CARTILHA

ELABORADA EM ABRIL/2020 - ATUALIZADA EM AGOSTO/2020

LGPD

LEI Nº 13.709/2018
LEI GERAL DE PROTEÇÃO DE DADOS

CGE
CONTROLADORIA GERAL
DO ESTADO DO PARANÁ

SUMÁRIO

1.APRESENTAÇÃO

A Lei nº 13.709 – Lei Geral de Proteção de Dados foi aprovada em agosto de 2018 e terá vigência a partir de agosto de 2020. O assunto é de suma importância, pois visa à segurança jurídica, padronizando normas e práticas, promovendo a proteção de dados pessoais de todos os cidadãos, em âmbito nacional.

Com a LGPD, o Brasil é inserido no seleto grupo de países com legislação específica sobre proteção de dados pessoais.

A Controladoria Geral do Estado – CGE, como órgão central do Sistema de Controle do Poder Executivo Estadual, tem por finalidade a coordenação, o controle, a avaliação, a promoção, a formulação e a implementação de mecanismos e diretrizes de prevenção e combate à corrupção, bem como regulamentação e normatização dos sistemas de controle do referido Poder (Decreto nº 2741/2019, Anexo I, art. 2º).

Considerando que a principal razão de existir dos órgãos de governo é servir ao interesse da população, o propósito desta cartilha, elaborada pela CGE, é informar aos gestores públicos os pontos primordiais da legislação de proteção de dados, antes da obrigatoriedade da efetiva aplicação da LGPD.

2.INTRODUÇÃO

A LGPD regula a atividade sobre o uso de dados pessoais, de colaboradores e de terceiros, por todos os tipos de organizações que operam em território brasileiro, estabelecendo rigorosas sanções, em caso de descumprimento de suas determinações.

A elaboração da LGPD foi pautada no General Data Protection Regulation (GDPR), Regulamento de Proteção de Dados da União Europeia. No Brasil, a proteção de dados possui natureza jurídica de direito e garantia fundamental, com base no inciso XII-A do art. 5º e o inciso XXX do art. 22 da Constituição Federal, acrescentados pela Emenda Constitucional nº 17.

Sua aplicação se estende a qualquer pessoa, natural ou jurídica, de direito público ou privado, que realize o tratamento de dados pessoais, online e/ou offline.

> Os dados deverão ser utilizados apenas para as finalidades específicas para as quais foram coletados e devidamente informadas aos titulares (Princípio da Finalidade). Somente devem ser colhidos os dados mínimos necessários para que se possa atingir a finalidade (Princípio da Minimização da Coleta).
> Após alcançada a finalidade pela qual eles foram coletados, deve ser feita a imediata exclusão dos dados (Princípio da Retenção Mínima).

Assim, a importância da referida Lei se reflete em maior segurança jurídica e proteção aos direitos dos titulares de dados.

3.PONTOS IMPORTANTES

A Lei Geral de Proteção de Dados (LGPD) apresenta pontos importantes em toda sua extensão. Com o intuito de facilitar a aplicação da referida legislação, relacionamos os principais a seguir:

1

ABRANGÊNCIA

Quaisquer dados pessoais obtidos em qualquer tipo de suporte (papel, eletrônico, em ambiente virtual, som, imagem, etc.).

2

REGRA PARA TODOS

Criação de um panorama de segurança jurídica para todo o país e em nosso contexto, para o Estado do Paraná.

3

FISCALIZAÇÃO CENTRALIZADA

Ficará a critério da Autoridade Nacional de Proteção de Dados Pessoais (ANPD).

4

TRANSPARÊNCIA

Ocorrendo vazamento de dados, a ANPD e os indivíduos afetados, devem ser comunicados.

5

FINALIDADE E NECESSIDADE

Os quesitos de tratamento devem ser previamente informados ao cidadão.

6

CONTRATOS DE ADESÃO

Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou serviço, o titular deverá ser claramente informado.

7

RESPONSABILIDADE CIVIL

O responsável que, em razão do exercício de atividade de tratamento de dados, causar dano patrimonial, moral, individual ou coletivo, será obrigado a repará-lo.

4.CONCEITOS ESPECÍFICOS

A interpretação do texto legal requer a observância de conceitos específicos relacionados na LGPD, conforme segue:

- **AGENTES DE TRATAMENTO**
  o controlador e o operador;

- **ANONIMIZAÇÃO**
  utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

- **AUTORIDADE NACIONAL**
  órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta lei;

- **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;

DADO PESSOAL
informação relacionada à pessoa natural identificada ou identificável. Essa informação representa todo e qualquer dado que possa tornar uma pessoa identificável, seja ela diretamente relacionada ao seu titular (como um nome ou número de documento) ou mesmo indiretamente relacionada, mas com potencial de identificá-lo (a) (como endereço, idade, informações sobre hábitos de compra etc).

✔ CONTROLADOR
pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais;

✔ DADO ANONIMIZADO
dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

✔ ELIMINAÇÃO
exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

✔ ENCARREGADO (DPO)
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;

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

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

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

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 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;

USO COMPARTILHADO DE DADOS

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

TRATAMENTO

toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

5.PRINCÍPIOS

As condutas conceituadas como “tratamento da informação” pelo agente público da Administração, deverá observar os seguintes princípios:

- ADEQUAÇÃO: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
- FINALIDADE: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
- 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;
- NÃO DISCRIMINAÇÃO: impossibilidade de realização do tratamento para fins discriminatórios, ilícitos ou abusivos;
- 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;
- PREVENÇÃO: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de 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;
- 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;
- 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 das informações sob custódia.

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.

6.PRIVACIDADE DOS DADOS PESSOAIS

Na atualidade, a informação tornou-se um dos bens mais valiosos. Diariamente, usamos, absorvemos, produzimos e transmitimos informações o tempo todo.

A LGPD ASSEGURA A TODA PESSOA NATURAL A TITULARIDADE DE SEUS DADOS PESSOAIS E GARANTIA DOS DIREITOS FUNDAMENTAIS DE LIBERDADE, INTIMIDADE E PRIVACIDADE.

Desta forma, podemos afirmar que um dos grandes desafios contemporâneos é assegurar a proteção e a privacidade para estes dados.

Esta garantia se aplica independente do meio ou forma de tratamento dos dados coletados ou recebidos, incorrendo que todo aquele que faz uso do dado deve observar as regras legais.

Desta forma, para que haja o cumprimento das obrigações e procedimentos previstos na lei, o conceito de privacidade dos dados pessoais deverá nortear qualquer tratamento de dados realizado pelos controladores.

7.PROGRAMA DE IMPLEMENTAÇÃO

Buscando a implementação da LGPD, sugerimos algumas ações básicas, como:

I. Conseguir o envolvimento dos gestores desde o início do plano de adequação para que a proteção de dados pessoais esteja incorporada aos valores do Estado e assim o tema ganhe engajamento e a força necessária;

II. Estabelecer as ações e um servidor líder para o plano, identificando os principais projetos e áreas do órgão/entidade afetadas pela LGPD e eventuais legislações setoriais;

III. Criar um programa de governança em proteção de dados com a elaboração de medidas e controles para o acompanhamento da implantação de padrões que estejam em conformidade com a LGPD e legislações setoriais aplicáveis;

IV. Elaborar e rever documentos jurídicos com a realização de eventuais adendos aos contratos existentes para adequação aos padrões de proteção de dados, principalmente para aqueles que envolvam o tratamento e compartilhamento de dados pessoais;

V. Garantir o exercício dos direitos dos titulares, mediamente a confirmação da implementação de medidas técnicas e organizacionais;

VI. Realizar treinamentos internos para apresentação das novas políticas de proteção de dados pessoais e disseminação da cultura sobre o tema.

Criado este panorama, os órgãos/entidades devem ainda estabelecer um Comitê de Segurança da Informação para analisar os procedimentos internos. Dentro deste órgão haverá um servidor exclusivo para a proteção dos dados e responsável pelo cumprimento da nova lei, o Data Protection Officer (DPO).

Considerando ainda que a Autoridade Nacional de Proteção de Dados (ANPD) pode solicitar a comprovação do cumprimento da lei, recomenda-se que seja elaborado um Manual de Boas Práticas e de Governança em privacidade.

7.1. MAPEAMENTO DE DADOS

> O PRIMEIRO PASSO PARA IMPLEMENTAÇÃO DA REFERIDA LEI É FAZER O MAPEAMENTO DE DADOS, QUE CONSISTE EM IDENTIFICAR E CATEGORIZAR TODA E QUALQUER RELAÇÃO DE COLETA, ARMAZENAMENTO E TRATAMENTO DOS DADOS SENSÍVEIS DE SEU ÓRGÃO PÚBLICO OU ENTIDADE.

Este levantamento poderá ser feito a partir da análise dos seguintes pontos:

- Tipos de dados sensíveis que fazem parte dos processos do órgão/entidade;
- Local em que ficam armazenados;
- Forma de tratamento;
- Por onde trafegam;
- Relação de profissionais que têm acesso aos dados e qual o tipo de acesso que cada um deles tem;
- Mecanismos de controle disponíveis para a aplicação da política interna de proteção;
- Profissional qualificado para análise e atualização da política interna de proteção de dados, caso necessário;
- Pontos frágeis e estratégias para minimizá-los;
- Se os dados foram avaliados e classificados de forma apropriada seguindo os conceitos atuais da LGPD.

Com base nestas informações, será possível identificar os sistemas e a equipe que lida diretamente com os dados pessoais e conhecer os pontos de risco da atual segurança de dados, ajudando a consolidar uma política interna eficaz em relação às normas da LGPD.

8.CRITÉRIOS PARA O USO DE DADOS

A REGRA É: O TITULAR SEMPRE DEVERÁ CONSENTIR PARA O USO DE SEUS DADOS.

O consentimento é a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada, exceto nas seguintes situações:

- Para a proteção do crédito, nos termos do Código de Defesa do Consumidor;
- Para o cumprimento de obrigação legal ou regulatória pelo responsável pelo tratamento;
- Para a realização de estudos por órgão de pesquisa, sem a individualização a pessoa;
- Para o exercício regular de direitos em processos judicial, administrativo ou arbitral;
- Para execução de contrato ou procedimentos preliminares relacionados a um contrato;
- Pela administração pública, para o uso compartilhado de dados necessários à execução de políticas públicas;
- Para a tutela da saúde, com procedimento realizado por profissionais da área ou por entidades sanitárias.

9.PROTEÇÃO DO DENUNCIANTE

A Controladoria Geral do Estado, através da Coordenadoria de Ouvidoria, que compõem sua estrutura organizacional, aprovou a Resolução nº 38, de 18 de outubro de 2019, que trata de medidas de proteção à identidade dos denunciantes que procuram as ouvidorias para registrar suas manifestações, quanto à prestação de serviços públicos e à conduta de agentes da Administração Pública.

Na referida resolução foram estabelecidos conceitos que auxiliam na aplicação adequada das cautelas aos processos de proteção de dados pessoais sensíveis, quais são:

- DENÚNCIA: ato que indica a prática de ilícito ou irregularidade cuja solução dependa da atuação dos órgãos ou entidades apuratórios competentes;
- DENUNCIANTE: toda pessoa física ou jurídica que denuncia às autoridades qualquer ilícito ou irregularidade;
- ELEMENTO DE IDENTIFICAÇÃO: qualquer dado ou informação que permita a associação direta ou indireta do denunciante à denúncia por ele realizada;
- REGRAS DE PROTEÇÃO À IDENTIDADE: conjunto de medidas ou procedimentos adotados com a finalidade de proteger a identidade do denunciante e garantir o tratamento adequado aos elementos de identificação da denúncia, implementado por meio do sistema de tecnologia utilizado pelo canal de ouvidoria (Sistema Integrado para Gestão de Ouvidorias – SIGO).

10.PENALIDADES

O tratamento de dados deverá ser feito com a máxima prudência, visto que a Lei Geral de Proteção de Dados, em seu artigo 52, prevê sanções em caso de infrações, conforme segue:

- A - Advertência, indicando o prazo para adoção de medidas corretivas;
- B - Multa simples, de até 2% (dois por cento) do faturamento 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;
- C - Multa diária, observado o limite total de R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
- D - Publicização da infração após devidamente apurada e confirmada a sua ocorrência;
- E - Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
- F - Eliminação dos dados pessoais a que se refere a infração.

> As penalidades previstas nos itens "A", "E" e "F", poderão ser aplicadas às entidades e aos órgãos públicos, ao disposto na Lei nº 8.112, de 11 de dezembro de 1990 (Estatuto do Servidor Público Federal), na Lei nº 8.429, de 2 de junho de 1992 (Lei de Improbidade Administrativa), e na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

A fiscalização e aplicação das penalidades elencadas acima, serão feitas pela Autoridade Nacional de Proteção de Dados (ANPD).

A Lei nº 14.010, de 10 de junho de 2020, definiu que as sanções previstas na LGPD serão aplicadas a partir de agosto de 2021.

10.1. RESPONSABILIDADE E RESSARCIMENTO DE DANOS

O tratamento de dados pessoais está centralizado em dois agentes, sendo o controlador e o operador, definidos no item 4 deste material. De acordo com a legislação, os operadores devem realizar o tratamento de dados conforme as instruções fornecidas pelo controlador, que possui obrigações mais intensivas.

O art. 42 da LGPD estabelece que o controlador ou o operador que causar dano patrimonial, moral, individual ou coletivo, no exercício da atividade, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

Regra geral, a responsabilidade entre tais agentes não é solidária. As responsabilidades são distintas, podendo ser maiores, no caso do controlador e menores para o operador.

11.LGPD X SERVIÇO PÚBLICO

O tratamento de dados pessoais pelas pessoas jurídicas de direito público deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

Consideram-se pessoas jurídicas de direito público para fins da LGPD:

- os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público;
- as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas de direito público.

As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares. Porém, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público.

O titular dos dados deverá ser informado quanto às hipóteses em que, no exercício de suas competências, as pessoas jurídicas de direito público realizarem o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos.

As formas de publicidade das operações de tratamento poderão ser estabelecidas pela Autoridade Nacional de Proteção de Dados (ANPD).

Porém, as pessoas jurídicas mencionadas não ficam dispensadas de instituir autoridades públicas para adoção de providências necessárias para que o pessoal a elas subordinado

hierarquicamente conheça as normas e observe as medidas e procedimentos de segurança para tratamento de informações sigilosas, em conformidade com a Lei nº 12.527/2011 (Lei de Acesso à Informação).

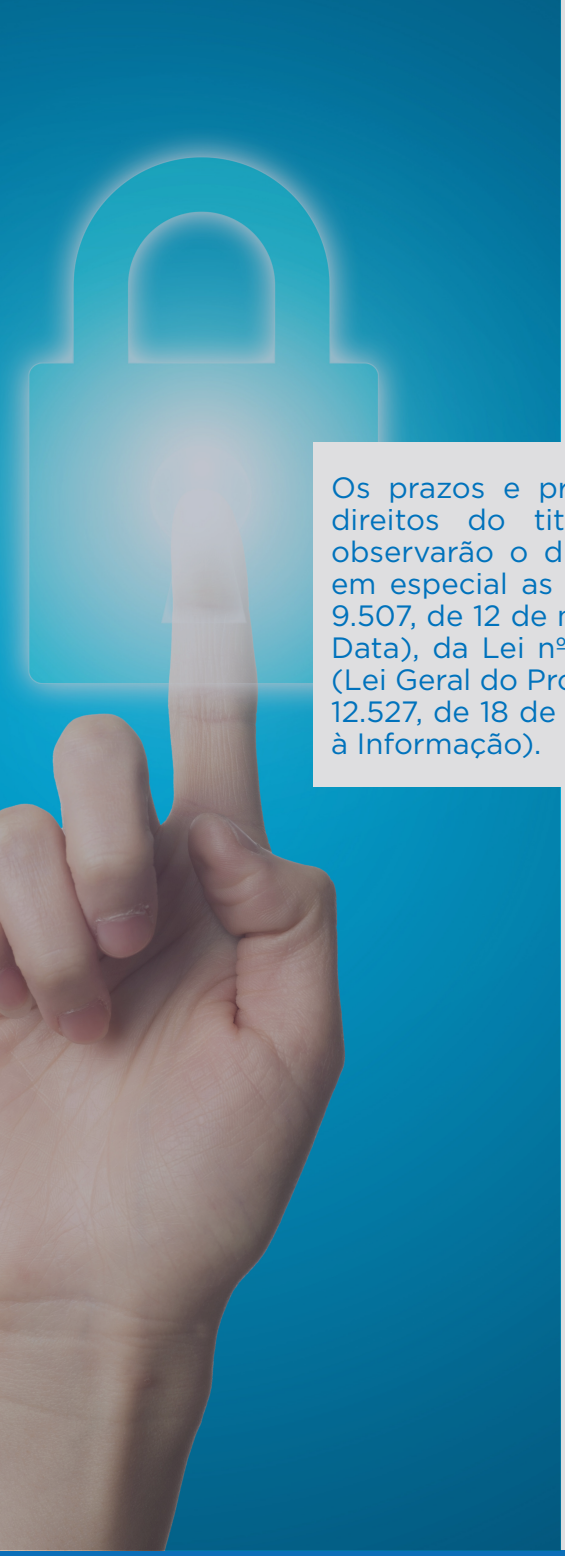
Os dados deverão ser mantidos em formato interoperável (capacidade de um sistema, informatizado ou não, de se comunicar de forma transparente ou o mais próximo disso, com outro sistema, semelhante ou não) e estruturado para o uso compartilhado, buscando a execução de políticas públicas, a prestação de serviços públicos, a descentralização da atividade pública e a disseminação e o acesso das informações pelo público em geral.

O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais, elencados no item 6 desta cartilha.

Ao Poder público é vedado transferir para entidades privadas dados pessoais constantes de bases de dados a que tenham acesso, exceto:

- em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);
- nos casos em que os dados forem acessíveis publicamente, observadas as disposições da LGPD;
- quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres. Estes contratos e convênios deverão ser comunicados à autoridade nacional; ou
- na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades.

Quando houver a comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado deverá ser feita a informação à autoridade nacional e dependerá de consentimento do titular, exceto nos casos previstos no art. 27 da LGPD.



A autoridade nacional poderá solicitar, a qualquer momento, aos órgãos e às entidades do poder público a realização de operações de tratamento de dados pessoais, informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento da LGPD.

Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data), da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo), e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

Nos casos de infração à LGPD por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação.

Ficará ainda a seu critério, 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 pelo Poder Público, quando julgar necessário.

12. CONSIDERAÇÕES FINAIS

Em relação aos dados pessoais armazenados nos bancos de dados do Estado do Paraná, é imprescindível identificar o interesse público ou o consentimento do titular para qualquer tratamento de dados, que resulte em compartilhamento das informações.

A LGPD faz parte do conjunto de normas, formado também pela Lei de Acesso à Informação (Lei nº 12.527/2011) e pela Lei de Transparência (LC nº 101/2009), que exige clareza na divulgação de atos e ações, ao mesmo tempo em que estabelece restrições quando à divulgação dos dados pessoais.

Para o atendimento a esse conjunto de leis, é importante a criação de uma cláusula geral de concordância para divulgação de dados, em documentos e contratos públicos, conforme dita a Lei da Transparência. Também para garantir o cumprimento da legislação, o armazenamento de dados sensíveis deverá ser seguro e com acesso controlado.

> Os sistemas de informática que fazem o tratamento dos dados pessoais devem estar protegidos por login e chaves de acesso, permitindo identificar o usuário que efetuou o tratamento dos dados e as eventuais alterações realizadas nas informações da pessoa natural.
>
> Independente da exigência legal de informações de dados sensíveis da pessoa natural em alguns documentos, recomenda-se que sejam feitos alertas quanto ao uso e compartilhamento, nas situações permitidas.

Diante da análise da legislação, verifica-se que a adequação às novas determinações legais é complexa e não será imediata. Portanto, é fundamental que os órgãos públicos e entidades sejam céleres em se preparar para o atendimento à LGPD.

A Controladoria Geral do Estado do Paraná tomou a iniciativa de instituir um grupo de trabalho, para elaborar a regulamentação da Lei Geral de Proteção de Dados – LGPD, no âmbito do Poder Executivo Estadual.

13.FUNDAMENTOS LEGAIS

BRASIL, Constituição Federal de 1988.

BRASIL, Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados.

BRASIL, Lei nº 13.460, de 26 de junho de 2017. Dispõem sobre a participação, proteção e defesa dos direitos dos usuários dos serviços públicos da administração pública.

BRASIL, Lei nº 14.010, de 10 de junho de 2020. Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (Covid-19).

PARANÁ, Resolução nº 38, de 18 de outubro de 2019. Trata de medidas de proteção à identidade dos denunciantes que procuram as ouvidorias para registrar suas manifestações, quanto a prestação de serviços públicos e a conduta de agentes da Administração Pública.

PARANÁ
GOVERNO
DO ESTADO

CARLOS MASSA RATINHO JÚNIOR
GOVERNADOR DO ESTADO

RAUL CLEI COCCARO SIQUEIRA
CONTROLADOR-GERAL DO ESTADO