POLÍTICA DE GOVERNANÇA

Manual de Proteção de Dados Pessoais e Boas Práticas

PREFEITURA MUNICIPAL DE SANTA ROSA DE LIMA, 2023.

Vol. 01

SUMÁRIO

1. DO OBJETIVO 3
2. DAS BREVES CONSIDERAÇÕES 3
3. DOS CONCEITOS DA LGPD 3
3.1. Dos conceitos GERAIS sobre a LGPD 3
3.2. Dos conceitos ESPECÍFICOS: PRINCÍPIOS da LGPD 5
3.3. Dos conceitos ESPECÍFICOS: DIREITOS DO TITULAR na LGPD 6
4. DOS DADOS PESSOAIS: ASPECTOS INICIAIS 7
5. DA LGPD: PRINCIPAIS BASES LEGAIS 8
5.1. Base legal: A Execução de Políticas Públicas 10
5.2. Base legal: A Obrigação Legal 11
5.3. Base legal: Legítimo Interesse 12
5.4. Base legal: O Consentimento 13
6. DA DIVULGAÇÃO DE DADOS PESSOAIS PELO SETOR PÚBLICO 16
7. DO AMBIENTE FÍSICO DE TRABALHO 18
8. DO AMBIENTE DIGITAL DE TRABALHO 19
9. DAS ATIVIDADES E ROTINAS 20
10. DAS SENHAS DE ACESSO 21
11. DAS CONSIDERAÇÕES FINAIS 21

1. DO OBJETIVO DO MANUAL

O presente Manual tem como objetivo fornecer orientações sobre a adequação da Prefeitura em relação a Lei Geral de Proteção de Dados (**LGPD**), destinando-se a orientar, de forma geral, as práticas que tenham por escopo: a coleta ou qualquer forma de tratamento de quaisquer **dados pessoais e dados pessoais sensíveis de pessoas físicas**.

Vale destacar que o processo de conformidade envolve um trabalho de interpretação da lei para definição das obrigações legais, diagnóstico dos fatos pertinentes e relevantes para a sua aplicação e levantamento de fluxos e processos que contribuem ou não para que os fatos estejam de acordo com o documento legal.

2. DAS BREVES CONSIDERAÇÕES

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – "**LGPD**"), aprovada em agosto de 2018, é uma lei transversal. O que quer dizer que ela perpassa por diferentes agentes econômicos no Brasil, sendo que toda a empresa/instituição brasileira que armazenar informações relacionadas a pessoas físicas (*sejam cidadãos, servidores, funcionários ou parceiros*) está obrigada a se amoldar às exigências previstas. Em razão disso, uma uma série de particularidades nos tratamentos de dados pessoais precisam atender às obrigações legais específicas, especialmente porque possuem sinergia entre setores, sob pena de aplicação de medidas punitivas pela ANPD (Agência Nacional de Proteção de Dados) ou, ainda, na esfera judicial.

Logo, a legislação prevê em seu artigo 50, §2º sobre as características mínimas para um Programa de Gerenciamento de Privacidade, conforme restará amplamente especificado na presente Política que tem como objetivo fornecer orientações sobre a adequação em relação a Lei Geral de Proteção de Dados (**LGPD**), bem como gerenciar as diversas atividades e operações de tratamento de dados dentro da presente instituição.

3. DOS CONCEITOS DA LGPD

A presente seção trata de conceitos-chave que serão mencionados ao longo deste Manual. Logo, para a sua melhor compreensão, os conceitos foram agrupados de acordo com: (i) conceitos gerais sobre a **LGPD**; (ii) conceitos específicos sobre princípios previstos na **LGPD**; (iii) conceitos específicos sobre direitos dos titulares consoante a **LGPD**; todos dispostos em ordem alfabética.

3.1. Dos conceitos GERAIS sobre a LGPD

AGENTE DE TRATAMENTO: são considerados agentes de tratamento o **Controlador** e o **Operador** de dados pessoais e dados pessoais sensíveis (art. 5º, IX, **LGPD**).

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 (art. 5º, XI, **LGPD**). O dado anonimizado, nos termos da lei, deixa de ser considerado **dado pessoal**, garantindo maior liberdade no seu tratamento (art. 12, **LGPD**).

BASE LEGAL: é o fundamento que autoriza o tratamento de dados pessoais por um agente, devendo ser definida, em casos concretos, a partir de uma das hipóteses dispostas na **LGPD** ao seu artigo 7º (caso de dados pessoais) ou ao seu artigo 11 (caso de dados pessoais sensíveis), ou ainda ao seu artigo 23 (caso

para execução de políticas públicas). As bases legais só não serão necessárias nos casos em que a **LGPD** não se aplica, como nas hipóteses do artigo 4º ou em situações de processamento que envolvam dados anonimizados, onde a identificação da titularidade não seja possível por meios razoáveis.

CONSENTIMENTO: manifestação livre, informada e inequívoca (art. 7º, I, **LGPD**) pela qual o titular concorda com o tratamento de seus dados pessoais para uma **finalidade** determinada (art. 5º, XII, **LGPD**). Deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular (art. 8º, **LGPD**).

CONTROLADOR: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (art. 5º, VI, **LGPD**). É quem determina como os dados são processados.

***COOKIE DE NAVEGADOR*:** na terminologia da informática,pequenos arquivos de texto depositados por um site servidor no computador do cliente usuário para "memorizar" algumas informações relativas àquela navegação.

DADO BIOMÉTRICO: qualquer dado atinente a características fisiológicas (como a face, a íris, o DNA, a voz, ou uma impressão digital) ou comportamentais (como o jeito de andar, de dançar ou de gesticular) de uma pessoa natural.

DADO PESSOAL: informação relacionada a pessoa natural identificada ou identificável (art. 5º, I, **LGPD**). Também são considerados dados pessoais para os fins da lei aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada (art. 12, §2º, **LGPD**).

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 (art. 5º, II, **LGPD**), ou seja, dados que devem ser tratados de forma mais cautelosa, uma vez que eventual incidente pode acarretar em consequências mais gravosas aos direitos e liberdades dos titulares. Em razão da sua especialidade e das inúmeras restrições impostas ao seu tratamento, o rol previsto no art. 5º, II da LGPD é taxativo.

ENCARREGADO DE DADOS (DPO – *DATA PROTECTION OFFICER*): o Encarregado é, nos termos previstos no art. 5º, VIII da LGPD, a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD).

INTERESSE LEGÍTIMO DO CONTROLADOR OU TERCEIRO: poderá ser utilizado como fundamento do tratamento de dados pessoais apenas para **finalidades** legítimas, analisadas conforme o caso concreto (art. 7º, IX, **LGPD**). Tais **finalidades** podem ser, por exemplo, o apoio e promoção de atividades do **controlador**, proteção ao titular do exercício regular de seus direitos ou prestação deserviços que o beneficiem, respeitadas suas legítimas expectativas e os direitos e liberdades fundamentais (art. 10, **LGPD**). O interesse legítimo não se aplica a **dados pessoais sensíveis**.

LGPD (LEI GERAL DE PROTEÇÃO DE DADOS): Lei 13.709/2018 dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado (art. 1º, **LGPD**). A LGPD é aplicável a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: (i) a operação de tratamento seja realizada no território nacional; (ii) a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou (iii) os dados pessoais objeto do tratamento tenham sido coletados no território nacional (art. 3º, caput e incisos I a III, **LGPD**).

OPERADOR: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados

pessoais em nome do **controlador** (art. 5º, VII, **LGPD**). É quem acata as ordens de como os dados devem ser processados.

PROFILING: perfilamento ou perfilagem, ato de processar dados pessoais, de forma automatizada ou não, para avaliar padrões de comportamento relativos a um indivíduo em concreto.

TITULAR: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (art. 5º, V, **LGPD**).

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 (art. 5º, X, **LGPD**).

TRATAMENTO AUTOMATIZADO: qualquer tipo de técnica de processamento de dados pessoais que atinja resultados concretos (*outputs*) sem a supervisão imediata de um ser humano.

3.2. Dos conceitos ESPECÍFICOS: PRINCÍPIOS da LGPD

Na terminologia jurídica, um princípio é um tipo de norma que deve ser cumprida na maior medida possível e cujo conteúdo serve como diretriz geral de interpretação para situações concretas. Na **LGPD**, os princípios estão listados ao longo do artigo 6°, são eles:

ADEQUAÇÃO: compatibilidade do tratamento com as **finalidades** informadas ao titular, de acordo com o contexto do tratamento (art. 6º, II, **LGPD**).

BOA-FÉ: significa a observância de um comportamento leal, correto e probo na realização das atividades de tratamento de dados pessoais. Esse princípio, opera como norte a todos os demais e servindo de baliza para interpretar conceitos abertos (art. 6º, caput, **LGPD**).

FINALIDADE: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível ou desvirtuada (art. 6º, I, **LGPD**).

LIVRE ACESSO: garantia, aos titulares, de consulta sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais (art. 6º, IV, **LGPD**).

NÃO DISCRIMINAÇÃO: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos (art. 6º, IX, **LGPD**).

NECESSIDADE: limitação ou minimização 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 (art. 6º, III, **LGPD**).

PREVENÇÃO: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento dedados pessoais (art. 6º, VIII, **LGPD**).

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 (art. 6º, V, **LGPD**).

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 proteçãode dados pessoais e, inclusive, da eficácia dessas medidas (art. 6º, X, **LGPD**).

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 (art. 6º, VII, **LGPD**).

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 (art. 6º, VI, **LGPD**).

3.3. Dos conceitos ESPECÍFICOS: DIREITOS DO TITULAR na LGPD

Os direitos dos titulares de dados estão previstos majoritariamente ao longo do artigo 18 da LGPD. Ademais, há ainda o direito de titularidade (artigo 17) e, com relação a tratamentos automatizados, os direitos de informação e de revisão (artigo 20):

ACESSO AOS DADOS: o titular de dados tem resguardado o seu interesse de receber uma cópia dos dados pessoais detidos pela instituição, se assim o requisitar (art. 18, II, LGPD).

ANONIMIZAÇÃO, BLOQUEIO OU ELIMINAÇÃO: o titular de dados tem o direito de solicitar que seusdados sejam anonimizados, bloqueados ou que haja a eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei (art. 18, IV, LGPD).

CONFIRMAÇÃO DA EXISTÊNCIA DE TRATAMENTO: direito do titular a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição de informações sobre a existência de tratamento (art. 18, I, LGPD), isto é, de toda operação realizada com seus dados pessoais (art. 5º, X, LGPD).

CORREÇÃO DE DADOS INCOMPLETOS, INEXATOS OU DESATUALIZADOS: o titular de dados pode requerer a retificação dos dados, caso estejam incorretos, insuficientes, imprecisos, não expressem a completude das informações armazenadas ou careçam de atualização (art. 18, III, LGPD).

ELIMINAÇÃO DOS DADOS PESSOAIS: o titular de dados pode requerer que seus dados sejam excluídos, de forma que a instituição deverá eliminar todos os dados coletados com relação a esse titular, a não ser que exista outra base legal para a manutenção desses dados em sua base de dados (art. 18, VI, LGPD).

INFORMAÇÃO SOBRE COMPARTILHAMENTO: o titular de dados pode solicitar informações das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados (art.18, VII, LGPD).

INFORMAÇÃO SOBRE O NÃO CONSENTIMENTO: o titular de dados pode solicitar informações sobre a possibilidade e hipóteses de não fornecimento do consentimento, além de entender sobre as consequências da negativa (art. 18, VIII, LGPD).

INFORMAÇÃO SOBRE TRATAMENTO AUTOMATIZADO: o titular de dados pode pedir informações a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada. Tais informações, a serem oferecidas pelo controlador, deverão apresentar clareza e adequação com oque foi solicitado (art. 20, §1º, LGPD).

OPOSIÇÃO: o titular de dados pode se opor ao contexto do tratamento de dados e/ou às finalidades do tratamento, incluindo tratamento realizado com fundamento em uma das hipóteses de dispensa do consentimento (art. 18, §2º, LGPD).

PETIÇÃO: o titular de dados pode fazer qualquer requerimento com relação aos seus dados contra o controlador perante a Autoridade Nacional de Proteção de Dados - ANPD (art. 18, §1º, LGPD).

PORTABILIDADE: disponibilização dos dados do titular a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador (art. 18, V, LGPD).

REVISÃO: o titular de dados pode pedir revisão das decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (art. 20, caput, LGPD).

REVOGAÇÃO DO CONSENTIMENTO: manifestação expressa do titular, por procedimento gratuito e facilitado (art. 18, IX, LGPD), ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação (art. 8º, §5º, LGPD).

TITULARIDADE DOS DADOS PESSOAIS: a toda pessoa natural é assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade (art. 17, LGPD), de modo que o titular é, portanto, a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (art. 5º, V, LGPD).

4. DOS DADOS PESSOAIS: ASPECTOS INICIAIS

A relação entre as instituições/empresas e dados **pessoais** se estreitou na medida em que novas tecnologias e dispositivos conectados à internet foram inseridos no cotidiano das organizações. Assim, o **dado pessoal** se tornou um importante elemento capaz de personalizar uma relação e de desenvolver vínculos mais estreitos e precisos de consumo e de divulgação de marcas, produtos e serviços. Se antes os **dados pessoais** figuravam como meras formalidades para selar uma relação entre pessoas e organizações, agora eles representam verdadeiros ativos intangíveis cujo tratamento deve ser balizado por princípios éticos e diretrizes claras.

Tendo em vista as novidades trazidas pela Lei 13.709/2018, a **LGPD**, a presente seção foi organizada para responder a cinco perguntas introdutórias ao tema, quais sejam: (i) qual a diferença entre **dado pessoal** e **dado pessoal sensível**? (ii) O que é titular de dados? (iii) Quem são os agentes de tratamento, **controlador** e **operador**? (iv) O que é uma operação de tratamento de dados?

Sobre a primeira pergunta, como já abordado, em tempos de internet, telefones celulares e de comunicações cada vez mais personalizadas, as atividades das instituições, órgãos públicos e empresas dependem, em boa medida, da capacidade de obtenção e análise de dados pessoais. Mas, o que seriam **dados pessoais** na terminologia da lei? A resposta passa por um tipo de dado relacionado a uma pessoa natural, desde que identificada ou identificável no contexto. Portanto, um primeiro traço distintivo é o de que dados estritamente relativos a pessoas jurídicas, como um registro contábil, estariam fora do escopo da legislação, a não ser que englobem indicativos sobre pessoas naturais. E a variação "identificada ou identificável" possui especial relevância para a caracterização de um dado como pessoal.

Quanto ao **dado pessoal sensível,** este é uma espécie do gênero **dado pessoal**, cuja capacidade de revelar aspectos individuais de ordem mais sensível, como diz o nome, é relativamente maior, o que abre riscos para práticas discriminatórias. Nos termos da lei estão incluídos os dados relativos à origem étnica e religiosa, de filiação a organização política, religiosa ou filosófica, de aspectos ligados à saúde ou à vida sexual, bem como os que tratam da origem genética ou biométrica da pessoa natural identificada ou identificável.

A importância e o destaque conferido ao **dado sensível** na legislação se dão ao fato de que esse tipo de dado pode ser manipulado de forma tendenciosa e discriminatória, causando danos aos indivíduos ou a certos grupos de indivíduos. Portanto, a **LGPD** trouxe esse conceito e o conectou a algumas exigências

adicionais de modo a resguardar as garantias e direitos individuais e coletivos dos **titulares**, o que nos leva à próxima pergunta.

Como visto, sendo o **dado pessoal** qualquer elemento atinente a uma pessoa física identificada ou identificável, o **titular de dados,** para a nova legislação, é justamente a pessoa natural a quem esse dado se refere.

Sendo assim, conforme estipula a legislação, os **agentes de tratamento** podem ser classificados por duas categorias: **controlador** e **operador**. O controlador é quem gerencia os dados dos titulares, enquanto o operador é quem executa as operações de tratamento conforme as instruções do controlador. Ou seja, ele não possui autonomia para decidir qualquer assunto relativo aos **dados pessoais**.

A importância dessa distinção se deve à repercussões de responsabilização em casos de ilícitos civis, administrativos e penais, bem como de cumprimento de obrigações legais frente a outras autoridades governamentais. O **controlador**, nesse caso, terá um grau de responsabilidades possivelmente maior a depender do contexto.

Sendo assim, uma **operação de tratamento** de **dados pessoais** na **LGPD** é qualquer tipo de ação relacionada a um **dado pessoal**. Na definição da lei são utilizados em torno de 20 verbos diferentes e não exaustivos para ilustrar essa ação, como por exemplo: acessar, coletar, classificar, avaliar, reproduzir, transmitir, arquivar, eliminar ou avaliar, entre outros. Portanto, pode-se dizer que são todas as condutas relativas ao tratamento de dados de pessoas naturais que as possam indentificar ou estejam suscetíveis a identificação.

	**ATENÇÃO:** A assinatura digital acompanhada do nome da instituição à qual o profissional/servidor está vinculado junto com seu nome, especialmente se através e-mail, como por exemplo "____@santarosadelima.sc.gov.br.", é um indício de que o dado se relaciona a atividades não pessoais. Entretanto, destaca-se a necessidade de uma avaliação cuidadosa caso a caso.

Na prática, contudo, a distinção pode não ser tão fácil, já que na relação com microempresários, por exemplo, a figura do representante comercial e do titular se confundem por muitas das vezes. Do mesmo modo, embora não inserida no contexto de relacionamentos corporativos de fornecimento, o ideal é que os meios de contato (como e-mails, telefones e endereços) sejam estritamente corporativos ou institucionais. Caso contrário, serão caracterizados como dados pessoais, uma vez que há um claro intuito de abordagem individualizada e a pessoa natural está devidamente identificada ou identificável na relação.

Para facilitação da aplicação, nas próximas seções deste Manual, serão melhor tratabalhados estes temas afim de se obter indicativos acerca da natureza do dado, se pessoal ou corporativo. E, no passo a seguir, serão investigadas as bases legais que fundamentam a realização de **operações de tratamento**.

5. DA LGPD: PRINCIPAIS BASES LEGAIS

Assim, para a adequação da Prefeitura a LGPD, qualquer **operação de tratamento** envolvendo **dados pessoais** necessitará ser justificada através de uma **base legal**. Uma **base legal** equivale a uma das hipóteses autorizativas previstas na **LGPD** que permitem o tratamento de **dados pessoais**, as quais darão sustentação jurídica para que a **operaçãode tratamento** ocorra de forma legítima.

Nos artigos 7º e 11º da **LGPD** há a previsão das hipóteses que autorizam o uso de **dados pessoais** para os mais variados contextos.

Dessas hipóteses, cumpre dar destaque ao **consentimento** que exige a obtenção de uma autorização específica do **titular dos dados pessoais** ou de seu **responsável legal** para o **tratamento** dos dados a ele relativos. Assim, antes de utilizar-se do **consentimento,** deve analisar se não há o enquadramento em outra base legal que dispense o mesmo**,** e a depender do contexto de tratamento deverá ser utilizada, uma vez que no consentimento o titular além da ciência, profere sua autorização formal para utilização dos seus dados para uma finalidade especifica, minimizando os riscos para a instituição que opera o tratamento. Ainda, esse assunto será mais aprofundadamente debatido no tópico a seguir. Entretanto, desde já, é preciso destacar que a utilização desta base legal exige a manifestação livre, informada e inequívoca do titular de dados, para que seja realizado o tratamento.

A base tratada pelo termo **obrigação legal**, por sua vez, é utilizada para casos que haja determinação legal de lei federal, estadual, municipal ou demais normas, sendo a maior parte dos casos dos Órgãos e Instituicões públicas e privadas. Em outras palavras, o armazenamento de dados pode ser justificado quando há a obrigação de cumprir uma outra lei, como, por exemplo, utilizar como produção de prova em processo judicial ou para elaboração de documentos públicos.

Quanto à **administração pública**, por ter previsão legal, dispensa consentimento específico. O único detalhe é que, o Órgão responsável pela coleta tem a obrigação de informar de forma esclarecedora o dado que será compartilhado e com quem este será compartilhado.

Para a realização de **Estudos por órgão de pesquisa** é permitido o tratamento de dados pessoais, desde que não seja possível identificar o titular dos danos, a fim de garantir a privacidade daqueles que fizeram parte do estudo.

No tocante ao tratamento de dados correspondente a base legal de **execução de contrato** também dispensa a necessidade de consentimento. Ainda, importante estar atento ao fato de que ambas as partes que compõem o contrato estarão protegidas pela LGPD enquanto durar a vigência do contrato, bem como após, conforme previsão contratual e/ou obrigação legal.

Já em **processos judiciais, administrativos ou arbitrais**, ambas as partes podem produzir provas, inclusive uma contra a outra, a partir do material coletado para tratamento de dados, sem violar as normas constitucionais da ampla defesa e do contraditório.

Quando da utilização dos dados do titular ou de terceiros ocorrer em prol da **proteção da vida ou da incolumidade física**, não há a necessidade de consentimento do titular. Isso porque, há interesse público neste ponto.

O que também ocorre quando se tratar de casos referentes a **tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde**, ou seja, não há necessidade de consentimento do titular no tratamento de dados quando esta for a finalidade.

Por fim, quanto ao tema **proteção do crédito**, a LGPD autoriza a realização do tratamento de dados pessoais em situações de pesquisa de crédito, cobrança ou dívidas contraídas. A ideia desta base, é justamente não deixar brecha para que pessoas inadimplentes se utilizem da LGPD de má-fé, ou seja, para que deixem de cumprir com suas obrigações.

Entretanto, somente a avaliação circunstancial será capaz de demonstrar qual a melhor **base legal** a ser sustentada e como os princípios e direitos da **LGPD** podem ser garantidos aos **titulares**.

	**ATENÇÃO:** É através da **base legal** constante na **LGPD** que se justificará o tratamento de **dados pessoais**. Aplicando-se a Prefeitura Municipal, as **bases legais** normalmente serão a **execução de políticas públicas, a obrigação legal, legítimo interesse e o consentimento, podendo ainda utilizar as outras em hipóteses específicas**.

No próximo tópico, será delimitado conceitualmente as principais bases legais aplicadas a Prefeitura, explicando a sua importância.

5.1. Base legal: Execucão de Políticas Públicas

No artigo 7º, inciso III, da LGPD há a previsão de que a "administração pública" pode realizar "o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres". E, quanto aos dados sensíveis, o artigo 11, inciso II, b, refere-se ao "tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos".

Essa base legal é muito especifica, pois aplica-se somente à administração pública e não abrange as empresas e instituições particulares, de modo que, garante que o poder público poderá tratar e compartilhar dados pessoais, e para aplicação desta base legal torna-se necessária a adequada compreensão dos principais termos utilizados no inciso do artigo acima identificado.

Nesse sentido, passaremos a expor orientações sobre a interpretação dos seguintes conceitos: (a) Administração Pública; (b) Políticas Públicas.

(a) Administração pública: O conceito de "administração pública" deve ser delimitado a partir da definição de Poder Público, abrangendo tanto órgãos e entidades do Poder Executivo quanto dos Poderes Legislativo e Judiciário, inclusive das Cortes de Contas e do Ministério Público, desde que estejam atuando no exercício de funções administrativas.

De fato, embora a função administrativa seja típica do Poder Executivo, órgãos dos demais Poderes também a exercem em determinadas circunstâncias, como no presente caso a Prefeitura que ao lado de suas funções típicas, tais como administrativas, também exercem diversas outras atividades. É o que ocorre, por exemplo, quando são firmados convênios ou acordos de cooperação técnica com outros órgãos públicos ou entidades sem fins lucrativos visando ao atendimento de alguma finalidade pública. Como explica José dos Santos Carvalho Filho:

> A Administração Pública, sob o ângulo subjetivo, não deve ser confundida com qualquer dos Poderes estruturais do Estado, sobretudo o Poder Executivo, ao qual se atribui usualmente a função administrativa. Para a perfeita noção de sua extensão é necessário pôr em relevo a função administrativa em si, e não o Poder em que é ela exercida. Embora seja o Poder Executivo o administrador por excelência, nos Poderes Legislativo e Judiciário há numerosas tarefas que constituem atividade administrativa, como é o caso, por exemplo, das que se referem à organização interna dos seus serviços e dos seus servidores. Desse modo, todos os órgãos e agentes que, em qualquer desses Poderes, estejam exercendo função administrativa, serão integrantes da Administração Pública.[11]

Portanto, pode-se afirmar que a base legal referida nos artigos 7º, inciso III e 11, inciso II, alínea b, da LGPD, é aplicável a órgãos e entidades dos três poderes e entes federativos, inclusive das Cortes de Contas

e do Ministério Público, desde que estejam atuando no exercício de suas funções administrativas, com vistas à execução de políticas públicas.

(b) Políticas públicas: O conceito de políticas públicas não é definido na LGPD, não tendo sido editada regulamentação da ANPD sobre o tema até o presente momento, motivo pelo qual, devem ser consideradas as definições usuais do termo.

Nesse sentido, devem ser considerados, ao menos, dois aspectos. O primeiro é a existência de ato formal que institui a política pública, o que pode ocorrer mediante ato normativo (lei ou regulamento) ou por ajustes contratuais (contratos, convênios e instrumentos congêneres).

Ressalte-se que o artigo 11, inciso I, alínea b, da LGPD, não fez referência às políticas públicas instituídas em ajustes contratuais, desse modo, no caso de tratamento de dados sensíveis pelo Poder Público, a base legal é mais restrita, uma vez que limitada a políticas públicas previstas em "leis e regulamentos".

Assim, considerando os elementos expostos, recomenda-se que o conceito de política pública seja interpretado de forma ampla, de modo a abranger qualquer programa ou ação governamental, definido em instrumento formal, isto é, lei, regulamento ou ajuste contratual, conforme o caso, cujo conteúdo inclui, em regra, objetivos, metas, prazos e meios de execução.

Por fim, também na hipótese de execução de política pública deve ser observado o disposto no art. 23 da LGPD, em especial a exigência de que o tratamento seja realizado para o atendimento da finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

5.2. Base legal: A Obrigação Legal

Para o Poder Executivo, como no presente caso da Prefeitura, a base legal do **cumprimento de obrigação legal ou regulatória** pode-se dizer que é uma das mais importantes.

Como é sabido, a atividade Prefeitura consiste em serviço público e, portanto, está submetida ao princípio da legalidade. Portanto, via de regra, referida atividade justificará o tratamento de dados pessoais e dados pessoais sensíveis dos titulares de dados na necessidade de cumprimento de obrigação legal ou regulatória, ou para execução de politica pública, conforme já explanado no tópico acima.

Salienta-se ainda, que apesar do respaldo legal para o tratamento de dados pessoais na maioria dos casos, caso o dado coletado pela Prefeitura necessite de consentimento específico do titular, ou seja, não esteja prevista a obrigatoriedade da sua coleta em Lei ou outros Regulamentos, exige-se um termo de consentimento do titular de dados, devendo o mesmo ser devidamente documentado.

	**ATENÇÃO:** O Controlador deve orientar os Operadores sobre o tratamento de dados, deixando claro que, caso o tratamento de dados depender de consentimento, deverá exigir documento de manifestação de vontade, por escrito ou por outro meio capaz de registrá-la, e com a finalidade bem definida.

Outrossim, se mostra necessária ciência do titular dos dados pessoais sobre o tratamento de seus dados, coletados pela Prefeitura, mesmo nos casos em que o consentimento é dispensado, sempre primando pela evidência do princípio da transparência.

Tais atos resultarão em boas práticas adotadas pela Prefeitura, diante dos efeitos da Lei Geral de Proteção de Dados, de modo que esta deverá buscar sempre representá-las também perante os titulares de dados, além de aplicá-las de maneira efetiva internamente.

5.3. Base legal: Legítimo Interesse

A base legal do legítimo interesse autoriza o tratamento de dados pessoais de natureza não sensível quando necessário ao atendimento de 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" (art. 7º, inciso IX). Trata-se, portanto, de base legal não aplicável ao tratamento de dados pessoais sensíveis.

Por ser uma base legal mais flexível, sua adoção deve ser precedida de uma avaliação em que seja demonstrada a proporcionalidade entre, de um lado, os interesses do controlador ou de terceiro para a utilização do dado pessoal e, de outro, os direitos e as legítimas expectativas do titular. Além disso, deve-se considerar que, conforme o art. 18, § 2º, o titular tem o direito de se opor ao tratamento realizado com base no legítimo interesse, em caso de descumprimento dos requisitos previstos na LGPD.

De forma similar ao que ocorre com o consentimento, a aplicação do legítimo interesse é limitada no âmbito do setor público. Em particular, a sua utilização não é apropriada quando o tratamento de dados pessoais é realizado de forma compulsória ou quando for necessário para o cumprimento de obrigações e atribuições legais do Poder Público.

Nessas situações, não há como se realizar, propriamente, uma ponderação entre as expectativas dos titulares e os supostos interesses estatais, visto que estes, por definição legal ou regulamentar, conforme o caso, tendem a estabelecer restrições aos direitos individuais nele envolvidos. Isto é, a própria legislação estabelece essa ponderação, ao fixar as condições a serem observadas para a realização do tratamento de dados pessoais. **Por isso, é recomendável que, em geral, órgãos e entidades públicos evitem recorrer ao legítimo interesse, preferindo outras bases legais, a exemplo de execução de políticas públicas e cumprimento de obrigação legal, para fundamentar os tratamentos de dados pessoais que realizam nessas condições.**

Não obstante, o legítimo interesse poderá eventualmente ser admitido como base legal para o tratamento de dados pessoais pelo Poder Público. Para tanto, a utilização dos dados não deve ser compulsória ou, ainda, a atuação estatal não deve se basear no exercício de prerrogativas estatais típicas, que decorrem do cumprimento de obrigações e atribuições legais. Nesse contexto, torna-se efetivamente possível realizar uma ponderação entre, de um lado, os interesses legítimos do controlador ou de terceiro e, de outro, as expectativas legítimas e os direitos dos titulares.

	**SEGURANÇA DA INFORMAÇÃO:** Entidade pública realiza tratamento de dados pessoais de seus servidores com a finalidade de garantir a segurança dos sistemas de informação utilizados, como, por exemplo, para viabilizar a autenticação de usuários e prevenir que softwares maliciosos possam criar vulnerabilidades na rede interna. Considerando que o tratamento não está associado ao exercício de prerrogativas estatais típicas, é possível recorrer à base legal do legítimo interesse. Nesse caso, devem ser observados os requisitos previstos na LGPD, em particular a necessidade de ponderação entre os interesses da entidade pública e os direitos e as expectativas legítimas dos titulares. É necessário, ainda, que sejam adotadas medidas para garantir a transparência do tratamento de dados pessoais baseado no legítimo interesse

5.4. Base legal: O Livre Consentimento

Previsto na **LGPD** como manifestação ***livre, informada e inequívoca*** do **titular** ou de seu **responsável** legal para concordância à realização de operações com seus **dados pessoais**, o **consentimento** é uma hipótese de importância para o desenvolvimento de certas atividades dentro de uma Instituição. Isso porque é a concordância do **titular** para o **tratamento** de seus dados que garante que o indivíduo concordou positivamente com as **operações** que serão realizadas com suas informações.

Por isso, é necessário assegurar que não exista vício de vontade, para que quaisquer **titulares** ou **responsáveis** expressem a sua anuência de modo a ceder seus **dados pessoais** para quaisquer fins, de forma livre. E não é a toa que a a LGPD exige que a manifestação de vontade ocorra através de um vocabulário simples e objetivo, e que contenha informações essenciais sobre a operação de tratamento, como seus modos, os agentes envolvidos e os eventuais riscos, para que não haja omissão seja do **titular** ou do **responsável**.

ATENÇÃO:

Além de **livre**, o consetimento também deve ser **informado,** ou seja, todas as informações básicas precisam ser fornecidas de forma clara e objetiva ao titular ou ao seu responsável legal, para que ele possa expressar sua concordância de forma **inequívoca**.

Aplicando-se ao cotidiano, o **consentimento** de dados pelo **titular** a alguma situação jamais poderá estar condicionado a outra situação. O que quer dizer que, ao ofertar um serviço devem ser ofertadas opções sem imposição de outra, como por exemplo: não posso condicionar a entrega de um documento público ao fornecimento de telefone pelo titular.

Cumpre destacar ainda que, a mera declaração vazia de concordância passiva a um link dos Termos de Uso de site não demonstra o interesse específico do **titular**. Ainda, com relação ao link para Termos de Uso ou Políticas de Privacidade, embora aconselhável que ele seja disponibilizado para consulta, não é possível atrelar o **consentimento** à mera menção desse documento. Logo, todas as cláusulas importantes devem estar destacadas já no termo, sobretudo as que tratem de **finalidade**, **compartilhamento** ou as que impliquem em **risco** ao **titular**. E para que o **consentimento** seja inequívoco, ele deve ser destacado para cada finalidade e, de preferência, com o uso de uma *checkbox* indicando a concordância específica para cada **tratamento**.

Dada a inexistência prévia de uma cultura de proteção de dados pessoais, é possível que receios acerca dos impactos negativos da **LGPD** e da necessidade de **consentimento** surjam. Por isso, antes de mais nada, é necessário entender que o **consentimento** e a própria **LGPD**, se devidamente respeitados e seguidos, terão verdadeiro efeito oposto: onde a Prefeitura apenas tratará os dados estritamente necessários para a finalidade pretendida, de modo que, não sendo o caso, poderá descartá-los, sempre de forma documentada.

No mais, o **consentimento** só pode ser considerado livre, informado e inequívoco se levada em conta a **finalidade** da **operação de tratamento** de dados pessoais. Por **finalidade**, tem-se o princípio da informação ligado à pessoa natural acerca das **operações** que serão realizadas para tratar os seus dados. Ou seja, que o agente responsável pelo tratamento de **dados pessoais** esclareça quais os propósitos para a coleta, armazenamento e uso dos dados dotitular. Dessa maneira, cada tipo de **operação de tratamento** de **dados pessoais** dependerá, do mesmo modo, de uma manifestação clara e específica de **consentimento**

por parte do **titular** envolvido ou de seu **responsável legal**.

ATENÇÃO: CONSENTIMENTO E FINALIDADE ANDAM JUNTOS

É necessário avaliar sempre qual o propósito do dado coletado: identifique a **finalidade** para qual este dado será usado. Em seguida, caso a **base legal** utilizada seja a do **consentimento**, avalie se ele está em sintonia com a **finalidade** estipulada. O **consentimento** é ***granular:*** **finalidades** distintas implicam em **consentimentos** distintos.

Obter o **consentimento** válido do titular é, portanto, uma tarefa que demandará criatividade. Afinal, em tempos tecnológicos e conectados como os de hoje, que exige rapidez e informação objetiva, a disposição de textos longos, com letras miúdas e sem proximidade com o público-alvo fica descontextualizada.

A **LGPD** exige que a obtenção do **consentimento** seja realizada por quaisquer meios pelos quais se possa provar que ele efetivamente existiu. Embora o **consentimento** por escrito seja o mais utilizado, a **lei** deixa abertura para outras formas de sua coleta, como o uso de vídeo, de imagens ou mesmo o auxílio da chamada "*checkbox*" interativa, pela qual o **titular** ou o seu **responsável legal** escolhe quaisas **finalidades** de **tratamento** estão efetivamente no seu gosto e quais ele deseja se desvincular.

ATENÇÃO:

Para a obtenção de estratégias criativas e transparentes de consentimento do titular de dados, não é necessário um texto escrito, longo e letras miúdas. Isso porque a LGPD permite a utilização de outras possibilidades, desde que respeitem e registrem o desejo do usuário. O uso de áudio, vídeo, de *checkbox* curtos e objetivos ou mesmo de guias de navegação interativos são bons exemplos a depender das circunstâncias concretas variadas.

Assim, a devida observância do requisito legal da descrição da **finalidade de tratamento**, aliada ao **consentimento** livre, inequívoco e informado trazem muito mais do que meras exigências.

Entretanto, cumpre destacar que as obrigações legais para tratar os dados pessoais não se encerram com a obtenção do **consentimento** válido do titular de dados nos termos da **LGPD**, ou seja, o **consentimento** de forma livre, informada e inequívoca. Isso porque, a LGPD exige outros requisitos para que sejam garantidos os direitos do titular durante o transcurso das **operações de tratamento de dados pessoais**. O consentimento é, portanto, requisito inicial ao se tratar de relacionamento com **titulares de dados pessoais**.

A LGPD elenca quais são os direitos do titular de dados pessoais. São alguns direitos do titular que expressam o desacordo com o tratamento de dados: (i) revogar o consentimento; (ii) de anonimizar ou bloquear informações desnecessariamente coletadas; (iii) de requisitar que os dados sejam eliminados em certas circunstâncias; e (iv) e de se opor a um **tratamento** irregular, ainda que realizado por outra **base legal** que não a do **consentimento**. Além disso, são direitos em que o titular se expressa de forma positiva em relação à entidade que executa o **tratamento** ou à autoridades reguladora: (v) peticionar à agência reguladora, a Agência Nacional de Proteção de Dados Pessoais (ANPD), contra os agentes de tratamento; (vi) obter a confirmação de que os dados de um certo indivíduo estão de fato sendo tratados; (vii) acessar estes dados na íntegra; (viii) ser informado acerca de eventual compartilhamento com terceiros; (ix) ter disponibilizada a possibilidade de negar o consentimento em certas circunstâncias e saber quais as consequências desse ato; (x) portar os dados pessoais para outras entidades públicas ou privadas e, por fim, (xi) atualizá-los ou corrigi-los. Ainda, se o tratamento de dados for realizado com o uso de tecnologias automatizadas (sem a supervisão humana imediata), o **titular** terá direito a (xii) requisitar explicações

acerca dos critérios utilizados; e (xiii) requerer a revisão da decisão.

ATENÇÃO:

É comum que os direitos do **titular** estejam entre constante comunicação entre os setores e unidades. Portanto, não raro, poderão ser exercidos em concomitância.
P.S.: um mesmo indivíduo poderá requisitar a Prefeitura e suas Secretarias a revogação do **consentimento** fornecido, como telefone ou *Whatsapp*, solicitar o acesso aos seus dados pessoais, e ainda, pleitear uma cópia integral dos seus dados.

Por isso, a construção da **matriz de risco** é super importante. Uma vez que se trata de uma ferramenta de análise e gerenciamento dos **riscos** inerentes a uma atividade. Ela reúne uma listagem de todos os **riscos** projetados para o exercício dos procedimentos, através da identificação do fluxo de dados dentro da Prefeitura, permitindo estabelecer as áreas e processos prioritários para adequação.

RESUMO: CONSENTIMENTO

O **consentimento** deve ser **livre** (sem vício de vontade), **informado** (com as condições, parceiros e objetivos bem delimitados ao **titular**) e **inequívoco** (ser emitido a partir de uma manifestação positiva e, assim, não ser presumido), bem como ser granular, correspondendo a **finalidades** bem delimitadas e individuais;
A obtenção do **consentimento** não finaliza o processo de atenção para com o **titular** de dados, mas é só o início. Os direitos do **titular** também devem ser assegurados e a ***matriz de risco***, é uma ferramenta que pode ser um importante aliado no gerenciamento.

Em que pese a matéria parecer ser complexa, é importante destacar que a **LGPD** não veio para engessar ou inviabilizar as operações pautadas em **dados pessoais**. Afinal, o tratamento de dados faz parte de um ecossistema digital em constantes transformações. Em razão disso, faz necessário assegurar que o **titular** esteja incluso em uma relação de confiança com a Prefeitura e não limitada somente ao oferecimento do **consentimento**, sendo a ele facultado o exercício de seus direitos sempre que julgar conveniente.

Além disso, é de fundamental importância destacar que, em que pese o tema consentimento ter sido amplamente abordado neste manual, **a atividade da Prefeitura** consiste em serviço público. E, portanto, está submetida ao **princípio da legalidade**. Logo, via de regra, o tratamento de dados do usuário estará justificado pela necessidade de execução de políticas públicas e **cumprimento de obrigação legal ou regulatória, conforme discriminados nos itens acima**.

Porém, em respeito a **LGPD**, se o responsável verificar algum caso que dependa do consentimento do titular, exige-se um registro documental.

Outrossim, quando dispensado o consentimento, mostra-se igualmente necessário o registro de ciência do titular sobre as especificidades do tratamento de dados inerentes ao serviço, o que demonstra uma boa prática da Prefeitura perante os cidadãos.

6. DA DIVULGAÇÃO DE DADOS PESSOAIS PELO SETOR PÚBLICO

Quanto tratamos da adequação de Órgãos e Instituições do Poder Público às disposições da LGPD surgem muitas dúvidas a respeito dos parâmetros a serem observados para a disponibilização pública de informações pessoais. De forma geral, a análise dessas situações envolve uma ponderação entre os direitos à privacidade e o direito à proteção de dados pessoais e o direito de todos os indivíduos à informação sobre as atividades do Poder Público. Mas, destaca-se que na grande maioria dos casos, para atender ao princípio da publicidade, o Munícipio é obrigado a divulgar dados pessoais.

Nesse sentido, observamos que, enquanto os direitos de privacidade e proteção de dados pessoais demandam uma posição de cautela e de análise de riscos a respeito da divulgação de informações pessoais, o direito a informação espelha a determinação legal de que a publicidade é a regra, admitindo-se o sigilo apenas em hipóteses excepcionais, nos termos da Lei de Acesso à Informação (Lei nº 12.527/11).

Não obstante, o tratamento de dados pessoais pelo Poder Público, incluindo a divulgação pública de dados pessoais, deve ser realizado em conformidade com as disposições da LGPD, observando ainda todas as normas que garantem a proteção integral dos dados pessoais, a autodeterminação informativa e o respeito à privacidade dos titulares durante todo o ciclo do tratamento, ou seja, desde a coleta até o fim da atividade realizada com os dados pessoais.

Nesse contexto, o cumprimento da LGPD demanda de entidades e órgãos públicos uma análise mais ampla, que não se limita à atribuição de sigilo ou de publicidade a determinados dados pessoais. Em termos práticos, considerando o reforço protetivo trazido pela LGPD ao titular de dados, é necessário realizar uma avaliação sobre os riscos e os impactos para os titulares dos dados pessoais bem como sobre as medidas mais adequadas para mitigar possíveis danos decorrentes do tratamento de dados pessoais.

Dados pessoais sensíveis (art. 5º, II, LGPD), por exemplo, estão submetidos a uma proteção jurídica especial, o que implica adotar maior cautela quando for necessário realizar o tratamento de dados pessoais dessa natureza. Nessa linha, pode ser mencionada a vedação de serem revelados dados pessoais sensíveis por ocasião da divulgação de resultados de estudos em saúde pública (art. 13, § 1º, LGPD).

Os princípios da finalidade, adequação e necessidade também impõem limites ao tratamento de dados pessoais. Em atenção a esses princípios, entidades e órgãos públicos devem verificar se as informações coletadas são, efetivamente, adequadas e necessárias para o atendimento das finalidades para as quais serão utilizadas, não podendo haver, desses dados, uso incompatível com as finalidades que justificaram sua coleta ou a sua obtenção. Muitas vezes, a coleta indiscriminada de dados pessoais é o ponto principal a ser considerado, de modo que, ao invés de eventual e posterior atribuição de sigilo, a proteção será mais efetiva com a própria dispensa da coleta ou com a eliminação da informação.

Em outras situações, nas quais a coleta seja necessária e não seja cabível a eliminação dos dados, podem ser adotadas medidas de mitigação de risco, que fortalecem e tornam mais segura a possibilidade de divulgação dos dados pessoais, haja vista a diminuição de seu potencial lesivo aos direitos dos titulares.

Uma possível salvaguarda a ser adotada é a limitação da divulgação àqueles dados efetivamente necessários para se alcançar os propósitos legítimos e específicos em causa, observados o contexto do tratamento e as expectativas legítimas dos titulares. A restrição de acesso a essas informações mitiga os riscos aos titulares de dados pessoais, sem, no entanto, comprometer a finalidade de garantia de transparência e de controle social sobre as despesas públicas.

Em atenção aos princípios da segurança, da prevenção e da responsabilização e prestação de contas, órgãos e entidades públicas devem adotar medidas técnicas e administrativas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, observado o disposto nos arts. 46 a 49 da LGPD. No mesmo sentido, conforme o art. 50, § 1º, constitui boa prática realizar o tratamento de dados pessoais levando em consideração a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes do tratamento de dados. Entre outras medidas, sempre que possível, os dados pessoais devem ser pseudonimizados ou anonimizados.

Por isso, mesmo nos casos de divulgação pública de dados pessoais, é recomendável que órgãos e entidades públicas avaliem a possibilidade de adoção de medidas técnicas e administrativas capazes de mitigar riscos e prevenir a ocorrência de danos aos titulares. Essas medidas adicionais se justificam, pois, em conformidade com os princípios acima referidos, a LGPD estabelece ampla proteção aos dados pessoais, inclusive para aqueles cujo acesso é público, seja por força de lei ou por manifestação de vontade do titular, conforme se extrai de seu art. 7º, §§ 3º, 4º e 7º.

ATENÇÃO:

Conforme decidido pelo STF, ***"a remuneração dos agentes públicos constitui informação de interesse coletivo ou geral",*** aplicando-se à hipótese o princípio constitucional da publicidade administrativa, que "propicia o controle da atividade estatal até mesmo pelos cidadãos." A Corte entendeu, ainda, que os riscos pessoais decorrentes da divulgação são atenuados com ***"a proibição de se revelar o endereço residencial, o CPF e a CI de cada servidor".*** Por fim, em atenção ao contexto e às expectativas dos titulares envolvidos, a decisão menciona que *"os dados objeto de divulgação em causa dizem respeito a agentes públicos mesmos; ou, na linguagem da própria Constituição, agentes estatais agindo nessa qualidade".* Suspensão de Liminar no 623/DF, Ministro Ayres Britto, 10 de julho de 2012.

Finalmente, a própria transparência a respeito dos tratamentos de dados realizados e a efetiva garantia de direitos aos titulares devem ser considerados como fatores relevantes para diminuir o uso indevido de dados pessoais. Afinal, a possibilidade de o interessado apresentar um requerimento ao órgão público responsável, relatando eventual violação a seus direitos, pode viabilizar a correção de erros, bem como a implementação de medidas como a anonimização, o bloqueio ou a eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD (art. 18, IV).

7. DO AMBIENTE FÍSICO DE TRABALHO

Para proteger os dados pessoais no ambiente de trabalho, deve-se:

- **Nunca divulguar informações pessoais no ambiente de trabalho, seja de cidadãos, servidores ou colaboradores, sem que tenha embasamento legal ou consentimento para isso. Além disso, confira sempre se a solicitação é do próprio titular, através de comprovação de documento com foto.**

- **Não deixar documentos com dados pessoais expostos ou ao alcance de outras pessoas. Adotar o conceito de mesa limpa.**

- **Não coletar currículos confeccionados pelo canditado, sejam eles físicos ou digitais, tendo em vista que não há controle sobre a qualidade de informações inseridas pelo candidato.**

Sugere-se a adoção de modelo padrão de currículo, no modelo de *formulário de candidatura a emprego*.

- **Evitar comentários acerca de dados pessoais nos corredores e lugares com circulação de pessoas.**

- **Todos os documentos físicos coletados devem ser armazenados nas respectivas pastas.**

- **No tratamento de dados dos cidadãos que realizam solicitações, fazer sempre o cadastro no sistema, inserindo somente os dados extremamente necessários e unicamente em arquivo digital.**

- **Caso haja a necessidade de consulta de documentos arquivados de forma física, sempre solicitar que os servidores com acesso autorizado ao local o façam.**

- **Descartar corretamente documentos com dados pessoais, preferencialmente picotando ou incinerando os documentos e deletando arquivos digitais de forma que não possibilite a recuperação das informações.**

- **Criar o hábito de ler documentos na tela, evitando impressões.**

- **Limitar o acesso de pessoas não autorizadas ao interior do estabelecimento, mantendo, ainda, os dados pessoais físicos em arquivos e/ou gavetas com chaves ou ainda em sala de arquivos cujo acesso será restrito.**

8. DO AMBIENTE VIRTUAL DE TRABALHO

Para proteger os dados pessoais no ambiente de trabalho, deve-se:

- **Utilizar-se de Redes Privadas Virtuais (VPNs).**

A VPN é uma rede que criptografa e transmite informações de um ponto a outro na Internet. Trata-se de uma solução que permite aos usuários enviar e receber dados mantendo a segurança e privacidade.

- **Não divulgar senhas da rede Wi-Fi com terceiros, salvo se houver rede distinta para uso de visitantes, diversa da rede interna da Prefeitura.**

Por exemplo: uma rede de Wi-Fi para servidores e outra para visitantes e terceiros, ou ainda, não divulgue a senha de sua internet com usuários alheios ao quadro de servidores.

- **Fazer Backups periódicos dos dados coletados.**

- **Contratar e checar eficácia de forma periódica de ferramentas de prevenção contra ameaças, como um antivírus de boa qualidade.**

O antivírus atua como um monitor de atividades anormais, agindo contra os ataques de invasores e as impedindo de enviar vírus aos servidores.

- **Se possível, fazer a utilização de sistemas próprios para o desenvolvimento das atividades e restrinja o acesso do sistema de seus servidores ou parceiros a somente o departamento que estão atuando.**

Exemplo: Somente o Setor Financeiro deverá ter acesso às contas bancárias.

- **Manter sempre as atualizações em dia de seus programas, sistemas e softwares.**

- **Ao sair da sua estação de trabalho, lembre-se sempre de bloquear a tela de seu computador.**

Normalmente, você pode fazer isso através do comando CTRL+ALT+DEL ou também clicando no botão INICIAR e selecionar a opção “Trocar de usuário”.

- **Restrinja documentos que versem sobre dados pessoais e que não estejam protegidos pelo sistema através de senha.**

Por exemplo: em documentos de Word, você pode fazer isso através do comando ARQUIVO – INFORMAÇÕES – PROTEGER DOCUMENTO – CRIPTOGRAFAR COM SENHA e digite a senha escolhida para abrir o arquivo. Não esqueça de anotar a senha em um local seguro para ter acesso ao documento ou caso precise compartilhar com alguém do mesmo setor. No caso de documentos físicos, o acesso também deve ser restringido, através do armazenamento de documentos em gavetas ou arquivos com chave e restrição de acesso aos locais de armazenamento de dados.

- **Criar e-mails corporativos para cada servidor, bem como suas assinaturas digitais.**

A assinatura digital acompanhada do nome da instituição à qual o profissional está vinculado junto com seu nome, especialmente se através e-mail “corporativo”, como por exemplo “____@santarosadelima.sc.gov.br.”, é um indício de que o dado se relaciona a atividades não pessoais.

- **Ao escrever um e-mail, ou mensagem certificare-se de que as informações que deseja enviar estão corretas, bem como o seu destinatário.**

- **Não clicar em links suspeitos ou abrir anexos de remetentes desconhecidos. Em caso de dúvidas, sempre entre em contato com seu Encarregado de Dados – DPO.**

- **Não divulgar informações pessoais de servidores e/ou qualquer outro cidadão, sem que tenha embasamento legal ou consentimento para isso.**

- **Preferencialmente, mantenha sempre seus microfones e webcans tapados.**

- **Criar logins individuais para cada servidor, com senhas individualizadas.**

Pois caso haja algum incidente relacionado ao vazamento de dados pessoais ou utilização indevida, é possível identificar o autor ou o local do vazamento ou do incidente, caso seja decorrente de erro humano ou virtual.

- **Não fazer o uso compartilhado de logins e senhas.**

Pois caso haja algum incidente relacionado ao vazamento de dados pessoais ou utilização indevida, ficará registrado o login do colaborador que compartilhou sua senha, podendo ser responsabilizado pelo ato.
Por exemplo: Ceritificado digital com assinatura do servidor A, que fornece sua senha para o servidor B.

9. DAS SENHAS DE ACESSO

A criação de senhas fortes para as contas de e-mail e acessos aos sistemas institucionais é um meio de reforçar a segurança dos dados e informações. Assim, algumas medidas precisam ser adotadas:

- **Criação de senhas fortes;**

- **Evitar o uso de senhas fáceis, como datas de nascimento, nomes próprios, endereços ou outras informações pessoais que possam ser facilmente identificadas;**

- **Utilização de caracteres especiais;**

- **Misturar letras, números e outros caracteres especiais;**

- **Evite repetir símbolos;**

- **Crie senhas diferentes para cada um dos seus acessos.**

Exemplo: E-mail e sistema;

- **Troca periódica das senhas;**

- **As senhas devem ser alteradas, no mínimo, a cada 6 meses;**

- **Evitar a utilização da senha anterior.**

Abaixo, traremos algumas dicas para a criação de senhas fortes:

- **Crie uma regra para substituição dos caracteres. Por exemplo: substituir a letra O por @, a letra E por 3, a letra A por 4.**

- **Utilize sinais de pontuação, como: aspas, parênteses, ponto de interrogação, etc.**

- **Utilize frases que você possa memorizar.**

- **Não compartilhe seus logins e senhas de acesso.**

10. DAS ATIVIDADES E ROTINAS

No desenvolver das atividades e rotinas da Prefeitura é necessário observar os seguintes pontos:

- **Certifique-se de listar quais os dados efetivamente serão utilizados;**

Evite termos genéricos como "o titular autoriza o uso de seus dados", no caso de necessidade da coleta de consentimento. Prefira sempre especificá-los e, preferencialmente, dê a opção de escolha ao titular acerca de quais dados deseja compartilhar para cada finalidade, quando a base legal não for a da obrigação legal. O titular pode, por exemplo, desejar ser contatado por e-mail pessoal, mas não desejar ser contatado por telefone. Assim, o ideal é, se possível ao caso, que ele tenha a opção de escolher quais dados autoriza o uso, como e-mails, telefones e, até mesmo, redes sociais ou aplicativos de mensagem.

- **Disponibilize em seu site um link, ou, caso não seja possível, um exemplar para que o titular consulte a política de privacidade e proteção de dados pessoais da Prefeitura;**

Em respeito ao princípio da transparência, é importante dar vistas ao titular quanto a sua política.

- **Disponibilize, também, em seu site ou através de outro meio, uma opção concreta ou uma instrução para que o titular se descadastre ou revogue seu consentimento;**

Afinal, ainda que o usuário tenha consentido de forma livre, informada e inequívoca, ele tem odireito de revogar o seu consentimento. Esteja pronto para gerenciar as opções de saída de acordo com o que o Titular indicar.

- **Se for o caso, disponibilize uma caixa de seleção na qual o usuário declare ter mais de 16 (dezesseis) anos completos ou, a depender do caso, 18 (dezoito) anos completos;**

Nos casos que envolvam menores de 18 (dezoito) anos, também será necessário obter o consentimento válido dos pais ou responsáveis.

- **Se for o caso, disponibilize as informações sobre os entes públicos ou privados com quem**

os dados serão compartilhados para o seu tratamento;

Caso os dados do titular venham a ser compartilhados com uma outra instituição pública ou privada, deixe essa informação clara desde o momento inicial sempre que possível.

11. DAS CONSIDERAÇÕES FINAIS

O presente Manual retratou situações de uso de **dados pessoais** na Prefeitura Municipal, com base na LGPD. De modo geral, viu-se que o tratamento de dados pessoais – seja por qualquer modo – precisa seguir critérios transparentes, registrados e fundamentados.

Por isso, é necessário iniciar um processo de mudança de cultura em relação ao tratamento de **dados pessoais** dentro da Prefeitura, uma vez que a manipulação incorreta de dados pessoais podem gerar danos individuais e coletivos.

Entretanto, cumpre destacar que a Lei Geral de Proteção de Dados Pessoais - **LGPD**, não veio para bloquear ou inviabilizar as atividades dentro da Prefeitura. O que a **lei** estabelece é, em verdade, que a forma de utilização dos dados e o relacionamento com as pessoas, **titulares** desses dados, precisam passar por um processo de filtragem e controle de qualidade maiores do que os padrões atualmente existentes.

As Prefeituras que compreenderem esse giro e o utilizarem em favor de seus modelos organizacionais conseguirão atingir verdadeira vantagem, além disso, criar relacionamentos qualitativamente mais significativos com os seus servidores, colaboradores e cidadãos.

Em vista disso, algumas conclusões podem ser retiradas deste manual. Primeiramente, que são através das **bases legais** previstas **LGPD** que se justificarão o tratamento de todos os **dados pessoais**. Sendo que, aplicando-se a Prefeitura, as **bases legais** normalmente serão **a execução de políticas publicas, cumprimento de obrigação legal, execução de contrato, legítimo interesse e o consentimento.**

Quanto a **execução de políticas públicas**, verifica-se que foi destacado neste manual que será a principal base legal utilizada para justificar as atividades de tratamento de dados desenvolvidas pela Prefeitura, de modo que a mesma pode realizar o tratamento e compartilhar os dados pessoais necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, ressaltando que, deve ser observada a exigência de que o tratamento seja realizado para o atendimento da finalidade pública.

A respeito do **cumprimento de obrigação legal**, demonstrou-se que essa **base legal** é uma segunda base que será mais utilizada pela Prefeitura no momento do tratamento de dados pessoais, uma vez que a atividade consiste em serviço público e, portanto, está submetida ao princípio da legalidade. Mesmo assim, há a necessidade de dar ciência ao titular do dado sobre de que forma seus dados serão tratados, se vai ocorrer o compartilhamento ou não de tais dados, bem como a finalidade da coleta, mesmo nos casos em que o concentimento é dispensado.

Sobre o **consentimento**, foi destacado ao longo de todo o Manual que ele precisa ser livre, informado, inequívoco, e que esteja sempre articulado à **finalidades** ou propósitos específicos. Desse modo, é importante que profissionais de comunicação, de direito e de tecnologia empenhem esforços no sentido de criar estratégias legalmente adaptadas e criativas para obtê-lo de forma específica.

No relacionamento com cidadãos por **e-mails e telefone**, restou claro a aconcelhabilidade de que devem ser registradas sob a base legal da **execução de politica pública e/ou cumprimento de obrigação legal**, como é o caso da coleta de outros dados, é necessário verificar se os dados coletado estão sendo utilizados para as finalidades informadas ao titular no momento da coleta do dado. Esse processo, se bem arquitetado, levará a uma melhora qualitativa do contato com os usuários.

Por fim, cumpre destacar que é de extrema importância que, além de tudo o que fora discorrido, que a Prefeitura elabore sua própria **Política de Privacidade e de Proteção de Dados Pessoais,** a qual trará em seu conteúdo informações sobre como o dado é tratado, regulando suas atividades internas no tocante a coleta, processamento e/ou armazenamento de dados relativos às pessoas naturais, o que, obviamente, devem estar ligados às finalidades institucionais, estabelecendo diretrizes gerais para a adequação das atividades às normais vigentes. Igual importância possui a **Política de Resposta a Incidentes,** que tem como objetivo preparar a Prefeitura para lidar com a gestão de incidentes de segurança e estabelecer o fluxo interno da comunicação, bem com definir as diretrizes acerca de como proceder em eventuais casos de vazamento de dados.