



CARTILHA LGPD

Apresentação

A Lei nº 13.709 de 2018 - Lei Geral de Proteção de Dados Pessoais entrou em vigor em setembro de 2020. A LGPD surge em um contexto de datificação das coisas - Big Data -, em que cresce cada vez mais a circulação de dados pela internet. A criação da internet e o desenvolvimento da sociedade de rede geram diversas oportunidades e desafios.

A expansão das Tecnologias de Informação e Comunicação - TIC's possibilita a interligação dos Estados, dos municípios, agiliza a comunicação, permite reuniões a distância, gera economia de recursos e reduz deslocamentos físicos. Entretanto, cresce a exposição, a vulnerabilidade, o monitoramento e a vigilância.

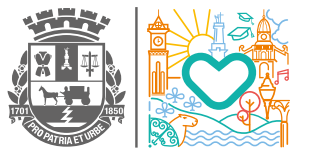
Todo esse contexto fez e ainda faz emergir diversas leis visando a proteção dos dados pessoais no mundo. Na atualidade, tem ganhado destaque as discussões sobre a privacidade e a possibilidade de o indivíduo participar do processamento de seus dados pessoais e, assim, controlar o uso de suas informações.

No Brasil, a proteção de dados no âmbito da Administração Pública relaciona-se com a Constituição Federal de 1988, com a Lei de Acesso à Informação - LAI (Lei nº 12.527/2011) e com o Marco Civil da Internet (Lei nº 12.965/2014).

Nesta Cartilha, a Prefeitura Municipal de Juiz de Fora estabelece importantes mandamentos da Proteção de Dados Pessoais no Município.

Introdução.....	4
O que é a Lei Geral de Proteção de Dados Pessoais?.....	7
Aplicabilidade e Inaplicabilidade da LGPD no setor público.....	12
Princípios.....	14
Tratamento de Dados Pessoais.....	17
Base Legal.....	19
Dados de Criança e de Adolescente.....	22
Direitos do Titular.....	24
LGPD, Poder Público e Transparência.....	26
Sanções.....	29
As boas práticas de governança em proteção de dados.....	31
Referências bibliográficas.....	33

Introdução



O uso de computadores tem possibilitado novas maneiras de coletar e de tratar informações, assim como, a crescente necessidade de coleta de dados pelas instituições públicas e privadas (RODOTÁ, 2008).

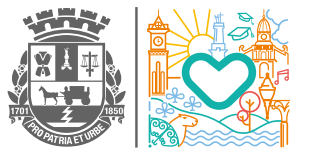
Com a expansão da internet e a utilização por diversos usuários do mundo, torna-se necessária, a preocupação com a governança da internet, especificamente, com a segurança. A governança da internet envolve os governos nacionais, as organizações internacionais, a sociedade civil, o setor empresarial e a comunidade técnica (KURBALIJA, 2016).

As novas tecnologias trazem diversos benefícios para a vida em sociedade, porém, existem alguns aspectos negativos como a crescente exposição, o monitoramento, assim como, os diferentes casos vazamentos de dados pessoais armazenados por organizações públicas e privadas. Nesse contexto, torna-se necessária a elaboração de diversas leis visando a proteção de dados pessoais e a implementação de Segurança da Informação nas organizações.

A discussão sobre privacidade tem ganhado novos contornos. A definição de privacidade como o “direito a ser deixado só” tem dado lugar a definições de que a privacidade compreende a possibilidade de cada um poder controlar o uso de suas informações (RODOTÁ, 2008).

A discussão sobre privacidade na atualidade não reflete somente a defesa contra invasões externas, mas nos instiga a considerar problemas da privacidade na organização do poder, já que a estrutura da informação hoje representa um dos componentes fundamentais (RODOTÁ, 2008).

A criação de leis de proteção de dados pessoais no mundo que disciplinam o uso e a coleta de dados impacta a proteção de valores democráticos, as liberdades civis e o livre desenvolvimento da personalidade natural.



No Brasil, as primeiras discussões sobre a Proteção de Dados Pessoais tiveram início em 2010, com a Consulta Pública do Ministério da Justiça sobre o Anteprojeto de Lei de Proteção de Dados Pessoais.

No ano seguinte foi publicada a Lei de Acesso à Informação - LAI – Lei nº 12.527 de 18 de novembro de 2011, que regulamenta a transparência dos dados pessoais pelo Poder Público. No mesmo ano foi proposto o Projeto de Lei nº 2126 do Marco Civil da Internet, que dispõe sobre os direitos e os deveres de usuários e de provedores.

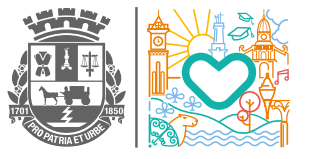
A LAI regula o acesso à informação disposto no Inciso XXXIII do artigo 5º, no inciso II do parágrafo 3º, do artigo 37 e no parágrafo 2º, do artigo 216, da Constituição Federal de 1988.

O Marco Civil da Internet entrou em vigor em 2014 pela Lei nº 12.965 e estabelece princípios, garantias, direitos e deveres para o uso na internet no Brasil. Embora o Marco Civil da Internet preveja a proteção de dados pessoais e o consentimento, informa-se que não prevê a proteção de dados de maneira completa.

Em 2016, foi publicado o Decreto nº 8.638, que dispõe sobre a Política de Governança Digital no âmbito de órgãos e de entidades da Administração Pública Direta, autárquica e fundacional. O referido Decreto foi revogado pelo Decreto nº 10.332 de 2020, que institui a estratégia de Governo Digital para o período de 2020 a 2021, no âmbito da Administração Pública Direta, autárquica e fundacional.

A Lei Geral de Proteção de Dados vem com o objetivo de regular o tratamento de dados efetuado pelas pessoas de direito público ou de direito privado, nos meios físicos e meios digitais, com o intuito de proteger os direitos fundamentais de liberdade e de privacidade, bem como, o livre desenvolvimento da personalidade da pessoa natural.

O que é a Lei Geral de Proteção de Dados Pessoais?



A LGPD

A Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados - LGPD dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (art. 1º, LGPD).

DADO PESSOAL

Informação relacionada a pessoa natural identificada ou identificável.

DADO PESSOAL SENSÍVEL

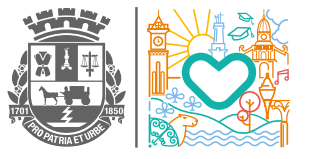
Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

DADO ANONIMIZADO

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

BANCO DE DADOS

Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.



TITULAR

Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

CONTROLADOR

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

OPERADOR

Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

ENCARREGADO

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

AGENTES DE TRATAMENTO

O controlador e o operador.

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.

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.

CONSENTIMENTO

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

BLOQUEIO

Suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

ELIMINAÇÃO

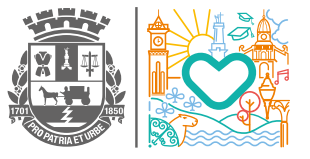
Exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

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 órgãos e entidades



públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

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.

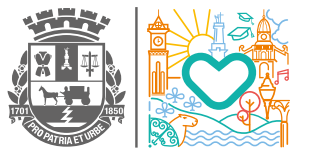
ÓRGÃO DE PESQUISA

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.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

Aplicabilidade e Inaplicabilidade no setor público

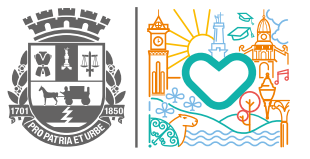


A LGPD aplica-se ao setor público e privado. No que se refere ao setor público, a aplicabilidade alcança qualquer órgão ou entidade pública, sociedades de economia mista e empresas públicas, nos termos do artigo 3º, da LGPD.

A LGPD não se aplica:

- # Aos casos de tratamento de dados pessoais para fins exclusivamente jornalísticos e artísticos; acadêmicos; fins exclusivos de segurança pública; defesa nacional; segurança do Estado ou atividades de investigação, assim como, de repressão de infrações penais;
- # Aos casos de tratamento de dados pessoais provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento do Brasil, ou objeto de transferência internacional de dados com país diferente do de proveniência, contanto que o país de proveniência garanta grau de proteção de dados pessoais adequado à LGPD;
- # Os casos de tratamento de dados de segurança pública embora não façam parte do escopo da LGPD, devem respeitar limitações de tratamento de dados para essas finalidades, tais limitações encontram-se dispostas nos parágrafos do artigo 4º, da LGPD.
- # Salienta-se que, na Administração Pública, busca-se estabelecer um equilíbrio entre a proteção de dados pessoais dos cidadãos e a elaboração de políticas públicas, bem como, a prestação de serviços públicos.

Princípios



FINALIDADE

Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

ADEQUAÇÃO

Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

NECESSIDADE

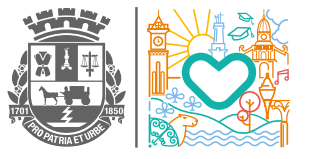
Limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

LIVRE ACESSO

Garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

QUALIDADE DOS DADOS

Garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.



TRANSPARÊNCIA

Garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

SEGURANÇA

Utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

PREVENÇÃO

Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

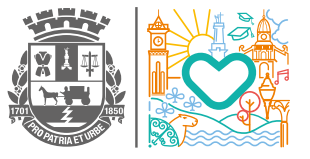
NÃO DISCRIMINAÇÃO

Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

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.

Tratamento

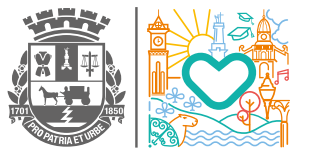


O tratamento de dados pessoais compreende toda operação efetuada com dados pessoais, como as que se referem a coleta, a produção, a recepção, a classificação, a utilização, o acesso, a reprodução, a transmissão, a distribuição, o processamento, o arquivamento, o armazenamento, a eliminação, a avaliação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

O tratamento de dados pessoais somente pode ocorrer quando o titular ou o responsável legal consentir, de maneira específica e destacada, para finalidades determinadas; ou sem o consentimento para determinadas situações previstas no art. 7º da Lei Geral de Proteção de Dados.

O tratamento de dados pessoais sensíveis somente pode ocorrer quando o titular ou o responsável legal consentir, de maneira específica e destacada, para finalidades determinadas; ou sem o consentimento para determinadas situações previstas no art. 11, inciso II, da Lei Geral de Proteção de Dados.

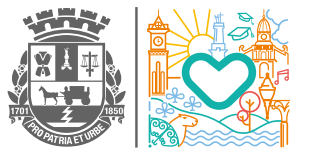
Base Legal



O tratamento de dados pessoais somente poderá ser realizado

- # Mediante o fornecimento de consentimento pelo titular;
- # Para o 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, observadas as disposições do Capítulo IV da LGPD;
- # Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- # Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- # Para o exercício regular de direitos em processo judicial, administrativo ou arbitral;
- # Para a proteção da vida ou da incolumidade física do titular ou de terceiro;
- # Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- # Quando necessário para atender 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; ou
- # Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Atenção! É dispensada a exigência do consentimento para os dados tornados manifestamente



públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.

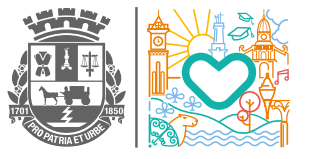
O tratamento de dados pessoais sensíveis somente poderá ser realizado

Quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

Sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

1. cumprimento de obrigação legal ou regulatória pelo controlador;
2. tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
3. realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
4. exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;
5. proteção da vida ou da incolumidade física do titular ou de terceiro;
6. tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
7. garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Dados de criança e de adolescente



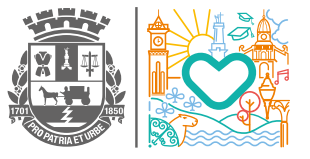
Atenção! Há um regramento especial no caso de tratamento de dados pessoais de crianças e adolescentes!

Esse tratamento deverá ser realizado em seu melhor interesse, observadas as proteções legais.

Fique atento!

O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal. Entretanto, poderão ser coletados dados pessoais de crianças sem esse consentimento quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento.

Direitos do titular



Os direitos dos titulares de dados pessoais estão dispostos no artigo 18, da Lei Geral de Proteção de Dados.

Os titulares de dados pessoais têm o direito de:

Confirmar a existência de tratamento de dados pessoais;

Acessar os dados pessoais;

Corrigir os dados incompletos, inexatos ou desatualizados;

Anonimização, bloqueio ou eliminação de dados (desnecessários, excessivos ou tratados em desconformidade com a LGPD);

Portabilidade de dados a outro fornecedor de serviço ou produto, por intermédio de requisição expressa, com base na regulamentação da Autoridade Nacional de Proteção de Dados – ANPD;

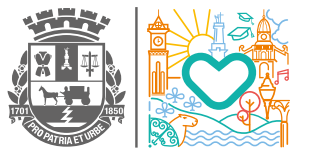
Eliminação dos dados pessoais tratados com o consentimento do titular (com exceção do artigo 16);

Informação das entidades públicas e privadas com as quais os dados foram compartilhados;

Informação sobre a possibilidade de não fornecer o consentimento e quais as implicações da negativa;

Revogação do consentimento a qualquer tempo.

LGPD, Poder Público e Transparência



A Administração Pública lida diariamente com diversos dados pessoais dos cidadãos, que muitas vezes são fundamentais para a execução e a implementação de políticas públicas.

A aplicação da LGPD ao Tratamento de Dados Pessoais realizado pelo Poder Público traz o desafio de conciliar as regras e os princípios dispostos na LGPD com os princípios aos quais a Administração Pública está submetida, tais como a eficiência, a publicidade e o interesse público.

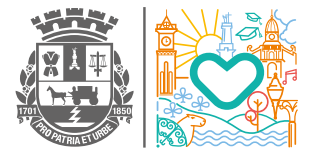
Nesse sentido, torna-se necessária a harmonização da LGPD, que visa garantir a privacidade dos dados pessoais (esfera privada dos cidadãos), com a Lei de Acesso à Informação – LAI, que objetiva assegurar a transparência da gestão pública. A base legal da LAI é o princípio da publicidade disposto no artigo 37, caput, da Constituição Federal de 1988.

Válido destacar que as leis LAI e LGPD se complementam, já que ambas visam garantir a privacidade dos cidadãos. A LGPD visa proteger a privacidade e a LAI objetiva proteger o direito de informação dos cidadãos.

O próprio conceito de dado pessoal disposto na LGPD foi previsto inicialmente na LAI e indicado como informação pessoal no artigo 4, Inciso I. A LGPD inovou ao prever a definição dado pessoal sensível.

O Capítulo IV da LGPD dispõe sobre o Tratamento de Dados Pessoais realizado pelo Poder Público. O artigo 23, da LGPD estabelece as regras específicas de tratamento de dados pessoais para o setor público.

Destaca-se que o Tratamento de Dados Pessoais realizado pelas pessoas jurídicas de direito público indicadas no artigo 1º, da Lei de Acesso à Informação – LAI, deve buscar alcançar a finalidade e o interesse público.



As empresas públicas e as sociedades de economia mista, que atuam em regime de concorrência, sujeitas ao disposto no artigo 173 da Constituição Federal de 1988, receberão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares.

Por outro lado, as empresas públicas e as sociedades de economia mista, quando operacionalizarem ou executarem políticas públicas, receberão o mesmo tratamento conferido aos órgãos e às entidades do Poder Público.

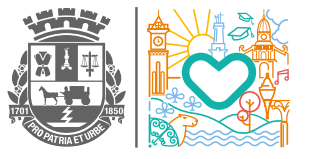
O compartilhamento de dados pessoais pelo Poder Público deve respeitar os princípios da LGPD, bem como, atender às finalidades para a execução de políticas públicas e para alcançar o interesse público.

Conforme já disposto no tópico de tratamento de dados pessoais, a LGPD no artigo 11, § 4º veda a comunicação ou o uso compartilhado entre os controladores de dados pessoais sensíveis relacionados à saúde, com o intuito de obter vantagem econômica, salvo nas hipóteses relacionadas à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares.

As organizações públicas são as maiores detentoras de bases de dados pessoais, já que a relação entre o Poder Público e os cidadãos têm início com o nascimento do indivíduo e se mantém, inclusive, após a morte.

Assim, o caráter contínuo da relação indicada demonstra a responsabilidade do Poder Público, na harmonização da transparência e da prestação de contas com a proteção dos dados pessoais. A LGPD e a LAI incidem sobre campos distintos e podem ampliar o acesso à informação. Ambas as leis são essenciais para a preservação de direitos fundamentais e das garantias do Estado Democrático de Direito.

Sanções



Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

- # Advertência, com indicação de prazo para adoção de medidas corretivas;

- # Multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado 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 a que se refere o inciso II;

- # 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;

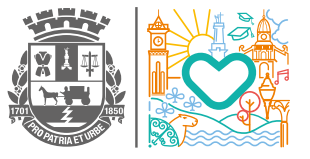
- # Suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;

- # Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Atenção!

A LGPD garantiu ao Poder Público tratamento diferenciado inclusive no momento de fiscalização e aplicação de sanções, que, no caso da Administração Pública não tem seu foco em multas, mas sim em advertência, publicização da infração, bloqueio do acesso aos dados, dentre outras sanções específicas.

As boas práticas de governança em proteção de dados



A regularidade de qualquer tratamento depende da adoção de medidas de segurança, mas também dos princípios trazidos pela Lei Geral de Proteção de Dados em seu art. 6º. A adequação vai muito além da simples execução de ações pontuais e isoladas!

É necessário que todos se comprometam com estratégias para o contínuo gerenciamento e monitoramento de seus processos, pessoas e tecnologias.

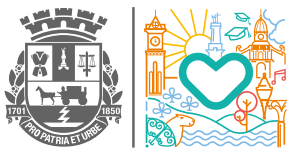
Há um dever constitucional para a Administração Pública de dupla dimensão ao Estado: não intervir ou agir com excesso em relação às liberdades individuais e, de forma reflexa, atuar no sentido de garantir que os direitos dos cidadãos (titulares) sejam concreta e suficientemente protegidos.

No caso da proteção dos dados, atuando com objetivo de evitar riscos para o cidadão em geral, por meio da adoção de medidas de proteção ou de prevenção.

Assim, considerados a natureza, o escopo, a finalidade, a probabilidade, a gravidade dos riscos e os benefícios relacionados ao tratamento dos dados do titular, a Lei Geral de Proteção de Dados, em seu art. 50, §1º, dispõe que os agentes de tratamento poderão formular ou aderir a regras de boas práticas e governança que, dentre outros aspectos, estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, normas de segurança, padrões técnicos, obrigações específicas, ações educativas, mecanismos de supervisão e de mitigação de riscos.

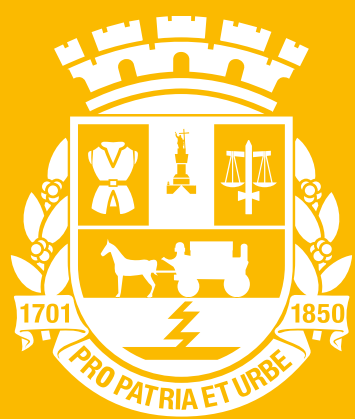
É o que se passa a fazer.

Referências Bibliográficas



BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Institui a Lei Geral de Proteção de Dados. Diário Oficial da União: seção 1, Brasília, DF, ano 197, p. 59, 15 ago. 2018. PL4060/2012

GOVERNO DO PARÁ. PROCURADORIA GERAL DO ESTADO DO PARÁ. Lei Geral de Proteção de Dados Pessoais. Manual de Aplicação na Administração Pública.



Juiz de Fora
Prefeitura



 @prefeiturajuizdefora

 /JuizdeForaPJF

 @PrefeituraJF