LGPD
MGi
Minas Gerais Participações S.A.

Cartilha sobre a Lei Geral de Proteção de Dados

Setembro/2020

A Comissão da LGPD elaborou a Cartilha de Proteção de Dados Pessoais, de forma objetiva e simplificada, apresentando as principais informações sobre a nova Lei Geral de Proteção de Dados, com a intenção de auxiliar os colaboradores da MGI, no desempenho das atividades perante a legislação em questão.

Introdução

A Lei Geral de Proteção de Dados (LGPD) foi aprovada no Brasil em agosto de 2018 e tem por base o Regulamento Geral de Proteção de Dados da União Europeia (GDPR – General Data Protection Regulation). A nova lei dispõe sobre a coleta e tratamento de dados pessoais, em que deverão ser cumpridas diversas obrigações legais, além de procedimentos preliminares de segurança e governança.

A 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, estabelecendo regras e limites para empresas a respeito da coleta, armazenamento, tratamento e compartilhamento de dados, o que favorece o desenvolvimento econômico.

Em linhas gerais, os titulares de dados passarão a ter maior controle sobre todo o processamento dos seus dados pessoais, do que decorrem diversas obrigações para controladores (a quem

competem as decisões sobre o tratamento dos dados) e operadores (aqueles que tratam os dados de acordo com o estipulado pelos controladores).

Assim, a LGPD trará mais segurança jurídica para empresas e maior proteção aos direitos dos titulares dos dados, sendo crucial entender os conceitos relevantes desta nova norma para compreensão dos seus impactos na prática.

Importante ressaltar que a LGPD não está adstrita ao ambiente virtual, como ocorre com a Lei do Marco Civil (Lei 12.965/2014), que estabelece vários direitos do usurário da internet. A LGPD vem para harmonizar as mais de 40 (quarenta) leis sobre o assunto que tem no Brasil.

LGPD – Aspectos Gerais

QUAL A IMPORTÂNCIA E O OBJETIVO DA LGPD?

- Defender os direitos fundamentais de liberdade e de privacidade;
- Oferecer ao titular dos dados maior conhecimento, controle e transparência sobre o tratamento efetivado em seus dados pessoais
- Fomentar o desenvolvimento econômico e tecnológico

QUAIS OS FUNDAMENTOS DA LGPD (ART. 2º)?

- Respeito à privacidade - ao assegurar os direitos fundamentais de inviolabilidade da intimidade, da honra, da imagem e da vida privada.
- Autodeterminação informativa - ao expressar o direito do cidadão ao controle, e assim, à proteção de seus dados pessoais e íntimos.
- Liberdade de expressão, de informação, de comunicação e de opinião - que são direitos previstos na Constituição brasileira.
- Desenvolvimento econômico e tecnológico e a inovação - a partir da criação de um cenário de segurança jurídica em todo o país.

(continuação): QUAIS OS FUNDAMENTOS DA LGPD (ART. 2º)?

- Livre iniciativa, livre concorrência e a defesa do consumidor - por meio de regras claras e válidas para todo o setor público e privado.
- Direitos humanos - o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas.

QUEM É O TITULAR DOS DADOS?

- É a pessoa natural (física) que tem o direito de ter os dados tratados observando a LGPD

QUAIS AS RESPONSABILIDADES DOS AGENTES DE TRATAMENTO DE DADOS

- Controlador: determina as finalidades, condições e meios do processamento de dados pessoais (art. 5º, VI)
- Operador: processa dados pessoais em nome do controlador (Art. 5º, VII)

RESPONSABILIDADES DO CONTROLADOR?

Função: Alocação de responsabilidades

Interna: Determinar quem será responsável pela conformidade com a lei de proteção de dados e como os indivíduos podem exercer seus direitos.

(continuação): RESPONSABILIDADES DO CONTROLADOR?

Orientar os operadores:

- POR QUÊ coleto os dados do titular
- COMO: qual a base legal para fazê-lo;
- QUEM: sobre quais indivíduos irá coletar os dados;
- O QUE: quais dados pessoais irá coletar (o conteúdo dos dados);
- PARA QUE: a finalidade ou os propósitos para os quais os dados serão usados;
- PARA QUEM: divulga, compartilha ou transfere os dados

Externa: Como as partes podem ser um controlador em uma transação e um processador em outra, determinar qual parte é um controlador é crucial para atribuir a responsabilidade e a responsabilidade da proteção de dados pessoais

QUAIS OS DIFICULDADES NA ADEQUAÇÃO À LGPD

- Identificar os dados pessoais no sistema de negócio
- Determinar quando, como, porque e por quem foram tratados
- Determinar a origem e destino destes dados dos processos de negócio

QUAIS AS BASES LEGAIS PARA QUE POSSA SER TRATADOS DE DADOS PESSOAIS (Art. 7º, I a X)

I - mediante o fornecimento de consentimento pelo titular

II para cumprir obrigação legal ou regulatória pelo controlador

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas

IV - para realizar estudos por órgão de pesquisa, garantindo sempre, que possível, a anonimização dos dados pessoais;

V - 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

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro

VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;

IX - 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

X para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente

QUANDO TERMINARÁ O TRATAMENTO DE DADOS (Seção IV – Art. 15 e 16)

- Finalidade alcançada
- Fim do período de tratamento (vigência)
- Determinação da ANPD

QUAL É A EXCEÇÃO PARA NÃO ELIMINAR OS DADOS PESSOAIS APÓS O TÉRMINO DA VALIDADE

- Cumprimento de obrigação legal e regulatória
- Estudo por órgão de pesquisa
- Se consentido transferência a terceiros
- Uso exclusivo do controlador se for dado anonimizado

QUAIS AS OPORTUNIDADES COM A IMPLANTAÇÃO DA LGPD

- Visibilidade e credibilidade da MGI
- Inovação dos processos
- Novos negócios

EXISTEM RISCOS A SEREM MITIGADOS

- Prejuízo à imagem da MGI
- Multa de 2% do faturamento no limite de 50 milhões
- Ressarcimento de danos causados

Qual a Importância e o Objetivo da LGPD?

Com o aumento dos escândalos envolvendo vazamentos e uso indevido de dados, o advento de uma legislação que trate do tema é essencial para resguardar os titulares dessas informações contra abusos e violação de privacidade.

Neste cenário, as organizações que envidarem esforços para se adequar à legislação (não somente à LGPD), poderão largar na frente e ter um diferencial competitivo que as colocará em vantagem perante a sua concorrência, quem ainda não estiver de acordo com a LGPD ou que não tiver em seu radar a preocupação com privacidade e segurança de dados pessoais.
Para as empresas que fazem tratamento de dados pessoais, há a necessidade de adaptar seu modelo de negócio para se adequar à legislação e à tendência mundial de segurança e proteção de dados

A LGPD beneficia ambas as partes, o titular de dados e a empresa. Ela veio para deixar a empresa eficiente e competitiva.

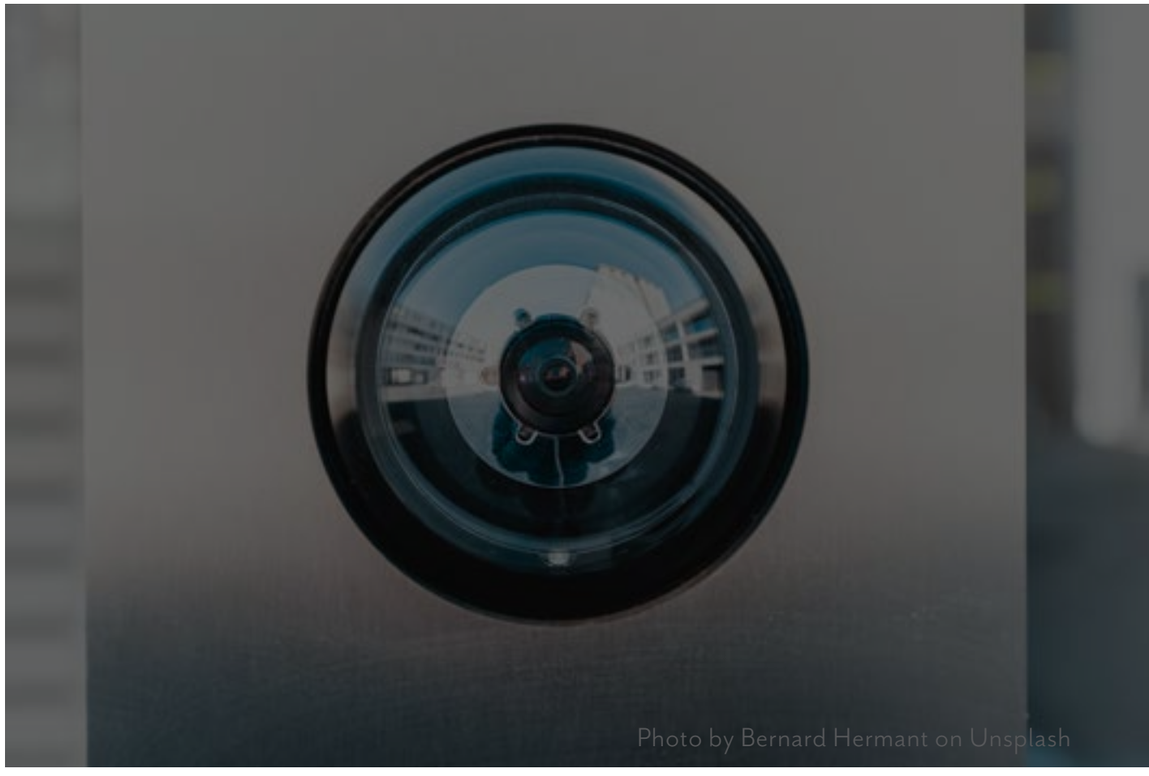


Photo by Bernard Hermant on Unsplash

São objetivos da LGPD:

- Proteger os direitos fundamentais de liberdade, privacidade
- Oferecer ao titular dos dados maior conhecimento, controle e transparência
- Fomentar o desenvolvimento econômico e tecnológico

Quais os fundamentos da LGPD (art. 2º)?

- Respeito à privacidade - ao assegurar os direitos fundamentais de inviolabilidade da intimidade, da honra, da imagem e da vida privada.
- Autodeterminação informativa - ao expressar o direito do cidadão ao controle, e assim, à proteção de seus dados pessoais e íntimos.
- Liberdade de expressão, de informação, de comunicação e de opinião - que são direitos previstos na Constituição brasileira.
- Desenvolvimento econômico e tecnológico e a inovação - a partir da criação de um cenário de segurança jurídica em todo o país.
- Livre iniciativa, livre concorrência e a defesa do consumidor - por meio de regras claras e válidas para todo o setor público e privado.
- Direitos humanos - o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas.

Quem é o titular dos dados?

É a pessoa **natural (física)** que terá seus dados tratados.

Photo by Ryoji Iwata on Unsplash

Quais são os direitos dos titulares da LGPD?

- Confirmação da existência de tratamento.
- Acesso facilitado aos dados.
- Correção de 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.
- Informações sobre compartilhamento de dados.
- Anulação do aceite

Acesso aos dados: o titular deve possuir acesso fácil, livre e gratuito referente a quais dados que a empresa detém seus. Entende-se por livre acesso a prestação de informações (quais dados, porque daqueles dados, se são transferidos para outro local).

Revogação do consentimento: Os controladores devem informar aos titulares que eles têm o direito de revogar seu consentimento a qualquer tempo e como podem exercer esse direito, preferencialmente, por meio de um procedimento rápido e simplificado e sem serem prejudicados.

Photo by Morning Brew on Unsplash

Quem são os agentes de tratamento?

Controlador: Pessoa física ou jurídica que tomará as decisões referente ao tratamento de dados pessoais.

Operador: Pessoa física ou jurídica que realizará o tratamento de dados pessoais a mando do Controlador.

Encarregado de Dados / (DPO- Data Protection Officer): pessoa natural indicada pelo controlador responsável por fazer comunicação entre controlador, titulares e autoridade nacional. Ele é um gestor, que não tratará os dados diretamente, mas garantirá que todos os processos de tratamento de dados estejam em conformidade com a LGPD.

Assim, dentre as funções do Encarregado, destacamos:

- recepcionar e atender demandas dos titulares de dados;
- interagir com a Autoridade Nacional de Proteção de Dados e
- orientar funcionários e contratados quanto a práticas de proteção de dados.

O DPO se reporta diretamente ao mais alto nível de direção, deve ser dotado de **autonomia** e **estabilidade**, i**ndependência orçamentária** e se mostra obrigatório para empresas que tratam dados pessoais como controladoras.

O que é ANPD (Autoridade Nacionaç de Proteção de Dados - art. 5º, XIX)?

É autoridade constituída como responsável por zelar, implementar e fiscalizar o cumprimento da LGPD. A ANPD foi regulamentada pela Lei 13.853/2019 e lhe cabe:

- Zelar pela proteção dos dados pessoais.
- Editar normas e procedimentos.
- Decidir sobre a interpretação da LGPD, inclusive sobre casos omissos.
- Requisitar informações às empresas que realizam tratamento de dados.
- Implementar mecanismos para o registro de reclamações.
- Instaurar processo administrativo;
- Fiscalizar e aplicar, exclusivamente, as sanções.

O que são dados pessoais (art. 5º)?

Dados pessoais segundo a Lei, é informação relacionada a **pessoa natural identificada ou identificável.** Assim, a LGPD traz um conceito amplo e aberto, pois qualquer dado, isoladamente (dado pessoal direto) ou agregado a outro (dado pessoal indireto) possa permitir a identificação de uma pessoa natural, pode ser considerado como dado pessoal.

Exemplos: dados cadastrais, data de nascimento, profissão, dados de GPS, identificadores eletrônicos, nacionalidade, gostos, interesses e hábitos de consumo, entre outros.

O que são dados pessoais sensíveis (art. 5º)?

A LGPD estabelece, também, que alguns dados pessoais estão sujeitos a cuidados ainda mais específicos, como os "dados sensíveis" e os dados sobre "crianças e adolescentes":

Dado pessoal sensível é o dado pessoal que verse 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.

O que não é considerado dado pessoal?

São os dados anonimizados ou que passam por processo de anonimização (art. 5º, III e XI).

O que são dados anonimizados (art. 5º, III)?

São os dados que não podem ser associados a um indivíduo. É o oposto ao dado pessoal. A LGPD não se aplica a ele, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

O que é anonimização (art. 5º, XI)?

É a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio das quais um dado perde a possibilidade de associação, direta ou indireta a um indivíduo.

O que é tratamento de dados?

O escopo da lei é bem amplo, sendo considerada qualquer operação efetuada sobre os dados pessoais, seja manual ou automatizada. Portanto, a mera visualização de dados por um funcionário caracteriza tratamento.

A lei elenca 20 (vinte) ações consideradas tratamento de Dados como as que se referem a:

- **Acesso** - possibilidade de comunicar-se com um dispositivo, meio de armazenamento, unidade de rede, memória, registro, arquivo etc., visando 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;
- **Distribuiçã**o - 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;
- T**ransferência** - 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; e
- **Utilização** - ato ou efeito do aproveitamento dos dados.

Exemplos de tratamento de dados:

- Quando um empresário ou um gestor público administra folhas de pagamentos;
- A ação de um comerciante que envia promoções por e-mail;
- O ato de publicar uma foto ou de deletar documentos em uma rede social;
- Fazer gravações em vídeo do movimento nos corredores de um shopping;
- Uma loja virtual armazena os endereços IP de seus clientes;
- Eliminação e descarte de documentos que contenham dados pessoais.

Quais os requisitos para a realização do tratamento de dados pessoais de crianças e adolecentes?

- Fornecimento de aprovação específica por pelo menos um dos pais ou pelo responsável legal - consentimento.
- As empresas deverão dispor de tecnologias capazes de verificar que a aprovação foi dada pelo responsável da criança e/ou adolescente.

Quando ocorre o término do tratamento de dados (art. 15º)?

- Quando a finalidade da coleta foi alcançada ou quando os dados deixarem de ser necessários ou pertinentes ao alcance da finalidade almejada.
- Através da solicitação do titular.
- Por determinação da Agencia Nacional de Proteção de Dados (ANPD).

Quem a LGPD protege?

A LGPD PROTEGE dados de pessoas físicas. Ela NÃO PROTEGE os dados de pessoas jurídicas.

A quem a LGPD se aplica?

A LGPD PROTEGE dados de pessoas físicas. Ela NÃO PROTEGE os dados de pessoas jurídicas.

Qual o âmbito de aplicação da LGPD (art. 3º)?

A LGPD aplica-se a qualquer operação de tratamento de dados pessoais realizada em território brasileiro ou relacionada a dados pessoais de indivíduos localizados no Brasil no momento em que os dados foram coletados, ou ainda se o tratamento de dados pessoais tem por objetivo oferecer produtos ou serviços no Brasil. Além disso, é importante notar que a LGPD não está restrita ao ambiente digital.

Quais as hipótesis de aplicação da LGPD?

- Dados relacionados à pessoa (brasileira ou não) que esteja no Brasil, no momento da coleta;
- Dados tratados dentro do território nacional, independentemente do meio aplicado, do país-sede do operador ou do país onde se localizam os dados;
- Dados usados para fornecimento de bens ou serviços.

Em quais situações não é aplicável a LGPD (art. 4º)?

- Ao tratamento de dados de pessoas jurídicas e dados anonimizados.
- Ao tratamento de dados pessoais realizados por pessoa natural para fins exclusivamente particulares e não econômicos.
- Para fins exclusivamente jornalísticos, acadêmicos e artísticos.
- Garantir a segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais.

A LGPD lista 10 (dez) princípios que devem ser levados em consideração no tratamento

I- Princípio da Finalidade: toda vez que houver tratamento de dados pessoais deve haver uma finalidade clara, específica e objetiva. A finalidade não pode ser determinável, mas sim determinada.

II- Princípio da Adequação: é a adequação da compatibilidade do tratamento de dados com a finalidade informada ao titular, de acordo como o contexto do tratamento. É coletar os dados que são necessários da maneira mais adequada, pensando sempre na finalidade da coleta.

III- Princípio da Necessidade: devem ser coletados aqueles dados que de fato são necessários para atingir a finalidade para o qual foi coletado.

Coletar dados não necessários aumenta o risco de vazamento de dados.

Novo mindset: Quanto menos dados eu coleto, mais eficiente é a empresa.

IV- Princípio do 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.

V- Princípio da Qualidade dos Dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados. Em outras palavras, A empresa deve manter o banco de dados fidedigno, correto, pois um dado incorreto pode trazer prejuízo para o titular.

VI- Princípio da Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento.

Transparência gera segurança. E segurança é a base de qualquer relação.

VII- Princípio da 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.

VIII- Princípio da Prevenção: é preciso buscar meios para evitar/prevenir a ocorrência de danos aos titulares de dados pessoais.

Registre-se que a LGPD não exige que a organização/empresa não tenha nenhum incidente de segurança, mas ela exige que ela esteja prevenida. Ou seja, que a organização/empresa saiba agir corretamente no caso de um incidente de segurança, para que os danos causados sejam minimizados.

Aqui está a importância de uma cultura de proteção de dados em um programa de conformidade. Pois com essa cultura disseminada haverá uma busca de prevenção de danos e de mitigação e/ou minimização de possíveis situações de risco.

IX- Princípio da Não-Discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

X- Responsabilização e Prestação de Contas (Accountability): 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 empresa deve prestar contas do tratamento de dados que ela trata. Ela precisa demonstrar aos titulares, ao mercado e à ANPD que possui estratégias de atenuar quaisquer possíveis riscos relacionados a proteção de dados pessoais.

Estes princípios não devem ser vistos apenas como obrigações impostas

pela lei, mas como os novos valores da empresa. Logo é tão importante criar uma nova cultura de proteção de dados.

O que são Bases Legais da LGPD (art. 7º)?

As empresas deverão comprovar ao menos uma das seguintes bases legais para realizar o tratamento dados pessoais.

As bases legais são as hipóteses que a lei autoriza/legitima para que o tratamento daqueles dados seja realizado. Em outras palavras, a base legal serve como uma "justificativa" para que ocorra o tratamento de dados. As bases legais variam de acordo com o fluxo de dados dentro da empresa. Das 10 (dez) hipóteses previstas na LGPD, 06 (seis) são aplicadas à MGI.

Uma base legal não tem preponderância sobre a outra. Ou seja, o consentimento não vale mais do que o legítimo interesse ou qualquer das outras 08 (oito) bases. Por exemplo, ao fundamentar o tratamento de dados com base no legítimo interesse, não é necessário obter o consentimento.

As bases legais que NÃO se aplicam à MGI são:

I- Pesquisa por Órgão: nesta o objeto social da empresa deve ser pesquisa cientifica ou acadêmica.

II- A tutela de saúde: é exclusivamente, em procedimentos realizado por profissionais de saúde ou autoridade sanitária.

III- Proteção ao crédito: está ligada a instituições financeiras. Não tem previsão na GDPR. Existe em razão do lobby das instituições financeiras.

IV- Políticas Públicas: não precisa de consentimento quando dados forem tratados para políticas públicas previstas em leis/ regulamentos ou respaldadas em contratos públicos. Esta base legal somente pode ser usada por órgãos da administração pública porque são eles os detentores das políticas públicas. Empresas privadas não podem usar essa base legal.

As bases legais que SE APLICAM à MGI são:

I- Obrigação Legal: é quando há uma norma de qualquer natureza (lei, decreto, MP) que me obrigue a tratar dados pessoais. Assim se houver uma base legal a empresa não precisa solicitar o consentimento. Porém precisa justificar ao titular dos dados qual é a obrigação legal.
Exemplos:
1. Hospitais tem a obrigatoriedade de armazenar prontuários médicos por 20 anos, ainda que o paciente não queira.

2. Raça é opcional no E-social, portanto, não pode ser exigida, não pode ser coletada pelo RH com fundamento na regulação ou

Obrigação Legal referente ao E-social, já que neste é opcional.

II- Processo Judicial ou Exercício Regular do Direito em Processo: é para exercer o direito constitucional de acesso à justiça (de mover ou se defender de uma ação judicial). Refere-se aos processos judiciais, administrativos, etc.

III- Execução de Contrato: refere-se ao tratamento, compartilhamento ou armazenamento. É quando trata-se de dados para cumprir uma obrigação legal.
Exemplo: 1. aplicativo de delivery (o aplicativo terá que transferir certos dados do titular para o restaurante e para o motoboy).

IV- Proteção à Vida: é para proteger a vida ou a integridade física de uma pessoa ou de um terceiro. Isso somente pode ser feito quando a vida de uma pessoa estiver em risco IMINENTE (se o dado não for tratado naquele exato momento, a vida daquela pessoa está seriamente em risco). A situação de proteção a vida deve ser concreta.

V- Legítimo Interesse: finalidades legítimas são consideradas a partir de situações concretas, respeitadas as legítimas expectativas do usuário. A LGPD não traz uma lista pré-determinada do que constitui ou não legítimo interesse. A empresa não pode alegar

lucro como legitimo interesse para tratar aquele dado.

- **Teste do Legitimo Interesse - LIA (legitimate interests assessment):** Se em qualquer das etapas a resposta for negativa, essa base deve ser descartada.

AVALIAÇÃO DE LEGITIMIDADE	1. Existe uma situação concreta? 2. O interesse da empresa é legítimo, lícito, adequado e proporcional?
TESTE DE NECESSIDADE	3. Existe alguma outra base legal na LGPD que seria mais adequada? 4. Apenas os dados estritamente necessários para atingir a finalidade pretendida estão sendo processados?
REGRA DE BALANCEAMENTO	5. O uso dos dados está dentro da legítima expectativa do usuário? 6. Os direitos e liberdades fundamentais dos usuários estão sendo observados?

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

Inequívoco: o consentimento não pode ser manipulado. A política de privacidade tem que ter informações com linguagem simples, acessível e objetiva. Não são mais aceitáveis aqueles documentos enormes com letras minúsculas, com linguagem rebuscada e jurídica.

Consentimentos que são considerados nulos:

- Os consentimentos genéricos para tratamento de dados;
- Se o dado for utilizado para finalidade diversa da inicialmente consentida.

Quando os dados pessoais devem ser eliminados (art.15º)?

A LGPD estipula a obrigatoriedade de eliminação dos dados pessoais ao término do tratamento. Isso ocorre nas seguintes hipóteses:

a) verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;

b) fim do período de tratamento;

c) comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento, resguardado o interesse público; ou

d) determinação da autoridade nacional, quando houver violação da lei.

Quando a LGPD autoriza a conservação dos dados pessoais (art. 16º.)?

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

c) transferência à terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na lei; ou

d) uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Quais as sanções previstas na LGPD (art. 52º)?

A LGPD implementa a aplicação de severas sanções para empresas que descumprirem as disposições legais e por que motivo, mostra-se relevante a adequação das empresas ao disposto na Lei.

Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas na Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional (art. 52º):

I- Advertência, com indicação de prazo para adoção de medidas corretivas;
II- 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;
III- Multa diária, observado o limite total a que se refere o inciso II;
IV- Publicização da infração após devidamente apurada e confirmada a sua ocorrência;
V- Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
VI- Eliminação dos dados pessoais a que se refere a infração.

Quem responde pelas sanções previstas na LGPD?

O Controlador e Operador (os agentes de tratamento) responderão solidariamente pelos danos que causarem no exercício de suas atividades, respondendo civil e administrativamente em caso de descumprimento da LGPD.
Há 03 (três) hipóteses em que, havendo um incidente de segurança o Controlador e Operador, não serão responsabilizados, se provarem que:
a) Não realizaram o tratamento daqueles dados
b) Não houve violação à lei
c) O dano é decorrente de alguma atividade do titular ou de terceiros

Como criar um programa de privacidade em prevenção de dados?

Através de um programa de adequação com as seguintes etapas:

1. Conscientização: A conscientização ajuda a implementação ser mais efetiva. Os colaboradores da empresa precisam compreender a lei para que haja uma cultura de proteção de dados e, assim estar em compliance/conformidade.

2. Mapeamento: no mapeamento será feito o fluxo de dados da empresa (quais são os dados pessoais, como são coletados... porque são coletados, por onde os dados chegam, onde estão armazenados, por quanto tempo ficam armazenados, são compartilhados externamente, qual a forma que são armazenados).

3. Gap Analysis: é analisar tudo que esteja em desacordo com a LGPD. O objetivo desta fase é identificar as principais vulnerabilidades relacionadas aos dados pessoais e indicar as melhores soluções dentro do modelo de negócio da empresa.

4. Planejamento: criar o plano de ação que determinará o que de fato será implementado na empresa para solucionar os problemas ou pelo menos minimizar/mitigar os riscos envolvidos.

5. Implementação: nesta fase será colocada em prática o plano de ação, serão elaborados os documentos necessários para instituição de uma nova Política de Privacidade, redigir novos contratos, novos aditivos, rever o Código de Conduta e outros. Quando essa fase acabar, a empresa estará em conformidade coma a LGPD e que ela tem um programa de governança em proteção de dados.

6. Monitoramento: Esta última fase é contínua. Cabe ao DPO monitorar se a empresa continua em conformidade quanto a privacidade de proteção de dados, assim como se a empresa continua com a cultura de proteção.

Regularmente, é preciso rever o programa, avaliar sua eficácia e aplicar as mudanças necessárias a ele (que pode ser uma mudança proveniente da própria empresa ou de uma mudança da própria LGPD).

Quais são os pilares de segurança da LGPD?

Confidencialidade: Ela está ligada ao nível de segurança que a informação se encontra dentro de determinada empresa.

Integridade: está diretamente ligada à confiabilidade das informações presentes em determinada empresa.

Disponibilidade: é o acesso a esses dados, a essas informações presentes dentro da empresa tanto pelos colaboradores quanto pelos próprios usuários.

Da segurança e sigilo dos dados

- A empresa deve adotar medidas de segurança aptas à proteção dos dados desde a coleta até a sua exclusão.
- Necessidade de comunicação à autoridade nacional e ao titular de eventual incidente de segurança que possa acarretar risco ou dano.
- Implantação de medidas técnicas adequadas que tornem os dados ininteligíveis em caso de incidente de segurança.

Da segurnaça de dados pessoais

A LGPD apresenta a segurança, prevenção e a adoção de medidas para o estabelecimento de boas práticas e governança no tratamento de dados pessoais como pilares, sendo relevante observar que a Autoridade Nacional de Proteção de Dados (ANPD) poderá dispor sobre os padrões técnicos mínimos para tornar aplicável os padrões de segurança e governança, em especial para o tratamento de dados pessoais sensíveis.

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

Da política de boas práticas e governanças

Do ponto de vista prático, um programa de governança em privacidade deve:

- Demonstrar o comprometimento da instituição em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
- Ser aplicável a todo o conjunto de dados pessoais que estejam sob o controle da empresa, independentemente do modo como se realizou sua coleta;
- Ser adaptado à estrutura, à escala e ao volume das operações da instituição, bem como à sensibilidade dos dados tratados;
- Estabelecer políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
- Ter o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

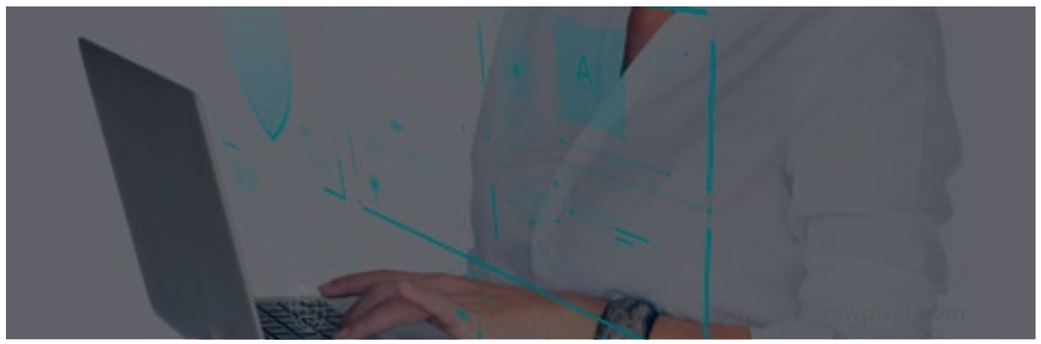
- Estar integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
- Contar com planos de resposta a incidentes e remediação; e
- Ser atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

O que é privacy by design?

O ***Privacy by design*** representa o emprego de mecanismos/soluções de privacidade durante todo o ciclo de vida dos dados. Por referido conceito, a privacidade é incorporada à própria arquitetura dos sistemas e processos desenvolvidos, de modo a garantir, pela infraestrutura do serviço prestado, condições para que o usuário seja capaz de preservar e gerenciar sua privacidade e a coleta e tratamento de seus dados pessoais.

O que é privacy by defalt?

Privacy by default representa a obrigatoriedade de que todas essas ferramentas estejam acionadas como padrão. Ou seja, estabelecer como configuração padrão a maior privacidade possível ao titular dos dados. Os agentes de tratamento devem, portanto, desde a concepção do produto ou do serviço, até a sua execução, adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (art. 46, §2º).



Conclusão

As mudanças da LGPD envolvem questões legais, tecnológicas e processuais e ela não deve ser encarada como um desafio pontual, mas um processo contínuo. Um dos pilares para sustentar essas mudanças de forma duradoura é através da construção e manutenção de um programa de privacidade.

Logo, a LGPD não deve ser encarada como um desafio pontual, mas um processo contínuo. É essa nova cultura que fortalecerá a MGI no quesito de proteção de dados pessoais.

Novo mindset
MENOS DADOS MELHOR
MENOS DADOS MAIS
TRANSPARENCIA

Perguntas frequentes

O que é GDPR?

O GDPR (General Data Protection Regulation): A sigla pode ser traduzida como Regulamento Geral sobre a Proteção de Dados. É um regulamento do Parlamento Europeu e Conselho da União Europeia que estabelece regras sobre a privacidade e proteção de dados de cidadãos da União Europeia e Espaço Econômico Europeu. Sua vigência teve início em maio de 2018.

Quais são as hipóteses em que pode ocorrer tratamento sem consentimento?

- Para o cumprimento de obrigação legal ou regulatória pelo controlador.
- Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais.
- Para a proteção da vida ou da incolumidade física do titular ou de terceiros.
- Para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias, por exemplo, para proteção da vida, as atividades exercidas pela Defesa Civil; todas as atividades de saúde, como a notificação compulsória de doenças e agravos e violências (leis 6259/75, 8069/90, 10.741/03, 13.146/15).
- 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, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem).
- Para a proteção da vida ou da incolumidade física do titular ou de terceiros.
- Quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.
- Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

O titular pode revogar o consentimento?

Sim, a qualquer tempo o titular pode revogar seu consentimento, exceto quando o consentimento for dispensável. Essa revogação

poderá ser requerida mediante manifestação expressa do titular, por procedimento gratuito e facilitado. Além disso, o cidadão pode solicitar que seus dados sejam deletados, ou pode solicitar transferir dados para outro fornecedor de serviços (esta opção não é usual no serviço público, uma vez que, de um modo geral não há opção de prestador).

O controlador, entretanto, poderá se opor à exclusão dos dados solicitados pelo titular, apresentando razões fundamentadas acerca da continuidade/guarda das informações. Por exemplo, na área da saúde, não é possível excluir dados de prontuários médicos, ainda que solicitados pelo paciente, haja vista a obrigação legal imposta pela Lei nº 13.787/18, que determina a guarda do prontuário pela instituição de saúde pelo prazo mínimo de 20 anos.

Há tipos de dado pessoal que exigem atenção extra ao serem tratados?

Sim. Claro, todo dado pessoal só pode ser tratado se seguir um ou mais critérios definidos pela LGPD, mas, dentro do conjunto de dados pessoais, há ainda aqueles que exigem um pouco mais de atenção: são os sobre crianças e adolescentes; e os "sensíveis", que são os que revelam origem racial ou étnica, convicções religiosas ou

filosóficas, opiniões políticas, filiação sindical, questões genéticas, biométricas e sobre a saúde ou a vida sexual de uma pessoa.

Quando o foco for menor de idade, é imprescindível obter o consentimento inequívoco de um dos pais ou responsáveis e se ater a pedir apenas o conteúdo estritamente necessário para a atividade econômica ou governamental em questão, e não repassar nada a terceiros. Sem o consentimento, só pode coletar dados se for para urgências relacionadas a entrar em contato com pais ou responsáveis e/ou para proteção da criança e do adolescente.

Sobre os dados sensíveis, autônomos, empresas e governo também podem tratá-los se tiverem o consentimento explícito da pessoa e para um fim definido. E, sem consentimento do titular, a Lei Geral de Proteção de Dados Pessoais define que isso é possível quando for indispensável em situações ligadas: a uma obrigação legal; a políticas públicas; a estudos via órgão de pesquisa; a um direito, em contrato ou processo; à preservação da vida e da integridade física de uma pessoa; à tutela de procedimentos feitos por profissionais das áreas da saúde ou sanitária; à prevenção de fraudes contra o titular.

Há alguma especificidade para o tratamento de dados de crianças e adolescentes?

Sim. Esse tratamento deverá ser realizado com o consentimento específico, e em destaque, dado por, pelo menos, um dos pais ou responsável legal. Órgãos sujeitos a tratamento de crianças e adolescentes deverão tomar a medida necessária para manter controle desse consentimento, uma vez que podem ser demandados, a qualquer momento, a demonstrar quais dados foram tratados, de que forma, e quais são os respectivos responsáveis. Sem o consentimento, só se pode coletar dados de crianças e adolescentes se for para urgências relacionadas a entrar em contato com os pais ou responsáveis e/ou para proteção da criança e do adolescente.

O que a lei considera criança e 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.

Como é feito o tratamento de dados de crianças e adolescentes?

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. Deverá ser coletado o consentimento dos pais ou responsáveis para efetuar tratamento de dados de criança ou adolescente.

Existem dados pessoais que exigem mais proteção do que outros?

Sim, o tratamento de algumas categorias de dados pessoais oferece maiores riscos de danos aos respectivos titulares e por isso são tratados pela LGPD como “dados sensíveis”. São considerados dados sensíveis pela LGPD: 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. É importante observar que a fotografia do rosto de uma pessoa pode ser considerada dado biométrico.

Posso usar dados públicos à vontade?

Dados pessoais publicamente disponíveis – seja porque foram tornados públicos pelo titular, seja porque encontram-se em bases de acesso público – não deixam de ser dados pessoais. Nesses casos, a LGPD permite que dados pessoais sejam utilizados sem necessidade de obtenção de consentimento do titular, mas continua sendo necessário enquadrar esse tratamento em uma das outras bases legais disponíveis e observar todos os direitos dos titulares de dados e os princípios estabelecidos pela LGPD. Ou seja, é necessário dar transparência ao tratamento desses dados publicamente disponíveis e às finalidades do tratamento, enquadrar o tratamento em uma base legal, franquear ao titular acesso a informações sobre quais dados pessoais estão sendo tratados, como e porque, entre outras obrigações aplicáveis.

O que é 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.

O que é Relatório de Impacto à Proteção de Dados Pessoais - RIPD (ART. 5º, XVII)?

É a documentação do controlador que deve conter 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 prevenção e mitigação de risco. O prazo de seu envio será regulamentado pela ANPD.

O que é direito de oposição?

O § 2º do artigo 18 da LGPD estipula que "o titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei". Em outras palavras, toda vez que a base legal de tratamento de dados não for o consentimento e houver descumprimento da LGPD, o titular pode se opor ao tratamento de seus dados pessoais, independentemente da adoção de medidas corretivas ou imposição de penalidades, exigindo a imediata interrupção de qualquer atividade de tratamento.

A MGI pode ser responsabilizada por atos de terceiros?

Sim. Todos os profissionais ou empresas que tomarem decisões e estiverem diretamente envolvidos nas atividades de tratamento de dados pessoais realizadas em violação à lei serão solidariamente responsáveis pelo ressarcimento dos danos causados aos titulares, salvo se puderem provar que:

- Não realizaram o tratamento de dados pessoais que lhes é atribuído, ou
- Embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados, ou
- O dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros. Por esses motivos, é bastante importante trabalhar com parceiros comerciais que estejam buscando se adequar à LGPD, já que eventual desconformidade alheia pode, conforme as circunstâncias do caso, acarretar responsabilidade solidária.

O que é vazamento de dados?

É a transmissão não autorizada de dados de dentro de uma organização para um destino ou recipiente externo. Os dados podem ser transferidos eletronicamente ou fisicamente, de forma

acidental ou intencional (pela ação de agentes internos, pela ação de agentes externos ou pelo uso de software malicioso).

O que é garantia da segurança da informação?

É a capacidade de sistemas e organizações assegurarem a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação. A Política Nacional de Segurança da Informação (PNSI) dispõe sobre a governança da segurança da informação aos órgãos e às entidades da administração pública federal em seu âmbito de atuação.

O que é Criptografia?

É a arte de proteção da informação através de sua transformação em um texto cifrado (criptografado), com o uso de uma chave de cifragem e de procedimentos computacionais previamente estabelecidos, a fim de que somente o(s) possuidor(es) da chave de decifragem possa(m) reverter o texto criptografado de volta ao original (texto pleno). A chave de decifragem pode ser igual (criptografia simétrica) ou diferente (criptografia assimétrica) da chave de cifragem.

O que é uso compartilhado de dados?

É a comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicas 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.

Bibliografia

1- O Guia Descomplicado da LGPD, Grupo Assaf. Disponível em: https://www.grupoassaf.com/

2- Aspectos Gerais sobre a Lei Geral de Proteção de Dados, Paulo Roberto Advogados Associados. Disponível em: www.paulorabelo.adv.br.

3- A regulação de proteção de dados e seu impacto para a publicidade online: um guia para a LGPD, Baptista Luz Advogados. Disponível em: https://baptistaluz.com.br/institucional/a-regulacao-de-protecao-de-dados-e-seu-impacto-para-a-publicidade-online-um-guia-para-a-lgpd/

4- LGPD – Lei Geral de Proteção de Dados, FIESP (Federação das Indústrias do Estado de São Paulo). Disponível em: https://www.fiesp.com.br/indices-pesquisas-e-publicacoes/cartilha-lei-geral-de-protecao-de-dados-out-2019-3a-edicao/

5- Manual de Boas Práticas para aplicação da Lei Geral de Proteção de Dados, ACREFI (Associação Nacional das Instituições de Crédito, Financiamento e Investimento). Disponível em: www.accrefi.org.br

6- Lei Geral de Proteção de Dados Pessoais – Prefeitura de Belo Horizonte: https://prefeitura.pbh.gov.br/sites/default/files/estrutura-de-governo/controladoria/2020/cartilha_lgpd-1.pdf

MGi
Minas Gerais Participações S.A.

MINAS GERAIS
GOVERNO DIFERENTE.
ESTADO EFICIENTE.