CARTILHA LGPD PARA SERVIDORES
MUNICÍPIO DE JOAÇABA

A Lei 13.709/2018, Lei Geral de Proteção de Dados Pessoais - LGPD, que entrou em vigor em setembro de 2020, tem como objetivo assegurar a proteção dos dados pessoais do cidadão, uma vez que, na essência, guardam estreita relação com o direito a liberdade, a privacidade e até mesmo o direito à não discriminação, garantindo também segurança jurídica para os agentes de tratamento. Para tanto, a lei em questão estipula para os agentes de tratamento uma série de obrigações sobre o tratamento de dados pessoais.

Visando nortear a adequação do tratamento de dados pessoais realizado no âmbito do município de Joaçaba/SC e estabelecer competências sobre a matéria na organização interna, foi estabelecido o Decreto Municipal n° 7.019, de 19 de dezembro de 2023.

Objetivando apresentar as premissas base da Lei Geral de Proteção de Dados aos servidores do município de Joaçaba/SC, é desenvolvida pelo Comitê Gestor de Proteção de Dados esta cartilha, que tem com o intuito de introduzir o assunto de maneira simples, trazendo exemplos adequados a realidade, auxiliando na compreensão e conscientização sobre a questão.

1. Comitê Gestor de Proteção de Dados e Encarregado

Há um setor especializado para apoiar os servidores a cumprir a lei geral de proteção de dados pessoais no exercício de suas atividades. Essa atribuição cabe ao Comitê Gestor de Proteção de Dados, instituído pelo Decreto n° 7.019, de 19 de dezembro de 2023. O Comitê presta apoio e orientação às diversas áreas na implementação das medidas necessárias à adequação do tratamento dos dados pessoais na execução das atividades administrativas e finalísticas do Município, em cumprimento ao disposto na Lei Geral de Proteção de Dados (Lei Federal nº 13.709/2018) e em atos normativos regulamentadores, oriundos da Autoridade Nacional de Proteção de Dados (ANPD).

O Comitê Gestor de Proteção de Dados também presta apoio ao Encarregado de Proteção de Dados Pessoais, que é um servidor que tem por atribuições atuar como canal de contato do Município com os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD) e prestar orientações sobre a matéria aos servidores do município, titulares de dados e outros interessados.
Os dados de contato do Encarregado estão disponíveis no site do Município.

2. Principais definições

Para melhor entendimento, conceituam-se os termos abaixo:

a) **Dado pessoal:** Dados pessoais englobam toda informação relacionada à pessoa natural identificada ou identificável, ou seja, se uma informação permite identificar, direta ou indiretamente, uma pessoa natural que esteja viva, então ela é considerada um dado pessoal. São exemplos de dados pessoais: Nome civil e social, apelido, sexo, data e local de nascimento, filiação, parentesco, IDs (RG, CPF, Previdência, Título de Eleitor, número de Passaporte), naturalidade, nacionalidade, placa de veículos, vínculo empregatício, característica hereditária, dados fiscais,

bancários e financeiros, relação de bens, renda, histórico de pagamentos, dados profissionais, endereço residencial, e-mail, números de telefone, dados telefônicos e telemáticos, localização via GPS, fotografias, vídeos de câme- ras de segurança, hábitos de consumo, preferências de lazer, informações contidas em aparelhos eletrônicos (IP, IMEI), cookies (rastreadores que monitoram o com- portamento do usuário na internet), entre outros.

b) **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. Por envolverem maiores riscos, esses dados demandam maior grau de proteção.
c) **Dados de crianças e adolescentes**: Dados pessoais vinculados a titulares menores de idade. Os dados pessoais de crianças e adolescentes gozam de maior grau de proteção, e só devem ser divulgados em situações excepcionais (maior ônus argumentativo). Nesses casos, o tratamento deve ser feito sempre para a proteção e no melhor interesse desses titulares; e, a depender das circunstâncias, será necessário o consentimento dos responsáveis. Além do uso de iniciais em lugar do nome, podem ser adotadas outras medidas de proteção, como a restrição de acesso a determinados usuários e a imposição de sigilo ao expediente.
d) **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. A mera visualização de dados por um servidor caracteriza tratamento;
e) **Titular:** pessoa natural identificada ou identificável;
f) **Consentimento:** Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

3. Fundamentos e Princípios da LGPD:

A LGPD traça os seguintes fundamentos necessários e aplicáveis a toda ação envolvendo o tratamento de dados pessoais:

a) o respeito à privacidade;
b) a liberdade de expressão, de informação, de comunicação e de opinião;
c) a inviolabilidade da intimidade, da honra e da imagem; e
d) os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Ainda, deve-se realizar uma análise dos dados, observando sua finalidade pública, levando em conta os fundamentos acima especificados para o tratamento dos dados pessoais na persecução do interesse público. Em resumo, **quando do tratamento dos dados pessoais, deverá ser observada a real necessidade dos dados**

compartilhados e, somente poderá manter os dados essenciais para execução das competências legais ou cumprimento das atribuições legais do serviço público.

4. Lei de Acesso à Informação e Lei Geral de Proteção de Dados Pessoais

As disposições da Lei de Acesso à Informação (LAI) reforçam os direitos dos titulares previstos na LGPD no que tange ao acesso e à transparência. Assim, os titulares poderão obter acesso aos dados pertinentes à sua pessoa, atados pelas instituições públicas, bem como todas as informações relacionadas ao tratamento dos seus dados.

No entanto, considerando que a relação entre o serviço público e o cidadão é diferente da relação entre ente privado e indivíduo, a LGPD destinou um capítulo próprio à esfera pública (artigos 23 a 30 da LGPD).

Na maioria das vezes, o tratamento de dados feito pelo poder público decorre do cumprimento de seus deveres constitucionais e legais. Porém, ao mesmo tempo em que deverá promover a tutela da proteção dos dados pessoais, o poder público deverá observar outros princípios como o da eficiência (artigo 37 da Constituição Federal) e o da transparência, previsto na Lei do Acesso à Informação.

Desta forma, não há falar que a divulgação de dados pessoais dos servidores pela municipalidade se configura como violação à Lei Geral de Proteção de Dados, uma vez que a remuneração dos agentes públicos é informação de interesse coletivo e fortalece o controle social e, por isso, a princípio, não há mudança com a entrada em vigor da LGPD.

5. Bases legais para o tratamento dos dados pessoais

Todas as ações realizadas com dados pessoais, devem estar embasadas em um fundamento legal para justificar o tratamento, os quais se encontram elencados no artigo 7º ou, no caso de dados sensíveis, no artigo 11 da LGPD, devendo ser interpretados em conjunto com os critérios previstos no artigo 23, que complementam e auxiliam a aplicação prática das bases legais no âmbito do Poder Público. Isto é, poderá ser realizado o tratamento de dados pessoais quando:

a) Exigido para o cumprimento de **obrigação legal ou regulatória (**artigo 7º, inciso II, e no artigo 11, inciso II, alínea a e artigo 23 da LGPD);
b) Exigido para a execução de políticas públicas (artigo 11, inciso II, alínea b da LGPD);
c) Autorizado expressamente pelo cidadão (artigo 14, §1º, LGPD).

Caso não seja possível configurar uma das hipóteses acima para realização do tratamento dos dados, a situação deverá ser direcionada para avaliação pelo Comitê Gestor de Proteção de Dados.

6. Compartilhamento

O uso compartilhado de dados é um mecanismo relevante para a execução de atividades do Poder Público. A LGPD reconhece a relevância ao estabelecer, em seu artigo 25, que os dados devem ser mantidos em formato interoperável e estruturado para o uso compartilhado, visando, entre outras finalidades, 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.

Não obstante, assim como ocorre com as demais operações de tratamento, o uso compartilhado de dados pessoais deve ser realizado em conformidade com a LGPD. Com esse intuito, são indicados a seguir os principais requisitos que devem ser observados nos processos de compartilhamento de dados pessoais pelo Poder Público:

a) **Formalização e registro:** O uso compartilhado de dados pessoais deve ser formalizado, seja em atenção às normas gerais que regem os procedimentos administrativos, seja em atenção à obrigatoriedade de registro das operações de tratamento, conforme disposto no artigo 37 da LGPD.
b) **Objeto e finalidade:** Independentemente da opção adotada para a formalização e registro, os dados pessoais, objeto de compartilhamento, devem ser indicados de forma objetiva e detalhada, limitando-se ao que for estritamente necessário para as finalidades do tratamento, em conformidade com o princípio da necessidade. A finalidade deve ser específica, indicando precisamente qual iniciativa, ação ou programa será executado ou, ainda, qual atribuição legal será cumprida mediante o compartilhamento dos dados pessoais.
c) **Base legal:** O ato que autoriza ou formaliza o compartilhamento deverá conter expressa indicação da base legal utilizada, conforme artigo 7º ou, no caso de dados sensíveis, artigo 11 da LGPD.
d) **Duração do tratamento:** Com exceção do disposto no artigo 16 da LGPD, o tratamento de dados pessoais é um processo com duração definida, após o qual, em regra, devem ser eliminados, observados as condições e os prazos previstos em normas específicas que regem a gestão de documentos e arquivos.
e) **Transparência e direitos dos titulares:** Os atos que regem e autorizam o compartilhamento de dados pessoais devem prever as formas de atendimento ao princípio da transparência, assegurando a disponibilização de informações claras, precisas e facilmente acessíveis aos titulares sobre a realização do compartilhamento e sobre como exercer seus direitos.
f) **Prevenção e segurança:** É importante que sejam estabelecidas as medidas de segurança, técnicas e administrativas, que serão adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

7. Compartilhamento de dados pessoais com entidades privadas

É vedado, exceto:

a) Na execução descentralizada de atividade publica que exija a transferência, exclusiva para esse fim especifico e determinado;
b) Nos casos em que os dados sejam publicamente acessíveis;
c) Quando houver previsão legal ou cláusula específica em contratos, convênios ou similares, sendo que a celebração deverá ser informada

pelo responsável ao Encarregado para comunicação à Autoridade Nacional de Proteção de Dados;

d) Quando a transferência objetivar exclusivamente a prevenção de fraudes, irregularidades, ou proteção, segurança e integridade do titular dos dados. (artigo 14, Decreto Estadual n° 15.572/2020)

8. Direitos dos titulares

A Lei Geral de Proteção de Dados concede ao titular uma série de direitos (artigo 18, LGPD), os quais relaciona-se abaixo:

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 tratados em desconformidade com a lei;

V. **Portabilidade** dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial.

VI. **Eliminação** dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses relacionadas no artigo 16 da LGPD.

Eventuais solicitações de titulares acerca do tratamento de seus dados pessoais pela Prefeitura devem ser direcionadas à Ouvidoria – Telefone/*WhatsApp* 049 35278833; presencialmente na Prefeitura de Joaçaba - Dentro da Secretaria de Transparência, Controle e Gestão Pública, e site: https://falabr.cgu.gov.br/publico/SC/Joacaba/Manifestacao/RegistrarManifestacao.

9. Responsabilização

Na hipótese de restar configurada violação às normas de proteção de dados e segurança, seja por descumprimento ou inobservância, incluindo a Lei Geral de Proteção de Dados, normas emitidas pelas Autoridade Nacional de Proteção de Dados, a legislação municipal de proteção de dados e orientações emitidas pelo Comitê Gestor de Proteção de Dados, enseja-se a incidência dos procedimentos de responsabilização estabelecidos no Estatuto dos Servidores Públicos do Município de Joaçaba, Autarquias e Fundações Públicas Municipais (Lei Complementar nº 76 de 11 de dezembro de 2003).

10. Orientações de segurança de informações para o Dia-a-Dia

Os servidores devem observar, sem exclusão às normas aplicáveis, as orientações relacionadas abaixo:

a) A comunicação institucional deve acontecer mediante uso de meios institucionais e formais autorizados (e-mail, telefone e whatsapp corporativo). No excepcional uso de meios de comunicação pessoais, isso deve acontecer de modo restrito e seguindo padrões de sigilo e segurança.

b) Evitar acessar a rede interna da prefeitura em locais públicos, entre eles: lan house; aeroportos; shoppings.

c) Nunca sair da estação de trabalho sem bloquear o computador. Em trabalho remoto, redobrar os cuidados quanto à exposição das

informações. Sempre que se ausentar, atentar-se em utilizar a tela de bloqueio de vídeo para impedir que estranhos acessem o computador.

d) Negar acesso aos espaços físicos e aos documentos a pessoas não autorizadas.
e) Criar senha institucional forte e diferente das utilizadas em acessos particulares, como em sistemas bancários, provedores de internet e contas de e-mail pessoal.
f) Não compartilhar suas senhas com outros servidores públicos ou terceiros e não anotar em agendas ou post-it.
g) Utilizar apenas programas certificados pela Secretaria de Tecnologia da Informação do Município.
h) Não clicando em e-mails ou links estranhos.
i) Tendo cuidado extra com spam e tentativas de phising (phising é uma técnica de engenharia social usada para enganar usuários e obter informações confidenciais como nome de usuário, senha e detalhes do cartão de crédito).
j) Comunicar ao Encarregado do órgão sobre falhas de segurança sobre o uso de dados pessoais.

11. Dúvidas e questionamentos

Quaisquer dúvidas e questionamentos com relação às normas emitidas pela municipalidade, bem como acerca das melhores práticas a serem adotadas na execução de atividades de tratamento de dados pessoais, deve ser direcionada ao Comitê Gestor de Proteção de Dados e Encarregado, disponíveis através dos seguintes meios de contato: comitelgpd@joacaba.gov.br, bem como pela ouvidoria, no telefone/*WhatsApp* 049 35278833; presencialmente na Prefeitura de Joaçaba - Dentro da Secretaria de Transparência, Controle e Gestão Pública, e site: https://falabr.cgu.gov.br/publico/SC/Joacaba/Manifestacao/RegistrarManifestacao.