CARTILHA

LEI GERAL DE PROTEÇÃO DE DADOS
LGPD 13.709/18

SUA APLICAÇÃO NAS ATIVIDADES DO PODER PÚBLICO

INTRODUÇÃO:

Esta cartilha para ser adequadamente entendida e validada deve contar com a leitura integral da **Lei Geral de Proteção de Dados Pessoais – LGPD 13.709 de 14 de agosto de 2018,** que versa quanto ao tatamento de Dados Pessoais, e da **Lei 14.129 de 29 de março de 20021,** que Dispõe sobre principios, regras e instrumentos para o Governo Digital, para o aumento da eficiência pública e da participação do cidadão, a qual veio provocar alteração na **Lei nº. 7.116 de 29/08/1983**; **Lei nº. 12.527 de 18/11/2011** (Lei de Acesso a Informação); **Lei nº. 12.682 de 09/07/2012** e na **Lei 13.460 de 16/07/2017**.

Muito tem-se falado sobre a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei 13.709/18, na perspectiva da inicativa privada.

Porem, deve-se levar em conta de que se apresenta de igual forma e relevancia quando se trata do tratamento de dados pessoais no âmbito do setor público (Executivo, Legislativo e Judiciário) e entes federativos (União, Estados, Distrito Federal e Municípios), em especial na elaboração e execução de políticas públicas.

Vale destacar de que a transparência dos dados pessoais tratados no ambiente do Poder Público, por sua vez, se resguarda constitucionalmente, e **Lei 14.129 de 29 de março de 20021,** conforme descrevemos acima.

Cabe reforçar de que a Lei Geral de Proteção de Dados – LGPD 13709/18, dedicou no capítulo (IV) as diretrizes quanto ao tratamento de dados pessoais pelo Poder Público.

Lei Federal n. 13.709/2018

A **Lei Geral de Proteção de Dados**, traz em seu bojo o marco regulatório que estabelece direitos e garantias para o cidadão em relação ao tratamento de seus dados pessoais.

Disponibilzando ao cidadão meios para que possa exercer efetivo controle sobre seus dados pessoais, tendo em seu escopo, em sua proteção, regras claras e bem definidas quanto ao tratamento de seus dados pessoais.

Em especial quando falamos no ambito do poder publico, com vistas a elaboração e execução de políticas públicas e variadas formas de prestação de serviços públicos

A QUEM SE APLICA:

(Artigo 3º)

- Qualquer órgão ou entidade pública.
- Empresas públicas e sociedades de economia mista

EXEÇÃO:

(Artigo 4º)

- Casos de tratamentos de dados realizados para:
    - Fins exclusivamente: jornalísticos e artísticos; acadêmicos;
    - Fins exclusivos de segurança pública, defesa nacional, segurança do Estado ouatividades de investigação e repressão de infrações penais.

- Casos de tratamentos de dados 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 à LGPD.

ATORES E ARTIGOS RELEVANTES:

(Artigo 5º)

- Titular

É a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. Titular será o contribuinte, servidor ou empregado público, gestor público, pessoa física com a qual o órgão ou entidade pública possui alguma relação contratual.

- Controlador

Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. No setor público: o órgão público, entidade pública, empresa pública ou sociedade de economia mista que toma as decisões a respeito do tratamento de dados pessoais.

O órgão público que mantém um banco de dados de seus servidores ou empregados públicos também se enquadram nesta definição.

- Operador

Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, quando processam dados pessoais em nome de outros órgãos ou entidades públicas.

- Encarregado

Pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados.

A Autoridade Nacional de Proteção de Dados – ANPD, através da Resolução CD/ANPD nº. 2 de 17/01/2022, regulamentou o tratamento juridico diferenciado previsto para agentes de tratamento de pequeno porte, regulamentação esta que veio a desenquadrar deste beneficio as atividades que exigem o tratamento de dados pessoais de Alto Risco, Larga Escala ou que tratem dados sensíveis, em especial crianças, adolescentes e idosos, e, assim elimina qualquer possibilidade de duvida quanto a necessidade dos orgão publicos em indicar um Encarregado.

- **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 entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

- **Órgãos 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, estendendo-se a Universidades Públicas e entidades de pesquisa pública.

PRINCIPIOS A LEI

(Artigo 6º)

A Lei Geral de Proteção de Dados - LGPD estabelece diferentes princípios no tratamento de dados pessoais.

- **Livre Acesso e Transparência**

É dado aos titulares o direito de consulta gratuita e facilitada de seus dados pessoais.

- **Finalidade**

Determina de que o tratamento dos dados pessoais, devem ter propósitos legítimos, específicos, explícitos e informados.

- **Adequação**

Determina que o tratamento dos dados pessoais seja compatível com as finalidades.

- **Necessidade**

Estabelece a necessidade de minimização da coleta de dados pessoais, restringindo apenas ao minimo necessário a atividade de tratamento.

- **Qualidade de dados**

Dados devem ser exatos, claros e adequados, de acordo com a finalidade.

- **Segurança e Prevenção**

Devem ser utilizadas medidas técnicas e administrativas para prevenir incidentes (como vazamentos de dados ou ataques cibernéticos).

- **Responsabilização e Prestação de Contas**

Evidencias técnicas e administrativas com os cuidados da segurança dos dados pessoais tratados.

- **Não Discriminação**

É vedado o tratamento de dados para fins discriminatórios ilícitos ou abusivos.

O QUE SE ENTENDE POR DADOS PESSOAIS

- **Dado pessoal**

A LGPD classifica como dado pessoal qualquer informação relacionada a pessoa natural identificada ou identificável.

Neste particluar, deve-se entender que pessoa natural não é apenas o contribuinte, mas também o servidor e o empregado público, pessoas físicas com as quais a administração pública se relaciona, e até mesmo os gestores públicos e demais representantes do povo com mandato eletivo.

Isso significa que um grande número de identificadores constituem o dado pessoal, como o nome, o CPF, RG, informações sobre localização e assinaturas online. Em resumo, praticamente toda informação coletada sobre uma pessoa será um dado pessoal.

- **Dado pessoal sensível**

A LGPD definiu como dado pessoal sensível aquele dado pessoal "sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a or- ganização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico" de uma pessoa natural.

Dados relacionados a políticas direcionadas a minorias, seguramente envolverão o tratamento de dados sensíveis. Na mesma linha, os sistemas de identificação biométrica, atrai para si, a necessidade de maior atenção, pois, se enquadra na categoria de Dados Pessoais Sensíveis, e seu tratamento tem um carater mais restritivo.

- **Dado anonimizado**

Refere-se a existencia de um dado pessoal que não é capaz de identificar o seu titular, utilizando os meios técnicos razoáveis e disponíveis na ocasião do seu tratamento, ele é chamado de dado anonimizado.

O dado anonimizado não será considerado dado pessoal para os fins da LGPD, salvo quando o processo de anonimização ao qual foi submetido for revertido, ou quando, com esforços razoáveis, puder ser revertido.

BASES LEGAIS PARA QUE A ADMINISTRAÇÃO PÚBLICA TRATE DADOS PESSOAIS

(Artigo 7º)

- **Mediante o consentimento do titular**

O consentimento é uma manifestação livre, informada e inequívoca que autoriza o tratamento de dados pessoais para uma finalidade determinada. Autorizações genéricas serão nulas. Não é admitido um consentimento implícito. Esse consentimento, diferente das demais bases legais autorizativas para o tratamento de dados pessoais, pode ser revogado a qualquer tempo.

- **Demais bases legais**:

  - Cumprimento de obrigação legal ou regulatória pelo controlador.

  - Pela Administração Pública, 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.

  - Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais.

- Quando é necessário para a execução de contrato ou de procedimentos preli-minares relacionados a contrato do qual seja parte o titular, a pedido do titulardos dados. É o caso, por exemplo, concessões de serviços públicos ou uso de bens públicos, contratos de parcerias público-privadas dentre outros instrumentos contratuais da Administração Pública.

- Para o exercício regular de direitos em processo judicial, administrativo ou arbitral. Essa hipótese se aplicaria, por exemplo, ao tratamento de dados pes- soais de servidores ou empregados públicos para fins de defesa dos interesses da administração pública em processos judiciais ou mesmo administrativos, o mesmo valendo para o tratamento de dados pessoais de contribuintes nas mes-mas hipóteses.

- Para a proteção da vida ou da incolumidade física do titular ou de terceiro. O tratamento de dados pessoais no âmbito da atuação da Defesa Civil, com vistas a proteger a vida e a incolumidade física do titular ou de terceiros se enquadra-ria nessa hipótese.

- Para a tutela da saúde, em procedimento a ser realizado por profissionais da área da saúde ou por entidades sanitárias. Hospitais públicos e demais entidades sanitárias públicas estão autorizadas a tratar dados dos respectivos pacientes, sem seu consentimento, para fins de tutela da saúde.

- Quando é necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentaisdo titular que exijam a proteção dos dados pessoais.

- Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

DADOS PESSOAIS SENSÍVEIS

(Artigo 11)

- **Mediante o consentimento do titular.**

  O consentimento é uma manifestação livre, informada e inequívoca que autoriza o tratamento de dados pessoais para uma finalidade determinada. Autorizações genéricas serão nulas. Não é admitido um consentimento implícito. Esse consentimento, pode ser revogado a qualquer momento. O consentimento necessita ainda, ser dado de forma específica e destacada, para finalidades determinadas.

- **Sem o consentimento do titular, nas hipóteses em que for indispensável para:**

  - Cumprimento de obrigação legal ou regulatória pelo controlador.

  - Tratamento compartilhado de dados necessários à execução, pela Administração Pública, de políticas públicas previstas em leis e regulamentos. A Lei, por sua vez, traz uma diferença se comparadas às hipóteses de tratamento de dados pesso ais não sensíveis, aos excluir os casos de políticas públicas respaldadas em contratos, convênios ou instrumentos congêneres.

  - Para realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais.

  - O exercício regular de direitos em processo judicial, administrativo ou arbitral. Essa hipótese se aplicaria, por exemplo, ao tratamento de dados pessoais de servidores ou empregados públicos para fins de defesa dos interesses da administração pública em processos judiciais ou mesmo administrativos, o mesmo valendo para o tratamento de dados pessoais de contribuintes nas mesmas hipóteses.

- Para a proteção da vida ou da incolumidade física do titular ou de terceiro. Por exemplo, o tratamento de dados pessoais sensíveis no âmbito da atuação da Defesa Civil, com vistas a proteger a vida e a incolumidade física do titular ou de terceiros seenquadraria nessa hipótese.

- Para a tutela da saúde, em procedimento a ser realizado por profissionais da área da saúde ou por entidades sanitárias. Assim, hospitais públicos e demais entidades sanitárias públicas estão autorizadas a tratar dados pessoais sensíveis dos respectivos pacientes, sem seu consentimento, para fins de tutela da saúde.

- Garantia da prevenção à fraude e da segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no Artigo 9º da Lei Geral de Proteção de Dados – LGPD, salvo no caso em que prevalecer direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

TRATAMENTO DE DADOS PESSOAIS POR ÓRGÃO DE PESQUISA (Artigo 13)

Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão 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 pseudoanonimização dos dados, bem como, considerem os devidos padrões éticos relacionados a estudos e pesquisas.

A LGPD também apresenta outras regras protetivas para a hipótese:

- Na divulgação dos resultados de estudos ou pesquisa não poderá ser revelado dados

pessoais.

- O órgão de pesquisa será responsável pela segurança da informação e não poderá em hipótese alguma, transferir os dados a terceiros.

- O acesso aos dados pessoais pelos órgãos de pesquisa para fins de realização de estudos em saúde pública estarão sujeitos a regulamentação por parte da Autoridade Nacional de Proteção de Dados – ANPD, e das autoridades das área de saúde e sanitárias, no âmbito de suas competências.

DIREITOS DOS TITULARES:

(Artigo 18)

- O titular tem o direito de:

    - Confirmar a existência de tratamento (Informação);
    - Acessar os dados;
    - Correção de seus dados (incompletos, inexatos ou desatualizados);
    - Anonimização, bloqueio ou eliminação de dados (desnecessários, excessivosou em desconformidade com a Lei);
    - Portabilidade dos dados;
    - Eliminação dos dados pessoais tratados com o consentimento do titular (ex-ceto Artigo 16);
    - Informação sobre entidades com as quais os dados foram compartilhados;
    - Informação sobre a possibilidade de não fornecer consentimento e consequências;
    - Revogação do consentimento.

REGISTRO DE PROCESSAMENTO DE DADOS PESSOAIS

(Artigo 37)

Os órgãos e entidades públicas, empresas públicas e sociedades de economia mista que se enquadrem nas definições de controlador ou operador deverão criar e manter um registro das operações de tratamento de dados que realizarem.

ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS

(Artigo 41)

O órgão ou entidade pública, empresa pública ou sociedade de economia mista, quando atuar na qualidade de controlador, deverá indicar encarregado pelo tratamento de dados pessoais.

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

Atividades do encarregado

- Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- Receber comunicações da autoridade nacional e adotar providências;
- Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
- Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

A Autoridade Nacional de Proteção de Dados – ANPD, através da Resolução CD/ANPD 2 de 17 de

Janeiro de 2022, veio definir o tratamento juridico diferenciado, para os agentes de tratamento de pequeno porte, vindo a excluir desta possibildiade a realização de tratamento de Alto Risco, dentre os quais enumerou: tratamento de dados pessoais em larga escala (número significativo de titulares, volume de dados envolvidos, duração, utilziação de dados pessoais sensiveis ou de dados pessoais de crianças, adolelescentes e idosos, dentre outras). Portanto, o Controlador do orgão público, deverá indicar um Encarregado do tratamento de Dados Pessoais.

INCIENTENS DE SEGURANÇA

(Artigo 48)

O que é um incidente de segurança?

Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação levando a perda de um ou mais princípios básicos de Segurança da Informação: **Confidencialidade, Integridade e Disponibilidade.**

Alguns exemplos de Incidentes de Segurança:

Uso impróprio:

- Uso de e-mail corporativo para spam ou promoção de negócios pessoais;
- Ferramenta não autorizada instalada;
- Uso de pendrive de forma não autorizada;
- Impressão de documentos de forma não autorizada.

Tentativas de acesso não autorizado a sistemas ou dados, como por exemplo:

- Tentativas não autorizadas de acesso;
- Má utilização de um sistema;
- Falhas no sistema que impede um acesso autorizado.

Ataques de negação de serviço:

- Forçar o sistema vítima a reinicializar ou consumir todos os recursos (como memória ou processamento por exemplo) de forma que ele não pode mais fornecer seu serviço;
- Obstruir a mídia de comunicação entre os utilizadores e o sistema vítima de forma a não se comunicarem adequadamente.
- Vírus e outros códigos maliciosos;
- Sequestro de dados (ransomware);
- Desfiguração de sites;
- Modificações em um sistema, sem conhecimento, instruções ou consentimento prévio do proprietário;
- Desrespeito à política de segurança ou à política de uso aceitável de uma empresa ou provedor de acesso.

Pelo que consta do caput do Artigo 46 da LGPD, os "acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito" deverão ser notificados.

Comunicação sobre a ocorrência de incidente de segurança que possa acar-retar risco ou dano relevante aos titulares

Esse é um tema de fundamental importância para o setor público, já que diver sos órgãos e entidades públicas, assim como empresas públicas e sociedades de economia mista, em todas as esferas de governo e da federação, tratam dados pessoais tanto de contribuintes como de servidores e empregados públicos, sendo que muitos desses dados se enquadram na definição de dado pessoal sensível. Portanto, o estabelecimento de uma política clara sobre o que fazer quando da ocorrência de incidentes de segurança é de vital importância.

Basicamente, o incidente deve ser comunicado à Autoridade Nacional de Proteção de Dados e ao titular dos dados, pelo órgão público, entidade pública, empresa pública ou sociedade de economia mista que desempenhar o papel de controlador, sempre que o

incidente de segurança "possa acarretar risco ou dano relevante aos titulares".

Prazo razoável

A Autoridade Nacional de Proteção de Dados – ANPD, em 22/02/2021 recomendou que os incidentes de segurança sejam comunicados a ANPD, em até 2 (dois) dias úteis a contar da ciencia do incidente.

Conteúdo

O conteúdo da notificação deve abarcar:

- Descrição da natureza dos dados pessoais afetados;
- Informações sobre os titulares envolvidos;
- Indicação das medidas técnicas e de segurança utilizadas para a proteção dosdados;
- Riscos relacionados ao incidente;
- Motivos da demora, no caso de a comunicação não ter sido imediata; e
- Medidas que foram ou que serão adotadas para reverter ou mitigar os efeitosdo prejuízo.

Outras providências

A Autoridade Nacional de Proteção de Dados (dependendo da gravidade do incidente) pode determinara adoção de outras providências, tais como:

- ampla divulgação do fato em meios de comunicação
- medidas para reverter ou mitigar os efeitos do incidente.

SERVIÇOS NOTORIAIS E DE REGISTRO

(Artigo 23, §§ 4º e 5º)

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

Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a Administração Pública.

QUANTO A ESTRUTURA DOS DADOS

(Artigo 25)

Os dados deverão ser mantidos em formato que possam atuar, operar, funcionar com outros, e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

PRINCIPAIS BASES LEGAIS PARA O TRATAMENTO DE DADOS NO SETOR PÚBLICO.

(Artigo 23)

Finalidade e interesse 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 pú-blico, desde que:

- Sejam informadas as hipóteses em que, no exercício de suas competências, realizam 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, preferencialmen- te em seus sítios eletrônicos;

- Seja indicado um encarregado.

Prazos

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), Lei nº. 14;129 de 29 de março de 2021.

Publicidade

A Autoridade Nacional de Proteção de Dados – ANPD, poderá dispor sobre as formas de publicidade das operações de tratamento pelo Poder Público.

O disposto na Lei Geral de Proteção de Dados – LGPD nº. 13.709/18, e a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Infomação), não concorrem entre si, portanto, observadas pelos orgão públicos competentes.

EMPRESAS PÚBLICAS E SOCIEDADES DE ECONOMIA MISTA

(Artigo 24)

O que devemos saber?

As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no Artigo 173 da Constituição Federal, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares.

As empresas públicas e as sociedades de economia mista, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão perante a Lei Geral de Proteção de Dados, o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público.

Para facilitar vamos dar um exemplo: A Caixa Econômica Federal (CEF), em algumas situações. Quando ela atuar como um banco, tratando dados de seus correntistas para, por exemplo, ela deverá seguir as regras aplicáveis ao setor privado.

Por outro lado, quando ela tratar dados pessoais no âmbito, por exemplo do FGTS, do Programa de Integração Social (PIS) ou do Seguro-Desemprego, ela deverá observar as regras aplicáveis ao setor público.

DO COMPARTILHAMENTO DE DADOS PESSOAIS PELA ADMINSITRAÇÃO PÚBLICA (Artigo 26)

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;
- Respeitar os princípios de proteção de dados pessoais elencados no Artigo 6º da Lei Geral de Proteção de Dados – LGPD .

DA TRANSFERÊNCIA INTERNACIONAL DE DADOS (Artigo 33)

A LGPD estabeleceu hipóteses taxativas em que a transferência internacional de dados é permitida, dentre elas:

- Países ou Organizações Internacionais com grau adequado de proteção (Artigo 33, I)
- Frente a cláusulas contratuais específicas, cláusulas-padrão, normas corporativas globais, selos, certificados e códigos de conduta (Artigo 33, II)
- Quando for necessária para a cooperação jurídica internacional entre órgãos públicos

de inteligência, de investigação e de persecução, de acordo com os ins-trumentos de direito internacional (Artigo 33, III)

- Quando for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro (Artigo 33, IV)

- Quando a Autoridade Nacional de Proteção de Dados autorizar (Artigo 33, V)

- Quando resultar em compromisso assumido em acordo de cooperação internacional (Artigo 33, VI)

- Consentimento específico e em destaque para a transferência de dados (Artigo33, VII)

- Quando o titular tiver fornecido o seu consentimento específico para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades (Artigo 33, VIII)

- Quando for necessária para o cumprimento de obrigação legal ou regulatória pelo controlador; para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados (Artigo 33, IX)

QUANTO DA TRANSFERÊNCIA DE DADOS PESSOAIS COM ENTIDADES PRIVADAS (Artigo 26)

Regra geral

É vedada a transferência de dados pessoais para entidades privadas.

Exceções

✓ Execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na LAI;

✓ Se for indicado um encarregado para as operações de tratamento de dados pessoais;

✓ Quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres (que deverão ser comunicados à autoridade nacional);

✓ Para a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados;

✓ Nos casos em que os dados forem acessíveis publicamente.

USO COMPARTILHADO COM ENTIDADES PRIVADAS (Artigos 27 a 30)

Regra geral

A comunicação e uso compartilhado de dados com entidades privadas, por pessoas jurídicas de direito público, dependerá do consentimento do titular.

Exceções

- Hipóteses de dispensa de consentimento previstas na LGPD;
- Os casos de uso compartilhado de dados;
- Exceções constantes do § 1º do Artigo 26 da LGPD (conforme item anterior).

COMPETÊNCIAS DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS NO TEMA

- A Autoridade Nacional de Proteçao de Dados – ANPD, 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 tratados e outros detalhes do tratamento realizado, e, ainda, poderá emitir parecer técnico complementar para garantir o cumprimento da LGPD.

- Também poderá estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais.

DAS RESPONSABILIDADES

(Artigos 31, 42, 43)

Da Administração Pública

Quando houver infração à LGPD em decorrência do tratamento de dados pessoais por órgãos públicos, a Autoridade Nacional de Proteção de Dados, poderá enviar informe com medidas cabíveis para fazer cessar a violação.

A Autoridade Nacional de Proteção de Dados, poderá solicitar a agentes do Poder Público a publicaçãode relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões de boas práticas para os tratamentos de dados pessoais em sua gestão.

Dos Agentes de Tratamento (Responsabilidade Civil)

O controlador ou o operador (inclusive os órgãos e entidades públicos, empresas públicas e sociedades de economia mista), respondem por dano em razão de ioncidente com dado pessoal, que der causa no exercício de atividade de tratamento de dados pessoais, em especial, se constatado ausencia de adoção ou tratamento adequado, relacionado a medidas técnicas, adminsitrativas, operacionais e tecnologia da informação.

O Controlador e o Operador respondem solidariamente pelos danos causados quando:

- Um deles vir a descumprir as obrigações da legislação de proteção de dados;
- O Operador não ter seguido as orientações e/ou instruções lícitas do controlador.

Inversão do ônus da prova

A possibilidade existe em favor do titular e a critério do juiz, em redação similar ao Artigo 6º, VIII do Código de Defesa do Consumidor.

Excludentes de responsabilidade

- Não realização do tratamento que é lhe atribuído;

- Não existência de violação à legislação de proteção de dados;
- Culpa exclusiva do titular dos dados ou de terceiro.

Tratamento de dados irregular

Ocorrerá quando a legislação não for observada ou quando não for fornecida a segurança esperada pelo titular. Nesse caso, há que se verificar o modo pelo qual é realizado, resultado e riscos que dele se esperam, técnicas de tratamento disponíveis à época.

EMPRESAS PÚBLICAS E SOCIEDADES DE ECONOMIA MISTA EM RELAÇÃO DE CONSUMO

(Artigos 45)

No caso de violação do direito do titular no âmbito das relações de consumo, ao atuar em regime de concorrência no âmbito de uma relação de consumo, serão aplicadas as normas sobre responsabilidade civil estabelecidas no Código de Defesa do Consumidor (CDC).

BOAS PRÁTICAS E GOVERNANÇA

(Artigo 50)

Os controladores e operadores pelo tratamento de dados pessoais, no âmbito de suas competências, individualmente ou por meio de associações, 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.

O desenvolvimento de uma política de governança de dados precedida de um mapeamento de dados realizados é uma medida recomendável a ser implementada pelo setor público.

INOBSERVÂNCIA DA LEI

(Artigo 52)

O Artigo 52 da LGPD impôs sanções administrativas aplicáveis, pela Autoridade Nacional de Proteção de Dados, aos agentes de tratamento de dados.

No caso específico de entidades e órgãos públicos, são excluídas as possibilidades de multa simples e multa diária, nos termos do parágrafo 3º do Artigo 52. Assim sendo, entre os riscos, podemos destacar:

Advertência

Com indicação de prazo para adoção de medidas corretivas.

Publicização da infração

Apenas após confirmada a ocorrência.

Reputação

O impacto não são apenas sanções administrativas. Também pode afastar outras entidades que busquem parcerias pelo risco de serem impactados.

Bloqueio

Até a regularização da situação, os dados pessoais serem bloqueados.

Eliminação

Confirmada a infração, os dados pessoais a ela relacionados serem eliminados.

BANCO DE DADOS EM FUNCIONAMENTO

(Artigo 63)

É necessário que o setor público adote medidas para sua adequação à LGPD.

PRINCIPAIS PONTOS NA ADEQUAÇÃO DO PODER PÚBLICO AOS TERMOS DA LEI

- A Lei Geral de Proteção de Dados - LGPD estabelece uma série de providências que devem ser adotadas pelos agentes de tratamento, que incluem o mapeamento e o registro das operações de tratamento de dados pessoais que realizarem, incluindo a identificação das respectivas bases legais e finalidades; a adoção de medidas técnicas e administrativas e de processos e políticas internas que assegurem o cumprimento das normas de proteção de dados pessoais; e o estabelecimento de um canal de contato com os titulares de dados pessoais.

- A Lei determina, no art. 41, que os controladores de dados devem indicar um Encarregado para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados.

- Compreender em qual medida a LGPD se aplica ao(s) tratamentos de dados que realiza;

- Identificar qual(is) base(s) legal(is) se aplica(m) ao(s) tratamento(s) de dados que realizam;

- Rever os processos internos de tratamentos de dados com vistas à adequação à LGPD;

- Revisar as políticas de privacidade (ou criá-las se não possuírem);

- Estabelecer uma política de segurança da informação com regras claras relacionadas a incidentes de segurança, especialmente no que toca ao cumprimento dos requisitos de notificação à ANPD;

- Capacitar o pessoal envolvido no tratamento de dados pessoais;

    - Criar e implementar o Registro das operações de tratamento de dados pessoais;

- Revisar contratos, convênios e outros instrumentos que impliquem no tratamento de dados pessoais, assim como eventuais contratos e outros instrumentos que regulem o relacionamento com eventuais operadores de tratamentos de dados pessoais

em nome do controlador;

- Estabelecer uma política clara de governança dos dados pessoais dentro do órgão ou entidade pública.

Material de apoio:

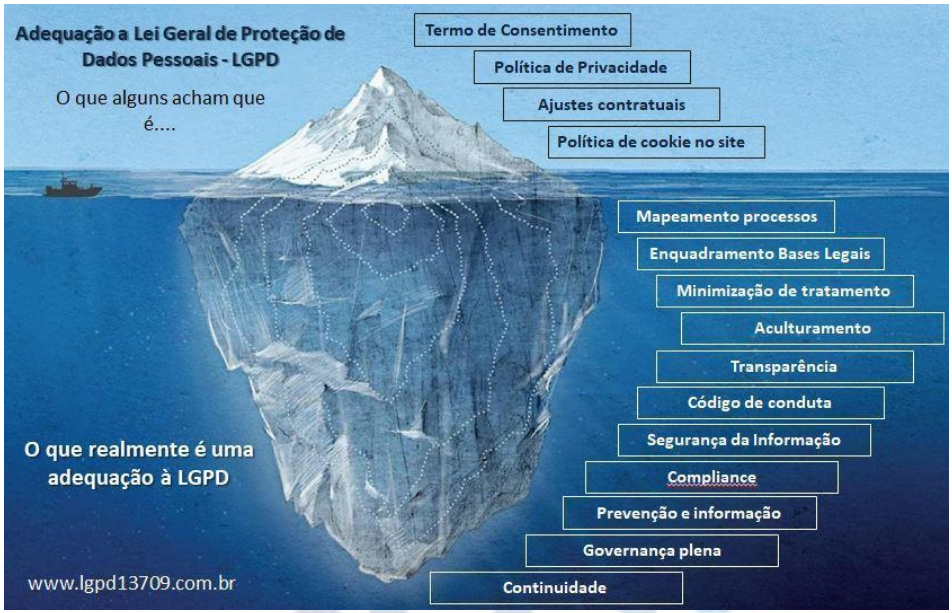
LEI GERAL DE PROTEÇÃO DE DADOS – LGPD Nº. 13.709/18

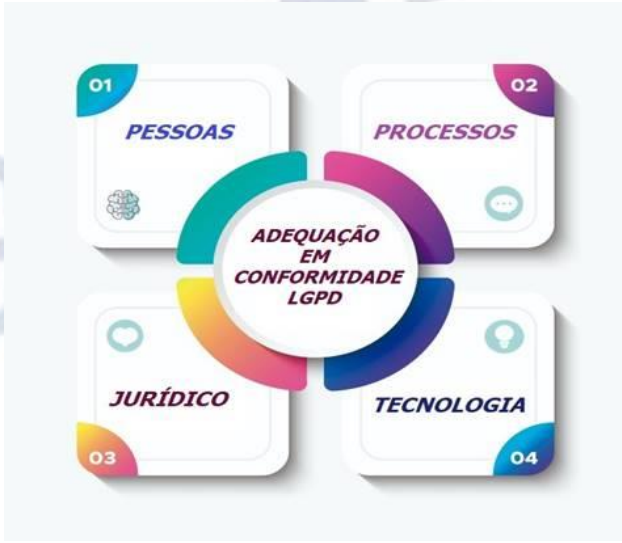
http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

LEI Nº 14.129 DE 29 DE MARÇO DE 2021 -

http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14129.htm

O QUE LEVA A UMA ADEQUAÇÃO A LEI GERAL DE PROTEÇÃO DE DADOS (ponta a ponta)





NOSSA APRESENTAÇÃO:

Somos um grupo eclético de Consultores especializados em suas áreas de atuação, que desde a promulgação da Lei Geral de Proteção de Dados, em agosto de 2018, nos dedicamos a estudá-la minuciosamente, tanto no aspecto jurídico, nas questões operacionais e na busca de um modelo eficaz quanto ao processo de adequação, em especial que refletisse em redução do tempo de entrega dos trabalhos e simultaneamente no valor de investimentos.

COORDENADORES DOS PROJETOS (CONSULTORES MASTER)

ENG. UMBERTO FORTI:

- Formado em Engenharia Elétrica pela Faculdade Engenharia São Paulo;
- Especialidade em tratamento e segurança da informação;
- Fundador e ex-sócio por 8 anos de empresa de proteção ao crédito;
- CEO da 1A1 Projetos e Marketing – empresa especializada em marketing digital com campanhas altamente segmentadas frente a extensa base de informações proprietárias;
- Certificados:
  - o Profissional em Privacidade de Dados;
  - o Estruturação e Adequação à LGPD;
  - o Gestão de Riscos da Informação; o LGPD e os impactos no Marketing.

JOSÉ ANTONIO FRANZZOLA:

- Advogado OAB/SP 68.165;
- Carreira profissional em grandes corporações, na área Administrativa, Financeira e Recursos Humanos, tendo ocupado posição de Diretoria e Controladoria;
- Especialista na área de Direito do Trabalho, Relações Trabalhistas, Sindicais, Direito Empresarial e Lei Geral de Proteção de Dados;
- Consultor especializado em Planejamento Estratégico e Gestão de Negócios;
- Autor do Livro A TRAJETÓRIA DO NEGÓCIO “da satisfação a depressão;
- CEO da empresa Franzzola Serviços Ltda.

Atualização Abril de 2022