RECIFE
PREFEITURA

CARTILHA LGPD

CONHECENDO A LEI GERAL DE PROTEÇÃO DE DADOS

2022

R484c Ribeiro, Adriano Aquino et al

Cartilha LGPD : conhecendo a Lei Geral de Proteção de Dados./ Adriano Aquino Ribeiro. Carmen Sofia C. do Nascimento. Lucas Carneiro Pessoa Canto. Recife: PCR, 2022.

28 p. il.:

1. Lei Geral de Proteção de Dados 2. LGPD - Princípios 3. Hipóteses de tratamento 4. Penalidades I. Título.

CDU: 34:004(094.4)

PREFEITURA DA CIDADE DO RECIFE

JOÃO HENRIQUE DE ANDRADE LIMA CAMPOS
Prefeito

ISABELLA MENEZES DE ROLDÃO FIORENZANO
Vice-prefeita

JOSÉ RICARDO WANDERLEY DANTAS DE OLIVEIRA
Controlador-Geral do Município

MARCO AURÉLIO GOMES DE ARAÚJO
Secretário Executivo

LUCIANA DE MACEDO MACHADO LAGES
Gerente Geral de Controle Social e Orientação

LUCAS CARNEIRO PESSOA CANTO
Gerente de Transparência e Orientação

CARMEN SOFIA CARVALHO DO NASCIMENTO
Chefe da Divisão de Orientação

Autores
ADRIANO AQUINO RIBEIRO
CARMEN SOFIA CARVALHO DO NASCIMENTO
LUCAS CARNEIRO PESSOA CANTO

Controladoria-Geral do Município
Av. Cais do Apolo, 925, 14º andar,
Bairro do Recife, Recife/PE
Telefone: (081) 3355-8457

Gerência de Transparência e Orientação
cgmorienta@recife.pe.gov.br
Telefone: (081) 3355-9011

1ª edição

Sumário

Introdução

O assunto sobre proteção de dados já é mundialmente discutido há algum tempo. Isso porque os dados têm se mostrado cada vez mais relevantes do ponto de vista econômico. Logo, possuindo valor, geram bastante interesse na exploração, comercialização, e possível uso indevido. Diante desse cenário, faz-se necessária a proteção contra abusos por quem tenha acesso a esses dados.

No Brasil, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), sancionada em 14 de agosto de 2018, foi inspirada pelo Regulamento de Proteção de Dados da União Europeia (GDPR - General Data Protection Regulation). A referida lei entrou em vigor dia 18 de setembro de 2020, com vigência a partir de agosto de 2021 quanto às sanções administrativas. A proteção de dados tem natureza jurídica de direito e garantia fundamental, tendo em vista o inciso XII do art. 5º da Constituição Federal.

Com a utilização dos meios digitais, o trânsito de dados alcançou basicamente todas as áreas da vida cotidiana, desde a compra de um medicamento em uma farmácia, aos gostos e preferências explicitadas em redes sociais, até as informações sobre a saúde, patrimônio, família, amigos, locais de lazer, entre outrosc. Essas informações, processadas por computadores de alta tecnologia, inteligências artificiais e algoritmos, mostram-se como um ativo valiosíssimo.

Importante lembrar a quem pertencem esses dados. Embora eles possam estar em computadores, nuvens, e-mails, redes sociais, arquivos físicos, tanto em empresas privadas quanto no setor público, esses dados pertencem à pessoa a qual se referem. Ela é a titular dos dados. Esse conceito inicial é a base de toda a discussão sobre o assunto de proteção de dados, pois o titular tem o direito de saber como, onde, para quê, e com a autorização de quem, seus dados estão sendo usados.

Diante desse cenário, a Controladoria-Geral do Município do Recife - CGM, no uso de suas atribuições, apresenta esta cartilha para que os órgãos e entidades do Município do Recife tenham acesso introdutório ao assunto, assim como possam iniciar ou aperfeiçoar o processo de adequação à Lei Geral de Proteção de Dados, fomentando a cultura de proteção de dados na Administração Pública Municipal.

Ressaltamos que este material não encerra as orientações sobre o assunto, sendo necessário o atendimento a todos os requisitos da LGPD. Destacamos que não existe um plano de adequação padrão aplicável a todas as organizações.

Desse modo, a Gerência de Transparência e Orientação da CGM fica à disposição para auxiliar em todo o processo de adequação e pode ser utilizada como canal de comunicação para dúvidas, debates e sugestões sobre o tema, através do e-mail **cgmorienta@recife.pe.gov.br**.

Conceitos iniciais

A LGPD traz alguns termos que ainda não estão completamente assimilados pela maioria das pessoas, por serem relativamente novos no cotidiano do servidor público. Torna-se necessário, portanto, apresentar alguns desses conceitos para familiarização com o assunto:

Dados Pessoais - São informações relacionadas à pessoa natural identificada ou identificável, independentemente de ser uma informação privada, de conhecimento público ou sobre a sua vida profissional. Nesse contexto, são considerados dados pessoais informações como nome, data de nascimento, filiação, apelido, CPF, RG, imagem, endereço residencial, endereço de e-mail, endereço IP, hábitos de navegação, interesses e preferências, posição geolocacional, formulários cadastrais, números de documentos, entre outros.

Dados Sensíveis - São dados pessoais que estão sujeitos a cuidados ainda mais específicos. São exemplos de dados pessoais sensíveis: religião, opinião política ou filosófica, origem racial ou étnica, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, informação referente à saúde ou à vida sexual, genética ou biometria.

Dado Anonimizado - Dado relativo a uma pessoa que passou por etapas de tratamento, através da utilização de meios técnicos razoáveis e disponíveis, com o objetivo de não ser possível identificar quem era a pessoa titular do dado. O dado anonimizado é aquele que perde a possibilidade de ser associado a uma pessoa, ou seja, é o dado relativo a titular que não possa ser identificado.

Titular - É o dono do dado, a própria pessoa ao qual este dado se refere. Pode ser o contribuinte de IPTU, a criança matriculada na escola municipal, o servidor público, o prestador de serviço contratado pela Administração Pública, o requerente que solicita informações através do Portal da Transparência, o próprio manifestante que apresenta reclamação na Ouvidoria, o munícipe que utiliza os serviços do posto médico de saúde, entre outros.

Controlador - Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, sendo o responsável pela definição das medidas de segurança que serão aplicadas no tratamento desses dados.

Operador - Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome e segundo as orientações do controlador.

Encarregado - Pessoa indicada pelo controlador para atuar como canal de comunicação entre este, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). É recomendável que o encarregado tenha conhecimentos de governança, compliance, direito, segurança da informação, ferramentas e processos de segurança, possuindo habilidades de gerenciamento e capacidade de interação com a equipe interna da entidade controladora, terceiros, titulares de dados e órgãos oficiais.

Tratamento - Qualquer operação efetuada sobre dados pessoais, por meios manuais ou automatizados, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. Ou seja, quase tudo que se faz com os dados é considerado tratamento.

Agentes de tratamento - São justamente as figuras do controlador e do operador.

ANPD - Autoridade Nacional de Proteção de Dados - órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento dos dispositivos da LGPD. Responsável, também, pela aplicação de sanções previstas na Lei.

Perguntas e respostas:

Inicialmente, a leitura da **Lei Geral de Proteção de Dados, Lei nº 13.709/2018**, é extremamente importante e necessária para se iniciar um estudo ou discussão sobre o assunto. Após a leitura inicial, podem surgir dúvidas introdutórias, conceituais e de aplicabilidade prática. Isso acontece com o estudo de qualquer área, principalmente quando ocorrem grandes modificações sobre o assunto.

Visando a facilitar a compreensão do assunto de proteção de dados pessoais e trazendo explicações voltadas ao cotidiano do servidor, apresentam-se algumas dessas dúvidas frequentes:

1) O que é tratamento de dados? A Prefeitura da Cidade do Recife - PCR realiza esse procedimento?

Praticamente todo uso/acesso a dados pode ser considerado tratamento, incluindo coleta, registro, armazenamento, utilização, análise, divulgação ou eliminação.
A própria LGPD traz, em seus artigos iniciais, alguns conceitos, entre eles, o de tratamento, que consiste em "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração."

A PCR realiza tratamento de dados no seu cotidiano, através dos servidores nas mais diversas áreas, seja com dados de servidores, fornecedores, terceirizados ou da população em geral.

Exemplos:

- Quando o servidor ***produz*** um documento para publicação no Diário Oficial do Município, ***utilizando*** nome, CPF (mesmo que pseudonimizado), período de licença ou férias, entre outros;
- Quando um órgão ou entidade acessa, em algum outro banco de dados, informações sobre o cidadão;
- Quando o servidor de uma escola municipal coleta dados do aluno a ser matriculado, arquiva cópias de documentos e processa essa matrícula perante a Secretaria de Educação.

2) Quem é o titular dos dados pessoais?

O titular, dono ou proprietário dos dados pessoais é a própria pessoa a qual o dado se relaciona. A Lei fala em pessoa natural, ou seja, não inclui pessoas jurídicas (cuja proteção se encontra em outras leis). Nesse sentido, toda a população, usuários dos serviços públicos, servidores públicos, fornecedores/contratados (apenas se forem pessoas físicas) são considerados titulares. Crianças e adolescentes também estão incluídos, sendo representados pelos responsáveis legais no exercício dos direitos relativos à proteção de dados pessoais. Não importa a nacionalidade, nem se a moradia é ou não no Brasil. Até mesmo o estrangeiro de passagem pelo país é titular dos seus dados pessoais e recebe a proteção da LGPD.

Exemplos:

» O cidadão "José" é o titular dos seus dados pessoais (nome, estado civil, CPF, imagem, endereço, título de eleitor, identidade civil, tipo sanguíneo, histórico de saúde, número de IP, e-mail, data de nascimento, dados sobre compras, entre outros);

» O contratado (pessoa física) é o titular dos seus dados constantes no contrato com a Administração Pública.

3) Quais são os direitos do titular dos dados pessoais?

A LGPD tem como principais objetivos proteger os direitos fundamentais de privacidade, liberdade, informação, comunicação e opinião, assim como a dignidade e o exercício da cidadania dos indivíduos. Estão elencados na Lei os seguintes direitos:

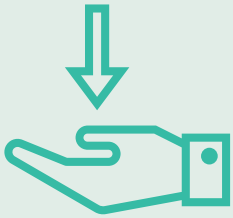
- acesso facilitado às informações sobre o tratamento de seus dados;
- disponibilização das informações de forma clara, adequada e ostensiva, principalmente no que se refere à confirmação da existência de tratamento e, em caso positivo, sua finalidade, forma, duração;
- correção de dados incompletos, inexatos ou desatualizados;
- anonimização, bloqueio ou eliminação de dados desnecessários;
- portabilidade de seus dados;
- revogação do consentimento/eliminação dos dados;
- informação sobre com quem os dados foram compartilhados;
- informação sobre o poder de não consentir e suas consequências;
- identificação do controlador e o contato de seu encarregado para comunicação;
- direito de petição em relação aos seus dados contra o controlador perante a autoridade nacional.

Embora não estabeleça a LGPD um procedimento específico para o exercício do direito de petição, faz referência expressa ao rito da Lei de Acesso à Informação - Lei Federal nº 12.527/2011, além de outros diplomas legais, sem prejuízo da aplicação do próprio Código de Defesa dos Usuários de Serviços Públicos – Lei Federal n° 13.460/2017.

4) Quais os princípios que devem ser observados no tratamento de dados pessoais?

Durante o tratamento de dados pessoais, devem ser observados, além da boa-fé, os princípios do art. 6º da LGPD. Abaixo, seguem os 10 (dez) princípios elencados na Lei.

Finalidade	I - realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; O titular dos dados precisa ser informado sobre qual o objetivo (propósito) do uso/tratamento de seus dados. Assim, o tratamento não pode ser realizado de forma incompatível com essa finalidade. **Exemplo:** Ao solicitar o e-mail de um cidadão em um pedido de acesso à informação, é necessário que fique claro qual o propósito, que pode ser "encaminhar a resposta da solicitação". Nesse caso, não se pode utilizar o dado solicitado para outra finalidade.
Adequação	II - compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; Trata-se de dar um tratamento ao dado compatível e restrito à finalidade informada ou hipótese legal de tratamento. **Exemplo:** Utilizando-se o exemplo anterior, deve-se verificar se o e-mail solicitado destina-se ao encaminhamento da resposta ao pedido de informação (finalidade informada). Caso seja usado para outra finalidade, o tratamento foi inadequado.



Necessidade	**III - 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;** O tratamento de dados gera, para quem está tratando, uma responsabilidade sobre esse uso, inclusive em casos de vazamento. Dessa forma, deve-se observar a necessidade do tratamento do dado para alcançar a finalidade informada. **Exemplo:** Em um tratamento de dados para produzir uma lista de contatos dos servidores responsáveis pelas gerências de uma secretaria, a divulgação do e-mail institucional atende o princípio da necessidade, já a divulgação do endereço residencial do servidor, não.

Livre acesso	**IV - 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;** O órgão/entidade que está realizando o tratamento de dados deve garantir ao titular o acesso a todos os dados sobre ele, de forma simples e gratuita. Além disso, os seguintes questionamentos devem ser feitos: como os dados são tratados (forma) e por quanto tempo (duração).

Qualidade dos dados	**V - 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;** **Exemplos:** A Secretaria de Educação, através das escolas, precisa garantir/permitir a atualização de dados dos alunos, tal como filiação, em caso de reconhecimento tardio de paternidade; outra situação é a atualização de nome social ou modificação de sobrenomes após casamento/divórcio.

Transparência	**VI - 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;** O titular precisa ter conhecimento sobre os tratamentos realizados com seus dados, inclusive sobre o compartilhamento deles, com outros entes, ou seja, o princípio visa a impedir o uso/compartilhamento dos dados de forma oculta.
Segurança	***VII - 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;*** No tratamento de dados, deve-se buscar procedimentos, meios e tecnologias que garantam a proteção dos dados pessoais contra os acessos por terceiros. **Exemplo:** Criação ou aperfeiçoamento de medidas de proteção contra invasão de sistemas e roubo de informações.
Prevenção	***VIII - adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;*** O princípio da prevenção visa à adoção de medidas de forma antecipada para evitar danos em decorrência do tratamento de dados pessoais. Em outras palavras, deve-se agir antes do problema e não depois. **Exemplo:** Em uma planilha em que conste dados financeiros de servidores (nome, dados bancários e valores de depósitos de remuneração) deve haver um acesso restrito aos servidores envolvidos na atividade, com o objetivo de evitar o vazamento de informações que possam gerar golpes financeiros contra o titular.

Não discriminação

IX - impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

Os dados pessoais jamais podem ser usados para discriminar ou promover abusos contra os seus titulares.

Exemplo: Um cidadão não pode ser impedido de acessar uma repartição pública por ser filiado a um partido político específico. Os dados de filiação partidária (ou quaisquer outros dados sensíveis) não podem ser utilizados de maneira discriminatória.

Responsabilização e prestação de contas

X - 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.

A Administração Pública precisa ter controle das medidas de proteção adotadas, tanto para avaliar a sua eficácia, quanto para prestar contas em caso de responsabilização, na hipótese de incidentes de segurança.

São formas de demonstrar o fiel cumprimento da LGPD: identificar a fundamentação legal que está sendo utilizada para o tratamento do dado; verificar se estão sendo atendidos os princípios da Lei; garantir os direitos dos titulares; e adotar medidas de governança e boas práticas, entre outras ações.

Exemplos: Oferecer treinamento aos servidores que realizam tratamento de dados; utilização de protocolos e sistemas que garantam a segurança dos dados; mapeamento dos processos com a identificação da base legal para tratamento de dados.

5) Quais as hipóteses para tratamento de dados pessoais?

Uma das principais contribuições da LGPD foi a listagem de situações em que é permitido o tratamento de dados pessoais. Trata-se de uma lista de hipóteses previstas no art. 7º (dados pessoais) e art. 11 (dados pessoais sensíveis), sendo esses dispositivos os fundamentos legais que permitem o tratamento.

A Administração Pública deve ter um compromisso com o fiel enquadramento legal quando realizar o tratamento de dados, inclusive em razão do princípio da responsabilização e prestação de contas, uma vez que, pode haver questionamento, por parte do titular do dado, acerca da fundamentação legal utilizada para o tratamento.

São hipóteses legais para o tratamento de dados pessoais:

- **consentimento do titular** - segundo a LGPD, é a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". Esse consentimento pode ser revogado pelo titular a qualquer momento, sendo, portanto, desaconselhável a utilização dessa hipótese autorizativa de forma isolada. Isso porque em caso de revogação do consentimento, haverá a necessidade de excluir o dado de toda a cadeia de tratamento, o que, operacionalmente, pode apresentar muitas dificuldades. Dispensa-se o consentimento quando os dados forem tornados manifestamente públicos pelo titular.

  Base legal: Art. 7º, I (dados pessoais); Art. 11, I (dados pessoais sensíveis).

  Exemplo:

  » Quando da utilização dos serviços do aplicativo para celulares Conecta Recife (por exemplo, para localização de postos de saúde, creches, solicitações de serviços, coleta de lixo, acompanhamento de processos, etc.), o cidadão concorda com os termos da "política de segurança e privacidade" disponível para consulta e download no próprio aplicativo, onde consta o consentimento do titular para tratamento de seus dados;

- **cumprimento de obrigação legal ou regulatória pelo controlador** - existem certos tratamentos de dados que já estão previstos/autorizados em outras leis, a exemplo da Lei de Acesso à Informação - LAI, Lei Federal nº 12.527/2011, e a LGPD previu essa hipótese, até mesmo para não gerar conflitos entre normas.

  Base legal: Art. 7º, II (dados pessoais); Art. 11, II, "a" (dados pessoais sensíveis).

  Exemplo:

  » A PCR tem obrigação de informar à Receita Federal dados sobre os pagamentos de salários dos servidores, para fins de cálculo de imposto de renda. Essa obrigação já é prevista em lei, não sendo necessário o consentimento por parte dos titulares dos dados para que esses dados sejam tratados com essa finalidade;

- **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, por parte da administração pública.**

  Base legal: Art. 7º, III (dados pessoais).

  Exemplo:

  » A execução do Plano Nacional de Operacionalização da Vacinação contra a Covid-19 (política pública de saúde, prevista na Lei nº 14.124/2021) determina que os estabelecimentos de saúde devem informar, diariamente, em sistema disponibilizado pelo Ministério da Saúde, dados sobre a vacinação e eventos adversos.

  Obs.: No tocante a dados pessoais sensíveis, apenas é possível o tratamento e uso compartilhado de dados quando necessários à execução de políticas públicas previstas em leis e regulamentos, restando vedado se o respaldo for exclusivamente contratual (art. 11, II, "b").

- **realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais** - o objetivo é cumprir com a pesquisa desejada, mas, ao mesmo tempo, evitar que os titulares dos dados sejam identificados através de associações entre os dados coletados.

  Base legal: Art. 7º, IV (dados pessoais); Art. 11, II, "c" (dados pessoais sensíveis)

  Exemplo:

  » Um projeto de pesquisa na área de saúde, desenvolvido por uma universidade, que, objetivando verificar possível impacto do uso das redes sociais nas taxas de distúrbios de comportamento, coleta dados pessoais como nome, idade, endereço, grau de instrução, hábitos de navegação, informação referente à saúde ou à vida sexual, etc.

- **execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados** - existem tratamentos de dados que ocorrem antes mesmo de um contrato ser iniciado, porém, são destinados à confecção, elaboração e concretização desse contrato. Nesse caso, não há necessidade de consentimento do titular, já que ele é o próprio interessado em que esses dados sejam tratados para concluir ou executar o contrato do qual ele será parte.

Base legal: Art. 7º, V (dados pessoais).

Exemplo:

» Um contratado por tempo determinado, para atender excepcional interesse público, após processo de seleção, fornece seus dados e cópias de documentos para que seja providenciada a sua contratação. A Administração Pública Municipal realizará tratamento desses dados, com o objetivo de verificar a sua autenticidade, elaborar o contrato e outros procedimentos que sejam necessários, como confecção de crachá, criação de login/senha, etc. Esse tratamento dispensa o consentimento.

- **exercício regular de direitos em processo judicial, administrativo ou arbitral** - na atuação processual (seja perante o Poder Judiciário, ou órgão da Administração Pública ou mesmo em juízo arbitral) pode haver a necessidade de tratamento de dados para que a parte exerça seu regular direito de peticionar, se defender, informar algo no processo, etc. Nesse caso, o tratamento de dados, desde que realizado dentro dos limites da lei, é uma hipótese permitida pela LGPD.

Base legal: Art. 7º, VI (dados pessoais); Art. 11, II, "d" (dados pessoais sensíveis).

Exemplos:

» Em um processo de cobrança de pensão alimentícia, uma das partes precisa informar o órgão em que o devedor trabalha, para que seja efetuado o desconto em folha de pagamento. Caso a parte pesquise e localize, no Portal de Transparência do Recife, que o devedor é servidor do município, ao fornecer o endereço profissional para intimação, agiu dentro da permissão legal;

» A Procuradoria-Geral do Município, ao realizar a cobrança de um débito tributário inscrito em dívida ativa de um cidadão, localiza, em algum sistema externo, dados do endereço do devedor. Da mesma forma, não precisa da autorização do titular para utilizar esses dados.

- **proteção da vida ou da incolumidade física do titular ou de terceiro** - quando o bem tutelado for a vida ou a incolumidade física do titular ou de terceiro, pode haver o tratamento de dados sem a necessidade de consentimento do titular. Isso se fundamenta tanto na importância do bem protegido, quanto pela urgência com que, muitas vezes, esse tratamento precisa ser realizado.

Base legal: Art. 7º, VII (dados pessoais); Art. 11, II, "e" (dados pessoais sensíveis).

Exemplo:

» Diante de uma ameaça de desabamento de determinada área, a Defesa Civil poderia acessar banco de dados sobre imóveis e proprietários daquela área, junto com número de telefone, para envio de mensagens de alerta e informações sobre segurança;

- **tutela de saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária** - diferentemente da hipótese anterior, esta previsão legal é específica para proteção da saúde e, ainda, trata-se de um permissivo exclusivo para profissionais de saúde (médicos, enfermeiros, odontólogos, etc.), serviços de saúde (clínicas médicas, laboratórios, etc.) ou autoridade sanitária (vigilância sanitária, agentes fiscalizadores de saúde, etc.).

  Base legal: Art. 7º, VIII (dados pessoais); Art. 11, II, "f" (dados pessoais sensíveis).

  Base legal: Art. 7º, IX (dados pessoais).

  Exemplos:

  » Quando o profissional da área de saúde acessa o histórico médico do paciente para verificar atendimentos anteriores, alergias, comorbidades, etc.;

  » O agente de saúde que coleta dados sobre os moradores para prestar orientações sobre vacinação, prevenção de doenças, etc.

- **atendimento aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais** - quando a Lei fala em legítimo interesse, não conceitua exatamente a que se refere. Alguns exemplos são apontados no art. 10º, mas a própria LGPD indica que não são apenas esses casos, cabendo uma análise da situação concreta. As hipóteses exemplificadas são: 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. A autoridade nacional poderá, ainda, descrever melhor esse conceito em regulamento futuro.

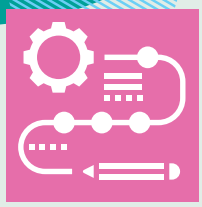
- **proteção do crédito, inclusive quanto ao disposto na legislação pertinente** - trata-se de uma hipótese preventiva para que devedores não utilizem a proteção da Lei, visando a dificultar a cobrança legal de dívidas.

  Base legal: Art. 7º, X (dados pessoais).

  Exemplo:

  » Uma entidade de proteção de crédito recebe o registro de um devedor, contendo dados de valor, data de vencimento do título, nome e CPF do titular da dívida. O tratamento para acesso, disponibilização e consulta, possui autorização legal, não havendo necessidade de consentimento do titular.

Uma das tarefas importantes que os agentes de tratamento precisam realizar é identificar a hipótese legal que está sendo utilizada em um determinado uso de dados pessoais. Poderá existir mais de uma hipótese legal que autorize o tratamento, o que é bastante recomendado, por exemplo, fundamentar o tratamento do dado no art. 7º, I e II (consentimento do titular e execução de políticas públicas). É prudente registrar todos os permissivos legais aplicáveis, oferecendo, assim, mais segurança jurídica aos envolvidos.



6) Como iniciar o procedimento de adequação à LGPD?

Um plano de adequação para proteção de dados pessoais precisa contar com o apoio dos gestores desde o início, assim, o tema ganha força para uma mudança de cultura necessária. Observadas as especificidades de cada órgão/entidade, uma sugestão de passos iniciais pode ser a adoção das seguintes medidas:

- identificar os impactos da LGPD nas atividades do órgão/entidade;
- localizar a base de dados pessoais existente no órgão respectivo, especialmente os sensíveis, para avaliação quanto à necessidade de sua manutenção, informando-a ao encarregado, ou à viabilidade de eliminação;
- promover a adequação das normas internas, documentos, portais de internet, entre outros, impactadas pela LGPD;
- elaborar um programa de proteção de dados com medidas e controles para o acompanhamento da implantação de padrões que estejam em conformidade com a LGPD e legislações setoriais aplicáveis;
- adequar os documentos jurídicos, com eventuais mudanças nos contratos existentes para adequação aos padrões de proteção de dados, principalmente para aqueles que envolvam o tratamento e compartilhamento de dados pessoais (termos aditivos);
- difundir a cultura sobre o tema através de treinamentos e acompanhamento das orientações mais atualizadas sobre o assunto.

7) O que acontece quando ocorre um incidente com os dados pessoais?

Todos aqueles agentes de tratamento de dados, ou qualquer outra pessoa que intervenha em uma das fases do tratamento, obrigam-se a adotar medidas de segurança com o objetivo de evitar tratamento inadequado ou ilícito dos dados. Caso ocorra algum incidente de segurança que possa acarretar risco ou dano relevante aos titulares, deverá ser informado tanto à autoridade nacional quanto ao titular dos dados. Essa comunicação deverá conter, no mínimo:

- a descrição da natureza dos dados pessoais afetados;
- as informações sobre os titulares envolvidos;
- a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- os riscos relacionados ao incidente;
- os motivos da demora, no caso de a comunicação não ter sido imediata; e
- as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Haverá apuração do ocorrido, por parte da ANPD, que poderá resultar em determinação direcionada ao controlador, para que providencie ampla divulgação do fato em meio de comunicação e medidas para reverter ou diminuir os efeitos

do incidente. Além disso, pode resultar na aplicação de uma das sanções previstas na Lei, sem prejuízo de apuração de responsabilidade civil, administrativa e criminal.

8) Quais as penalidades em caso de descumprimento da LGPD?

Caso o tratamento de dados não seja realizado em conformidade com a Lei, desde que apurado mediante procedimento específico, pode haver sanções aplicadas pela Autoridade Nacional de Proteção de Dados - ANPD. A LGPD aponta em seu art. 52 as possíveis sanções:

- advertência, indicando o prazo para adoção de medidas corretivas;
- multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica ou do grupo no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
- multa diária, observado o limite total de R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
- publicização da infração, após devidamente apurada e confirmada a sua ocorrência;
- bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
- eliminação dos dados pessoais a que se refere a infração;
- suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
- suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
- proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Vale destacar que a LGPD conferiu um tratamento diferenciado para a Administração Pública em relação aos entes privados, não estando sujeita a sanções pecuniárias.

Caso ocorra infração em decorrência do tratamento de dados pessoais pela Administração Pública, a Autoridade Nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação e também poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais (Arts. 31 e 32).

Importa lembrar que as sanções previstas na Lei não impedem a aplicação de outras medidas previstas em normas diversas, como o Estatuto dos Funcionários Públicos do Município de Recife (Lei Municipal nº 14.728/85), o Código de Ética do Servidor Público do Poder Executivo Municipal (Decreto Municipal

nº 27.627/2013), Lei de Improbidade Administrativa (Lei nº 8.429/1992), Lei de Acesso à Informação (Lei nº 12.527/2011), dentre outras normas aplicáveis aos servidores públicos.

A ANPD é a instituição responsável pela fiscalização e aplicação das penalidades previstas na LGPD. As sanções previstas na LGPD serão aplicáveis a partir de agosto de 2021.

9) Como transformar todo o conteúdo teórico da LGPD em realidade prática no cotidiano do servidor?

Conceitos como governança, gestão de riscos, integridade, *compliance* e boas práticas são elementos que migraram do setor privado para o setor público e precisam ser acelerados para o alcance de resultados de excelência na Administração Pública.

A própria LGPD traz apontamentos sobre boas práticas e governança (arts. 50 e 51), mas antes é necessário se familiarizar com o conceito do que é governança. Quando se trata de Administração Pública, o Decreto nº 9.203/2017, (que dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional) conceitua governança pública como sendo o:

"conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade."

Assim, dentro de suas competências, os agentes de tratamento poderão formular regras de boas práticas e de governança que estabeleçam:

- as condições de organização;
- o regime de funcionamento;
- os procedimentos, incluindo reclamações e petições de titulares;
- as normas de segurança;
- os padrões técnicos;
- as obrigações específicas para os diversos envolvidos no tratamento;
- as ações educativas;
- os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Segundo a própria de LGPD, ao se implementar um programa de governança em privacidade, espera-se, no mínimo, que:

- demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
- seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

- seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;

- estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
- tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

- esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
- conte com planos de resposta a incidentes e remediação; e
- seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

10) Como o servidor pode verificar se suas atividades, e a atuação do respectivo órgão/entidade, estão efetivamente atendendo o disposto na LGPD?

A LGPD vem reforçar a cultura de proteção dos dados do titular já presente na Administração Pública, em disposições específicas no Código Civil, no Código de Defesa do Consumidor, no Marco Civil da Internet, na Lei de Acesso à Informação, entre outras legislações. Houve agora um foco maior nos dados pessoais e no titular desses dados, além dos aspectos preventivos, de segurança e responsabilidade. Porém, a Lei não fixou um procedimento próprio a ser utilizado na verificação de atendimento à norma, trazendo, na verdade, diretrizes e tópicos norteadores.

As particularidades do tipo de tratamento de dados feitos por cada órgão/entidade precisam ser levadas em conta, mas existem aspectos gerais que precisam ser observados:

I - Princípios: durante todo o tratamento de dados, foram observados os princípios da LGPD? Ou seja, o tratamento atendeu à **finalidade** informada ao titular? A forma de tratamento foi **adequada** à finalidade? Havia **necessidade** daquele tratamento específico? O titular teve assegurado o **livre** acesso aos seus dados, possibilitando avaliar a qualidade destes com as informações necessárias de forma **transparente**? Houve medidas que promovessem a **segurança** dos dados de forma **preventiva**, a fim de evitar danos? O tratamento foi realizado de forma a **não discriminar** o titular? E por fim, é possível **prestar contas**, demonstrando a eficácia e **responsabilidade** das medidas adotadas?

II - Enquadramento legal: outro ponto de verificação é o **enquadramento legal** em uma (ou mais) hipótese(s) permissiva(s) do tratamento de dados pessoais (art. 7º) ou dados pessoais sensíveis (art. 11) prevista(s) na LGPD. Lembrando ainda que o consentimento do titular, por ser revogável a qualquer momento, configura hipótese mais frágil, que merece vir acompanhada de outro enquadramento nas normas autorizadoras, garantindo, assim, mais segurança ao tratamento dos dados.

III - Direitos dos titulares dos dados: Deve-se observar também se os **direitos dos titulares dos dados** (arts. 17 a 22) foram respeitados: a) se houve acesso facilitado às informações sobre o tratamento de seus dados; b) se houve disponibilização das informações de forma clara, adequada e ostensiva, principalmente no que se refere à confirmação da existência de tratamento e, em caso positivo, sua finalidade, forma, duração; c) se foi garantida a correção de dados incompletos, inexatos ou desatualizados; d) se houve anonimização, bloqueio ou eliminação de dados desnecessários; e) se foi permitida a portabilidade de seus dados; f) se foi respeitado o pedido de revogação do consentimento/eliminação dos dados; g) se foram disponibilizadas informações sobre com quem os dados foram compartilhados, sobre a possibilidade de não fornecer consentimento e as consequências dessa negativa e, ainda, sobre a identificação do controlador e o contato do encarregado para comunicação; e g) se foi garantido direito de petição em relação aos seus dados contra o controlador perante a autoridade nacional.

IV - Medidas de segurança, governança e boas práticas: Além desses tópicos, é preciso verificar se estão sendo adotadas **medidas de segurança**, tanto de forma preventiva, quanto em caso de incidentes (observadas as orientações do art. 46 a 49), e, ainda, se estão sendo adotadas providências de **governança e boas práticas** (arts. 46 a 51).

Considerações Finais

Para uma boa adequação aos parâmetros da LGPD, não basta seguir um manual ou checklist de tarefas a serem realizadas pela Administração Pública. É necessário que seja criada uma cultura de proteção de dados alinhada com as boas práticas de governança.

Transformar teoria em prática é o desafio que se apresenta. Para isso, algumas ferramentas podem ser utilizadas: capacitações, atualizações, debates, fóruns, desde que com a participação efetiva dos servidores. Sem esse comprometimento interno com as atividades que envolvam tratamento de dados pessoais, aumenta consideravelmente o risco de descumprimento da Lei, podendo ocasionar a responsabilização do órgão/entidade, e também do servidor.

Fica, portanto, o convite para que cada servidor se torne promotor de boas práticas de proteção de dados e privacidade em seu ambiente de trabalho.

A Controladoria-Geral do Município do Recife está presente e comprometida com esse movimento de transformação, fornecendo auxílio e suporte aos demais órgão/entidades com objetivo de concretizar as medidas de proteção de dados e adequação à legislação.

Glossário

Agentes de tratamento: o controlador e o operador.

Anonimização: utilização de técnicas de conversão de dados pessoais em dados anônimos, ou que assegurem, de forma robusta, que os dados não permitam a identificação da pessoa do titular. Também é definida como o processo pelo qual a informação pessoal identificável é irreversivelmente alterada, de tal forma que a informação pessoal identificável principal não pode mais ser identificada direta ou indiretamente.

ANPD: Autoridade Nacional de Proteção de Dados, órgão da administração pública responsável por zelar pela proteção dos dados pessoais, bem como implementar e fiscalizar o cumprimento dos dispositivos da LGPD. Responsável, também, pela aplicação de sanções previstas na LGPD.

Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.
Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

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

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

Dado anonimizado: dado relativo a titular que não possa ser identificado, considerando-se a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

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

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

Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente a saúde ou vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.
Encarregado: pessoa indicada pelo Controlador para ser a ponte entre o Controlador, os titulares e a ANPD (ou órgão que o substituir), bem como para orientar os funcionários do Controlador sobre práticas de tratamento de dados, entre outras.

Garantia da segurança da informação (dados): capacidade de sistemas e organizações assegurarem a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

Garantia da segurança de dados: ver garantia da segurança da informação.
Incidente de segurança: É a ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de Segurança da Informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a Segurança da Informação.

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

LGPD: Lei Geral de Proteção de Dados.

Operador/processador: pessoa jurídica ou física que realiza o tratamento de dados pessoais sob as ordens do Controlador.

Órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

Pseudonimização: é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

Relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

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

Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.
Tratamento: toda operação realizada com dados pessoais; como as que se referem a:

- *acesso* – possibilidade de se comunicar com um dispositivo, meio de armazenamento, unidade de rede, memória, registro, arquivo etc., visando a receber, fornecer, ou eliminar dados;
- armazenamento – ação ou resultado de manter ou conservar em repositório um dado
- *arquivamento* – ato ou efeito de manter registrado um dado embora já tenha perdido a validade ou esgotada a sua vigência;
- *avaliação* – ato ou efeito de calcular valor sobre um ou mais dados;
- classificação – maneira de ordenar os dados conforme algum critério estabelecido;
- *coleta* – recolhimento de dados com finalidade específica;
- comunicação – transmitir informações pertinentes a políticas de ação sobre os dados;
- *controle* – ação ou poder de regular, determinar ou monitorar as ações sobre o dado;
- *difusão* – ato ou efeito de divulgação, propagação, multiplicação dos dados;
- *distribuição* – ato ou efeito de dispor de dados de acordo com algum critério estabelecido;
- *eliminação* – ato ou efeito de excluir ou destruir dado do repositório;
- *extração* – ato de copiar ou retirar dados do repositório em que se encontrava;
- *modificação* – ato ou efeito de alteração do dado;
- *processamento* – ato ou efeito de processar dados;
- *produção* – criação de bens e de serviços a partir do tratamento de dados;
- *recepção* – ato de receber os dados ao final da transmissão;
- *reprodução* – cópia de dado preexistente obtido por meio de qualquer processo;
- *transferência* – mudança de dados de uma área de armazenamento para outra, ou para terceiro;
- *transmissão* – movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos etc;
- *utilização* – ato ou efeito do aproveitamento dos dados;

Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre estes e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

Vazamento de dados: Situações acidentais ou ilícitas de acessos não autorizados a dados pessoais.


RECIFE
PREFEITURA