PREFEITURA DE PIRACEMA

PROGRAMA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Manual de governança pública e boas práticas em privacidade e proteção de informações pessoais e sensíveis (LGPD).

SUMÁRIO

INTRODUÇÃO

A governança no tratamento de dados pessoais pelo Município de Piracema, Minas Gerais, segue as diretrizes estabelecidas no Decreto Municipal nº 41/2022 e no disposto na Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais ("LGPD"), e suas alterações, necessitando ser compreendida à luz do estabelecido pela legislação e dos requisitos de segurança da informação.

Este manual tem como objetivo fornecer orientações de boas práticas e governança aos órgãos e entidades da Administração Pública Municipal para as operações de tratamento de dados pessoais, conforme previsto no art. 50, da LGPD.

A adequação dos órgãos e entidades à LGPD envolve considerar a privacidade dos dados pessoais do cidadão desde a fase de concepção do serviço público até sua utilização para prestação dos serviços públicos (*privacidade por concepção e por padrão*), uma verdadeira transformação cultural alicerçada nos níveis estratégico e operacional da Administração Municipal, promovendo ações de conscientização de todo corpo funcional no sentido de incorporar o respeito à privacidade dos dados pessoais nas atividades institucionais cotidianas.

Convém ressaltar, ainda, que grande parte dos dados e informações pessoais e sensíveis estão contidos em documentos arquivísticos, em diversos suportes, tais como os documentos arquivísticos digitais, que se apresentam em uma diversidade crescente de formatos: texto não estruturado (.doc, .pdf, .odf, .txt, entre outros formatos), planilhas, páginas web, fotografias, imagem em movimento, registro sonoro, bases de dados, multimidia e mídias sociais.

Frequentemente, o registro das atividades de um órgão ou entidade é realizado por meio de um sistema informatizado, mantido em uma base de dados, que se constitui, ou contém documentos arquivísticos digitais e físicos.

Vale lembrar a Lei nº 12.527, de 18 de novembro de 2011, Lei de Acesso à Informação ("LAI"), apresenta regras específicas para o acesso a documentos que, embora apresentem dados pessoais, possuem valor permanente e foram recolhidos a instituições arquivísticas públicas. A LGPD e a LAI também devem, portanto, ser interpretadas sistematicamente.

Este documento, que será atualizado, aperfeiçoado, ampliado permanentemente, tem por objeto o contato inicial e a familiarização com o novo universo da proteção e tratamento de dados pessoais em âmbito municipal.

1. DIREITOS FUNDAMENTAIS DO TITULAR DO DADOS

1.1 BASE LEGAL E CONCEITUAL PARA TRATAMENTO DOS DADOS PESSOAIS PELA PREFEITURA DE PIRACEMA

A Lei Geral de Proteção de Dados Pessoais foi editada com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo, dispondo sobre o tratamento de dados pessoais, em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado e engloba um amplo conjunto de operações efetuadas em meios manuais ou digitais.

Nesse sentido, inclusive, o Congresso Nacional incluiu no texto da Constituição da República o inciso LXXIX, registrando ser assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais (Emenda Constitucional nº 115, de 2022).

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 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”).

1.1.1 AGENTES DE TRATAMENTO

No âmbito da LGPD, o tratamento dos dados pessoais será realizado pelos agentes de tratamento, o Controlador e o Operador:

- **Controlador** é definido pela Lei como a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, tais como as finalidades e os meios do tratamento (art. 5º, VI). No âmbito da Administração Municipal, o *Controlador será a pessoa jurídica do órgão ou entidade pública sujeita à Lei, representada pela autoridade do Prefeito Municipal responsável pela tomada de decisões acerca do tratamento de tais dados*.

- **Operador** é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (art. 5º, VII), aí incluídos agentes públicos no sentido amplo que exerçam tal função, bem como pessoas jurídicas diversas daquela representada pelo Controlador, que exerçam atividade de tratamento no âmbito de contrato administrativo ou instrumento congênere.

Além dos agentes de tratamento, outra figura essencial para o adequado cumprimento da LGPD é o **Encarregado**, definido pelo art. 5º, VIII, como a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD.

1.1.2 TRATAMENTO DE DADOS

O tratamento de dados abrange qualquer atividade que utilize um dado pessoal na execução da sua operação, como, por exemplo: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Vistos os conceitos essenciais de Controlador, Operador, Encarregado e tratamento de dados, é importante estar atento às particularidades de cada caso concreto, a fim de serem evitadas confusões que ponham em risco a correta delimitação de responsabilidades entre os agentes envolvidos no tratamento de dados. Convém, portanto, destacar que a identificação dos responsáveis depende necessariamente, em cada situação, da existência da capacidade de decidir sobre os meios e a finalidade do tratamento de dados.

As operações de tratamento são destacadas a seguir:

- ACESSO - ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;
- ARMAZENAMENTO - ação ou resultado de manter ou conservar em repositório um dado;
- ARQUIVAMENTO - ato ou efeito de manter registrado um dado em qualquer das fases do ciclo da informação, compreendendo os arquivos corrente, intermediário e permanente, ainda que tal informação já tenha perdido a validade ou esgotado a sua vigência;
- AVALIAÇÃO - analisar o dado com o objetivo de produzir informação;
- 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 visando organizá-los para obtenção de um resultado determinado;
- 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.

Ainda sobre o tratamento de dados, é preciso esclarecer que, por taxativa previsão da LGPD (art. 4°), as disposições da Lei não são aplicadas ao tratamento de dados pessoais nas seguintes situações:

> *I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;*
>
> *II - realizado para fins exclusivamente jornalísticos, artístico e acadêmico (aplicando-se a esta última hipótese os arts. 7º e 11 da LGPD);*
>
> *III - realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, ou;*
>
> *IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na LGPD.*

Os casos de tratamento de dados que são permitidos pela LGPD serão explicados a seguir. Mas é muito importante destacar que eles não são amplos e absolutos; ao contrário, existem limites para essa operação que estão dados pela **boa-fé e demais princípios previstos no art. 6º da LGPD**.

Antes de iniciar alguma espécie de tratamento de dados pessoais, o agente deve se certificar previamente que a finalidade da operação esteja registrada de forma clara e explícita e os propósitos especificados e informados ao titular dos dados.

1.1.3 TRATAMENTO DE DADOS PELO PODER PÚBLICO

No caso do setor público, *a finalidade do tratamento está relacionada à execução de políticas públicas, devidamente previstas em lei, regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres*. Tais políticas públicas, vale destacar, devem estar inseridas nas atribuições legais do órgão ou da entidade da administração pública que efetuar o referido tratamento.

Outra finalidade corriqueira para o tratamento de dados no serviço público *é o cumprimento de obrigação legal ou regulatória pelo controlador.* Nessas duas situações, o consentimento do titular de dados é dispensado.

Além disso, no tratamento feito pelo poder público, as regras previstas no art. 23 (procedimentos de atuação) e no art. 30 (regulamentos da ANPD) da LGPD sempre devem ser seguidas de forma complementar.

A LGPD previu expressamente em seu artigo 7°, dez hipóteses que autorizam o tratamento de dados, bem como estabeleceu os requisitos para execução de tal procedimento. **São as chamadas bases legais de tratamento de dados pessoais.**

Nos casos de tratamento de dados em que a base legal não é o consentimento, é possível o compartilhamento de dados com órgãos públicos ou transferência de dados a terceiro fora do setor público. Quando isso acontecer, os agentes de tratamento devem comunicar as operações executadas, de forma clara, aos titulares dos dados, garantindo-lhes o exercício aos direitos previstos no art. 18, da LGPD, com destaque aos direitos de acesso, retificação, oposição, eliminação e informação das entidades públicas e privadas com as quais o controlador irá realizar o uso compartilhado de dados.

É importante registrar que tal comunicação deve ser renovada na alteração da finalidade ou em qualquer alteração nas operações de tratamento, inclusive de novo compartilhamento ou transferência.

Além disso, é necessário que a cada tratamento de dados seja feita uma análise de se os princípios da necessidade e adequação também estão sendo cumpridos pelo controlador. Já nos casos de tratamento de dados feitos com base no consentimento, cada nova operação realizada com os dados pessoais deve ser objeto de nova requisição de consentimento, inclusive para o compartilhamento dos dados com outras entidades, de dentro ou fora da administração pública.

O compartilhamento dentro da administração pública no âmbito da execução de políticas públicas é previsto na lei e dispensa o consentimento específico.

Contudo, o órgão que coleta deve informar claramente que o dado será compartilhado e com quem. Do outro lado, o órgão que solicita acesso a dado colhido por outro, isto é, solicita receber o compartilhamento, precisa justificar esse acesso com base na execução de uma política pública específica e claramente determinada, descrevendo o motivo da solicitação de acesso e o uso que será feito com os dados. Informações protegidas por sigilo seguem protegidas e sujeitas a normativos e regras específicas.

1.2 DIREITOS DO TITULAR

A LGPD estabeleceu uma estrutura legal que empodera os titulares de dados pessoais, fornecendo-lhes direitos a serem exercidos perante os controladores de dados. Esses direitos devem ser garantidos durante toda a existência do tratamento dos dados pessoais do titular realizado pelo órgão ou entidade.

Os direitos a serem garantidos aos titulares de dados estão organizados nas tabelas a seguir, as quais estão segregadas em direitos decorrentes dos princípios estabelecidos pelo art. 6º da LGPD e em direitos específicos dos titulares constantes dos demais artigos da referida Lei.

Na sequência, são apresentadas considerações sobre as hipóteses legais de tratamento de dados da LGPD, assegurando a conformidade do tratamento de dados pessoais de acordo com as referidas hipóteses legais e princípios da LGPD.

TABELA 1 – DIREITOS GARANTIDOS AOS TITULARES DE DADOS

DIREITOS DOS TITULARES DE DADOS QUE DECORREM DOS PRINCÍPIOS	PRINCÍPIO CORRESPONDENTE	REFERÊNCIAS NORMATIVAS (LGPD)
Direito ao tratamento adstrito aos propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.	Princípio da finalidade	Art. 6º, inciso I
Direito ao tratamento adequado, compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento.	Princípio da adequação	Art. 6º, inciso II
Direito à 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.	Princípio da necessidade	Art. 6º, inciso III
Direito à consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.	Princípio do livre acesso	Art. 6º, inciso IV
Direito à exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade para o cumprimento da finalidade de seu tratamento.	Princípio da qualidade dos dados	Art. 6º, inciso V
Direito a informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.	Princípio da transparência	Art. 6º, inciso VI
Direito à segurança dos dados, ao qual se contrapõe o dever, por parte dos agentes de tratamento, de utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações	Princípio da segurança	Art. 6º, inciso VII

acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.		
Direito à adequada prevenção de danos, ao qual se contrapõe o dever, por parte dos agentes de tratamento, de adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.	Princípio da prevenção	Art. 6º, inciso VIII
Direito de não ser discriminado de forma ilícita ou abusiva.	Princípio da não discriminação	Art. 6º, inciso IX
Direito de exigir a adequada responsabilização e a prestação de contas por parte dos agentes de tratamento, ao qual se contrapõe o dever, por parte destes, de adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais.	Princípio da responsabilização e prestação de contas	Art. 6º, inciso X

Nessa esteira, a LGPD não só assegura aos titulares de dados os direitos decorrentes dos princípios (art. 6º), mas também outros direitos específicos, conforme referidos na seguinte tabela:

TABELA 2 – DIREITOS ESPECÍFICOS DOS TITULARES DE DADOS PESSOAIS

DIREITOS DOS TITULARES DE DADOS QUE DECORREM DOS PRINCÍPIOS	REFERÊNCIAS NORMATIVAS (LGPD)
Direito de condicionar o tratamento de dados ao prévio consentimento expresso, inequívoco e informado do titular, salvo as exceções legais.	Arts. 7º, I, e 8º
Direito de exigir o cumprimento de todas as obrigações de tratamento previstas na lei, mesmo para os casos de dispensa de exigência de consentimento.	Art. 7º, § 6º
Direito à inversão do ônus da prova quanto ao consentimento.	Art. 8º, § 2º
Direito de requerer a nulidade de autorizações genéricas para o tratamento de dados pessoais.	Art. 8º, § 4º
Direito de requerer a nulidade do consentimento caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou, ainda, não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.	Art. 9º, § 1º
Direito de requerer a revogação do consentimento a qualquer tempo, mediante manifestação expressa do titular, por procedimento gratuito e facilitado.	Art. 8º, § 5º

Direito de revogar o consentimento caso o titular discorde das alterações quanto ao tratamento de dados, seja na finalidade, forma e duração do tratamento, alteração do controlador ou compartilhamento.	Arts. 8º, § 6º e 9º, § 2º
Direito de acesso facilitado ao tratamento de dados, cujas informações devem ser disponibilizadas de forma clara, adequada e ostensiva acerca de (entre outras): finalidade específica do tratamento; forma e duração do tratamento, observados os segredos comercial e industrial; identificação do controlador; informações de contato do controlador; informações acerca do uso compartilhado de dados pelo controlador; finalidade, responsabilidades dos agentes que realizarão o tratamento e direitos do titular, com menção explícita aos direitos contidos no art. 18.	Art. 9º
Direito de ser informado sobre aspectos essenciais do tratamento de dados, com destaque específico sobre o teor das alterações supervenientes no tratamento.	Art. 8º, § 6º
Direito de ser informado, com destaque, sempre que o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço, ou, ainda, para o exercício de direito, o que se estende à informação sobre os meios pelos quais o titular poderá exercer seus direitos.	Art. 9º, § 3º
Direito de ser informado sobre a utilização dos dados pela administração pública para os fins autorizados pela lei e para a realização de estudos por órgão de pesquisa.	Art. 7º, III e IV c/c art. 7º, § 1º
Direito de que o tratamento de dados pessoais cujo acesso é público esteja adstrito à finalidade, à boa-fé e ao interesse público que justificaram sua disponibilização.	Art. 7º, § 3º
Direito de condicionar o compartilhamento de dados por determinado controlador que já obteve consentimento a novo e específico consentimento. No caso da Administração Pública em que o tratamento é embasado nas hipóteses de dispensa de consentimento original, o compartilhamento demandará uma nova justificativa de tratamento.	Art. 7º, § 5º
Direito de ter o tratamento de dados limitado ao estritamente necessário para a finalidade pretendida quando o tratamento for baseado no legítimo interesse do controlador.	Art. 10, § 1º
Direito à transparência do tratamento de dados baseado no legítimo interesse do controlador.	Art. 10, § 2º
Direito à anonimização dos dados pessoais sensíveis, sempre que possível, na realização de estudos por órgão de pesquisa.	Art. 11, II, c
Direito de ter a devida publicidade em relação às hipóteses de dispensa de consentimento para: tratamento de dados sensíveis no cumprimento de	Art. 11, § 2º

obrigação legal ou regulatória pelo controlador; ou tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos.	
Direito de impedir a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde, com o objetivo de obter vantagem econômica (exceto nos casos de portabilidade de dados quando consentido pelo titular).	Art. 11, § 4º
Direito de que os dados pessoais sensíveis utilizados em estudos de saúde pública sejam tratados exclusivamente dentro do órgão de pesquisa e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.	Art. 13
Direito de não ter dados pessoais revelados na divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa sobre saúde pública.	Art. 13, § 1º
Direito de não ter dados pessoais utilizados em pesquisa sobre saúde pública transferidos a terceiros pelo órgão de pesquisa.	Art. 13, § 2º
Direito ao término do tratamento, quando verificado que: (i) a finalidade foi alcançada ou que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; (ii) houve o fim do período de tratamento; (iii) houve comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento, conforme disposto no § 5º do art. 8º da Lei e resguardado o interesse público; ou (iv) por determinação da autoridade nacional, quando houver violação ao disposto na Lei.	Art. 15
Direito à eliminação ou ao apagamento dos dados, no âmbito e nos limites técnicos das atividades, sendo autorizada a conservação somente nas exceções legais.	Art. 16

1.3 EXERCÍCIO DOS DIREITOS DOS TITULARES PERANTE A ADMINISTRAÇÃO MUNICIPAL

Para o exercício dos direitos dos titulares, a LGPD prevê um conjunto de ferramentas, que, no âmbito público, traduzem-se em mecanismos que aprofundam obrigações de transparência ativa e passiva, bem como criam meios processuais para provocar a Administração Pública.

Essas obrigações são apresentadas como: ***(i) meios de acesso à informação em transparência passiva; e (ii) meios de petição e manifestação à administração pública.***

Em todos os casos, o titular do dado tem a faculdade de optar por resposta por meio eletrônico, seguro e idôneo para esse fim ou sob forma impressa, oportunidade em que foi alterado o sítio

eletrônico da Prefeitura Municipal visando garantir maior transparência e interação entre a Administração Municipal e os titulares de dados.

1.3.1 MEIOS DE ACESSO À INFORMAÇÃO EM TRANSPARÊNCIA PASSIVA

Parte substancial dos direitos dos titulares perante o poder público são exercidos por meio do exercício do direito de acesso à informação. É sempre importante salientar que a Lei nº 12.527/2011 ("LAI"), já previa, em seu art. 31, procedimentos e diretrizes básicas para o tratamento de dados pessoais no âmbito público. Entre eles, estão o tratamento transparente, a garantia expressa aos direitos de personalidade e o consentimento do titular para a disponibilização de suas informações àqueles que não possuíssem a necessidade de conhecê-la no exercício de sua função pública.

A LGPD, reconhecendo o legado deixado pela LAI, informa que, no âmbito público, os prazos e procedimentos para o exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, citando (mas sem se ater exclusivamente) a Lei de Acesso à Informação, a Lei do Processo Administrativo e a Lei do Habeas data (essa última no âmbito judicial).

Desta forma, submetem-se aos prazos e procedimentos já estabelecidos pela LAI - inclusive com o recebimento dos requerimentos junto ao Serviço de Informação ao Cidadão - o exercício dos seguintes direitos expressamente previstos na LGPD:

a) acesso à informação sobre a confirmação da existência de tratamento (art. 18, I);

b) acesso aos dados pessoais de que é titular e que são objeto de tratamento pela Administração Pública (art. 18, II);

c) acesso à informação sobre entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados (art. 18, VII);

d) nos casos em que o tratamento tiver origem no consentimento do titular ou em contrato, o acesso à cópia eletrônica integral de seus dados pessoais. Devem ser observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente inclusive em outras operações de tratamento (art. 19, §3º); e

e) acesso às informações a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial (art. 20, §1º).

1.3.2 MEIOS DE PETIÇÃO E MANIFESTAÇÃO À ADMINISTRAÇÃO PÚBLICA

Como já mencionado, no âmbito administrativo, a LGPD cita expressamente a Lei de Acesso à Informação e a Lei nº 9.784/1999 (processo administrativo federal) como referência não exclusiva para o exercício dos direitos dos titulares. É de se repisar que, ao mesmo tempo, ela aparta os

procedimentos que ela prevê daqueles a serem utilizados em face do poder público, ao mencionar que o exercício de tais direitos seria realizado por meio de legislação específica.

Como a Lei não estabelece a observância exclusiva daquele conjunto da Lei de Acesso à Informação e da Lei Geral do Processo Administrativo, e considerando a existência de procedimentos mais benéficos ao titular para o exercício de seus direitos no que se refere a esse último conjunto apresentado, o mecanismo mais célere estabelecido pelo Código de Defesa dos Usuários de Serviços Públicos (Lei n° 13.460/2017) poderia ser adotado como padrão para o recebimento de solicitações de providências e reclamações relativas ao tratamento de dados.

Além da vantagem em termos de prazo e procedimentos padronizados, com unidades de recebimento de petições e reclamações padronizadas e coordenadas, a Lei nº 13.460/2017, diferentemente da Lei Geral do Processo Administrativo, tem abrangência nacional, permitindo melhor coordenação entre instituições públicas na defesa dos direitos dos titulares de dados.

O titular do dado tem o direito, mediante requerimento expresso seu ou de representante legalmente constituído, sem custos, nos prazos e nos termos previstos em regulamento, de requisitar manifestação conclusiva do controlador ou agente responsável pelo tratamento sobre os seguintes itens:

a) correção de dados incompletos, inexatos ou desatualizados (art. 18, III);

b) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD (art. 18, IV);

c) eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da LGPD (art. 18, VI); e

d) revisão de 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).

A resposta deve ser providenciada de imediato e em formato simplificado; ou por declaração clara e completa, fornecida no prazo previsto em Lei e que indique: origem dos dados, a inexistência de registro, critérios utilizados, finalidade do tratamento (observados os segredos comercial e industrial).

O titular do dado tem a faculdade de optar por resposta por meio eletrônico, seguro e idôneo para esse fim ou sob forma impressa (pode ser utilizado o e-SIC).

A petição deve ser respondida com agilidade, clareza e completude, sob pena de o titular dos dados ter a prerrogativa de representar contra o responsável na ANPD, organismos de defesa do consumidor ou ajuizar pretensão com tal causa de pedir.

Na impossibilidade de atendimento imediato do requerimento do titular do dado pessoal, o controlador poderá comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

Por último, o titular dos dados tem direito a solicitar a revisão de 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.

Nas hipóteses acima, o controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial. Quando tais segredos impossibilitarem o oferecimento de informações, a ANPD poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

Os dados pessoais referentes ao exercício regular de direitos pelo titular, previstos no art. 18, da LGPD, não podem ser utilizados em seu prejuízo. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.

1.4 TIPOLOGIA DE DADOS PESSOAIS

No âmbito da administração municipal, de acordo com o inciso IV do artigo 4° da Lei n° 12.527/11 ("LAI"), ***informação pessoal é aquela relacionada à pessoa natural identificada ou identificável.*** Entende-se por pessoa natural a pessoa física, ou seja, o indivíduo. Os contornos mais relevantes desse conceito são apresentados pelo art. 31, da LAI.

Segundo o art. 31, da LAI, não é toda e qualquer informação pessoal que goza de um regime específico de proteção. Apenas aquela com potencial de vulnerar os direitos de personalidade, tais como definidos no art. 5º, X, da Constituição Federal, estaria sob uma proteção especial. No núcleo desse conjunto de dados, estaria o que se denominou, com amparo na doutrina existente, a informação pessoal sensível. **Ou seja, aquela informação que viola o direito de autodeterminação da imagem ou que possa levar a que terceiros adotem ações discriminatórias contra o titular daquele dado.**

A existência de gradações desta natureza mostrou-se bastante importante ao longo dos últimos anos, pois passou a indicar limites à mitigação da expectativa de privacidade no caso em que os titulares dos dados eram os próprios agentes públicos.

A LGPD manteve o conceito de dado pessoal trazido pela Lei nº 12.527/2011 e evoluiu sobre o conceito de informação 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).*

No entanto, diferentemente da LAI, os direitos e salvaguardas sobre dados pessoais da LGPD incidem sobre todos os tipos de dados pessoais, observadas as legislações existentes, inclusive os regimes existentes de transparência e acesso à informação. Ou seja, a tutela da lei se estende não mais apenas aos dados pessoais sensíveis ou diretamente relacionados aos direitos de personalidade, mas, em maior ou menor medida, a todos os dados pessoais.

Para desenvolvimento de uma governança em privacidade e proteção de dados é importante reiterarmos e apresentarmos alguns conceitos importantes:

- atributos biográficos - dados de pessoa natural relativos aos fatos da sua vida, tais como nome civil ou social, data de nascimento, filiação, naturalidade, nacionalidade, sexo, estado civil, grupo familiar, endereço e vínculos empregatícios;
- atributos biométricos - características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar;
- dados cadastrais - informações identificadoras perante os cadastros de órgãos públicos, tais como:
  a) os atributos biográficos;
  b) o número de inscrição no Cadastro de Pessoas Físicas - CPF;
  c) o número de inscrição no Cadastro Nacional de Pessoas Jurídicas - CNPJ;
  d) o Número de Identificação Social - NIS;
  e) o número de inscrição no Programa de Integração Social - PIS;
  f) o número de inscrição no Programa de Formação do Patrimônio do Servidor Público - Pasep;
  g) o número do Título de Eleitor;
  h) a razão social, o nome fantasia e a data de constituição da pessoa jurídica, o tipo societário, a composição societária atual e histórica e a Classificação Nacional de Atividades Econômicas - CNAE; e
  i) outros dados públicos relativos à pessoa jurídica ou à empresa individual.

- atributos genéticos - características hereditárias da pessoa natural, obtidas pela análise de ácidos nucleicos ou por outras análises científicas;
- autenticidade - propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa natural, ou por um determinado sistema, órgão ou entidade;
- base integradora - base de dados que integra os atributos biográficos ou biométricos das bases temáticas;
- base temática - base de dados de determinada política pública que contenha dados biográficos ou biométricos que possam compor a base integradora;
- compartilhamento de dados - disponibilização de dados pelo seu gestor para determinado recebedor de dados;

- confidencialidade - propriedade que impede que a informação fique disponível ou possa ser revelada à pessoa natural, sistema, órgão ou entidade não autorizados e não credenciados;
- custo de compartilhamento de dados - valor dispendido para viabilizar a criação e a sustentação dos recursos tecnológicos utilizados no compartilhamento de dados;
- custodiante de dados - órgão ou entidade que, total ou parcialmente, zela pelo armazenamento, pela operação, pela administração e pela preservação de dados, coletados pela administração pública, que não lhe pertencem, mas que estão sob sua custódia;
- disponibilidade - propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa natural ou determinado sistema, órgão ou entidade;
- gestor de dados - órgão ou entidade responsável pela governança de determinado conjunto de dados;
- gestor de plataforma de interoperabilidade - órgão ou entidade responsável pela governança de determinada plataforma de interoperabilidade;
- governança de dados - exercício de autoridade e controle que permite o gerenciamento de dados sob as perspectivas do compartilhamento, da arquitetura, da segurança, da qualidade, da operação e de outros aspectos tecnológicos;
- informação - dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
- integridade - propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
- interoperabilidade - capacidade de diversos sistemas e organizações trabalharem em conjunto, de modo a garantir que pessoas, organizações e sistemas computacionais troquem dados;
- item de informação - atributo referente a determinada informação que pode ser acessado em conjunto ou de forma isolada;
- mecanismo de compartilhamento de dados - recurso tecnológico que permite a integração e a comunicação entre aplicações e serviços do recebedor de dados e dos órgãos gestores de dados, tais como serviços web, cópia de dados, lago de dados compartilhado e plataformas de interoperabilidade;
- plataforma de interoperabilidade - conjunto de ambientes e ferramentas tecnológicas, com acesso controlado, para o compartilhamento de dados da administração pública entre órgãos e entidades especificados no art. 1º;
- recebedor de dados - órgão ou entidade que utiliza dados após ser concedida permissão de acesso pelo gestor dos dados;
- requisitos de segurança da informação e comunicações - ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;
- requisitos de segurança da informação e comunicação - ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;
- solicitante de dados - órgão ou entidade que solicita ao gestor de dados a permissão de acesso aos dados;

- solicitante de dados - órgão ou entidade que solicita ao gestor de dados a permissão de acesso aos dados;
- cadastro base - informação de referência, íntegra e precisa, centralizada ou descentralizada, oriunda de uma ou mais fontes, sobre elementos fundamentais para a prestação de serviços e para a gestão de políticas públicas, tais como pessoas, empresas, veículos, licenças e locais.

Não existe uma perfeita coincidência entre tais atributos e os conceitos que vimos até agora; porém, a compatibilização destes conceitos é bastante simples.

Primeiramente, cabe destacar que todos os tipos de atributos constituem informações pessoais, pois são relativos à pessoa física identificada ou identificável. **Atributos genéticos e biométricos**, por definição legal, constituem dados pessoais sensíveis.

Atributos biográficos, em conjunto com dados como números de cadastro tais como CPF, CNPJ, NIS, PIS, PASEP e Título de Eleitor são o que se denomina de dados cadastrais, que são, à luz da LGPD, dados pessoais. Isso porque, se qualquer dado, inclusive o cadastral, trouxer informação relacionada a pessoa natural identificada ou identificável, será considerado um dado pessoal.

Por sua vez, **a depender do seu conteúdo, atributos biográficos poderão ou não ser considerados sensíveis**. Nos termos da Lei, serão considerados sensíveis aqueles atributos biográficos que digam respeito à convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político.

Assim, geralmente, o tratamento de atributos biométricos e genéticos se dará com base no regime de tratamento de dados pessoais sensíveis; já o tratamento de atributos biográficos será feito de acordo com o seu conteúdo, o qual definirá a tipologia do dado à luz da LGPD.

2. DO TRATAMENTO DE DADOS PESSOAIS

2.1 HIPÓTESES DE TRATAMENTO

A LGPD autoriza, em seu art. 23, os órgãos e entidades da administração pública a realizar o tratamento de dados pessoais unicamente 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, desde que as hipóteses de tratamento sejam informadas ao titular.

O tratamento de dados pessoais poderá ser realizado desde que enquadrado em uma das hipóteses elencadas na Lei. Tais hipóteses podem ser compreendidas como condições necessárias para verificar se o tratamento de dados pelo controlador ou operador é permitido. As hipóteses de tratamento de dados pessoais são enumeradas no art. 7º da LGPD.

Nesta seção, destacaremos também as previsões constantes do art. 11, que trata das hipóteses autorizativas para o tratamento de informações pessoais sensíveis.

Segundo a LGPD, os dados pessoais sensíveis de pessoas naturais são aqueles *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* (art. 5º, II). São dados cujo tratamento pode ensejar a discriminação do seu titular, e por isso, são sujeitos a proteção mais rígida.

Cabe destacar que a lei autoriza o tratamento de dados sensíveis apenas em **situações indispensáveis**. Isso traz para o controlador o ônus da prova da alegada indispensabilidade.

É necessário que os órgãos e entidades da Administração Municipal conheçam as hipóteses para:

- *Analisar os casos de tratamento de dados pessoais já realizados, objetivando verificar se há hipótese legal que os autorize; e*

- *Avaliar previamente cada novo caso de tratamento que pretenda realizar, identificando as hipóteses legais autorizativas aplicáveis.*

A tabela a seguir elenca resumidamente as hipóteses de tratamento autorizadas pela LGPD, informando, em cada caso, a base legal referente ao tratamento de dados pessoais em geral (art. 7º), bem como a correspondente base legal para o tratamento de dados pessoais sensíveis (art. 11).

TABELA 3 – HIPÓTESES DE TRATAMENTO DE DADOS PESSOAIS

HIPÓTESES DE TRATAMENTO	DISPOSITIVO LEGAL (LGPD) PARA O TRATAMENTO DE DADOS PESSOAIS	DISPOSITIVO LEGAL (LGPD) PARA O TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS
Hipótese 1: Mediante consentimento do titular	art. 7º, inciso I	art. 11º, inciso I
Hipótese 2: Para o cumprimento de obrigação legal ou regulatória	art. 7º, inciso II	art. 11º, inciso II, “a”
Hipótese 3: Para a execução de políticas públicas	art. 7º, inciso III	art. 11º, inciso II, “b”
Hipótese 4: Para a realização de estudos e pesquisas	art. 7º, inciso IV	art. 11º, inciso II, “c”
Hipótese 5: Para a execução ou preparação de contrato	art. 7º, inciso V	Não se aplica
Hipótese 6: Para o exercício de direitos em processo judicial, administrativo ou arbitral	art. 7º, inciso VI	art. 11º, inciso II, “d”
Hipótese 7: Para a proteção da vida ou da incolumidade física do titular ou de terceiro	art. 7º, inciso VII	art. 11º, inciso II, “e”

Hipótese 8: Para a tutela da saúde do titular	art. 7º, inciso VIII	art. 11º, inciso II, “i”
Hipótese 9: Para atender interesses legítimos do controlador ou de terceiro	art. 7º, inciso IX	Não se aplica
Hipótese 10: Para proteção do crédito	art. 7º, inciso X	Não se aplica
Hipótese 11: Para a garantia da prevenção à fraude e à segurança do titular	Não se aplica	art. 11º, inciso II, “g”

2.2 PRINCÍPIOS LEGAIS QUE FUNDAMENTAM O TRATAMENTO DE DADOS PESSOAIS

A LGPD estabelece também, em seu art. 6º, que o tratamento de dados pessoais deve observar a boa-fé e dez princípios fundamentais específicos:

- **Finalidade:** realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
- **Adequação:** compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
- **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;
- **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;
- **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;
- **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;
- **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;
- **Prevenção:** adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
- **Não discriminação:** impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; e
- **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.

Não basta, portanto, o enquadramento em uma das hipóteses legais autorizativas para se iniciar o tratamento de dados pessoais. É fundamental garantir que os princípios listados acima sejam respeitados.

2.2.1 IDENTIFICAÇÃO DAS HIPÓTESES DE TRATAMENTO APLICÁVEIS

Como determinar a hipótese legal que autoriza o tratamento de dados pessoais? Isso depende das finalidades e contextos específicos de cada situação.

É natural imaginar que, para órgãos e entidades públicas, seriam sempre aplicáveis as hipóteses 2 e 3 da Tabela 3, quais sejam: "Para o cumprimento de obrigação legal ou regulatória" e "Para a execução de políticas públicas". No entanto, não existe um caso geral que se adeque a todas as situações, mesmo considerando tratar-se de órgãos e entidades públicas. Poderá haver inclusive situações em que mais de uma hipótese legal seja cabível, se houver múltiplos propósitos para o tratamento do dado.

O importante é avaliar caso a caso e manter atualizada a planilha de Inventário de Dados Pessoais - IDP com a(s) hipótese(s) aplicável(is), uma vez que o titular deverá conhecer a hipótese legal que autoriza o processamento de seus dados pessoais.

Além disso, o princípio da responsabilização e prestação de contas requer que o órgão ou entidade que realiza o tratamento de dados pessoais possa demonstrar que está plenamente aderente à LGPD, comprovando a observância e o cumprimento das normas de proteção de dados pessoais estabelecidas, inclusive quanto a sua eficácia.

Por essa razão, cabe ao órgão ou entidade pública avaliar bem a hipótese de tratamento aplicável, pois mudanças posteriores podem abalar a confiança do titular quanto aos interesses legítimos da instituição no uso de seus dados, além de comprometer os requisitos de transparência, responsabilização e prestação de contas.

HIPÓTESE 1: Tratamento mediante consentimento do titular

Essa é uma hipótese em que o titular tem chance real de escolha sobre o tratamento de seus dados. Trata-se de hipótese possível quando as demais do art. 7º forem descartadas.

Uma vez descartadas as demais hipóteses, o órgão/entidade deve avaliar:

1. *Serão viáveis a coleta e o armazenamento da opção de consentimento do titular de modo a poder comprovar posteriormente a sua expressa manifestação de vontade?*

2. *Se o consentimento se der de forma escrita, será garantido que a opção pelo consentimento conste de cláusula destacada das demais, em que o titular seja instado a escolher livremente pela anuência ou não ao consentimento solicitado?*

3. *O consentimento será solicitado para cada uma das finalidades de tratamento, e será informado ao titular que tipo de tratamento será realizado, antes que este opte pelo consentimento?*

Observações:

a) É vedado o tratamento de dados pessoais mediante vício de consentimento.
b) O consentimento será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.
c) Se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o titular deverá ser informado previamente sobre as mudanças de finalidade, podendo revogar o consentimento, caso discorde das alterações.
d) As autorizações genéricas para o tratamento de dados pessoais serão consideradas nulas.

4. *Será dada ao titular a opção de revogação do consentimento, a qualquer momento, mediante manifestação expressa, por procedimento gratuito e facilitado?*

5. *No caso de tratamento de dados de crianças e adolescentes, será solicitado o consentimento específico por pelo menos um dos pais ou pelo responsável legal?*

6. *No caso do tratamento de dados pessoais sensíveis, será registrada a manifestação de vontade do titular de forma específica e destacada, dando ciência do conhecimento sobre as finalidades específicas daquele tratamento?*

Ressalta-se que todas as questões acima, se aplicáveis, devem ser respondidas positivamente para que a hipótese de tratamento do dado por consentimento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

HIPÓTESE 2: Tratamento para o cumprimento de obrigação legal ou regulatória

Essa hipótese é aplicável quando é necessário processar dados pessoais para o cumprimento de obrigações legais ou regulatórias específicas. Não se enquadram nessa hipótese as obrigações estabelecidas por contrato.

Para enquadramento nessa hipótese, deve-se avaliar:

1. *É possível identificar a obrigação legal ou regulatória específica que requer o processamento do dado?*

2. *É possível identificar a competência legal do órgão que dará cumprimento à obrigação legal ou regulatória?*

3. *O titular do dado será informado sobre a norma que determina a obrigação legal ou regulatória que exige o tratamento do dado?*

4. *Em se tratando de dados pessoais sensíveis, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 da Lei?*

As questões acima devem ser respondidas positivamente para que essa hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

HIPÓTESE 3: Tratamento para a execução de políticas públicas

Essa hipótese é aplicável para 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. Trata-se de uma hipótese que dispensa o consentimento do titular e que deve ser realizada por controladores que sejam pessoas jurídicas de direito público.

Os controladores podem, no entanto, envolver operadores para a realização do tratamento de dados pessoais necessários à consecução de políticas públicas. Estes últimos podem ser pessoas jurídicas de direito privado.

Para enquadramento nessa hipótese, deve-se avaliar:

1. *O controlador é pessoa jurídica de direito público?*

2. *Não sendo pessoa jurídica de direito público, o controlador é empresa pública ou sociedade de economia mista que realizará o tratamento de dados para execução de políticas públicas, e não para atividades inerentes ao regime de concorrência?*

3. *O tratamento do dado será realizado para a execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres?*

4. *É possível identificar claramente a lei, regulamento ou outro instrumento legal que especifique a política pública que exige o tratamento de dados pessoais?*

5. *É possível identificar a competência legal que autoriza o órgão à execução da política pública?*

6. *O titular do dado será informado sobre a lei, regulamento ou outro instrumento legal que especifique a política pública que exige o tratamento do dado?*

7. *Em se tratando de dados pessoais sensíveis, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 da Lei, inclusive quando da necessidade de compartilhamento de dados?*

8. *Será indicado um encarregado (art. 5º, inciso VIII) para garantir a comunicação do órgão ou entidade pública com o titular do dado e com a ANPD, que verificará a observância das instruções e normas sobre a política pública em questão?*

As questões acima devem ser respondidas positivamente para que essa hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

Segundo o art. 23 da LGPD, os órgãos e entidades públicas deverão realizar o tratamento de dados apenas para o atendimento de sua finalidade pública, na persecução do interesse público e com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

Nesse contexto, não havendo uma delimitação inequívoca das atribuições legais que poderiam ser diretamente relacionadas à execução de políticas públicas, cabe aos órgãos e entidades analisar, no caso concreto, a possibilidade de enquadrar o tratamento do dado na hipótese prevista no art. 7º, inciso III, combinada com o disposto no art. 23.

HIPÓTESE 4: Tratamento para a realização de estudos e pesquisas

Essa hipótese é aplicável para o tratamento de dados para realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais.

Para enquadramento nesta hipótese, deve-se avaliar:

1. *O controlador ou operador é órgão de pesquisa?*

2. *Os dados pessoais serão utilizados dentro do órgão estritamente para a finalidade estabelecida para o estudo ou pesquisa?*

3. *Em se tratando de estudos em saúde pública, os dados serão mantidos em ambiente seguro e controlado, e será garantida, sempre que viável, a anonimização ou pseudonimização dos dados?*

4. *O órgão de pesquisa garante que não serão revelados dados pessoais em caso de divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa realizada?*

5. *O órgão de pesquisa que tiver acesso aos dados pessoais assume a responsabilidade pela segurança da informação e se compromete a não transferir os dados a terceiros em circunstância alguma?*

As questões acima devem ser respondidas positivamente para que essa hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

Especificamente no que tange à realização de estudos em saúde pública, o art. 13 da LGPD possibilita que os órgãos tenham acesso a bases de dados pessoais, inclusive os atributos sensíveis, que serão tratados exclusivamente dentro do referido órgão e estritamente para a finalidade de

realização de estudos e pesquisas. Nessa hipótese, o órgão ou entidade deverá garantir que os dados sejam mantidos em ambiente controlado e seguro, e que, sempre que possível, sejam anonimizados ou pseudonimizados.

HIPÓTESE 5: Tratamento para a execução de contrato ou de procedimentos preliminares relacionados a contrato

Essa hipótese é aplicável para o tratamento de dados necessário à execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular. As hipóteses de tratamento de dados estarão previstas no contrato. O consentimento é fornecido no ato de formalização do termo ou decorrente do mesmo.

Para enquadramento nessa hipótese, deve-se avaliar:

1. *O tratamento de dados pessoais se faz necessário para a consecução dos termos do contrato ou para a realização de procedimentos preliminares relacionados ao contrato?*

Essa pergunta deve ser respondida positivamente para que tal hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

HIPÓTESE 6: Tratamento para o exercício de direitos em processo judicial, administrativo ou arbitral

Essa hipótese é aplicável para o tratamento de dados necessário ao exercício regular de direitos do titular em processo judicial, administrativo ou arbitral, por quaisquer das partes envolvidas.

Para enquadramento nessa hipótese, deve-se avaliar:

1. *O tratamento de dados pessoais se faz necessário para o exercício de direitos do titular em processo judicial, administrativo ou arbitral?*

2. *O titular do dado será informado com destaque quando essa hipótese de tratamento for aplicada?*

As questões acima devem ser respondidas positivamente para que essa hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

HIPÓTESE 7: Tratamento para a proteção da vida ou da incolumidade física do titular ou de terceiro

Essa hipótese é aplicável para o tratamento de dados para a proteção da vida ou da incolumidade física do titular ou de terceiros.

Para enquadramento nessa hipótese, deve-se avaliar:

1. *O tratamento de dados pessoais se faz necessário para proteger a vida ou a incolumidade física do titular ou de terceiros?*

2. *O titular está impossibilitado de oferecer o consentimento para o tratamento do dado pessoal?*

As questões acima devem ser respondidas positivamente para que essa hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

HIPÓTESE 8: Tratamento para a tutela da saúde do titular

Essa hipótese é aplicável para o tratamento de dados para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

Para enquadramento nessa hipótese, deve-se avaliar:

1. *O tratamento de dados pessoais será realizado por profissional de saúde, serviço de saúde ou autoridade sanitária?*

2. *O tratamento de dados pessoais se faz necessário para a tutela da saúde do titular?*

As questões acima devem ser respondidas positivamente para que essa hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

HIPÓTESE 9: Tratamento para atender interesses legítimos do controlador ou de terceiro

Essa hipótese é aplicável para o tratamento de dados 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.

Órgãos e entidades públicas não devem recorrer a essa hipótese se o tratamento de dados ocorre para a consecução de políticas públicas ou de suas próprias competências legais. No entanto, em caso de finalidade diversa, essa opção poderá ser aplicável.

Para enquadramento nessa hipótese, deve-se avaliar:

1. *Foi identificado interesse legítimo do controlador, considerado a partir de situações concretas, que respeite as legítimas expectativas do titular em relação ao tratamento de seus dados?*

2. *O controlador se responsabiliza por garantir a proteção do exercício regular dos direitos do titular ou a prestação de serviços que o beneficiem, respeitados os direitos e liberdades fundamentais do titular?*

3. *O titular do dado será comunicado sobre a hipótese de tratamento de dados aplicada?*

4. *Serão adotadas medidas para garantir a transparência do tratamento de dados baseado no legítimo interesse do controlador?*

As questões acima devem ser respondidas positivamente para que essa hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

HIPÓTESE 10: Tratamento para proteção do crédito

Essa hipótese é aplicável para o tratamento de dados para proteção do crédito do titular.

Para enquadramento nessa hipótese, deve-se avaliar:

1. *Foi identificada necessidade de tratamento de dados pessoais para a proteção do crédito do titular?*

2. *O titular do dado será comunicado sobre a hipótese de tratamento de dados aplicada?*

As questões acima devem ser respondidas positivamente para que essa hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

HIPÓTESE 11: Tratamento para a garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos

Essa hipótese é aplicável para o tratamento de dados pessoais sensíveis para assegurar a identificação e autenticação do titular para a autenticação de cadastro em sistemas eletrônicos, visando à prevenção de fraudes e à garantia da segurança do titular.

Para enquadramento nessa hipótese, deve-se avaliar se não há outro meio para a identificação do titular sem a necessidade do tratamento de dados sensíveis.

Esta hipótese refere-se, por exemplo, à possibilidade de uso de biometria para identificação e autenticação em sistemas eletrônicos.

Destaca-se que essa hipótese não pode ser utilizada no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

2.2.2 VERIFICAÇÃO DE CONFORMIDADE DO TRATAMENTO DE DADOS QUANTO AOS PRINCÍPIOS DA LGPD

Uma vez identificada(s) a(s) hipótese(s) de tratamento aplicável(is) às situações específicas de processamento de dados por órgãos e entidades da Administração Pública, deve-se partir para outras questões importantes para a verificação da conformidade quanto aos princípios da LGPD.

Para tanto, o órgão ou entidade pública deverá analisar outras questões, detalhadas a seguir:

1. Identifique a finalidade para a qual o tratamento de dado é necessário. Os propósitos devem ser legítimos, específicos e explícitos (princípio da finalidade).

2. Defina como a finalidade do tratamento será informada ao titular, o que deve ser realizado antes do início do tratamento do dado (princípio da finalidade).

3. No caso de tratamento de dados que tenha sido iniciado antes da vigência da Lei, indique que providências serão tomadas para comunicar o titular sobre o tratamento realizado e a finalidade a qual se destina (princípio da finalidade).

4. Garanta que o tratamento do dado será apenas para a finalidade informada ao titular (princípio da adequação). Quaisquer mudanças na finalidade de tratamento deverão ser também comunicadas ao titular do dado.

5. Ao planejar a forma de tratamento de dados, atente para limitar a utilização ao mínimo de informações necessárias, garantindo abrangência pertinente e proporcional à consecução das finalidades informadas ao titular (princípio da necessidade).

6. Ao decidir realizar o tratamento de dados, defina antecipadamente os mecanismos e procedimentos que os titulares dos dados deverão utilizar para consultar o conteúdo, a forma e a duração do tratamento dos seus dados pessoais, de maneira facilitada e gratuita (princípio do livre acesso).

7. Garanta que quaisquer alterações quanto à finalidade especificada para o tratamento do dado; à forma ou à duração do tratamento; ao controlador responsável pelo dado; ou, ainda, à abrangência de compartilhamento sejam comunicadas ao titular (princípio do livre acesso).

8. Defina procedimento de verificação contínua quanto à exatidão, à clareza, à relevância e à atualização dos dados do titular. O objetivo é manter-se fiel à finalidade de tratamento informada (princípio da qualidade do dado).

9. Observe a necessidade de garantir ao titular a opção de obter facilmente informações claras e precisas, mediante requisição, sobre o tratamento que é dado a seus dados e sobre os respectivos agentes de tratamento (princípio da transparência).

10. Defina e documente as medidas técnicas e administrativas que serão adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (princípio da segurança).

11. Identifique e registre as medidas que serão adotadas para prevenir a ocorrência de danos ao titular ou a terceiros em virtude do tratamento de dados pessoais (princípio da prevenção).

12. Comprometa-se a não realizar o tratamento do dado para fins discriminatórios ilícitos ou abusivos (princípio da não discriminação).

13. Comprometa-se a adotar medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais (princípio da responsabilização e prestação de contas).

Para iniciar novos tratamentos de dados, é fundamental que os órgãos e entidades da Administração Municipal analisem todas as questões citadas acima e documentem a forma de aplicação de cada um dos princípios da LGPD. *O Relatório de Impacto à Proteção de Dados Pessoais – RIPD representa um instrumento importante de verificação e demonstração da conformidade do tratamento de dados pessoais realizado pela instituição*. Serve tanto para a análise quanto para a documentação. Na seção 2.5 constam orientações no sentido de auxiliar os órgãos e entidades a elaborar um RIPD.

A análise das questões acima deve também ser realizada para os casos de tratamento de dados anteriores à vigência da Lei. Nesses casos, é importante identificar os pontos de não conformidade com a LGPD, para os quais deverão ser elaborados planos para adaptação à Lei.

2.2.3 ESPECIFICIDADES PARA O TRATAMENTO DE DADOS DE CRIANÇAS E ADOLESCENTES

Assim como para o caso das informações pessoais sensíveis, a LGPD dedica também atenção especial ao tratamento de dados de crianças e adolescentes.

A Lei determina, em seu art. 14, que o tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse. A Lei requer consentimento específico e em destaque, dado por pelo menos um dos pais ou pelo responsável legal. Nessa hipótese, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para acesso às informações tratadas.

É também dever do controlador envidar todos os esforços razoáveis para verificar se o consentimento foi dado realmente pelo responsável pela criança ou adolescente, consideradas as tecnologias disponíveis. Esse é, portanto, um dos grandes desafios para a coleta de dados pessoais de crianças, pois o consentimento é exigido inclusive no caso de execução de políticas públicas, o que não ocorre com adultos.

As hipóteses que dispensam o consentimento mencionado acima ocorrem quando:

a) A coleta for necessária para contatar os pais, ou o responsável legal, ou, ainda, para a própria proteção da criança ou adolescente. Nesses casos, os dados deverão ser utilizados uma única vez, vedados o armazenamento e o seu repasse a terceiros;

b) O Tratamento de dados for imprescindível para o exercício de direitos da criança ou adolescente ou para lavratura de registros públicos.

2.3 COLETA DE DADOS PESSOAIS

A coleta é uma das operações de tratamento referenciadas pelo art. 5º, inciso X da LGPD.

Considerando que o tratamento de dados pode ser representado por um ciclo de vida, essa operação representa a etapa inicial responsável por obter os dados pessoais do cidadão (titular dos dados).

Tendo em vista que a coleta é a operação inicial de tratamento dos dados pessoais, a realização de tal operação pela instituição somente deve ser realizada mediante o atendimento das hipóteses de tratamento, das medidas de segurança, dos princípios, dos diretos do titular e demais regras dispostas pela LGPD.

Com isso, a incorporação da privacidade como padrão para o tratamento dos dados pessoais, indicando a limitação da coleta como uma das práticas a serem adotadas.

2.4 CATEGORIZAÇÃO DOS DADOS PESSOAIS PARA FUTURO COMPARTILHAMENTO

O compartilhamento de dados entre os órgãos públicos da administração pública direta e indireta do Município deve se dar com intuito de preservar os princípios previstos na LGPD, com a finalidade de:

- simplificar a oferta de serviços públicos;
- orientar e otimizar a formulação, a implementação, a avaliação e o monitoramento de políticas públicas;
- possibilitar a análise das condições de acesso e manutenção de benefícios sociais e fiscais;
- promover a melhoria da qualidade e da fidedignidade dos dados custodiados pela administração pública; e
- aumentar a qualidade e a eficiência das operações internas da administração pública municipal.

O compartilhamento de dados entre os órgãos públicos da administração pública direta e indireta do Município será categorizado em **três níveis**, de acordo com sua confidencialidade:

- **Compartilhamento amplo**, quando se tratar de dados públicos que não estão sujeitos a nenhuma restrição de acesso, cuja divulgação deve ser pública e garantida a qualquer interessado, na forma da legislação;

- **Compartilhamento restrito**, quando se tratar de dados protegidos por sigilo, nos termos da legislação, com concessão de acesso a todos os órgãos e entidades da administração direta e indireta para a execução de políticas públicas, cujo mecanismo de compartilhamento e regras sejam simplificados ou que detenham regras estabelecidas anteriormente; e

- **Compartilhamento específico**, quando se tratar de dados protegidos por sigilo, nos termos da legislação, com concessão de acesso a órgãos e entidades específicas, nas hipóteses e

para os fins previstos em lei, cujo compartilhamento e regras sejam definidos pelo Controlador.

2.4.1 REGRAS DE COMPARTILHAMENTO

2.4.1.1 Regras Gerais

Recomenda-se priorizar a categorização os dados seguindo a seguinte ordem:

- primeiro os dados estruturados, depois os não estruturados;
- primeiro as informações mais solicitadas, depois as demais informações;
- os dados que forem categorizados como Restritos ou Específicos devem ter uma justificativa para tal categorização;
- os órgãos que recebem dados deverão manter um histórico de que bases receberam e de quais órgãos;
- dados recebidos não devem ser recategorizados. Vale a categorização recebida;
- caso a categorização de um conjunto de dados mude com o tempo, os dados já distribuídos e presentes em outros órgãos também mudarão;
- no caso de dados combinados - isto é, aqueles constituídos pela junção de um ou mais conjunto de dados, quando não for viável sua separação, para efeito de categorização, deve-se classificar o conjunto na categoria mais privativa;
- os dados recebidos por compartilhamento restrito poderão ser retransmitidos ou compartilhados com outros órgãos ou entidades que comprovem a necessidade de acesso, exceto se proibido expressamente na autorização concedida pelo gestor de dados ou controlador, ou se houver posterior revogação da permissão desse, mediante fundamentação, nas duas hipóteses.

2.4.1.2 Identificação de pessoa física

Todas as identificações de pessoas físicas na **categoria ampla** serão com nome e CPF mascarados da seguinte forma:

Nome no formato: D. M. S. S.
CPF no formato: *.999.999-****

A publicação de leis, decretos, portarias, resoluções, editais, contratos e atos administrativos que contenham dados pessoais de titular interessado, **poderá constar o nome completo do titular dos dados, sem abreviações, com vistas ao cumprimento de obrigações legais ou garantia de direitos.**

Outras informações pessoais no ato, deve a Administração Municipal avaliar a necessidade de publicação do documento em sua integralidade.

Todas as identificações de pessoas físicas na **categoria restrita e específica** serão com nome e CPF completo e todos os demais identificadores disponíveis (PIS, Carteira de trabalho, PASEP, Identidade estadual etc.).

2.4.1.3 Identificação de pessoa jurídica

Todas as identificações de pessoas jurídicas, em qualquer categoria, serão com nome e CNPJ completos.

2.4.1.4 Prazos

Dados de categorização **ampla** deverão ser entregues em 30 dias, visto que não há critérios a serem atendidos observada a legislação vigente.

Dados de categorização **restrita** deverão ser entregues em 30 dias após atenderem as regras desse documento.

Dados de categorização **específica**, caso seja concedida a permissão de acesso pelo gestor dos dados, **restrita** deverão ser entregues em 30 dias após atenderem as regras definidas pelo gestor dos dados.

No caso de solicitação a dados de categorização **específica**, o órgão gestor dos dados deverá se manifestar sobre a solicitação no prazo de 30 dias.

2.4.1.5 Regras de Compartilhamento de dados Restritos e Específicos

- **Identificação do Solicitante:** O solicitante deve enviar um ofício indicando seu interesse nos dados e finalidade do acesso. Este ofício deve ser assinado pelo gestor do órgão requisitante ou entidade, e é suficiente para a identificação do solicitante como representante de órgão ou entidade pública.
- **Controle de acessos feito:** O gestor de dados deverá manter um controle sobre todos os órgãos que acessam os seus dados. Esse controle deve prever plataformas de interoperabilidade e repasses de informação entre órgãos. Nessa fase, este controle deverá incluir, no mínimo todos os novos pedidos. Posteriormente, serão tratados os acessos anteriores.
- **Formulários de acesso**: Os solicitantes deverão apresentar documento por escrito em que apresentam justificativa para solicitação e termo de responsabilidade com as seguintes informações, no mínimo:

    - ✓ Órgão solicitante com nome, endereço, nome do titular e substituto e telefones e e-mails respectivos; e
    - ✓ Motivo da solicitação. Descrição do motivo da solicitação e do uso que será feito dos dados em conformidade com o art. 23 da Lei nº 13.709, de 2018. Essa descrição não

será motivo para recusa de acesso, mas o órgão poderá ser advertido, pelo gestor de dados ou encarregado, em caso de descrições vagas ou improcedentes.

2.4.2 CATEGORIZAÇÃO

Categorizar significa enquadrar um conjunto de informações nas categorias Ampla, Restrita ou Específica.

2.4.2.1 Ampla

- Informação gerada, ou publicada, em evento público.
- Exemplo: diploma universitário, informações publicadas no Diário Oficial ou outros documentos públicos oficiais.
- Informação sobre o governo incluindo funcionamento, gasto e serviço.
- Exemplos: Funcionamento inclui estrutura organizacional, recursos, pessoal (nome e dados funcionais), horários de funcionamento. Gasto inclui compras governamentais e pagamentos a servidores. Serviço inclui lista de serviços, locais, regras de funcionamento.
- Informações declaradas públicas pelos órgãos competentes.
- Situação de regularidade com a Administração Pública de Pessoas Jurídicas.
- Exemplo: dívida ativa, certificados, certidões, alvarás etc. Deverá incluir tipo de regularidade (qual alvará, permissão etc.), situação (regular, irregular), validade (início e fim, se houver), nome e CNPJ.
- Informações estatísticas.
- No caso de informações pessoais anonimizadas não basta retirar identificadores. É necessário garantir que o indivíduo não seja identificado.
- Beneficiários de programas sociais do governo.
- Relação de beneficiários diretos de programa social do governo. Informações devem conter no mínimo o nome, CPF mascarado e valor.

2.4.2.2 Restrita

- Dados cadastrais.
  Inclui nome, identificadores (CPF, NIS, título eleitoral etc.), data de nascimento, situação civil, endereço, contatos (telefone, e-mail etc.), filiação, nome social.
- Situação de regularidade com a Administração Pública de Pessoas Físicas.
  Exemplo: CPF, dívida ativa, certificados, certidões, alvarás etc. Deverá incluir tipo de regularidade (qual alvará, permissão etc.), situação (regular, irregular), validade (início e fim, se houver), nome e CPF.
- Beneficiários de programas sociais do governo.
- Informações completas sobre beneficiários de programa social do governo.

2.4.2.3 Específica

- Informações com restrições legais sobre o compartilhamento dentro da Administração Pública (informações cujas restrições legais de controle de acesso façam restrições a compartilhamentos com outros órgãos do governo). Exemplo: CTN restringe acesso a servidores da Fazenda Pública.
- Segurança pública e Segurança Nacional (informações que comprometam a segurança pública e segurança nacional).
- Informações internas de sistemas (informações internas de sistemas que possam ter implicações sobre segurança, incluindo número IP, logs etc.).
- Informações que coloque pessoas em risco (informações que coloque pessoas em situação de risco, incluindo quantidade de fiscais em postos de fiscalização, localização de bens confiscados, beneficiados do programa de proteção à testemunha etc.).
- Informações médicas (informações relativas à saúde do cidadão identificado).

2.5 ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO

Segundo a LGPD, dado anonimizado é o dado que, considerados os meios técnicos razoáveis no momento do tratamento, perde a possibilidade de associação, direta ou indireta, a um indivíduo.

A não identificação da relação entre o dado e seu proprietário decorre da utilização da técnica de anonimização, a fim de impossibilitar a associação entre estes, seja de forma direta ou indireta.

A partir do momento em que o dado é considerado anonimizado, e não permite mais qualquer identificação do seu titular, esse dado sai do escopo da legislação, por não mais se tratar de um dado pessoal, conforme previsto no art. 12, da LGPD.

É importante ressaltar que, ainda que o dado seja considerado anonimizado pelo controlador, uma vez observada a possibilidade de reversão do processo que obteve a anonimização, permitindo se identificar do titular de dados novamente, não se está diante de um dado verdadeiramente anonimizado, mas de um dado potencialmente pseudonimizado.

Pseudonimização é a técnica de tratar dados pessoais de uma forma em que os dados somente possam ser atribuídos a um titular de dados mediante a utilização de informações adicionais, não disponíveis a todos, desde que essas informações sejam mantidas em ambiente separado, controlado e seguro.

A título ilustrativo, criptografia é um método de pseudonimização, quando os dados somente podem ser atribuídos a um titular mediante o conhecimento da chave criptográfica. Sem conhecer a chave, os dados são ininteligíveis.

De acordo com a legislação em vigor, esses processos devem ser utilizados, sempre que possível, por meio da aplicação de meios técnicos razoáveis e disponíveis, na ocasião do tratamento dos dados.

Pode-se registrar algumas recomendações para subsidiar a escolha da técnica a ser utilizada nesses casos:

- *Elencar os principais processos de trabalho que realizam tratamento de dados pessoais para a realização de estudos, especialmente em órgão de pesquisa, conforme Art. 7º, IV.*
- *Identificar os dados pessoais a que se referem os processos de trabalho listados, que não podem ter os titulares relacionados.*
- *Analisar o ciclo de vida de tratamento do dado a fim de mitigar riscos de violação de dados que não são mais de uso corrente. E, ainda, propor arquivamento ou eliminação dos dados, visto que a gestão de dados desnecessários no ambiente de produção causa aumento não apenas do quantitativo de dados a serem geridos, como também a manutenção do custo operacional relacionado a este processo (em atividades como armazenamento e gestão da segurança).*
- *Avaliar o risco de identificação do titular dos dados listados. Deve-se levar em consideração que, quanto maior o uso de tecnologias de análise de dados, quanto maior o volume de dados processados e quanto mais significativos forem estes dados, maior será o risco de violação.*
- *Quando houver a obrigatoriedade de proteção de dados pessoais, sem a necessidade de guarda dos dados que associam estes aos titulares, pode-se optar pelo processo de anonimização, sem prejuízo de atividades do órgão ou entidade. Caso contrário, pode-se optar pela técnica de pseudonimização.*
- *Definir um plano de comunicação para incidentes de violação de dados. O objetivo é propiciar maior celeridade na solução de incidentes e padronização de atividades a serem executadas, assim como prever responsáveis pelo cumprimento das atividades.*
- *Documentar violações atestadas e incidentes ocorridos, a fim de analisar riscos de violação periodicamente.*
- *Promover a conscientização contínua acerca da importância da proteção de dados no órgão ou entidade.*

Cabe destacar que a pseudonimização, como técnica utilizada para proteção de dados pessoais, pode ser utilizada, por exemplo, para preservação da identidade do denunciante. A pseudonimização também pode ser utilizada para proteger a identidade do usuário de serviço público ou autor de manifestação conforme previsão da Lei nº 13.460, de 26 de junho de 2017.

2.6 PUBLICIDADE

O inciso I do art. 23 da LGPD impõe às pessoas jurídicas de direito público obrigações de transparência ativa. Isto é, de publicar informações sobre os tratamentos de dados pessoais por elas realizados em seus sítios eletrônicos de forma clara e atualizada, detalhando a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução desses tratamentos.

Também deve ser dada publicidade aos tratamentos de dados pessoais sensíveis em que seja dispensado o consentimento do titular, seja para cumprimento de obrigação legal ou regulatória, seja para tratamento compartilhado de dados necessários para a execução de políticas públicas previstas em leis ou regulamentos, conforme prevê o §2º do art. 11 da LGPD.

Outra informação a ser publicizada é a identidade e informações de contato do encarregado, por força do art. 41, §1º da LGPD.

Quando o tratamento de dados pessoais envolver a obrigação legal de difusão destes em transparência ativa, estes devem ser publicados em formato acessível e estruturado para o uso compartilhado, em cumprimento ao disposto no art. 25 da LGPD e como já previa o art. 8º, §3, da Lei nº 12.527/2011.

Quanto à localização da publicação das informações sobre o tratamento de dados pessoais, sensíveis ou não, sugere-se que, além dos itens especificados para serem publicados em seção específica denominada "Acesso à Informação" no sítio eletrônico da Prefeitura Municipal.

Sugere-se como texto de introdução:

"Nesta seção, são divulgadas informações sobre o tratamento de dados pessoais realizado pelo(a) [nome do órgão ou entidade], compreendendo a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução desse tratamento, em cumprimento ao disposto no inciso I do art. 23 da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD)".

Em seguida, devem ser publicadas as seguintes informações sobre o encarregado:

DADOS DO ENCARREGADO
I. Nome e cargo do encarregado indicado pelo controlador;
II. Localização;
III. Contatos (e-mail e telefone).

2.6.1 PUBLICIZAÇÃO DE DADOS PESSOAIS EM DOCUMENTOS OFICIAIS

A publicação de leis, decretos, portarias, resoluções, editais, contratos e atos administrativos que contenham dados pessoais de titular interessado, poderá constar o nome completo do titular dos dados, sem abreviações, com vistas ao **cumprimento de obrigações legais ou garantia de direitos**, **preservando-se informações pessoais e sensíveis que não influenciem nos motivos que geraram o dever de publicidade**, tais como, a divulgação de CPF, endereço, filiação, endereço eletrônico, orientação sexual etc.

Quando da publicização, pode a Administração Municipal avaliar a necessidade de publicação do documento em sua integralidade, observando os princípios basilares da LGPD, tendo em vista a vinculação administrativa ao dever de publicidade imposto pela Constituição Federal e Lei de Acesso à Informação. Nesses casos, pode a Administração Municipal divulgar tais informações de forma "mascarada", seguindo a mesma orientação para publicização de dados de pessoas físicas para compartilhamento na categoria ampla.

Por certo, os dados pessoais e sensíveis não divulgados em sua integralidade, nos meios próprios utilizados pela Administração Municipal, devem constar de forma integral nos documentos originais arquivados em âmbito municipal.

2.7 RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

2.7.1 O QUE É O RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS - RIPD

O Relatório de Impacto à Proteção dos Dados Pessoais (RIPD) representa documento fundamental a fim de demonstrar que o controlador realizou uma avaliação dos riscos nas operações de tratamento de dados pessoais que são coletados, tratados, usados, compartilhados e quais medidas são adotadas para mitigação dos riscos que possam afetar as liberdades civis e direitos fundamentais dos titulares desses dados.

Segundo o inciso XVII do art. 5º da LGPD, o RIPD é documentação que deve ser mantida pelo controlador dos dados pessoais.

> *Art. 5º Para os fins desta Lei, considera-se:*
>
> *XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;*

Enquanto o art. 5º inciso XVII define o que é um RIPD, o seu conteúdo mínimo é indicado pelo parágrafo único do art. 38:

> *Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.*
>
> *Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.*

O formulário de RIPD apresentado neste instrumento de orientação constitui uma sugestão para auxiliar os órgãos e entidades na documentação da avaliação de impacto sobre dados pessoais. Dessa forma, e caso seja considerado pertinente pela instituição, as seções e o conteúdo do modelo podem ser adaptados para se adequar a cada contexto particular.

2.7.2 COMO ELABORAR

O RIPD deve ser elaborado antes de a instituição iniciar o tratamento de dados pessoais, preferencialmente, na fase inicial do programa ou projeto que tem o propósito de usar esses dados.

2.7.2.1 Identificar os Agentes de Tratamento e o Encarregado

Esta etapa consiste em identificar os agentes de tratamento (controlador e operador) e o encarregado no RIPD (art. 5º, VI, VII e VIII, da LGPD). Esses atores desempenham papel essencial no levantamento das informações necessárias para elaboração do RIPD.

> *Art. 5º Para os fins desta Lei, considera-se: [...]*
>
> *VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;*
>
> *VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;*
>
> *VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); (Redação dada pela Lei nº 13.853, de 2019)*

A conclusão desta etapa envolve registrar o e-mail e o telefone de contato do encarregado, já que ele é o canal de comunicação entre o controlador, titulares dos dados e ANPD.

2.7.2.2 Identificar a necessidade de elaborar o Relatório

Inicialmente, é fundamental conhecer os casos específicos previstos pela LGPD em que o RIPD deverá ou poderá ser solicitado:

- *Para tratamento de dados pessoais realizados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (exceções previstas pelo inciso III do art. 4º);*
- *Quando houver infração da LGPD em decorrência do tratamento de dados pessoais por órgãos públicos (arts. 31 e 32 combinados); e*
- *A qualquer momento sob determinação da ANPD (art. 38).*

Quando for necessária a elaboração do RIPD, a instituição deve avaliar se os programas, sistemas de informação ou processos existentes ou a serem implementados geram impactos à proteção dos dados pessoais, a fim de decidir sobre a elaboração ou atualização do RIPD.

A elaboração de um único RIPD para todas as operações de tratamento de dados pessoais ou de um RIPD para cada projeto, sistema, ou serviço deve ser avaliada por cada instituição de acordo com os processos internos de trabalho. Assim, uma instituição que realiza tratamento de quantidade

reduzida de dados pessoais, com poucos processos e serviços, pode optar por um RIPD único. Já uma instituição que implementa vários processos, projetos, sistemas e serviços que envolvam o tratamento de expressiva quantidade e diversidade de dados pessoais pode considerar que a elaboração de um único RIPD não seja a opção mais indicada, optando por elaborar RIPDs segregados por ser mais adequado à sua realidade.

É indicada, ainda, a elaboração ou atualização do Relatório de Impacto sempre que existir a possibilidade de ocorrer impacto na privacidade dos dados pessoais, resultante de:

- *uma tecnologia, serviço ou outra nova iniciativa em que dados pessoais e dados pessoais sensíveis sejam ou devam ser tratados;*
- *rastreamento da localização dos indivíduos ou qualquer outra ação de tratamento que vise a formação de perfil comportamental de pessoa natural, se identificada; (LGPD, art. 12 § 2º);*
- *tratamento de 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" (LGPD, art. 5º, II);*
- *processamento de dados pessoais usado para tomar decisões automatizadas que possam ter efeitos legais, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (LGPD, art. 20);*
- *tratamento de dados pessoais de crianças e adolescentes (LGPD, art. 14);*
- *tratamento de dados que possa resultar em algum tipo de dano patrimonial, moral, individual ou coletivo aos titulares de dados, se houver vazamento (LGPD, art. 42);*
- *tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais (LGPD, art. 4º, § 3º);*
- *tratamento no interesse legítimo do controlador (LGPD, art. 10, § 3º);*
- *alterações nas leis e regulamentos aplicáveis à privacidade, política e normas internas, operação do sistema de informações, propósitos e meios para tratar dados, fluxos de dados novos ou alterados, etc.; e*
- *reformas administrativas que implicam em nova estrutura organizacional resultante da incorporação, fusão ou cisão de órgãos ou entidades.*

Em síntese, nessa etapa deve(m) ser explicitado(s) qual(is) dos itens elencados acima expressa(m) a necessidade de o RIPD ser elaborado ou atualizado pela instituição.

2.7.2.3 Descrever o tratamento

A descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais envolve a especificação da natureza, escopo, contexto e finalidade do tratamento.

Lembrando que a LGPD (art. 5º, X) considera tratamento *"toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso,*

produção, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

O objetivo principal desta descrição é fornecer cenário institucional relativo aos processos que envolvem o tratamento dos dados pessoais, fornecendo subsídios para avaliação e tratamento de riscos.

Caso a instituição considere mais adequado para sua realidade de tratamento de dados pessoais, pode-se sintetizar a natureza, escopo, contexto e finalidade do tratamento em uma única seção do RIPD, sem necessidade de segregar a descrição do tratamento em subseções.

2.7.2.3.1 Natureza do tratamento

A natureza representa como a instituição pretende tratar ou trata o dado pessoal. Importante descrever, por exemplo:

- *como os dados pessoais são coletados, retidos/armazenados, tratados, usados e eliminados;*
- *fonte de dados (ex: titular de dados, planilha eletrônica, arquivo xml, formulário em papel etc.) utilizada para coleta dos dados pessoais;*
- *com quais órgãos, entidades ou empresas os dados pessoais serão compartilhados;*
- *quais são os operadores que realizam o tratamento de dados pessoais em nome do controlador e destacar em quais fases (coleta, retenção, processamento, compartilhamento, eliminação) eles atuam;*
- *se adotou recentemente algum tipo de nova tecnologia ou método de tratamento que envolva dados pessoais. A informação sobre o uso de nova tecnologia ou método de tratamento é importante no sentido de possibilitar a identificação de possíveis riscos resultantes de tal uso; e*
- *medidas de segurança atualmente adotadas.*

Na elaboração dessa descrição, é importante considerar a possibilidade de consultar um diagrama ou qualquer outra documentação que demonstre os fluxos de dados da instituição.

2.7.2.3.2 Escopo do tratamento

O escopo representa a abrangência do tratamento de dados.

Nesse sentido, considerar destacar:

- *as informações sobre os tipos dos dados pessoais tratados, ressaltando quais dos dados são considerados dados pessoais sensíveis.*
- *o volume dos dados pessoais a serem coletados e tratados;*
- *a extensão e frequência em que os dados são tratados;*
- *o período de retenção, informação sobre quanto tempo os dados pessoais serão mantidos, retidos ou armazenados;*

- *o número de titulares de dados afetados pelo tratamento; e*
- *a abrangência da área geográfica do tratamento.*

O levantamento das informações elencadas acima auxilia a determinar se o tratamento de dados pessoais é realizado em alta escala.

2.7.2.3.3 Contexto do tratamento

Nesta etapa, convém destacar um cenário mais amplo, incluindo fatores internos e externos que podem afetar as expectativas do titular dos dados pessoais ou o impacto sobre o tratamento dos dados.

O levantamento das informações destacadas abaixo proporciona a obtenção de parâmetros que permitirão demonstrar o equilíbrio entre o interesse e a necessidade do controlador em tratar os dados pessoais e os direitos dos titulares de tais dados:

- *natureza do relacionamento da organização com os indivíduos;*
- *nível ou método de controle que os indivíduos exercem sobre os dados pessoais;*
- *destacar se o tratamento envolve crianças, adolescentes ou outro grupo vulnerável;*
- *destacar se o tipo de tratamento realizado sobre os dados é condizente com a expectativa dos titulares dos dados pessoais. Ou seja, o dado pessoal não é tratado de maneira diversa do que é determinado em leis e regulamentos, e comunicado pela instituição ao titular de dados;*
- *destaque de qualquer experiência anterior com esse tipo de tratamento de dados;*
- *destaque de avanços relevantes da instituição em tecnologia ou segurança que contribuem para a proteção dos dados pessoais.*

2.7.2.3.4 Finalidade do tratamento

A finalidade é a razão ou motivo pelo qual se deseja tratar os dados pessoais. É importantíssimo estabelecer claramente a finalidade, pois é ela que justifica o tratamento e fornece os elementos para informar o titular dos dados.

Nesta etapa, é importante detalhar o que se pretende alcançar com o tratamento dos dados pessoais, considerando os exemplos de finalidades elencadas abaixo, embasados nos artigos 7º e 11 da LGPD, no que for aplicável:

- *cumprimento de obrigação legal ou regulatória pelo controlador;*
- *execução de políticas públicas;*
- *alguma espécie de estudo realizado por órgão de pesquisa;*
- *execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;*
- *exercício regular de direitos em processo judicial, administrativo ou arbitral;*
- *proteção da vida ou da incolumidade física do titular ou de terceiros;*

- *tutela da saúde;*
- *atender aos interesses legítimos do controlador ou de terceiros;*
- *proteção do crédito; e*
- *garantia da prevenção à fraude e à segurança do titular.*

Cumpre destacar que os exemplos de finalidades apresentados neste documento não são exaustivos. Desse modo, deve-se informar e detalhar qualquer outra finalidade específica do controlador para tratamento dos dados pessoais, mesmo que tal finalidade não conste dos citados exemplos.

Ao detalhar a finalidade do tratamento dos dados pessoais, é importante:

- *indicar qual(is) o(s) resultado(s) pretendido(s) para os titulares dos dados pessoais, informando o quão importantes são esses resultados;*
- *informar os benefícios esperados para o órgão, entidade ou para a sociedade como um todo.*

Neste momento, deve-se atentar para o caso de a finalidade ser para atender o legítimo interesse do controlador. Nesse caso, somente poderá ser fundamentado tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, conforme previsto pelo art. 10 da LGPD.

> *Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:*
>
> *I - apoio e promoção de atividades do controlador; e*
>
> *II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.*
>
> *§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.*
>
> *§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.*
>
> *§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.*

Cumpre ressaltar que a instituição deve equilibrar seus interesses com os dos indivíduos com os quais ela tem relacionamento.

2.7.2.4 Identificar partes interessadas consultadas

Partes interessadas relevantes, internas e externas, consultadas a fim de obter opiniões legais, técnicas ou administrativas sobre os dados pessoais que são objeto do tratamento.

Nessa etapa, é importante identificar:

- *quais partes foram consultadas, como, por exemplo: operador (LGPD, art. 5º, VII), encarregado (LGPD, art. 5º, VIII), gestores, especialistas em segurança da informação, consultores jurídicos etc.; e*
- *o que cada parte consultada indicou como importante de ser observado para o tratamento dos dados pessoais em relação aos possíveis riscos referentes às atividades de tratamento em análise. Também deve-se observar os riscos de não-conformidade ante a LGPD e os instrumentos internos de controle (políticas, processos e procedimentos voltados à proteção de dados e privacidade).*

Caso não seja conveniente registrar o que foi consultado, então é importante apresentar o motivo de não ter realizado tal registro. Como, por exemplo, apresentar justificativa de que informar o registro das opiniões das partes internas comprometeria segredo comercial ou industrial; fragilizaria a segurança da informação; ou seria desproporcional ou impraticável realizar o registro das opiniões obtidas.

2.7.2.5 Descrever necessidade e proporcionalidade

Descrever como a instituição avalia a necessidade e proporcionalidade dos dados. É necessário demonstrar que as operações realizadas sobre os dados pessoais limitam o 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 (LGPD, art. 6º, III).

Nesse sentido, destacar:

- *a fundamentação legal para o tratamento dos dados pessoais.*
- *Caso o fundamento legal seja embasado no legítimo interesse do controlador (LGPD, art. 10), demonstrar que:*
- *esse tratamento de dados pessoais é indispensável;*
- *não há outra base legal possível de se utilizar para alcançar o mesmo propósito;*
- *esse processamento de fato auxilia no propósito almejado.*
- *Como será garantida a qualidade [exatidão, clareza, relevância e atualização dos dados] e minimização dos dados.*
- *Quais medidas são adotadas a fim de assegurar que o operador (LGPD, art. 5º, VII) realize o tratamento de dados pessoais conforme a LGPD e respeite os critérios estabelecidos pela instituição que exerce o papel de controlador (LGPD, art. 5º, VI).*

Como estão implementadas as medidas que asseguram o direito do titular dos dados pessoais obter do controlador o previsto pelo art. 18 da LGPD.

- *como a instituição pretende fornecer informações de privacidade para os titulares dos dados pessoais.*
- *quais são as salvaguardas para as transferências internacionais de dados.*

O artigo 18 da LGPD é bem extenso e trata do direito que o titular tem de requisitar do controlador ações e informações específicas em relação ao tratamento realizado sobre os dados pessoais.

2.7.2.6 Identificar e avaliar os riscos

O art. 5º, XVII da LGPD preconiza que o Relatório de Impacto deve descrever *"medidas, salvaguardas e mecanismos de mitigação de risco".*

Antes de definir tais medidas, salvaguardas e mecanismos, é necessário identificar os riscos que geram impacto potencial sobre o titular dos dados pessoais.

Para cada risco identificado, define-se: a probabilidade de ocorrência do evento de risco, o possível impacto caso o risco ocorra, avaliando o nível potencial de risco para cada evento.

Como exemplo, parâmetros escalares podem ser utilizados para representar os níveis de probabilidade e impacto que, após a multiplicação, resultarão nos níveis de risco, que direcionarão a aplicação de medidas de segurança.

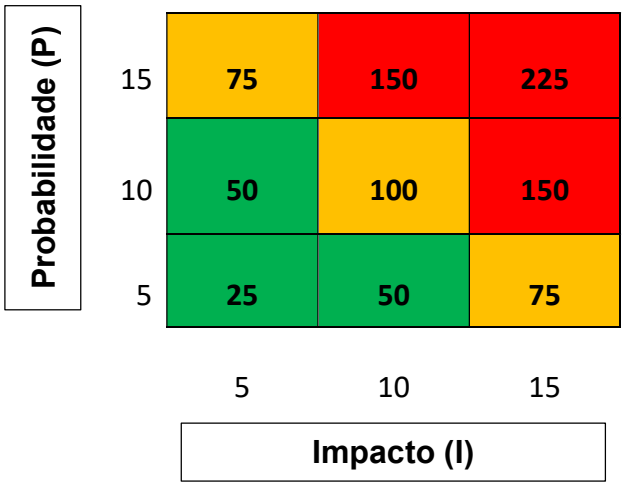
Os níveis de risco estão representados da seguinte forma:

- ***verde**, é entendido como baixo;*
- ***amarelo**, representa risco moderado; e*
- ***vermelho**, indica risco alto.*

Os parâmetros escalares adotados neste documento são apresentados na tabela a seguir:

Classificação	Valor
Baixo	**5**
Moderado	**10**
Alto	**15**

Utilizando-se destes parâmetros, a definição do risco deve observar a ***matriz de probabilidade versos impacto***, conforme tabela abaixo que servirá de instrumento de apoio para a definição dos critérios de classificação do nível de risco.



As definições e conceitos de riscos adotados neste documento são utilizados como forma de ilustrar a identificação e avaliação de riscos realizada no RIPD. Desse modo, é importante destacar que o gerenciamento de riscos relacionado ao tratamento dos dados pessoais deve ser realizado em harmonia com o disposto no RIPD já realizado.

No levantamento dos riscos operacionais à proteção de dados pessoais, os eventos potenciais são analisados nas categorias a seguir:

1. Acesso não autorizado	Acesso aos dados pessoais sem o prévio consentimento expresso, inequívoco e informado do titular, salvo exceções legais.
2. Modificação não autorizada	Modificação de dados pessoais sem a anuência do titular. Viola o princípio da segurança.
3. Perda	Destruição ou extravio ou furto de dados pessoais. Viola os princípios da segurança e da prevenção.
4. Apropriação	Apropriação ou uso indébito de dados de pessoais. Possibilidades de fraude e vazamento intencional de dados. Viola os princípios da segurança e da prevenção.
5. Remoção não autorizada	Retirada de dados pessoais sem autorização do titular.
6. Coleção excessiva	Extração de mais dados do que o necessário para a realização do trabalho, ou do que é previsto em Lei ou foi autorizado pelo usuário. Viola o princípio da necessidade.

7. Informação insuficiente sobre a finalidade do tratamento	A finalidade declarada para o uso das informações pessoais é insatisfatória, não é específica ou pode suscitar interpretações diversas.
8. Tratamento sem consentimento do titular dos dados pessoais	Tratamento dos dados pessoais sem a devida prévia permissão expressa, inequívoca e informada do titular, salvo exceções legais.
9. Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais	Compartilhamento dos dados pessoais com outras entidades privadas (fora da administração pública) sem a devida permissão do titular.
10. Retenção prolongada de dados pessoais sem necessidade	Manter os dados pessoais do titular para além do necessário ou do que estava consentido/autorizado. Viola o princípio da necessidade.
11. Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular	Erro ao vincular dados do verdadeiro titular a outro. Viola o princípio da qualidade dos dados.
12. Falha ou erro de processamento	Processamento dos dados de forma imperfeita ou equivocada. Ex.: execução de script de banco de dados que atualiza dado pessoal com informação equivocada, ausência de validação dos dados de entrada etc. Viola o princípio da qualidade dos dados.
13. Reidentificação de dados pseu-donimizados	Anonimização insatisfatória de dados pessoais sensíveis possibilitando inferir quem é a pessoa em questão. Viola o direito à anonimização.

A identificação e avaliação de riscos envolve elencar os eventos de risco, a probabilidade, o impacto e o nível de risco.

1. Probabilidade: chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente; ou se descrita utilizando-se termos gerais ou matemáticos (ISO/IEC 31000:2018 item 2.19).

2. Impacto: resultado de um evento que afeta os objetivos (ISO/IEC 31000:2018, item 2.18).

3. Nível de Risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades (ISO/IEC 31000:2018, item 2.23 e IN SGD/ME nº 1, de 2019, art. 2º, inciso XIII).

2.7.2.7 Identificar medidas para tratar os riscos

Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (LGPD, art. 46).

Importante reforçar que as medidas para tratar os riscos podem ser: de segurança, técnicas ou administrativas.

A coluna "Medida(s)" pode ser preenchida com uma medida de segurança ou controle específico adotado para tratamento de cada risco identificado na etapa "Identificar e avaliar riscos".

A instituição nem sempre precisa eliminar todos os riscos. Nesse sentido, pode-se decidir que alguns riscos são aceitáveis - até um risco de nível alto –, devido aos benefícios do processamento dos dados pessoais e dificuldades de mitigação. **No entanto, se houver um risco residual de nível alto, é recomendável consultar a ANPD antes de prosseguir com as operações de tratamento dos dados pessoais.**

Neste momento, e a critério do responsável pela elaboração do RIPD, a coluna "Medida(s)" também pode ser preenchida de forma mais detalhada, indicando os principais aspectos da medida segurança ou controles de segurança adotados para tratar o risco. Esse procedimento propicia mais visibilidade em relação ao tratamento do risco.

2.7.2.8 Aprovar o Relatório

Esta etapa visa formalizar a aprovação do RIPD por meio da obtenção das assinaturas do responsável pela elaboração do RIPD, pelo encarregado e pelas autoridades que representam o controlador e operador.

O responsável pela elaboração do Relatório pode ser o próprio encarregado ou qualquer outra pessoa designada pelo controlador com conhecimento necessário para realizar tal tarefa.

2.7.2.9 Manter revisado

O RIPD deve ser revisto e atualizado anualmente ou sempre que existir qualquer tipo de mudança que afete o tratamento dos dados pessoais realizados pela instituição.

De uma forma geral, essa mudança pode ser motivada por alteração:

- *significativa na finalidade do tratamento de dados pessoais;*
- *que impacte no processo de como esses dados são tratados;*

- *expressiva na quantidade de dados pessoais coletados; e*
- *no contexto do tratamento de dados resultantes de identificação de falha de segurança, uso de uma nova tecnologia, nova preocupação pública sobre o tipo de tratamento de dados realizado pela instituição ou vulnerabilidade de um grupo específico de titulares de dados pessoais.*

Cumpre destacar que as orientações referentes à identificação da necessidade de elaborar ou atualizar o RIPD constantes do item 2.6.2 deste documento também contribuem para a identificação de casos em que o Relatório de Impacto deve ser atualizado.

A instituição deve manter revisão do RIPD a fim de demonstrar que avalia continuamente os riscos de tratamento de dados pessoais que surgem em consequência do dinamismo das transformações nos cenários tecnológico, normativo, político e institucional.

2.8 TÉRMINO DO TRATAMENTO DE DADOS

Nos termos da LGPD, o término do tratamento de dados pessoais ocorre em quatro hipóteses:

a) exaurimento da finalidade para os quais os dados foram coletados ou quando estes deixam de ser necessários ou pertinentes para o alcance desta finalidade;
b) fim do período de tratamento;
c) revogação do consentimento ou a pedido do titular, resguardado o interesse público;
d) determinação da autoridade nacional em face de violação do disposto na Lei.

Na incidência de qualquer uma das hipóteses acima, a Lei determina que os dados sejam eliminados, a não ser nos casos em que:

a) remanesça o cumprimento de obrigação legal ou regulatória pelo controlador;
b) sejam necessários para estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados;
c) ocorra a transferência a terceiro, desde que respeitados os requisitos de tratamento dispostos em Lei; e
d) seja utilizado exclusivamente pelo controlador, vedado seu acesso por terceiro, e desde que anonimizados.

No âmbito da Administração Pública, é importante que este dispositivo seja harmonizado com a legislação de arquivos, em especial com o que preceitua a Lei nº 8.159/1991 (dispõe sobre a política nacional de arquivos públicos e privados), e suas regulamentações. Isso porque, desse ponto de vista, os dados pessoais coletados pelo poder público passam a constituir o que se denomina arquivo público (art. 7°) e a sua eliminação deverá obedecer aos procedimentos de gestão de documentos.

2.8.1. O CICLO DE VIDA DO TRATAMENTO DOS DADOS PESSOAIS

O dado pessoal é coletado para atender a uma finalidade específica e pode, por exemplo, ser eliminado a pedido do titular dos dados (LGPD, art. 18, IV), ao cumprimento de uma sanção aplicada pela Autoridade Nacional de Proteção de Dados (LGPD, art. 52, VI) ou ao término de seu tratamento (LGPD, art. 16). Dessa forma, percebemos a configuração de um ciclo que se inicia com a coleta e que determina a "vida" (existência) do dado pessoal durante um período, de acordo com certos critérios de eliminação.

É fundamental destacar que a LGPD considera como tratamento todas as operações realizadas com dados pessoais. Assim, a LGPD não adota qualquer tipo de segregação, considerando como tratamento, por exemplo, tanto a coleta quanto o armazenamento de dados pessoais, mesmo essas operações tratando de propósitos diferentes.

Para orientar a prática do tratamento e apresentar os ativos institucionais envolvidos, divide-se o ciclo de vida do tratamento dos dados pessoais em cinco fases: coleta, retenção, processamento, compartilhamento e eliminação.

Nesta seção, abordaremos o que é cada fase do ciclo de vida, a relação das fases do ciclo com as operações de tratamento da LGPD, os tipos de ativos organizacionais e o relacionamento desses ativos com as fases do ciclo de tratamento, destacando as ações a serem executadas em tais fases.

2.8.1.1 Fases do ciclo de vida dos dados pessoais

Para implementar o correto tratamento dos dados pessoais e as medidas correlatas, o órgão precisa conhecer os dados pessoais que gerencia e quais processos, projetos, serviços e ativos perpassam o ciclo de vida do tratamento dos dados pessoais.

A LGPD considera como tratamento toda operação realizada com os 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.

Para além da legislação de proteção de dados pessoais, é preciso também observar a legislação de arquivos, que deve ser considerada conjuntamente na realização das operações com os dados pessoais contidos em documentos arquivísticos, ainda que estes sejam mantidos em sistemas informatizados e bases de dados. Do mesmo modo, vale lembrar, a LAI (Lei nº 12.527, de 18 de novembro de 2018) e o seu regulamento (Decreto nº 7.724, de 16 de maio de 2012) igualmente apresentam regras específicas para o acesso a documentos que, embora apresentem dados pessoais, possuem valor permanente e foram recolhidos a instituições arquivísticas públicas. A LGPD e a LAI também devem, portanto, ser interpretadas sistematicamente.

Nesse cenário, o ciclo de vida do tratamento tem início com a coleta do dado e se encerra com a eliminação ou descarte. Cada fase do ciclo de vida tem correspondência com operações de tratamento definidas na LGPD.

A fase coleta refere-se à **coleta**, produção e recepção de dados pessoais independente do meio utilizado (documento em papel, documento eletrônico, sistema de informação etc.).

A **retenção** corresponde ao arquivamento ou armazenamento de dados pessoais independente do meio utilizado (documento em papel, documento eletrônico, banco de dados, arquivo de aço etc.).

O **processamento** é qualquer operação que envolva classificação, utilização, reprodução, processamento, avaliação ou controle da informação e extração e modificação de dados pessoais retidos pelo controlador.

O **compartilhamento**, por sua vez, envolve qualquer operação de transmissão, distribuição, comunicação, transferência, difusão e uso compartilhamento de dados pessoais.

Por fim, a **eliminação** é qualquer operação que visa excluir um dado ou conjunto de dados pessoais armazenados em banco de dados, em virtude do tratamento da LGPD. Quando se tratar da eliminação de documentos arquivísticos, devem ser levadas em consideração as recomendações constantes nesse manual.

A figura a seguir sintetiza as fases do ciclo de vida do tratamento de dados pessoais:

Coleta: obtenção, recepção ou produção de dados pessoais independente do meio utilizado (documento em papel, documento eletrônico, sistema de informação etc.).

Retenção: arquivamento ou armazenamento de dados pessoais independente do meio utilizado (documento em papel, documento eletrônico, banco de dados, arquivo de aço etc.).

Processamento: qualquer operação que envolva classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação de dados pessoais.

Compartilhamento: qualquer operação que envolva transmissão, distribuição, comunicação, transferência, difusão e compartilhamento de dados pessoais.

Eliminação: qualquer operação que visa apagar ou eliminar dados pessoais. Esta fase também contempla descarte dos ativos organizacionais nos casos necessários.

A operação de tratamento “acesso” (LGPD, art. 5º, X) está presente em todas as fases do ciclo de vida dos dados pessoais, pois de alguma forma temos que realizar acesso ao dado pessoal para viabilizar sua coleta, retenção, processamento, compartilhamento ou eliminação.

Essas operações de tratamento de dados pessoais se cruzam com os procedimentos e operações da gestão de documentos, nas diversas fases do ciclo de vida do documento. Quando os dados pessoais integrarem documentos arquivísticos, os procedimentos e operações da gestão de documentos

também precisam ser efetivados conjuntamente, como por exemplo, produção, recebimento, tramitação, arquivamento, classificação, indexação, atribuição de restrição de acesso, avaliação, transferência, acesso e eliminação. Alguns desses procedimentos e operações da gestão de documentos, apesar de serem referidos pelo mesmo termo, tem entendimento distinto daquele utilizado no contexto do tratamento de dados pessoais, e cada um deve ser entendido e realizado em conformidade com seu contexto.

2.8.1.2 Gestão de documentos

No contexto da gestão de documentos, o ciclo de vida dos documentos de arquivo compreende três fases, a saber: **produção, utilização e destinação final** (eliminação ou guarda permanente). Em cada uma dessas fases são realizados os procedimentos e operações de gestão de documentos apresentadas a seguir.

Produção: operações referentes à elaboração de documentos em razão da execução das atividades de um órgão ou entidade.

Utilização (uso e manutenção): operações referentes ao fluxo percorrido pelos documentos para o cumprimento de sua função administrativa, assim como de sua guarda, após cessar o seu trâmite.

Destinação final: operações referentes ao ato de decidir quais documentos devem ser eliminados (mediante autorização, conforme legislação vigente), bem como quais documentos devem ser mantidos por razões administrativas, legais ou fiscais. Para tal, envolve as atividades de análise, seleção e fixação de prazos de guarda dos documentos.

Relacionamento das fases do ciclo de vida dos documentos de arquivo X procedimentos e operações de gestão de documentos.

DOCUMENTOS DE ARQUIVO	
Documentos de arquivo fase do ciclo de vida dos documentos de arquivo	Operações de tratamento na gestão de documentos (independentemente do suporte material e da entidade produtora) – Lei nº 8.159/1991 e norma ABNT NBR ISO 15489:2018

Produção	Elaboração, recebimento, registro, classificação, indexação e atribuição de restrição de acesso
Utilização (uso e manutenção)	Tramitação, controle, arquivamento, transferência para guarda intermediária, acesso e empréstimo
Destinação final	Avaliação, seleção, eliminação e recolhimento para guarda permanente

2.8.1.3 Ativos organizacionais

É importante identificar quais ativos organizacionais estão envolvidos em cada fase do ciclo de vida do tratamento dos dados pessoais. Os **principais ativos** são: **bases de dados, documentos, equipamentos, locais físicos, pessoas, sistemas e unidades organizacionais**.

A seguir, são apresentadas definições para os ativos envolvidos no ciclo de vida do tratamento dos dados pessoais.

Base de dados: é uma coleção de dados logicamente relacionados, com algum significado. Uma base de dados é projetada, construída e preenchida (instanciada) com dados para um propósito específico.

Documento: unidade de registro de informações, qualquer que seja o suporte e formato (Arquivo Nacional, 2005).

Equipamento: objeto ou conjunto de objetos necessário para o exercício de uma atividade ou de uma função.

Local físico: determinação do lugar no qual pode residir de forma definitiva ou temporária uma informação de identificação pessoal. Por exemplo, uma sala, um arquivo, um prédio, uma mesa etc.

Pessoa: qualquer indivíduo que executa ou participa de alguma 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.

Sistema: qualquer aplicação, software ou solução de TI que esteja envolvida com as fases do ciclo de vida do tratamento dos dados pessoais: coleta, retenção, processamento, compartilhamento e eliminação de dados pessoais.

Unidade organizacional: órgãos e entidades da Administração Pública.

2.8.1.4 Relacionamento do ciclo vida do tratamento dos dados pessoais com ativos organizacionais

Para cada fase do ciclo de tratamento de dados é importante identificar os **ativos organizacionais** que estarão envolvidos.

Na fase de **Coleta (1ª)** deve-se identificar os ativos envolvidos na coleta de dados pessoais. Esses dados podem entrar na Administração por algum **documento**, algum **sistema** hospedado em algum **equipamento** localizado em **local físico** do órgão público. Podem ser coletados pela prestação de algum serviço externo ou serviço prestado pelo próprio órgão público por meio de alguma de suas **unidades organizacionais**.

Na fase de **Retenção (2ª)**, deve-se avaliar os ativos utilizados para armazenar os dados pessoais. Esses dados podem estar armazenados em **bases de dados, documentos, equipamentos ou sistemas**. É preciso considerar também as **unidades organizacionais** responsáveis pelo armazenamento e guarda dos dados, bem como os **locais físicos** onde estão localizados os ativos que armazenam esses dados. Se o armazenamento for em "nuvem", por exemplo, é necessário considerar o serviço de armazenamento contratado e/ou utilizado.

A fase de **Processamento (3ª)** segue a mesma linha de raciocínio das anteriores. Identifica-se os ativos onde são realizados os tratamentos dos dados. O tratamento pode ser realizado em **documento**, pode ser feito por um **sistema** interno ou contratado pelo órgão. É preciso identificar as **pessoas** (papeis organizacionais), **unidade organizacionais e equipamentos** envolvidos nesse tratamento. Onde estão **localizadas fisicamente** essas unidades organizacionais e os equipamentos envolvidos nesse tratamento também são importantes.

Na fase de **Compartilhamento (4ª)** é preciso mapear os ativos envolvidos na distribuição ou divulgação dos dados pessoais para dentro e para fora do órgão público. Quais **sistemas** são usados para transmitir, exibir ou divulgar dados pessoais? Quais **pessoas** são destinatárias dessas informações? Quais **unidades organizacionais**, quais **equipamentos** são usados para tal?

No que se refere à fase de **Eliminação (5ª)**, deve-se avaliar os ativos que armazenam os dados pessoais que possam ser objeto de: solicitação de eliminação de dados a pedido do titular dos dados pessoais; ou descarte nos casos necessários.

Os dados pessoais a serem eliminados podem estar armazenados em ativos relacionados com **bases de dados, documentos, equipamentos ou sistemas**. É necessário considerar também as **unidades organizacionais** responsáveis pelo armazenamento e guarda dos dados que possam ser objeto de eliminação ou descarte, bem como os **locais físicos** onde estão localizados os ativos que contenham dados a serem eliminados ou descartados. Se a eliminação do dado pessoal ou descarte do ativo tiver relação com solução em "nuvem", por exemplo, é preciso considerar o serviço de armazenamento contratado ou utilizado.

Quando os dados pessoais estiverem contidos em documentos arquivísticos, qualquer que seja o suporte ou formato, esses dados poderão ser tratados no contexto da LGPD, mas os documentos

arquivísticos propriamente ditos, deverão seguir os procedimentos definidos pela gestão de documentos.

O ideal é que se estabeleçam ações de **mapeamento e análise dos processos organizacionais**, tendo em vista que, desta forma, o órgão conseguirá identificar de maneira mais eficaz os ativos descritos anteriormente.

Uma vez identificados os ativos, é necessário analisá-los para verificar quais medidas técnicas de segurança estão efetivamente implementadas nesses ativos, com vistas a prover a adequada proteção aos dados pessoais de que trata a LGPD.

2.9 INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

A LGPD exige que quaisquer incidentes ou violações relacionadas a dados pessoais devam ser informados para a Autoridade Nacional de Proteção de Dados - ANPD e aos titulares dos dados, sejam eles incidentes reais ou que potencialmente possam ser afetados por violação de qualquer tipo, cabendo a Administração Municipal gerenciar as notificações, comunicações, crises, evidências, reinvindicações e reclamações.

O **incidente de segurança** com dados pessoais é conceituado como sendo qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

Sempre que o incidente de segurança tiver potencial de acarretar um risco ou dano relevante aos titulares afetados, deve a Administração Municipal comunicar o incidente aos titulares de dado.

Pode-se extrair da lei que a probabilidade de risco ou dano relevante para os titulares será maior sempre que o incidente envolver dados sensíveis ou de indivíduos em situação de vulnerabilidade, incluindo crianças e adolescentes, ou tiver o potencial de ocasionar danos materiais ou morais, tais como discriminação, violação do direito à imagem e à reputação, fraudes financeiras e roubo de identidade.

Da mesma forma, deve-se considerar o volume de dados envolvido, o quantitativo de indivíduos afetados, a boa-fé e as intenções dos terceiros que tiveram acesso aos dados após o incidente e a facilidade de identificação dos titulares por terceiros não autorizados.

2.9.1. O QUE FAZER CASO OCORRA UM INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

1- Deve a Administração Municipal avaliar internamente o incidente (natureza, categoria e quantidade de titulares de dados afetados, categoria e quantidade dos dados afetados, consequências concretas e prováveis). **A ANPD disponibiliza formulário de avaliação em seu sítio eletrônico.**

2- O encarregado de dados pessoais do Município deve ser comunicado (art. 5º, VIII da LGPD);

3- A ANPD e o titular de dados devem ser comunicados, em caso de risco ou dano relevante aos titulares (art. 48 da LGPD);

4- A Administração Municipal deve elaborar documentação com a avaliação interna do incidente, medidas tomadas e análise de risco, para fins de cumprimento do princípio de responsabilização e prestação de contas (art. 6º, X da LGPD).

2.9.2. QUEM DEVE FAZER A COMUNICAÇÃO DO INCIDENTE

O art. 48 da LGPD determina que é obrigação do controlador comunicar à ANPD e ao titular dos dados pessoais a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

Recomenda-se que a Administração Municipal adote posição de cautela, de modo que a comunicação seja efetuada mesmo nos casos em que houver dúvida sobre a relevância dos riscos e danos envolvidos.

2.9.3. O QUE DEVE SER COMUNICADO À ANPD

As informações devem ser claras e concisas. Além do que prescreve o § 1º do artigo 48 da LGPD, a comunicação deve conter as seguintes informações, **disponíveis no formulário de comunicação de incidentes de segurança com dados pessoais da ANPD disponibilizado em seu sítio eletrônico.**

2.9.3.1 Identificação e dados de contato

- Da entidade ou pessoa responsável pelo tratamento.
- Do encarregado de dados ou outra pessoa de contato.
- Indicação se a notificação é completa ou parcial. Em caso de comunicação parcial, indicar que se trata de uma comunicação preliminar ou de uma comunicação complementar.

2.9.3.2 Informações sobre o incidente de segurança

- Data e hora da detecção.
- Data e hora do incidente e sua duração.
- Circunstâncias em que ocorreu a violação de segurança de dados pessoais, por exemplo, perda, roubo, cópia, vazamento, dentre outros.
- Descrição dos dados pessoais e informações afetadas, como natureza e conteúdo dos dados pessoais, categoria e quantidade de dados e de titulares afetados
- Resumo do incidente de segurança com dados pessoais, com indicação da localização física e meio de armazenamento.
- Possíveis consequências e efeitos negativos sobre os titulares dos dados afetados.
- Medidas de segurança, técnicas e administrativas preventivas tomadas pelo controlador de acordo com a LGPD.
- Resumo das medidas implementadas até o momento para controlar os possíveis danos.

- Outras informações úteis às pessoas afetadas para proteger seus dados ou prevenir possíveis danos.

Caso não seja possível fornecer todas as informações no momento da comunicação preliminar, informações adicionais poderão ser fornecidas posteriormente.

No momento da comunicação preliminar deverá ser informado à ANPD se serão fornecidas mais informações posteriormente, bem como quais meios estão sendo utilizados para obtê-las. A ANPD também poderá requerer informações adicionais a qualquer momento.

2.9.3.3 Prazos

A LGPD determina que a comunicação do incidente de segurança seja feita em prazo razoável (art. 48, §1º), conforme orientações específicas da ANPD. Embora não tenha havido regulamentação nesse sentido, a realização da comunicação demonstrará transparência e boa-fé e será considerada em eventual fiscalização.

2.9.3.4 Forma de comunicar à ANPD

Preenchendo formulário eletrônico disponível no sítio eletrônico da ANPD e enviando por meio de Peticionamento Eletrônico (“Usuário Externo”).

3. BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO

3.1 PRIVACIDADE DESDE A CONCEPÇÃO E POR PADRÃO

3.1.1 PRIVACIDADE DESDE A CONCEPÇÃO

Os agentes de tratamento ou qualquer outra pessoa que participe das fases do ciclo de vida do tratamento de dados pessoais são obrigados a assegurar a segurança da informação para proteção dos dados pessoais, pois ambas estão relacionadas.

Segundo o previsto pelo caput do art. 46 da LGPD, a proteção dos dados pessoais é alcançada por meio de **medidas de segurança**, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito:

> *Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.*
>
> *§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados: a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia,*

> *especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.*
>
> *§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.*

O art. 46, §2º menciona que as medidas de segurança, técnicas e administrativas para proteção de dados pessoais deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução. Isso apresenta um conceito fundamental para a proteção da privacidade dos dados pessoais denominado **privacidade desde a concepção**.

O conceito de privacidade desde a concepção significa que a privacidade e a proteção de dados devem ser consideradas desde a concepção e durante todo o ciclo de vida do projeto, sistema, serviço, produto ou processo. Tal privacidade pode ser alcançada por meio da aplicação de sete princípios fundamentais destacados a seguir.

3.1.1.1 Proativo, e não reativo; preventivo, e não corretivo

A abordagem de privacidade desde a concepção é caracterizada por medidas proativas e não reativas. Ou seja, essa abordagem antecipa e evita eventos invasivos de privacidade antes que eles aconteçam. Desse modo, não espera que riscos de privacidade se materializem nem ofereçam soluções para as infrações de privacidade após a ocorrência, mas visa impedir que eles ocorram. Em resumo, a Privacidade desde a Concepção vem antes do fato, não depois.

Se aplicada a tecnologias da informação, práticas organizacionais, projeto físico ou em rede de ecossistemas de informação, a privacidade desde a concepção começa com um reconhecimento explícito do valor e dos benefícios de adoção de práticas de privacidade fortes, de forma precoce e consistente. Por exemplo, prevenindo a ocorrência de violações de dados, internas ou externas. Isso implica:

- *um compromisso claro da alta administração em definir e fazer cumprir altos padrões de privacidade;*
- *um compromisso de privacidade comprovadamente compartilhado pelas comunidades de usuários e pelas partes interessadas e inserido em uma cultura de melhoria contínua; e*
- *métodos estabelecidos para reconhecer projetos de privacidade inadequados, antecipar práticas inadequadas de privacidade e corrigir quaisquer impactos negativos, muito antes de ocorrerem.*

3.1.1.2 Privacidade incorporada ao projeto (design)

A privacidade deve estar incorporada ao projeto e arquitetura dos sistemas de Tecnologia da Informação. Isto significa que não deve ser considerada como complemento adicional, após o sistema, projeto ou serviço já estar em implementação ou em execução. O resultado é que a privacidade se torna um componente essencial da funcionalidade principal que está sendo entregue. A privacidade é parte integrante do sistema, sem diminuir a funcionalidade.

A privacidade deve ser incorporada às tecnologias, operações e arquiteturas de informação de maneira holística, integrativa e criativa:

- *holística significa que contextos adicionais mais amplos devem sempre ser considerados;*
- *integrativa indica que todas as partes interessadas devem ser consultadas; e*
- *criativa, pois incorporar privacidade às vezes significa reinventar as escolhas atuais quando as alternativas forem inaceitáveis.*

Para alcançar esse objetivo, deve-se adotar uma abordagem sistemática apoiada em padrões e frameworks reconhecidos, os quais necessitam ser revistos e passíveis de auditorias externas. Todas as práticas de informação equitativa precisam ser aplicadas com igual rigor a cada etapa do projeto e da operação. O impacto do uso, configuração incorreta ou erros relativos à tecnologia, à operação ou à arquitetura de informações sobre a privacidade devem ser comprovadamente minimizados.

Por isso, avaliações de impacto e risco na privacidade devem ser realizadas e publicadas, documentando claramente os riscos à privacidade e todas as medidas tomadas para mitigá-los.

3.1.1.3 Funcionalidade total

A privacidade desde a concepção não envolve simplesmente a formalização de declarações e compromissos de privacidade. Refere-se a satisfazer todos os objetivos do projeto, não apenas os objetivos de privacidade. A privacidade desde a concepção é habilitadora duplamente em natureza, permitindo funcionalidade total com resultados reais e práticos.

Ao incorporar privacidade em uma determinada tecnologia, processo ou sistema, isso é realizado de uma forma que não comprometa a plena funcionalidade e permita que todas as exigências do projeto sejam atendidas.

A questão da privacidade é frequentemente vista como de nenhuma ou baixa relevância e que compete com a objetividade do projeto, com as capacidades técnicas de um produto ou serviço e com outros interesses das partes envolvidas. A privacidade desde a concepção visa justamente contrapor essa visão, pois objetiva satisfazer todos os objetivos da instituição, e não somente os de privacidade. Evitando a pretensão de dicotomias falsas, como privacidade X segurança, a privacidade desde a concepção demonstra que é possível — e mais desejável — ter ambos.

3.1.1.4 Segurança e proteção de ponta a ponta durante o ciclo de vida de tratamento dos dados

Por ser incorporado ao sistema antes de o primeiro elemento de informação ser coletado, a privacidade desde a concepção estende-se por todo o ciclo de tratamento dos dados envolvidos no projeto, sistema ou serviço. Medidas fortes de segurança são essenciais para a privacidade, do início ao fim.

A privacidade deve ser protegida continuamente em todo o domínio e ao longo do ciclo de vida do tratamento dos dados em questão. Não deve haver lacunas na proteção ou na prestação de contas.

O princípio “segurança” tem relevância especial porque, em sua essência, sem segurança forte, não pode haver privacidade.

As instituições devem assumir a responsabilidade pela segurança dos dados pessoais, geralmente proporcional ao grau de sensibilidade, durante todo o ciclo de tratamento, consistente com os padrões que foram definidos por organismos reconhecidos de desenvolvimento de padrões.

Os padrões de segurança aplicados devem garantir a confidencialidade, integridade e disponibilidade dos dados pessoais durante todo o seu ciclo de tratamento, incluindo, entre outros, métodos de destruição segura, criptografia apropriada, e métodos fortes de controle de acesso e registro.

Na LGPD, a segurança é um princípio a ser observado no tratamento de dados pessoais, destacado pelo art. 6º, inciso VII:

> *Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:*
>
> *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;*

3.1.1.5 Visibilidade e Transparência

A privacidade desde a concepção objetiva garantir a todos os interessados que, independentemente da prática ou tecnologia comercial envolvida, está de fato operando de acordo com as premissas e objetivos declarados, os quais devem ser objeto de verificação independente. Esse cenário pode ser sintetizado pelo seguinte lema: confie, mas verifique.

Visibilidade e transparência são essenciais para estabelecer responsabilidade e confiança. A avaliação independente deste princípio fundamental deve concentrar-se, especialmente, sobre os seguintes aspectos:

- **Responsabilização** - A coleta de dados pessoais implica um dever de cuidar de sua proteção. A responsabilidade por todas as políticas e procedimentos relacionados à privacidade deve ser documentada e comunicada conforme apropriado e atribuído a um indivíduo especificado. E ao transferir dados pessoais para terceiros, medidas equivalentes de proteção à privacidade devem ser asseguradas por contratos ou outros tipos de acordos formais.
- **Abertura** - Abertura e transparência são fundamentais para a prestação de contas. Informações sobre as políticas e práticas relacionadas ao gerenciamento de dados pessoais devem estar prontamente disponíveis para consulta dos titulares de dados. Mecanismos de reclamação e reparação dos dados pessoais devem ser estabelecidos e comunicados para os titulares dos dados.

- **Conformidade** - As etapas necessárias para monitorar, avaliar e verificar a conformidade com as políticas e procedimentos de privacidade devem ser estabelecidas.

A responsabilização, abertura e transparência estão expressas na LGPD pelos seguintes princípios destacados no art. 6º:

> *Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...]*
>
> *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;*
>
> *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; e*
>
> *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.*

3.1.1.6 Respeito pela privacidade do usuário

Acima de tudo, a privacidade desde a concepção exige que as instituições respeitem os direitos dos titulares dos dados pessoais. Isso é alcançado por meio de medidas como padrões fortes de privacidade, avisos apropriados e interfaces amigáveis que empoderem o titular dos dados.

Os melhores resultados da privacidade desde a concepção, geralmente, são aqueles projetados de acordo com os interesses e necessidades dos titulares dos dados pessoais, que têm o maior interesse em gerenciar seus próprios dados.

Empoderar os titulares de dados a desempenhar um papel ativo no gerenciamento de seus próprios dados pessoais pode ser o meio mais eficaz de verificação contra abusos de e uso indevido. O respeito à privacidade do titular dos dados pessoais é suportado pelos seguintes aspectos:

- **Consentimento ou hipótese de tratamento prevista em lei** - é necessário o consentimento livre e específico do titular dos dados para a coleta, uso ou divulgação de dados pessoais, exceto onde permitido por lei. As hipóteses de tratamento de dados pessoais e dados pessoais sensíveis estão preconizadas pelos arts. 7º e 11 da LGPD.
- **Precisão** - os dados pessoais devem ser precisos, completos e atualizados, conforme necessário para cumprir finalidades especificadas.
- **Acesso** - os titulares devem ter acesso aos seus dados pessoais e ser informados do uso e divulgação de tais dados. Os mencionados titulares devem ser capazes de contestar a precisão e integridade dos dados e alterá-los conforme apropriado.
- **Conformidade** - as instituições devem estabelecer mecanismos de reclamação e reparação e comunicar informações sobre eles ao público.

3.1.2 PRIVACIDADE POR PADRÃO

Os agentes de tratamento devem implementar medidas adequadas para garantir que, por padrão, apenas serão processados os dados pessoais necessários para cumprimento da(s) finalidade(s) específica(s) definida(s) pela instituição que desempenha o papel de controlador dos dados pessoais.

Essa obrigação de implementação significa que a instituição deve limitar a quantidade de dados pessoais coletados, extensão do tratamento, período de armazenamento e acessibilidade ao mínimo necessário para a concretização da finalidade do tratamento dos dados pessoais. Essa medida deve garantir, por exemplo, que nem todos os usuários dos agentes de tratamento tenham acesso ilimitado e por tempo indeterminado aos dados pessoais tratados pela instituição.

Na LGPD, a **Privacidade por Padrão** está diretamente relacionada ao princípio da necessidade, expresso pelo art. 6º, inciso III:

> *Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:*
>
> ***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.***

A privacidade por padrão é obtida por meio da adoção das seguintes práticas:

- **Especificação da finalidade** - os objetivos para os quais os dados pessoais são coletados, usados, retidos e divulgados devem ser comunicados ao titular dos dados antes ou no momento em que as informações são coletadas. As finalidades especificadas devem ser claras, limitadas e relevantes em relação ao que se pretende ao tratar os dados pessoais.
- **Limitação da coleta** - a coleta de dados pessoais deve ser legal e limitada ao necessário para os fins especificados.
- **Minimização dos dados** - a coleta dos dados pessoais que possa identificar individualmente o titular de dados deve obter o mínimo necessário de informações pessoais. A concepção de programas, tecnologias e sistemas de informação e comunicação deve começar com interações e transações não identificáveis, como padrão. Qualquer vinculação de dados pessoais deve ser minimizada. A possibilidade de informações serem usadas para identificar o titular de dados deve ser minimizada.
- **Limitação de uso, retenção e divulgação** - o uso, retenção e divulgação de dados pessoais devem limitar-se às finalidades relevantes identificadas para o titular de dados, para as quais ele consentiu ou é exigido ou permitido por lei. Os dados pessoais serão retidos apenas pelo tempo necessário para cumprir as finalidades declaradas e depois eliminados com segurança.

Quando a necessidade ou uso de dados pessoais não forem claros, deve haver uma presunção de privacidade e o princípio da precaução deve ser aplicado. Dessa forma, as configurações padrão devem ser as de maior proteção à privacidade.

3.1.2.1 Privacidade deve ser o padrão dos sistemas de TI

A privacidade por padrão procura oferecer o máximo grau de privacidade, garantindo que os dados pessoais sejam protegidos automaticamente em qualquer sistema de Tecnologia da Informação. É uma forma de evitar que qualquer ação seja necessária por parte do titular dos dados pessoais para proteger a sua privacidade, pois ela já estará embutida no sistema, por padrão.

Com relação aos documentos arquivísticos, a privacidade precisa ser resguardada de acordo com legislação vigente, seguindo os procedimentos de gestão de documentos. Os sistemas que mantêm e gerenciam documentos arquivísticos devem ter controles para garantir esse resguardo.

3.2 FRAMEWORKS DE SEGURANÇA E APLICAÇÕES WEB

A Administração Municipal deve adotar controles de segurança ao armazenar as informações para garantir que os dados estejam em segurança, promovendo mecanismos que garantam a proteção de dados pessoais e de dados pessoais sensível.

Conforme já dito, a LGPD exige que quaisquer incidentes ou violações relacionadas a dados pessoais devam ser informados para a Autoridade Nacional de Proteção de Dados - ANPD e aos titulares dos dados, sejam eles incidentes reais ou que potencialmente possam ser afetados por violação de qualquer tipo, cabendo a Administração Municipal gerenciar as notificações, comunicações, crises, evidências, reinvindicações e reclamações.

Assim sendo, a manutenção de padrões de frameworks e controles de segurança da informação, contribuem para a identificação, o acompanhamento e o preenchimento das lacunas de segurança presentes nos órgãos públicos, sendo um conjunto de ações priorizadas que atuam coletivamente na defesa de sistemas e infraestrutura, por meio das melhores práticas para mitigar os tipos mais comuns de ataques.

O processo de proteção de dados pessoais deve estar alinhado com os procedimentos operacionais, segurança da informação, normas de governança, definindo as finalidades, limitações e controles, utilizando-se da abordagem de desenvolvimento de software e hardware que visa minimizar as vulnerabilidades dos sistemas e reduzir a superfície de ataque em todas as fases do ciclo de vida de desenvolvimento de sistemas com privacidade desde a concepção.

O Guia de Segurança em Aplicações Web estrutura-se basicamente em requisitos gerais e requisitos específicos:

3.2.1 Requisitos Gerais

- Gerenciamento de ambiente;

- Proteção do perímetro da aplicação.

3.2.2 Requisitos Específicos

- Validação dos dados de entrada;
- Codificação de dados de saída;
- Autenticação e gerenciamento de credenciais;
- Gerenciamento de sessões;
- Controle de acesso;
- Criptografia;
- Tratamento de erros e logs;
- Proteção de dados;
- Segurança nas comunicações;
- Configuração do sistema;
- Segurança em Banco de Dados;
- Gerenciamento de Arquivos;
- Gerenciamento de memória;
- Práticas Gerais de Codificação.

As aplicações devem proteger os dados tratados pela Administração Pública, de forma que o acesso às suas informações pessoais se restrinja ao mínimo necessário (política de privilégio mínimo, restringindo aos usuários apenas às funcionalidades, dados e informações do sistema que são necessárias para executarem suas tarefas).

Deve-se ainda adotar controles de segurança ao armazenar as informações para garantir a segurança das informações, tais como a criptografia (criptografar informações altamente sensíveis quando armazenadas – como dados de verificação de autenticação – mesmo que estejam no lado servidor, usando sempre algoritmos conhecidos, padronizados e bem testados).

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Presidência da República. Casa Civil. Decreto Nº 9.637, de 26 de dezembro de 2018. Institui a Política de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm>. Acesso em: 09 jun. 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#art1>. Acesso em: 09 jun. 2022.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-_2014/2014/lei/l12965.htm>. Acesso em: 09 jun. 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>. Acesso em: 09 jun. 2022.

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: 09 jun. 2022.

GARCIA, Lara Rocha. Lei Geral de Proteção de Dados Pessoais (LGPD): guia de implementação. São Paulo: Blucher, 2020.

PINHEIRO, Patrícia Peck. Proteção de dados pessoais: comentários à Lei nº 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva Educação, 2020.

POZZO, Augusto Neves; MARTINS, Ricardo Marcondes (Coord.). LGPD e administração pública: uma análise ampla dos impactos. São Paulo: Thomson Reuters Brasil, 2020.

SERPRO. Glossário LGPD Disponível em: <https://www.serpro.gov.br/lgpd/menu/a-lgpd/glossario-lgpd>. Acesso em: 09 jun. 2022.

ZENKNER, Marcelo; CASTRO, Rodrigo Pironti Aguirre de (Coord.). Compliance no setor público. 1. Reimpr. Belo Horizonte: Fórum, 2020.