

2022

CARTILHA

LEI GERAL DE PROTEÇÃO DE DADOS - LGPD

PREFEITURA MUNICIPAL DE PIRACEMA
PRAÇA JOSÉ RIBEIRO DE ASSIS, 42, CENTRO
PIRACEMA, MINAS GERAIS, CEP 35536-000

SUMÁRIO

APRESENTAÇÃO	2
GLOSSÁRIO	3
O QUE É A LGPD?	5
O QUE É TRATAMENTO DE DADOS?	6
O QUE SÃO DADOS PESSOAIS?	7
O QUE SÃO DADOS SENSÍVEIS?	8
QUAIS SÃO OS FUNDAMENTOS DA LGPD?	8
POR QUE AS PREFEITURAS DEVEM FAZER O CONTROLE DE DADOS PESSOAIS?	9
PARA QUAIS TIPOS DE DADOS PESSOAIS NÃO SE APLICA A LGPD?	9
QUEM SÃO CONSIDERADOS AGENTES DE TRATAMENTO?	10
QUEM SÃO OS TITULARES DE DADOS PESSOAIS?	10
QUAIS SÃO OS DIREITOS DO TITULAR DE DADOS?	10
QUEM SÃO O CONTROLADOR, OPERADOR E O ENCARREGADO?	12
O QUE É O RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS – “RIPD”?	13
O QUE É O CONSENTIMENTO DO TITULAR?	13
COMO DEVERÁ SER OBTIDO O CONSENTIMENTO DO TITULAR?	14
QUAIS SÃO AS HIPÓTESES EM QUE PODE OCORRER TRATAMENTO SEM CONSENTIMENTO?	14
COMO OS DADOS PODERÃO SER TRATADOS?	15
O TITULAR PODE REVOGAR O CONSENTIMENTO?	16
HÁ ALGUMA ESPECIFICIDADE PARA O TRATAMENTO DE DADOS DE CRIANÇAS E ADOLESCENTES?	16
O QUE É DADO ANONIMIZADO?	17
QUAL É A AUTORIDADE MÁXIMA DA ESTRUTURA DE IMPLANTAÇÃO DA LGPD?	17
MONITORAMENTO	18
QUAIS SÃO AS PENALIDADES E SANÇÕES CABÍVEIS A QUEM DESCUMPRIR A LGPD?	18
IMPROBIDADE ADMINISTRATIVA: QUANTO AOS AGENTES DE TRATAMENTO (CONTROLADOR E OPERADOR), ESTES RESPONDERÃO SOLIDARIAMENTE PELOS DANOS QUE CAUSAREM NO EXERCÍCIO DE SUAS ATIVIDADES, RESPONDENDO CIVIL E ADMINISTRATIVAMENTE EM CASO DE DESCUMPRIMENTO DA LGPD.	18
ADVERTÊNCIA.	18
MULTA SIMPLES.	18
MULTA DIÁRIA.	18
PUBLICIZAÇÃO DA INFRAÇÃO APÓS DEVIDAMENTE APURADA E CONFIRMADA A SUA OCORRÊNCIA.	19
BLOQUEIO DOS DADOS PESSOAIS A QUE SE REFERE A INFRAÇÃO ATÉ A SUA REGULARIZAÇÃO.	19
ELIMINAÇÃO DOS DADOS PESSOAIS A QUE SE REFERE A INFRAÇÃO.	19
BLOQUEIO DOS DADOS PESSOAIS A QUE SE REFERE A INFRAÇÃO ATÉ A SUA REGULARIZAÇÃO.	19
REFERÊNCIAS	19

APRESENTAÇÃO

A presente cartilha tem por objetivo de apresentar um conjunto de orientações e conceitos fundamentais para o conhecimento prévio a respeito das obrigações e regras estabelecidas na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – “LGPD”), especialmente, diante da Emenda à Constituição nº 115/2022 que acrescentou no art. 5º, o inciso LXXIX, que assegura a todos os indivíduos, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

As diretrizes estabelecidas nesta cartilha são aplicáveis a todos os processos de tratamentos de dados pessoais realizados pela Prefeitura de Piracema/MG 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 e diretrizes apresentadas nessa cartilha devem servir como princípios gerais para o estabelecimento dos processos de tratamento de dados pessoais na Prefeitura Municipal de Piracema/MG, sendo compatibilizados, portanto, com as demais políticas e atividades em andamento, especialmente aquelas decorrentes da Lei de Acesso à Informação (LAI).

A presente cartilha foi elaborada em conjunto com o escritório Marçoni Santos Advocacia e Consultoria.

GLOSSÁRIO

Agente de tratamento: o controlador e o operador;

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;

Autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional;

Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

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

Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

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;

Dado pessoal: informação relacionada à pessoa natural identificada ou identificável;

Dado pessoal de criança e de adolescente: o Estatuto da Criança e do Adolescente (ECA) considera criança a pessoa até 12 anos de idade incompletos e adolescente aquela entre 12 e 18 anos de idade. Em especial, a LGPD determina que as informações sobre o tratamento de dados pessoais de crianças e de adolescentes deverão ser fornecidas de maneira simples, clara e acessível de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança;

Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à 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;

Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

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);

Garantia da segurança da informação: capacidade de sistemas e organizações assegurarem a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação. A Política Nacional de Segurança da Informação (PNSI) dispõe sobre a governança da segurança da informação aos órgãos e às entidades da administração pública federal em seu âmbito de atuação;

Garantia da segurança de dados: ver garantia da segurança da informação;

Interoperabilidade: capacidade de sistemas e organizações operarem entre si. A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, além dos padrões de interoperabilidade de governo eletrônico (ePING);

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

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;

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;

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

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

Tratamento: toda operação realizada com dados pessoais; como as que se referem a:

- ✓ acesso - possibilidade de comunicar-se com um dispositivo, meio de armazenamento, unidade de rede, memória, registro, arquivo etc., visando receber, fornecer, ou eliminar dados
- ✓ armazenamento - ação ou resultado de manter ou conservar em repositório um dado
- ✓ arquivamento - ato ou efeito de manter registrado um dado embora já tenha perdido a validade ou esgotada a sua vigência
- ✓ avaliação - ato ou efeito de calcular valor sobre um ou mais dados
- ✓ classificação - maneira de ordenar os dados conforme algum critério estabelecido

- ✓ coleta - recolhimento de dados com finalidade específica
- ✓ comunicação - transmitir informações pertinentes a políticas de ação sobre os dados
- ✓ controle - ação ou poder de regular, determinar ou monitorar as ações sobre o dado
- ✓ difusão - ato ou efeito de divulgação, propagação, multiplicação dos dados
- ✓ distribuição - ato ou efeito de dispor de dados de acordo com algum critério estabelecido
- ✓ eliminação - ato ou efeito de excluir ou destruir dado do repositório
- ✓ extração - ato de copiar ou retirar dados do repositório em que se encontrava
- ✓ modificação - ato ou efeito de alteração do dado
- ✓ processamento - ato ou efeito de processar dados
- ✓ produção - criação de bens e de serviços a partir do tratamento de dados
- ✓ recepção - ato de receber os dados ao final da transmissão
- ✓ reprodução - cópia de dado preexistente obtido por meio de qualquer processo
- ✓ transferência - mudança de dados de uma área de armazenamento para outra, ou para terceiro
- ✓ transmissão - movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos etc.
- ✓ utilização - ato ou efeito do aproveitamento dos dados.

Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicas 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.

O QUE É A LGPD?

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018), popularmente conhecida como “LGPD”, dispõe sobre o tratamento de dados pessoais em âmbito nacional, com o objetivo de proteger os direitos fundamentais de liberdade, privacidade e a livre formação da personalidade de cada indivíduo.

Sua finalidade consiste em oferecer ao titular dos dados maior conhecimento, controle e transparência na coleta, processamento, uso e compartilhamento de suas informações pessoais, tanto aquelas armazenadas em bancos de dados físicos ou digitais, de instituições privadas e de órgãos públicos.

A LGPD foi aprovada e publicada em agosto de 2018, entrando em vigor em agosto de 2020.

A regulação e fiscalização especializada quanto a aplicação da legislação ficará a cargo da Autoridade Nacional de Proteção de Dados (“ANPD”), sendo certo que o controle externo será exercido pelo Tribunal de Contas de Minas Gerais (“TCE/MG”), Ministério Público do Estado de Minas Gerais (“MPMG”) e Programa Estadual de Proteção e Defesa do Consumidor (“Procon/MG”).

O que é tratamento de dados?

Tratamento é qualquer operação efetuada sobre dados pessoais, por meios manuais ou automatizados, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Diante da amplitude do conceito de tratamento de dados, a mera visualização de dados por um servidor pode caracterizar tratamento! Por isso, é fundamental criar-se procedimentos internos para o tratamento pela Prefeitura.

Desta feita, a Administração Pública, ao tratar os dados do cidadão/usuário, deve ponderar a real necessidade da solicitação de alguma informação específica para viabilizar a oferta dos serviços públicos. Por exemplo, não se recomenda a solicitação do CPF para a aquisição de um medicamento na farmácia básica, sem que se esclareça previamente o titular e se comprove a necessidade de tal informação e recolha o seu consentimento.

De igual forma, deve-se ponderar a necessidade de solicitar informações sobre religião, opinião política, filosófica, orientação sexual do cidadão/usuário para a prestação de serviço público, pois quanto mais dados são coletados, maior a responsabilidade do Poder Público acerca da segurança da informação sob sua guarda.

O art. 6º da LGPD trouxe expressamente quais são os princípios que direcionam a atividade de tratamento de dados:

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.

O que são dados pessoais?

São informações relacionadas à pessoa natural/física identificada ou identificável como nome, data de nascimento, filiação, apelido, CPF, RG, Boletim Médico, foto, endereço residencial, endereço de e-mail, endereço IP, cookies, hábitos/histórico de navegação, posição geolocalacional, formulários cadastrais, números de documentos.

O que são dados sensíveis?

A LGPD estabelece, também, que alguns dados pessoais estão sujeitos a cuidados ainda mais específicos, como os “dados sensíveis” e os dados sobre “crianças e adolescentes”.

Nesse sentido, as informações 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 (prontuários e exames) ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Esses dados podem expor o indivíduo de forma indesejada, social ou profissionalmente, dando margem a uma possível discriminação.

Em razão disso, os dados sensíveis exigem um tratamento ainda mais delicado, com a adoção, pelas entidades controladoras, de medidas de segurança mais rígidas, como, por exemplo, a anonimização¹ desses dados e camadas de proteção mais extensas.

Assim sendo, a Prefeitura Municipal pode tratar dados pessoais sensíveis quando houver o consentimento explícito da pessoa e com finalidade definida.

QUAIS SÃO OS FUNDAMENTOS DA LGPD?

Nos termos do art. 2º da LGPD, a disciplina de proteção de dados pessoais se fundamenta:

I - No respeito à privacidade;

II - Na autodeterminação informativa;

III - Na liberdade de expressão, de informação, de comunicação e de opinião;

IV - Na inviolabilidade da intimidade, da honra e da imagem;

V - No desenvolvimento econômico e tecnológico e a inovação;

VI - Na livre iniciativa, a livre concorrência e a defesa do consumidor; e

¹ 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.

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

POR QUE AS PREFEITURAS DEVEM FAZER O CONTROLE DE DADOS PESSOAIS?

As prefeituras municipais tratam dados pessoais a todo momento, recebendo e guardando um grande volume de dados pessoais, dos cidadãos e dos próprios servidores, no âmbito de seus diversos órgãos públicos.

O texto legal dispõe em seu art. 23 que:

*“o tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as **competências legais** ou cumprir as **atribuições legais** do serviço público”.*

Assim sendo, é extremamente necessário a realização do controle de dados tratados pelas prefeituras, evitando-se o uso de dados pessoais com desvio de finalidade pública, de forma não persecutória ao interesse público, fora das competências legais do órgão de tratamento e em descumprimento às atribuições legais, evitando-se responsabilizações previstas nos casos de descumprimento da LGPD.

PARA QUAIS TIPOS DE DADOS PESSOAIS NÃO SE APLICA A LGPD?

Àqueles usados para fins exclusivamente particulares e não econômicos jornalísticos ou artísticos, para fins acadêmicos, para investigações, repressão de crimes, ou em casos de segurança pública e defesa nacional, nos termos da legislação de regência.

QUEM SÃO CONSIDERADOS AGENTES DE TRATAMENTO?

São agentes de tratamento de dados pessoais o **CONTROLADOR** que é a pessoa física ou jurídica, de direito público ou privado, responsável pelas decisões referentes ao tratamento de dados pessoais e o **OPERADOR** que é a pessoa física ou jurídica que realiza o tratamento de dados pessoais em nome do controlador.

O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse e para o atendimento de sua finalidade pública, na persecução do interesse público.

A qualquer momento pode ser necessária a demonstração clara dessas operações aos titulares dos dados ou órgãos de controle externo, podendo eles serem responsabilizados por eventual infração à LGPD.

QUEM SÃO OS TITULARES DE DADOS PESSOAIS?

A pessoa natural a quem se referem esses dados, como os cidadãos usuários dos serviços públicos, os agentes públicos e políticos, os servidores estatutários, celetistas, temporários, ocupantes de cargo em comissão e de confiança.

O dono do dado é a própria pessoa ao qual este dado se refere.

Envolve tanto dados corporativos, dos próprios servidores e contratados, como, é claro, do público externo com o qual o cada órgão se relaciona.

QUAIS SÃO OS DIREITOS DO TITULAR DE DADOS?

Dispõe o texto legal que os titulares de dados são todas as pessoas naturais a quem se referem os dados pessoais que são objeto de tratamento.

Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

Quais são os direitos dos titulares:

- ✓ É direito de todos os cidadãos ter acesso facilitado às informações sobre o tratamento realizado por pessoa jurídica de direito público ou privado sobre seus dados pessoais, sendo obrigação dessas pessoas jurídicas informar de forma clara, adequada e ostensiva, a existência de tratamento e, em caso positivo, sua finalidade, forma, duração.
- ✓ Com isso, determinada secretaria municipal deve informar as hipóteses em que, no exercício de suas competências previstas no art. X, da Lei nº Y que trata sobre organização administrativa e atribui competências para execução de determinado serviço público pelo órgão que realiza o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades.
- ✓ Acesso e correção de dados incompletos, inexatos ou desatualizados.
- ✓ Anonimização, bloqueio ou eliminação de dados desnecessários.
- ✓ Portabilidade de seus dados.
- ✓ Revogação do consentimento/eliminação dos dados, sendo assegurado o direito de petição à autoridade nacional.
- ✓ Informação sobre com quem os dados que por algum motivo foram compartilhados.
- ✓ Informação sobre o poder de não consentir e suas consequências.
- ✓ Identificação do controlador, operador e encarregado e seus, respectivos, contatos.

QUEM SÃO O CONTROLADOR, OPERADOR E O ENCARREGADO?

O **CONTROLADOR** é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, sendo responsável pela definição das medidas de segurança que serão aplicadas no tratamento desses dados.

Podem ser eles o Prefeito Municipal, secretários municipais, procurador-geral, controlador-geral e diretores-presidentes de entidades da Administração Indireta, por exemplo.

O **OPERADOR** é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

São eles os chefes de setor, coordenadores ou todo aquele designado ou contratado pelo controlador para essa função.

ENCARREGADO ou **DATA PROTECTION OFFICER – DPO** é a pessoa natural ou jurídica indicado pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados - ANPD.

É recomendável que o Encarregado tenha conhecimentos de governança, compliance, direito, segurança da informação, ferramentas de segurança e processos de segurança, possuindo habilidades de gerenciamento e capacidade de interação com a equipe interna do órgão controlador, terceiros, titulares de dados e órgãos oficiais.

A **identificação e informações de contato** do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva no **sítio eletrônico** do controlador.

No âmbito da Administração Pública, sua indicação é obrigatória, podendo o titular do órgão indicar mais de um encarregado, a depender da complexidade e volume dos dados tratados.

O QUE É O RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS – “RIPD”?

Documento criado pelo controlador que contém a descrição das fases de tratamento dos dados pessoais, a identificação de quem acessa esses dados pessoais, bem como quais são os mecanismos de privacidade, segurança e mitigação de risco, cujo prazo de envio ainda será regulamentado pela ANPD.

Isto é, o RIPD tem como objetivo definir e implementar estratégia para atuar preventivamente nas frentes de segurança da informação e privacidade de dados, com o intuito de fomentar a cultura de proteção de dados, implementando ações que visam avançar no processo de adequação à LGPD, minimizando os riscos.

O QUE É O CONSENTIMENTO DO TITULAR?

É a concordância e autorização do titular quanto ao tratamento de seus dados pessoais. Deve ocorrer de forma livre, informada, inequívoca e para uma finalidade determinada, **por escrito** (neste caso, de maneira destacada das demais cláusulas) **ou por outro meio que demonstre a manifestação de vontade do titular.**

Autorizações/consentimentos genéricos para tratamento de dados serão nulos, bem como se o dado for utilizado para finalidade diversa da inicialmente consentida.

Importante destacar que a Administração Pública pode tratar dados sem o consentimento em atividades de interesse público determinadas em lei, desde que informe ao titular quando, como, para que e com base em qual artigo de lei.

COMO DEVERÁ SER OBTIDO O CONSENTIMENTO DO TITULAR?

Por escrito ou por outro meio que demonstre a livre e inequívoca manifestação de sua vontade.

O titular deve concordar não só com o tratamento, mas com a finalidade daquele tratamento.

Quando o tratamento de dados envolver o compartilhamento destes com algum outro controlador, deve haver consentimento específico para que possa haver tal compartilhamento, ressalvadas as hipóteses legais de dispensa de consentimento, respeitados, sempre, os princípios de proteção dos dados pessoais elencados no art. 6º da LGPD.

QUAIS SÃO AS HIPÓTESES EM QUE PODE OCORRER TRATAMENTO SEM CONSENTIMENTO?

- ✓ Para o cumprimento de obrigação legal ou regulatória pelo controlador.
- ✓ Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais.
- ✓ Para a proteção da vida ou da incolumidade física do titular ou de terceiros.
- ✓ Para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias, por exemplo, para proteção da vida, as atividades exercidas pela Defesa Civil; todas as atividades de saúde, como a notificação compulsória de doenças e agravos e violências (Leis nº 6259/75, nº 8069/90, nº 10.741/03, nº 13.146/15).
- ✓ Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados.

- ✓ 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).
- ✓ Para a proteção da vida ou da incolumidade física do titular ou de terceiros.
- ✓ Quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.
- ✓ Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Portanto, sem o consentimento do titular, a LGPD permite o tratamento, quando for indispensável, nas seguintes situações:

- **Cumprimento de obrigação legal;**
- **Execução de políticas públicas;**
- **Estudos por órgão de pesquisa, garantindo sempre que possível a anonimização;**
- **Exercício de direitos, em contrato ou processo;**
- **Preservação da vida e da integridade física de uma pessoa;**
- **Tutela de saúde, em procedimentos por profissionais das áreas da saúde ou sanitária;**
- **Prevenção a fraudes e segurança do titular.**

COMO OS DADOS PODERÃO SER TRATADOS?

O titular do dado deverá assinar um termo de consentimento, que deverá ter redação clara, indicando a finalidade específica do tratamento.

A prefeitura poderá tratar e compartilhar os dados necessários à execução de políticas públicas previstas em lei e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, independentemente do consentimento do titular dos dados, desde que sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a

execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos.

Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

O TITULAR PODE REVOGAR O CONSENTIMENTO?

A qualquer tempo o titular pode revogar seu consentimento, exceto quando o consentimento for dispensável. Essa revogação poderá ser requerida mediante manifestação expressa do titular, por procedimento gratuito e facilitado.

Além disso, o cidadão pode solicitar que seus dados sejam deletados, ou pode solicitar transferir dados para outro fornecedor de serviços (**esta opção não é usual no serviço público, uma vez que, de um modo geral não há opção de prestador**).

O controlador, entretanto, poderá se opor à exclusão dos dados solicitados pelo titular, apresentando razões fundamentadas acerca da continuidade/guarda das informações. Por exemplo, na área da saúde, não é possível excluir dados de prontuários médicos, ainda que solicitados pelo paciente, haja vista a obrigação legal imposta pela Lei nº 13.787/18, que determina a guarda do prontuário pela instituição de saúde pelo prazo mínimo de 20 anos.

HÁ ALGUMA ESPECIFICIDADE PARA O TRATAMENTO DE DADOS DE CRIANÇAS E ADOLESCENTES?

SIM! Esse tratamento deverá ser realizado **com o consentimento específico** e em destaque, dado por, pelo menos, um dos pais ou responsável legal.

Órgãos sujeitos a tratamento de crianças e adolescentes deverão tomar a medida necessária para manter controle desse consentimento, uma vez que podem ser demandados, a qualquer momento, a demonstrar quais dados foram tratados, de que forma, e quais são os respectivos responsáveis.

Sem o consentimento, só se pode coletar dados de crianças e adolescentes se for para urgências relacionadas a entrar em contato com os pais ou responsáveis e/ou para proteção da criança e do adolescente.

O QUE É DADO ANONIMIZADO?

É aquele que, originariamente, era relativo a uma pessoa, mas que passou por etapas que garantiram sua desvinculação com essa pessoa, não permitindo que, via meios técnicos e outros, se reconstrua o caminho para “**descobrir**” quem era a pessoa titular do dado.

Se um dado for anonimizado, a LGPD não se aplicará a ele.

Lembramos que a anonimização é a 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.

QUAL É A AUTORIDADE MÁXIMA DA ESTRUTURA DE IMPLANTAÇÃO DA LGPD?

A fiscalização e a regulação da LGPD ficarão a cargo da Autoridade Nacional de Proteção de Dados Pessoais (“ANPD”), que será um elo entre sociedade e governo, permitindo que as pessoas enviem dúvidas, sugestões, denúncias ligadas à LGPD para apuração.

Lembramos, ainda, que o controle externo poderá ser exercido pelo Tribunal de Contas de Minas Gerais (“TCE/MG”), Ministério Público do Estado de Minas Gerais (“MPMG”) e Programa Estadual de Proteção e Defesa do Consumidor (“Procon/MG”).

MONITORAMENTO

A Administração 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.

QUAIS SÃO AS PENALIDADES E SANÇÕES CABÍVEIS A QUEM DESCUMPRIR A LGPD?

Improbidade Administrativa: Quanto aos agentes de tratamento (controlador e operador), estes responderão solidariamente pelos danos que causarem no exercício de suas atividades, respondendo civil e administrativamente em caso de descumprimento da LGPD.

Advertência. Com indicação de prazo para adoção de medidas corretivas.

Multa simples. Multa de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, limitada, no total, a R\$ 50.000.000,00 por infração (não se aplica à Administração Direta dos Municípios).

Multa diária. Multa diária limitada a R\$ 50.000.000,00 (não se aplica à Administração Direta dos Municípios).

Publicização da infração após devidamente apurada e confirmada a sua ocorrência.

Bloqueio dos dados pessoais a que se refere a infração até a sua regularização.

Eliminação dos dados pessoais a que se refere a infração.

Bloqueio dos dados pessoais a que se refere a infração até a sua regularização.

A responsabilidade do operador pode ser limitada em comparação com a responsabilidade do controlador, visto que o operador realiza o tratamento de dados em nome e conforme orientações do controlador. Assim, a responsabilidade do operador pode ser circunscrita às suas obrigações contratuais e de segurança da informação, desde que não descumpra as exigências da LGPD.

Quanto a órgãos da Administração Indireta, se estes estiverem na operacionalização de políticas públicas, terão o mesmo tratamento destinado às demais entidades públicas. Assim, a penalidade de multa não será aplicável.

REFERÊNCIAS

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Constituição da República Federativa do Brasil. Brasília, DF, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 29.03.2022.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: <[http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm#:~:text=L13709&text=LEI%20N%C2%BA%2013.709%2C%20DE%2014%20DE%20AGOSTO%20DE%202018.&text=Disp%C3%B5e%20sobre%20a%20prote%C3%A7%C3%A3o%20de,\(Marco%20Civil%20da%20Internet\).>](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm#:~:text=L13709&text=LEI%20N%C2%BA%2013.709%2C%20DE%2014%20DE%20AGOSTO%20DE%202018.&text=Disp%C3%B5e%20sobre%20a%20prote%C3%A7%C3%A3o%20de,(Marco%20Civil%20da%20Internet).>)>. Acesso em 29.03.2022.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/ato2011-2014/2011/lei/l12527.htm>. Acesso em: 29.03.2022.