil comportamental.

§ 1º Deverá ser permitida a realização de auditoria de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, inclusive com a inserção de novos dados e o acesso ao seu resultado;

§ 2º O controlador deverá fornecer informações claras e adequadas a respeito dos critérios, procedimentos e instruções utilizados para a decisão automatizada;

§ 3º O controlador deverá emitir relatório de impacto à privacidade, levando-se em consideração os direitos e liberdades fundamentais do titular;

Art. 20. Os dados pessoais referentes a exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.

Art. 21. A defesa dos interesses e direitos dos titulares de dados poderá ser exercida em juízo individual ou coletivamente, na forma do disposto na Lei n° 9.507, de 12 de novembro de 1997, nos arts. 81 e 82 da Lei n° 8.078, de 11 de setembro de 1990, na Lei n° 7.347, de 24 de julho de 1985, e nos demais instrumentos de tutela individual e coletiva.

Art. 22. Aplicam-se as normas e os procedimentos previstos na Lei 12.527, de 18 de novembro de 2011, para facilitar o acesso à informação sobre o tratamento dos dados pessoais pelo seu titular.

CAPÍTULO IV

DO USO COMPARTILHADO DE DADOS

Art. 23. O uso compartilhado de dados por órgãos e entidades públicos ou entre órgãos e entidades públicos e entes privados deverá:

I - observar os princípios de proteção de dados elencados no art. 6º desta Lei, em particular:

a) as finalidades específicas de execução de políticas públicas ou para a prestação de serviços públicos, no cumprimento das competências legais dos órgãos e entidades públicos;

b) as legítimas expectativas do titular, de acordo com o disposto no art. 6º, II, frente à finalidade para a qual o seu dado foi coletado originariamente;

c) aos dados pessoais estritamente necessários para a finalidade pretendida, devendo ser anonimizados sempre que compatível com a finalidade do tratamento.

II - ser antecedido pela emissão de relatório de impacto à privacidade;

III - ser objeto de publicidade nos termos do art. 13, sendo fornecida informações claras e atualizadas sobre:

a) data;

b) periodicidade e frequência;

c) as finalidades do tratamento realizados com os dados;

d) a necessidade de compartilhamento;

e) descrição dos dados;

f) descrição de eventual formação do perfil comportamental de uma pessoa natural, ainda que não identificada ou identificável;

g) medidas de segurança adotadas para a proteção dos dados.

Art. 24. É vedado aos órgãos e entes da Administração Pública transferir dados pessoais constantes das suas bases de dados a entidades privadas, exceto em casos de execução descentralizada de atividade pública e nas hipóteses previstas na Lei n° 12.527, de 18 de novembro de 2011.

§ 1º Aplicam-se as normas e os procedimentos previstos na Lei 8.666, de 21 de junho de 1993, bem como a Lei 11.079, de 30 de dezembro de 2014, para que o uso compartilhado dos dados esteja em estrita conformidade com os princípios básicos da administração pública, devendo ser precedida de licitação que:

I - não será sigilosa, sendo públicos e acessíveis os atos de seu procedimento;

II - não admitirá prever, incluir ou tolerar, nos atos de convocação, cláusulas ou condições que comprometam, restrinjam ou frustrem o seu caráter competitivo;

III - priorizará:

a) bens e serviços com tecnologia desenvolvida no País;

b) programas de computação de código aberto, livres de restrições quanto à cessão, alteração e distribuição de suas cópias eletrônicas, nos termos do artigo 37;

c) adoção de medidas técnicas e administrativas constantemente atualizadas, proporcionais à natureza dos dados compartilhados e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

d) a adoção de padrões técnicos que facilitem o controle dos titulares sobre seus dados pessoais.

IV - não admitirá que os dados compartilhados sejam:

a) utilizados para outras finalidades estranhas à execução descentralizada da atividade pública;

b) como parte do preço ou como qualquer tipo de contraprestação a favor da contratada para a execução descentralizada da atividade pública, observando-se o princípio da moralidade na administração pública;

V - O instrumento de convocação deverá levar em consideração medidas técnicas de segurança e de boas práticas, nos termos do artigo 37.

Art. 25. Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado para a execução de políticas públicas, prestação de serviços públicos e a descentralização da atividade pública.

Art. 26. Considerada as diretrizes do Conselho Municipal de Proteção de Dados e da Privacidade, o Ouvidor estipulará diretrizes para o cumprimento do disposto nesta seção.

CAPÍTULO V

AGENTES E RESPONSABILIDADE NO TRATAMENTO DE DADOS PESSOAIS

Seção I

Do Controlador e do Operador

Art. 27. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem.

Parágrafo único. Considerada as diretrizes do Conselho Municipal de Proteção de Dados e da Privacidade, o Ouvidor poderá estipular recomendações sobre formato, estrutura e tempo de guarda do registro.

Art. 28. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e do quanto disposto nesta Lei.

Art. 29. O Ouvidor poderá solicitar aos agentes do tratamento de dados pessoais que publiquem relatórios de impacto de privacidade e sugerir adoção de padrões e boas práticas aos tratamentos de dados pessoais.

Art. 30. Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, o Ouvidor poderá enviar informe com medidas cabíveis para fazer cessar a violação.

§ 1º As punições cabíveis a agente público no âmbito desta Lei serão aplicadas pessoalmente aos operadores de órgãos públicos, conforme disposto na Lei n° 1.399, de 08 de novembro de 1995, e na Lei n° 8.429, de 2 de junho de 1992.

§ 2º - Aplicam-se no que couber as normas e os procedimentos previstos na Lei 12.846, de 1º de agosto de 2013, para as punições cabíveis e a responsabilização administrativa e civil das pessoas jurídicas sujeitas ao regime dessa lei.

Seção II

Encarregado pelo Tratamento de Dados Pessoais

Art. 31. O controlador e as pessoas jurídicas de direito privado sujeitas ao regime desta Lei indicarão um encarregado pelo tratamento de dados pessoais, devendo:

§ 1º Divulgar publicamente de forma clara e objetiva, preferencialmente na página eletrônica na Internet, a identidade e as informações de contato do encarregado;

§ 2º Assegurar que o encarregado:

I - esteja envolvido em todas as operações relativas ao tratamento de dados pessoais,

II - exerça com autonomia sua função, não podendo ser penalizado por não seguir instruções ou diretrizes que não estejam em conformidade com o disposto nesta Lei;

Art. 32. As atividades do encarregado consistem em:

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

II - receber comunicações do Ouvidor e do Conselho Municipal de Proteção de Dados e da Privacidade e adotar providências;

III - orientar os funcionários e contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais, de acordo com o disposto nesta Lei;

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

V - orientação para a elaboração dos relatórios de impacto à privacidade e a observância dos parâmetros nele estabelecidos para o tratamento dos dados pessoais;

CAPÍTULO VI

SEGURANÇA E BOAS PRÁTICAS

Seção I

Segurança e Sigilo de Dados

Art. 33. O operador deve 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 Consideradas as diretrizes do Conselho Municipal de Proteção de Dados e da Privacidade, o Ouvidor poderá recomendar padrões técnicos e organizacionais para tornar aplicável o disposto no caput, levando-se em consideração a natureza das informações tratadas, características específicas do tratamento e o estado atual da tecnologia, em particular no caso de dados sensíveis.

§ 2º As medidas de segurança deverão ser observadas desde a fase de concepção do produto ou serviço até a sua prestação.

Art. 34. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se ao dever de sigilo em relação aos dados pessoais, mesmo após o seu término.

Seção II

Incidente de Segurança

Art. 35. O controlador deverá comunicar ao Ouvidor e ao Conselho Municipal de Proteção de Dados e da Privacidade a ocorrência de qualquer incidente de segurança que possa acarretar risco ou prejuízo relevante aos titulares.

Parágrafo único. A comunicação será feita em prazo razoável, conforme definido pelo órgão competente, e deverá mencionar, no mínimo:

I - descrição da natureza dos dados pessoais afetados;

II - informações sobre os titulares envolvidos;

III - indicação das medidas de segurança utilizadas para a proteção dos dados, inclusive procedimentos de encriptação;

IV - riscos relacionados ao incidente;

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

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

Art. 36. O Ouvidor verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, recomendar ao controlador a adoção de outras providências, tais como:

I - pronta comunicação aos titulares;

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

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

Parágrafo único. A pronta comunicação aos titulares afetados pelo incidente de segurança será obrigatória, independente de recomendação do Ouvidor, nos casos em que for possível identificar que o incidente coloque em risco a segurança pessoal dos titulares ou lhes possa causar danos.

Seção III

Sistemas de Proteção de Dados Pessoais e Softwares Livres

Art. 37. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

§ 1º Os estabelecimentos públicos municipais da Administração Direta e Indireta e entidades privadas sujeitas ao regime deste Lei deverão utilizar em seus sistemas e equipamentos de informática, prioritariamente, programas de computação de código aberto, livres de restrições quanto à cessão, alteração e distribuição de suas cópias eletrônicas.

I - o formato padrão de documentos que operam nos equipamentos de informática dos estabelecimentos dispostos no caput deste artigo deverão ser livres de restrição proprietária.

II - caso exista a necessidade de aquisição de programas de propriedade de entidades privadas, mediante justificativa prévia, será dada preferência para aquelas que possibilitem a conversão dos arquivos e o intercâmbio entre os sistemas, permitindo sua execução sem restrições em sistemas operacionais baseados em código aberto.

III - entende-se por programa de computação de código aberto aquele cuja licença de propriedade industrial ou intelectual não restrinja sob nenhum aspecto a sua cessão, distribuição, utilização ou alteração de suas características originais, assegurando, ao usuário, acesso irrestrito e sem custos adicionais ao seu código fonte, permitindo a alteração parcial ou total do programa para seu aperfeiçoamento ou adequação.

a) o código fonte deve ser o recurso preferencial utilizado pelo programador para modificar o programa, não sendo permitido ofuscar a sua acessibilidade.

IV - a licença de utilização dos programas abertos deve permitir modificações e trabalhos derivados e a sua livre distribuição sob os mesmos termos da licença do programa original, não podendo ser utilizados programas cujas licenças:

a) impliquem em qualquer forma de discriminação a pessoas ou grupos;

b) sejam específicas para determinado produto impossibilitando que programas derivados deste tenham a mesma garantia de utilização, alteração e distribuição;

c) restrinjam outros programas distribuídos conjuntamente.

V - quando houver justificativa técnica comprobatória da ineficiência dos programas abertos em determinada contratação, a Administração Pública poderá adquirir, mediante concorrência prévia, programas de informática não caracterizados como abertos, desde que haja a apresentação de justificativa técnica, nos termos da Lei n° 8.666, de 21 de junho de 1993;

VI - é obrigatória a utilização de programa de computação de código aberto para decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem interesses do titular, inclusive as decisões destinadas a definir o seu perfil comportamental;

VII - A Administração Pública deverá promover educar e promover a utilização de programas de computação de código aberto para o exercício do controle parental dos dados pessoais de crianças e adolescentes, nos termos dos princípios desta Lei e da Lei n° 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente.

Seção IV

Boas Práticas

Art. 38 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, deverá ser levado em consideração a natureza, escopo e finalidade do tratamento e dos dados, bem como a probabilidade e gravidade dos riscos de danos aos indivíduos.

§ 2º As regras de boas práticas serão disponibilizadas publicamente e atualizadas.

§ 3º Devem ser priorizados a adoção de padrões técnicos que facilitem o controle dos titulares sobre seus dados pessoais.

Seção V

Relatório de Impacto à Privacidade

Art. 39. O operador deverá emitir relatório de impacto à privacidade quando o tratamento de dados pessoais implicar em alto risco para os direitos e liberdades fundamentais do titular, tais como em:

I - decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses;

II - traçar perfil comportamental;

III - monitoramento sistemático de áreas públicas;

IV - uso de novas tecnologias para prevenir a ocorrência de danos, nos termos do artigo 6º, inciso VIII

V - nas demais hipóteses previstas nesta Lei, em particular:

a) no tratamento de dados sensíveis;

b) no uso compartilhado de dados;

Art. 40. O relatório de impacto à privacidade deve ser composto ao menos dos seguintes elementos:

I - descrição de que o tratamento dos dados respeita os princípios de proteção de dados elencados no art. 6º dessa Lei, em particular:

a) finalidade e adequação pelo qual o tratamento dos dados é realizado para uma finalidade específica, informadas e com as legítimas expectativas do titular, de acordo com o contexto do tratamento;

b) necessidade pelo qual o tratamento dos dados pessoais limita-se ao estritamente necessários para a finalidade pretendida, abrangendo dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados, o que envolve;

c) anonimização sempre que compatível com a finalidade do tratamento.

d) qualidade com a implementação de mecanismos que garantam a exatidão, a clareza, relevância e a atualização dos dados, de acordo com a periodicidade necessária para o cumprimento da finalidade de seu tratamento;

II - adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos indevidos nos termos desta Lei, particularmente para se evitar acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

III - Considerada as diretrizes do Conselho Municipal de Proteção de Dados e da Privacidade, o Ouvidor poderá estipular diretrizes complementares para o cumprimento do disposto nesse artigo.

Art. 41. O operador deverá tornar pública uma lista sobre quais tipos de tratamento de dados estão sujeitos ou não à exigência de relatórios de impacto à privacidade, sem prejuízo de publicá-los nos termos do inciso IV do § 1° do artigo 12, desta Lei.

CAPÍTULO VII

MONITORAMENTO

Seção I

Da Ouvidoria

Art. 42. As Ouvidorias do Poder Executivo e Legislativo do Município de São Paulo terão, entre suas atribuições, a função de garantia ao cumprimento desta lei, a finalidade de

descentralizar, tornar acessível, inclusive para pessoas com deficiência, bem como dar publicidade a relatórios e encaminhamento, por meio de ações integradas e acordos com instituições competentes do sistema de justiça, todas as informações que forem demandas visando a defesa dos direitos e interesses dos cidadãos com relação a proteção de dados pessoais.

Art. 43. Fica alterado o artigo 136 da Lei Municipal 15.764, de 27 de maio de 2013, com a seguinte redação:

Art. 136...

XI - Zelar pela proteção dos dados pessoais, nos termos da legislação;

XII - garantir a difusão para a população sobre direitos e deveres, medidas de segurança e informações sobre as políticas públicas de proteção de dados pessoais;

XIII - coordenar ações e promover acordos com instituições competentes do sistema de justiça visando encaminhar, de forma intersetorial, as demandas, irregularidades ou ilegalidades decorrentes de violações de proteção aos dados pessoais, sob pena de responsabilidade solidária.

Art. 44. Fica alterado o artigo 2º da Lei Municipal 15.507, de 13 de dezembro de 2011, com a seguinte redação:

Art. 2º...

VIII - Zelar pela proteção dos dados pessoais, nos termos da legislação;

IX - garantir a difusão para a população sobre direitos e deveres, medidas de segurança e informações sobre as políticas públicas de proteção de dados pessoais;

X - coordenar ações e promover acordos com instituições competentes do sistema de justiça visando encaminhar, de forma intersetorial, as demandas, irregularidades ou ilegalidades decorrentes de violações de proteção aos dados pessoais, sob pena de responsabilidade solidária.

Seção II

Conselho Municipal de Proteção de Dados e da Privacidade

Art. 45. Fica criado o Conselho Municipal de Proteção de Dados Pessoais e da Privacidade que é um órgão consultivo, deliberativo e normativo.

Art. 46. Compete ao Conselho Municipal de Proteção de Dados Pessoais e da Privacidade:

I - participar e fornecer subsídios para a elaboração da Política Municipal de Proteção de Dados Pessoais e da Privacidade;

II - elaborar relatórios anuais de avaliação da execução das ações da Política Municipal de Proteção de Dados Pessoais e da Privacidade;

III - sugerir ações a serem realizadas pela Ouvidoria;

IV - realizar estudos e debates sobre a proteção de dados pessoais e da privacidade;

V - disseminar o conhecimento sobre proteção de dados pessoais e privacidade à população em geral;

VI - ser instância de democratização nas ações educativas executadas pelo Poder Público Municipal;

VII - estabelecer diretrizes relacionadas à proteção de dados pessoais;

VIII - estabelecer diretrizes para a elaboração de relatórios de impacto à privacidade;

IX - elaborar e alterar seu Regimento Interno;

X - eleger o seu presidente;

Art. 47. O Conselho Municipal de Proteção de Dados Pessoais e da Privacidade respeitará os critérios de gênero, raça, representação do Poder Público e da Sociedade Civil,

composto por treze representantes titulares e treze suplentes designados, com mandato de dois anos, podendo ser renovado uma única vez por igual período, sendo:

I - 01 (um) representante da Controladoria Geral do Município;

II - 03 (três) representantes do Poder Público Municipal que tenham atribuição de gestão de programas, projetos e ações relacionados com os objetivos do Conselho;

III - 03 (três) representante da academia, que desenvolvam atividades conexas aos objetivos deste Conselho;

IV - 03 (três) representantes do terceiro setor, com dois anos de atividade e previsão dos objetivos deste Conselho em seu estatuto;

V - 03 (três) representantes dos Conselhos Participativos Municipais, que desenvolvam atividades conexas a programas, projetos e ações relacionados com os objetivos do Conselho.

§ 1º Os representantes dos incisos III e IV serão eleitos por seus pares, dentre as respectivas entidades representativas constituídas há pelo menos 3 (três) anos e que tenham objetivos estatutários relacionados com os objetivos do Conselho;

§ 2º Os representantes dos incisos V serão escolhidos por seus pares, representando diferentes regiões da cidade, mediante processo eletivo;

§ 3º A participação no Conselho Municipal de Proteção de Dados Pessoais e da Privacidade será considerada atividade de relevante interesse público, não remunerada.

§ 4º As reuniões do Conselho Municipal de Proteção de Dados Pessoais e da Privacidade serão públicas e transmitidas pela rede mundial de computadores.

§ 5º O Conselho poderá, por deliberação de sua maioria absoluta, convidar pessoas especialista para, na qualidade de convidado ouvinte, integrar suas reuniões visando contribuição técnica para temáticas a serem deliberadas pelo Conselho.

CAPÍTULO VIII

DISPOSIÇÕES TRANSITÓRIAS E FINAIS

Art. 48. Esta Lei entrará em vigor no prazo de 180 dias contados da data da sua publicação.

Art. 49. Esta Lei revoga todas as disposições contrárias.

Sala da Comissão de Finanças e Orçamento, em 14/09/2022.

Ver. Jair Tatto (PT) Presidente

Ver. Atílio Francisco (REPUBLICANOS) - Relator

Ver. Dr Sidney Cruz (SOLIDARIEDADE)

Ver. Janaína Lima (MDB)

Ver. Marcelo Messias (MDB)

Ver. Noemi Nonato (PL)

Ver. Rodolfo Despachante (PSC) abstenção