LGPD

Lei Geral de Proteção de Dados Pessoais

QUALITEC
CONSULT

GLOSSÁRIO.

- **Dado pessoal:** Trata-se de informação relacionada à pessoa natural/pessoa física identificada ou identificável ("Titular" ou "Titular dos Dados"), ou seja, qualquer informação que permita identificar, direta ou indiretamente uma pessoa. São exemplos de dados pessoais: nome, RG, CPF, endereço residencial, número de telefone, data de nascimento, e-mail, dados de localização, endereço de IP, elementos específicos da identidade física/aparência, aspectos específicos de sua personalidade, histórico de compras ou preferência de consumo.
- **Dado pessoal sensível:** São dados pessoais cujo tratamento pode levar a vulnerabilidades/fragilidades ou ensejar a discriminação do seu titular, tendo em vista que estão diretamente relacionados aos aspectos mais íntimos da vida de uma pessoa, como origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico relativos a esta pessoa singular.
- **O que não são dados pessoais:** Toda informação que não pode ser associada a uma pessoa física específica. Informação relacionada a uma pessoa jurídica (por exemplo, uma empresa ou uma instituição) não é dado pessoal. Dado anonimizado também não é dado pessoal.
- **Anonimização:** Técnica de tratamento que retira a possibilidade de os dados pessoais serem associados, direta ou indiretamente, a um indivíduo/titular, ou seja, é um dado que passa por uma técnica que torna inviável identificar a pessoa a quem se refere tal dado. Portanto, o dado anonimizado é aquele que foi submetido à anonimização.
- **Titulares:** Titular é a pessoa física/natural a quem se refere os dados pessoais que são objeto do tratamento. Pela lei, você é titular dos seus dados pessoais.
- **Controlador:** Pessoa física ou jurídica, pública ou privada, a quem cabe decidir a respeito do tratamento de dados dos indivíduos/titulares. Determina as finalidades e os meios de tratamento.
- **Operador:** Pessoa física ou jurídica, pública ou privada, que realiza o tratamento dos dados pessoais por designação/instruções do Controlador. Obedece a lei e as ordens do Controlador.
- **Agentes de tratamento:** Controlador e Operador. Eles devem manter registro de todas as operações de tratamento de dados pessoais que realizam.
- **Encarregado pelo Tratamento de Dados Pessoais (DPO – *Data Protection Officer*, em inglês):** Profissional que terá, entre outras atribuições legais, a função de atuar como canal de comunicação entre o Controlador, os Titulares e a Agência Nacional de Proteção de Dados (ANPD). É a pessoa indicada pelo Controlador ou pelo Operador que tem como função receber reclamações dos Titulares, prestar esclarecimentos, adotar providências e orientar os funcionários da instituição sobre a proteção de dados pessoais.
- **Tratamento de dados:** São todas as operações realizadas com dados pessoais das pessoas físicas/naturais, assim entendidos como 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.
- **Consentimento:** Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.
- **Relatório de impacto à proteção de dados pessoais (RIPD):** Documento elaborado pelo Controlador que contém medidas, salvaguardas, mecanismos de mitigação de risco, assim como a descriçãodos processos de tratamento de dados que podem gerar riscos às liberdades e aos direitos fundamentais.
- **Mapeamento de dados:** Procedimento por meio do qual a empresa poderá identificar quais os procedimentos que realiza, onde se encontram os dados pessoais que detém, como é o fluxo destes dados e quais dados pessoais são efetivamente tratados pela empresa.

1. Introdução.

A Lei Geral de Proteção de Dados Pessoais (LGPD) foi sancionada em 14/08/2018 e entrou em vigor em 18/09/2020, momento em que se tornou necessário o empenho e comprometimento de todos os envolvidos em prol da adequação às novas regras voltadas à proteção e ao tratamento de dados pessoais, considerando que toda interação entre empresas, clientes, funcionários, fornecedores e qualquer outro parceiro de negócios se dá a partir da coleta e uso de dados pessoais.

Deste modo, a LGPD tem como principal objetivo proteger os direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade da pessoa física, bem como garantir a proteção dos dados pessoais, tanto nos meios físicos quanto digitais, conforme se observa do disposto no artigo 5º, inciso LXXIX[1], da Constituição Federal (CF). Além disso, a LGPD também objetiva criar um cenário de segurança jurídica, com a padronização de regulamentos e práticas para promover a efetiva proteção dos dados pessoais de todo cidadão que esteja no Brasil, de acordo com os parâmetros internacionais existentes.

Para tanto, é importante destacar que a LGPD se aplica a qualquer operação de tratamento de dados pessoais realizado por pessoa física ou jurídica, de direito público ou privado, seja no meio físico ou digital, exceto para finalidades particulares, isto é, de uso pessoal, ou ainda para uso jornalístico, artístico e acadêmico, ou ainda para fins de segurança pública, defesa nacional, segurança do Estado e para atividades de investigação e repressão de infrações penais.

Portanto, a LGPD estipula uma série de obrigações para empresas públicas e privadas, com ou sem fins lucrativos, que realizem, dentre outras operações, a coleta, armazenamento, compartilhamento e eliminação de dados pessoais. Por isso, é de extrema importância que todas as empresas, independentemente de seu porte e segmento, estejam preparadas e munidas de informações para um processo de revisão e adequação das práticas de gestão à esta nova norma, avaliando os riscos, planejando as mudanças internas necessárias e se organizando para garantir a efetiva proteção dos dados e informações pessoais.

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 os Controladores (a quem competem as decisões sobre o tratamento de dados) e Operadores (aqueles que tratam os dados de acordo com o estipulado pelos Controladores).

[1] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

2. A importância dos Dados.

2.1. Por que os dados são importantes?

Nossos dados pessoais estão por todos os lugares, fornecemos estes dados para receber promoções em lojas, para comprar remédios na farmácia, para receber um serviço em um órgão público, para poder realizar um curso técnico, para contratar um plano de saúde, entre outros. Não bastando, também na *internet*, em troca da utilização gratuita de aplicativos e redes sociais, fornecemos nossos dados, tanto pessoais quanto de interesses gerais.

Assim, com base nos dados coletados, as empresas podem traçar nossas preferências e perfis de consumo – inclusive podem fazer previsões sobre o nosso comportamento – ou mesmo identificar melhores locais para investir. Além dos proveitos para o setor privado, os dados também geram significativos ganhos sociais e econômicos para o setor público. Os dados permitem reconhecer, filtrar e extrair valor de informações sobre políticas públicas para tomar melhores decisões. Fornecem ainda novas percepções em tempo real e previsões sobre onde agir para lidar com riscos e identificar novas oportunidades.

Os grandes conjuntos de dados – pessoais e não pessoais – formam uma cadeia de valor e estão se tornando um ativo fundamental na economia, estimulando novos setores, processos e produtos e criando significativas vantagens competitivas.

2.2. Por que os dados devem ser protegidos?

O crescente valor dos dados tem sido acompanhado pela preocupação acerca da coleta excessiva e imoderada destes dados, bem como da vulnerabilidade dos cidadãos por causa de usos inadequados, abusos flagrantes ou mesmo consequências indesejadas. Muitos dados têm sido usados, compartilhados, vendidos ou vazados com pouco – ou nenhum – envolvimento das pessoas mais afetadas e com pouca – ou nenhuma – consciência ética por parte das organizações responsáveis.

Nesse contexto, a proteção de dados pessoais tem por objetivo manter nossos dados seguros e garantir que sejam usados de maneira justa e responsável. É preciso construir confiança entre pessoas e organizações, reconhecendo o direito de um indivíduo de ter controle sobre suas informações pessoais – mesmo quando são mantidas por terceiros – e encontrando um equilíbrio entre esses direitos individuais e os interesses da sociedade.

3. O que é a Lei Geral de Proteção de Dados Pessoais (LGPD)?

A Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº. 13.709/2018), sancionada em 14/08/2018 e em vigor desde 18/09/2020, estabelece regras sobre o tratamento de dados pessoais, realizados por pessoa física ou jurídica, de direito público ou privado, com ou sem fins lucrativos, o que acaba englobando um amplo conjunto de operações que podem ocorrer tanto em meios manuais como em meios digitais.

O artigo 1º da LGPD dispõe sobre o tratamento de dados pessoais com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Cabe observar que a LGPD visa proteger tanto os dados mantidos em meios físicos, quanto digitais. Nesse aspecto, é importante observar que o risco de vazamento de dados não envolve apenas a cibersegurança dos meios digitais, mas também questões que envolvem a forma como os dados são coletados, armazenados e tratados em documentos físicos, devendo seguir os requisitos exigidos pela legislação.

O propósito da LGPD, portanto, é proporcionar transparência e proteção no tratamento de dados pessoais, devolvendo às pessoas maior controle sobre suas informações pessoais, além de assegurar o respeito aos direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade da pessoa física, conforme dispõe o artigo 5º, inciso LXXIX, da Constituição Federal (CF).

No âmbito da LGPD, o tratamento dos dados pessoais pode ser realizado por dois agentes de tratamento – o Controlador e o Operador. Além deles, há a figura do Encarregado pelo Tratamento de Dados Pessoais (*Data Protection Officer* – DPO), que é a pessoa indicada pelo Controlador para atuar como canal de comunicação entre o Controlador, o Operador, os titulares dos dados e a Agência Nacional de Proteção de Dados (ANPD).

4. A quem se aplica a Lei Geral de Proteção de Dados Pessoais (LGPD)?

A LGPD é aplicável a toda e qualquer atividade de tratamento de dados pessoais realizada por pessoa física ou jurídica, de direito público (exemplo: INSS) ou privado (exemplo: Lojas), independentemente do meio (físico ou digital), do país de sua sede ou do país onde estejam localizados os dados, desde que:

I) A operação de tratamento seja realizada no território nacional (Brasil);

II) A atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens/serviços para titulares que se encontrem no Brasil, seja de modo gratuito ou oneroso, e independentemente do país em que o tratamento ocorra;

III) Os dados pessoais, objeto do tratamento, tenham sido coletados no território nacional (Brasil).

Deste modo, as empresas devem se adequar à LGPD se, por exemplo: coletam dados de clientes para envio de ações promocionais ou de negócios; coletam dados através de site e aplicativos para venderprodutos ou serviços; analisam comportamento dos clientes para sugerir conteúdo específico; mantêm dados dos colaboradores e os utilizam para pagamentos de salários, ou terceirizam a coleta, armazenamento e/ou tratamento de dados pessoais.

No entanto, A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) NÃO SE APLICA ao tratamento de dados pessoais quando realizado nas seguintes situações:

I) Realizado por pessoa física para fins exclusivamente particulares e não econômicos. (Exemplo: um usuário do *Instagram* posta, em sua conta pessoal, uma fotografia de uma terceira pessoa ou coleta o número do telefone de um terceiro para armazenar na lista telefônica do próprio celular);

II) Realizado para fins exclusivamente: jornalístico, artísticos ou acadêmicos. (Exemplo: Jornalista que publica em site de notícias o nome, o sobrenome e a fotografia de um suspeito de cometer um crime);

III) Realizado para fins exclusivos de: segurança pública, defesa nacional, segurança do Estado, atividades de investigação e repressão de infrações penais. (Exemplo: Pesquisador de uma Universidade Federal utiliza dados pessoais, de forma anonimizada, para fundamentar sua pesquisa sobre longevidade da população brasileira ou quando autoridades divulgam um cartaz de "procurado", contendo o nome, sobrenome e o endereço do suspeito de cometer crimes);

IV) 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 ao previsto na LGPD. (Exemplo: Uma empresa brasileira é contratada por uma empresa europeia para realizar o tratamento de dados pessoais de cidadãos europeus, sendo que a empresa brasileira apenas tratou estes dados para aquilo que foi contratada, e, após, devolveu os referidos dados para a empresa europeia, atuando como mero Operador neste caso, razão pela qual não se aplica as disposições da LGPD, mas sim as disposições da legislação europeia – GDPR).

5. Quais os Fundamentos da LGPD?

O artigo 2º, da LGPD, estabelece que são fundamentos da legislação, ou seja, são os sustentáculos da disciplina de proteção de dados, os seguintes:

- O RESPEITO À PRIVACIDADE.

A privacidade possui posição de destaque nos fundamentos da LGPD. Está em consonância com a Declaração Universal dos Direitos Humanos (artigo 12), bem como com a nossa Constituição Federal (artigo 5º, inciso X), segundo as quais o direito à privacidade é garantia fundamental do ser humano, tratando-se de condição essencial para o livre desenvolvimento da personalidade humana. A proteção da privacidade, conforme a LGPD, tem como objetivo primordial garantir ao titular dos dados pessoais o controle sobre o acesso de terceiros à sua vida privada. Por esse motivo, a legislação versa sobre as condições e hipóteses de tratamento dos dados pessoais.

- A AUTODETERMINAÇÃO INFORMATIVA.

Desdobramento do direito à privacidade, o segundo fundamento abriga a filosofia de que o indivíduo titular de dados pessoais deve ser o protagonista das matérias relacionadas ao tratamento de seus dados pessoais, trazendo ao sujeito o foco das operações, em preocupação perpétua com a privacidade. Ou seja, o indivíduo titular de dados pessoais deve ter controle, ou ao menos plena transparência, sobre a destinação dada às suas informações pessoais, bem como as metodologias utilizadas para tanto.

- A LIBERDADE DE EXPRESSÃO, DE INFORMAÇÃO, DE COMUNICAÇÃO E DE OPINIÃO.

Em virtude do fato da LGPD ser uma legislação regulatória no que tange à informação, o tratamento e a transmissão de dados está, intimamente, ligada a outros princípios constitucionais soberanos do Estado Democrático de Direito, qual sejam: o da liberdade de expressão, informações e opinião (artigos 5º, inciso IV e IX, ambos da CF/88). Assim, o fundamento continho no artigo 2º, inciso III, da LGPD visa a garantir que as interpretações ao seu texto sejam realizadas em observância das liberdades de expressão, informação, comunicação e opinião, afastando qualquer entendimento que importe em censura.

- A INVIOLABILIDADE DA INTIMIDADE, DA HONRA E DA IMAGEM.

Assim como o respeito à privacidade, o legislador cuidou de incluir os demais direitos da personalidade no rol de fundamentos da LGPD, direitos estes garantidos também por força do artigo 5º, inciso X, da CF/88. De acordo com esse fundamento, todas as operações de tratamento de dados pessoais devem observar o cuidado com a intimidade, a honra e a imagem dos titulares dos dados pessoais.

- O DESENVOLVIMENTO ECONÔMICO E TECNOLÓGICO E A INOVAÇÃO.

A promoção e incentivo ao desenvolvimento econômico e científico é dever do Estado, garantido pela Constituição Federal (artigo 218 e artigo 219), devendo ser interpretados como princípios funcionais da República Federativa do Brasil quanto ao desenvolvimento nacional. Assim, a inclusão do desenvolvimento econômico e tecnológico e da inovação dentre os fundamentos da LGPD aponta que a lei não foi elaborada a fim da impor freios ao livre avanço da tecnologia e de suas utilidades, mas sim garantir que o seu desenvolvimento seja compatível à proteção dos dados pessoais.

- A LIVRE INICIATIVA, A LIVRE CONCORRÊNCIA E A DEFESA DO CONSUMIDOR.

A Constituição Federal define a livre iniciativa como fundamento da ordem econômica (artigo 170, *caput*), a garantia da propriedade privada dos meios de produção como direito individual fundamental, o estabelecimento da livre concorrência como princípio da ordem econômica (artigo 170, inciso IV), e, finalmente, a liberdade de atuação como base da economia nacional (artigo 170, parágrafo único). A inclusão de tais fundamentos na LGPD tem como escopo, novamente, demonstrar a plena aplicabilidade das normas de proteção dos dados pessoais com o desenvolvimento econômico do país.

- OS DIREITOS HUMANOS, O LIVRE DESENVOLVIMENTO DA PERSONALIDADE, A DIGNIDADE E O EXERCÍCIO DA CIDADANIA EPLAS PESSOAS NATURAIS.

As inclusões desses fundamentos na LGPD demonstram, mais uma vez, a preocupação do legislador em garantir os objetivos traçados no *caput* do artigo 1º da própria lei, isto é, a proteção dos direitos fundamentais à liberdade e à privacidade e ao livre desenvolvimento da personalidade da pessoa natural. Visa a ampliar a proteção do titular dos dados pessoais para além dos direitos da personalidade, reafirmando a proteção à liberdade. A dignidade e a cidadania são fundamentos da República Federativa do Brasil, também reafirmados pela LGPD.

6. Quais são os Princípios da LGPD (artigo 6º)?

A Lei Geral de Proteção de Dados (LGPD) conta com 11 (onze) princípios balizadores, os quais devem ser observados e respeitados frente a todo e qualquer tratamento de dados realizados pelas empresas, companhias, órgãos e entidades, conforme se observa a seguir:

- FINALIDADE.

A LGPD obriga que as empresas, companhias, órgãos e entidades tenham propósitos bem determinados ao tratar dados pessoais, mas não apenas isto, também é necessário deixar claro as suas intenções para o titular dos dados, justificando e apontando o uso dos dados pessoais. Assim, ao coletar um endereço de *e-mail* com a finalidade exclusiva de enviar um boleto bancário ou fatura para o cliente, por exemplo, a empresa não pode utilizar o e-mail para enviar ofertas e promoções.

Sobre o princípio da finalidade, o artigo 6º, inciso I, da LGPD, determina o seguinte: "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades".

- ADEQUAÇÃO.

O princípio da adequação, segundo o artigo 6º, inciso II, da LGPD, refere-se à "compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento". Em outras palavras, a empresa precisa justificar e garantir que os dados coletados tenham valor e sejam condizentes com o modelo de negócio da organização.

Assim, apresenta-se dois exemplos: Primeiro, os clientes de uma farmácia, ao fazer compras *on-line*, precisam preencher um cadastro e fornecer informações sobre sua orientação sexual. Segundo, uma academia solicita, na matrícula, informações de caráter religioso e político. Portanto, nota-se que nos dois exemplos apresentados acima o tratamento dos dados não é compatível com o negócio e, consequentemente, com a lei, tornando a coleta e o tratamento injustificáveis e, inclusive, passíveis de punições e multas.

- NECESSIDADE.

Devem ser tratados apenas os dados pessoais necessários para aquela finalidade descrita, dispensando-se os excessivos e/ou desnecessários. Na prática, quanto mais dados pessoais você trata, maior é a sua responsabilidade e, por consequência, maior é a cobrança e mais caras são as multas em casos de erros e falhas, razão pela qual a empresa precisa garantir que apenas os dados pessoais essenciais para o desenvolvimento do negócio sejam coletados e tratados.

De acordo com o artigo 6º, inciso III, da LGPD, o princípio da necessidade envolve "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.

O princípio do livre acesso é um dos pontos fundamentais, previsto no artigo 6º, inciso IV, da LGPD, que assim dispõe: "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". Na prática, a empresa deve criar mecanismos para que o titular dos dados tenha o direito de consultar os seus próprios dados e informações de forma gratuita. Além disso, a empresa precisa deixar evidente os seus objetivos e o período de tempo que os dados serão utilizados.

- QUALIDADE DE DADOS.

O princípio da qualidade dos dados, segundo o artigo 6º, inciso V, da LGPD, se refere à "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". Ou seja, para respeitar as normas da LGPD, é necessário que a empresa mantenha sua base de dados atualizada somente com informações verdadeiras e que esteja alinhada com o propósito do negócio.

- TRANSPARÊNCIA.

A transparência é outro princípio essencial da LGPD, que, em resumo, determina que as empresas, companhias, órgãos e entidades precisam ser honestas com os titulares dos dados, inclusive, devem informar aos proprietários dos dados sobre os respectivos agentes de tratamento, que são, basicamente, outras organizações envolvidas no processo de tratamento dos dados.

O princípio da transparência, de acordo com o artigo 6º, inciso VI, da LGPD, é a "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.

Como o próprio nome sugere, o princípio da segurança envolve a adoção de procedimentos, tecnologias e soluções que garanta maior proteção dos dados pessoais em casos de acessos não autorizados, como em ataques *hackers*, e de situações acidentais ou ilícitas de perda e alteração, por exemplo.

Sobre o princípio de segurança, o artigo 6º, inciso VII, da LGPD, diz ser necessário a "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.

O princípio da prevenção versa justamente sobre o ato de estar preparado para lidar com eventuais problemas envolvendo o tratamento de dados pessoais antes mesmo que eles surjam. Por isso, o artigo 6º, inciso VIII, da LGPD determina a "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais".

- NÃO DISCRIMINAÇÃO.

O tratamento de dados pessoais jamais pode ser realizado com objetivos de discriminar ou de promover abusos contra os seus titulares. Neste caso, geralmente, estamos falando dos dados pessoais sensíveis, como os que tratam sobre origem racial ou étnica, convicção religiosa e opinião política, por exemplo. Assim, o princípio da não discriminação, de acordo com o artigo 6º, inciso IX, da LGPD, refere-se à "impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos".

- RESPONSABILIDADE E PRESTAÇÃO DE CONTAS – *ACCOUNTABILITY*.

O princípio da responsabilização e prestação de contas dispõe sobre o cumprimento da lei, tendo em vista provas e evidências de que medidas e procedimentos foram tomados pelas empresas, companhias, órgãos e entidades, a fim de garantir a proteção de dados. Deste modo, o artigo 6º, inciso X, da LGPD, determina a necessidade de "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".

- *PRIVACY BY DESIGN.*

Este princípio de governança, previsto no artigo 46 da LGPD, determina que todos os agentes de tratamento de dados devem incorporar a privacidade a todos os estágios (modelagem, operação, gerenciamento e encerramento) de um determinado sistema, projeto ou negócio.

7. Como devo cuidar destes dados?

A Lei Geral de Proteção de Dados (LGPD) estipula como deve ser realizado o tratamento de dados, prevendo os cuidados que devem ser adotados desde a coleta até a eliminação, ou seja, qualquer ação realizada com os dados pelo controlador é caracterizada como tratamento, e, portanto, deve observar a proteção destes dados.

Deste modo, o "tratamento", segundo o artigo 5°, inciso X, da LGPD, compreende toda a operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

No entanto, para a realização de tratamentos de dados pessoais, é indispensável que os processos/procedimentos realizados e/ou adotados pelas empresas, companhias, órgãos e entidades estejam enquadrados em, ao menos, uma das bases legais discriminadas no artigo 7º da LGPD.

Pela nova regra, passando por uma premissa de segurança e boas práticas, as empresas, companhias, órgãos e entidades devem adotar medidas de segurança, técnicas ou administrativas, que sejam aptas a protegerem os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento inadequado ou ilícito.

8. Quais são as hipóteses para o tratamento de dados (bases legais)?

A LGPD também estabelece hipóteses em que o tratamento de dados pessoais poderá ser realizado pelas diferentes empresas, companhias, órgãos e entidades. Assim, se faz necessário elencar as referidas hipóteses para o tratamento de dados, previstas no artigo 7º da LGPD:

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I – mediante o fornecimento de **consentimento pelo titular**. (Exemplo: você baixa um aplicativo, informa seus dados pessoais e clica em aceitar os termos de uso e a política de privacidade);

II – para o cumprimento de **obrigação legal ou regulatória pelo controlador**. (Exemplo: para cumprir obrigações trabalhistas e previdenciárias ou determinações da Lei de Acesso à Informação);

III – 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 similares. (Exemplo: fornecimento do auxílio-emergencial ou concessão de passe livre);

IV – para a realização de **estudos por órgão de pesquisa**, garantida, sempre que possível, a anonimização dos dados pessoais. (Exemplo: dados que o IBGE coleta para realizar o censo);

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. (Exemplo: para cumprir o contrato de fornecimento de telefonia móvel, a empresa precisa de alguns dos seus dados pessoais);

VI – para o **exercício regular de direitos em processo judicial, administrativo ou arbitral**. (Exemplo: uso dos dados necessários para cobrar pensão alimentícia em ação judicial);

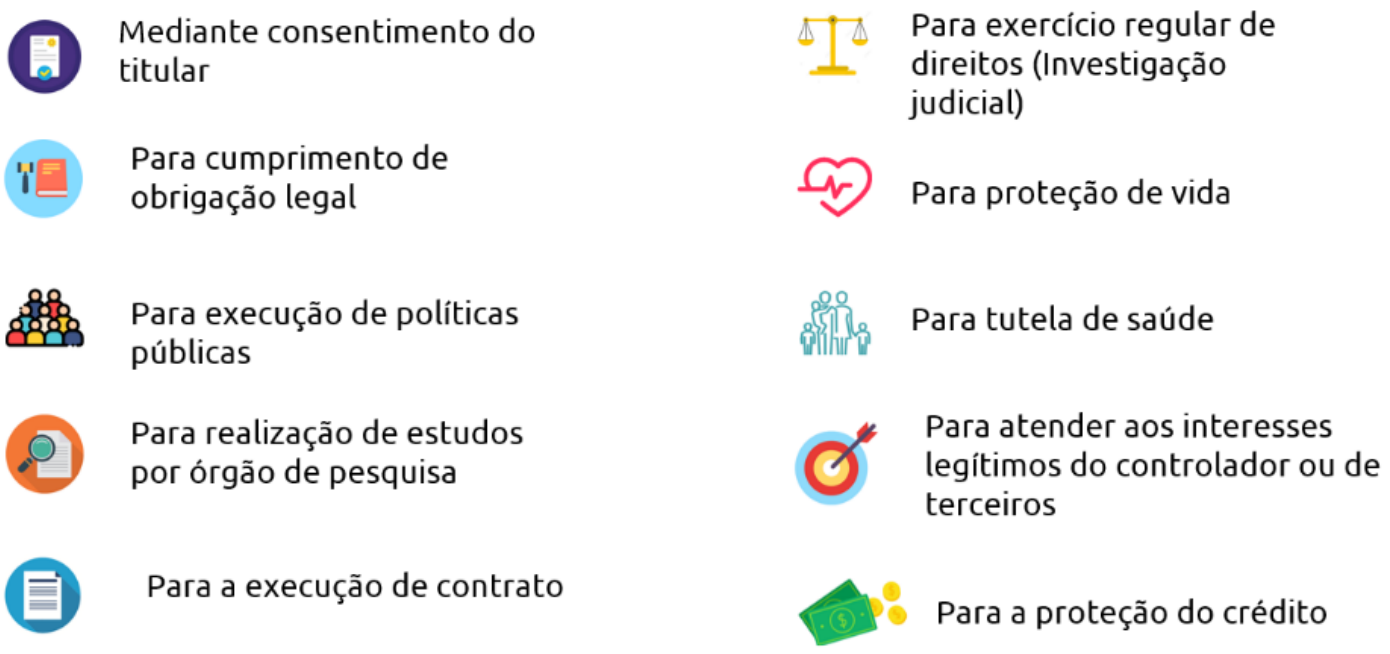
VII – para a **proteção da vida ou da incolumidade física** do titular ou de terceiro. (Exemplo: uso dos dados de geolocalização do celular de uma pessoa desaparecida);

VIII – para a **tutela da saúde**, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária. (Exemplo: acesso ao prontuário de uma pessoa que necessita de atendimento pelo SUS);

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. (Exemplo: envio de propaganda sobre promoção de um produto para clientes antigos de uma loja de óculos);

X – para a **proteção do crédito**, inclusive quanto ao disposto na legislação pertinente. (Exemplo: avaliação do *score* de crédito da pessoa para concessão de um novo empréstimo).

Portanto, a LGPD prevê dez bases legais que autorizam o tratamento de dados pessoais, as quais não têm dependência ou predominância entre si, razão pela qual, é necessário, para se definir a melhor base legal para cada tipo de tratamento, que sejam avaliados os processos, as pessoas envolvidas e as necessidades do negócio em análise.



7.1. O que é o Consentimento, previsto no Artigo 7º, inciso I, da LGPD?

Consentimento é a manifestação de vontade livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. Livre, porque o titular pode escolher entre aceitar ou recusar o tratamento. Informado, porque o titular tem a seu dispor informações claras, necessárias e suficientes sobre o tratamento para analisar e formar sua escolha. Inequívoco, porque fornecido por escrito, em cláusula destacada, ou de outra forma evidente e adequada. Logo, não pode ser extraído da omissão, nem de forma implícita, genérica, enganosa ou abusiva.

O consentimento pode ser revogado a qualquer momento através de manifestação expressa do titular, de modo gratuito e facilitado. Caso haja mudanças na finalidade do tratamento ou na forma como é realizado, que não sejam compatíveis com o consentimento original, o Controlador deverá informar previamente o titular sobre tais alterações, podendo o titular revogar o consentimento, caso não concorde mais.

Por fim, não é necessário obter o consentimento do titular para todo e qualquer tipo de tratamento de dados, desde que outra base legal seja compatível com a atividade de tratamento ou ainda no caso de os dados serem tornados manifestamente públicos pelo próprio titular, mas sempre observando e preservando os direitos do titular e os princípios em lei.

7.2. O que é o Legítimo Interesse, previsto no Artigo 7º, inciso IX, da LGPD?

A base legal do legítimo interesse do Controlador somente pode fundamentar o tratamento de dados pessoais para finalidades que sejam legítimas, consideradas a partir de situações concretas. Por exemplo, para o apoio e promoção de atividades do Controlador. Ou para a proteção, em relação ao titular, do exercício regular de seus direitos ou para a prestação de serviços que o beneficiem.

Para saber se a finalidade é legítima, pode ser feito um teste de proporcionalidade de quatro etapas, analisando: a legitimidade, a necessidade, o balanceamento e as salvaguardas. Na sua escolha, o Controlador deve sempre respeitar as legítimas expectativas do titular e seus direitos e liberdades fundamentais. Além do mais, deve haver transparência e somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

9. Dados Pessoais Sensíveis (Artigo 11 da LGPD).

São dados pessoais cujo tratamento pode levar a vulnerabilidades/fragilidades ou ensejar a discriminação do seu titular, tendo em vista que estão diretamente relacionados aos aspectos mais íntimos da vida de uma pessoa, como origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico relativos a esta pessoa singular (artigo 5º, inciso II, da LGPD).

O tratamento de dados pessoais sensíveis somente pode acontecer **(1)** quando o titular ou seu responsável legal der consentimento, de forma específica e destacada, para finalidades específicas ou **(2)** sem o consentimento do titular, nas hipóteses em que for indispensável para:

- Cumprimento de obrigação legal ou regulatória pelo Controlador;
- Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;
- Realização de estudos por órgão de pesquisa, sendo garantida, sempre que possível, a anonimização;
- Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
- Cuidado da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- Proteção da vida ou da integridade física do titular ou de terceiro;
- Prevenção à fraude e à segurança do titular nos processos de identificação de cadastro em sistemas eletrônicos, a não ser que no caso de prevaleçam direitos e liberdades fundamentais do titular.

10. Dados de Crianças e Adolescentes (Artigo 14 da LGPD).

Criança é a pessoa com até 12 (doze) anos de idade incompletos e adolescente é aquela entre 12 (doze) e 18 (dezoito) anos de idade, de acordo com o Estatuto da Criança e do Adolescente (ECA). O tratamento de dados pessoais de crianças e de adolescentes deve ser realizado sempre em seu melhor interesse.

Deste modo, o artigo 14, da LGPD, dispõe que o tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado sempre observando o melhor interesse do menor, devendo ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal. Porém, poderão ser coletados dados pessoais de crianças e adolescentes sem o referido consentimento quando a coleta for necessária para contatar os pais ou o responsável legal, ou, ainda, para sua própria proteção.

No entanto, o Conselho Diretor da Agência Nacional de Proteção de Dados (ANPD), exercendo as suas competências normativas e após a realização de Estudo Preliminar sobre as "Hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes"[2], editou o ENUNCIADO CD/ANPD Nº. 1, DE 22 DE MAIO DE 2023[3] que determina o seguinte:

> "O tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas hipóteses legais previstas no artigo 7º ou no artigo 11 da Lei Geral de Proteção de Dados Pessoais (LGPD), desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do artigo 14 da Lei."

Portanto, segundo este enunciado da ANPD, é possível a realização de tratamento de dados pessoais de crianças e adolescentes com base nas hipóteses previstas no artigo 7º e artigo 11, ambos da LGPD, dispensando-se o consentimento dos pais ou responsável legal, desde que a hipótese legal seja condizente com o respectivo tratamento de dados e que sempre seja observado o princípio do melhor interesse da criança/adolescente.

11. Quais os Direitos dos Titulares?

Toda pessoa física tem assegurada a titularidade de seus dados pessoais (artigo 17 da LGPD), significa que, ao permitir o tratamento de seus dados pessoais de modo algum e em nenhuma circunstância, a pessoa transfere a *outrem* a condição de dono de seus próprios dados pessoais. Na verdade, segundo o artigo 18, da LGPD, o titular dos dados pessoais tem o direito de obter do controlador, a qualquer momento e mediante requisição:

I – A **confirmação da existência** de tratamento;

O direito à confirmação da existência de tratamento decorre lógica e juridicamente dos princípios do livre acesso e da transparência (artigo. 6º, inciso IV e inciso VI). Refere-se ao direito garantido ao titular de confirmar se o controlador ou operador realiza o tratamento de seus dados pessoais.

O direito à confirmação da existência de tratamento pode ser efetivado de forma simplificada e imediata (com a negativa ou afirmativa da existência do tratamento) ou em formato completo, no prazo de 15 (quinze) dias, ou seja, através da declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento (artigo 19, inciso I e inciso II), respeitando-se os segredos comercial e industrial.

---

[2] ESTUDO PRELIMINAR - Hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes. Agência nacional de Proteção de Dados (ANPD). Setembro/2022. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/estudo-preliminar-tratamento-de-dados-crianca-e-adolescente.pdf>.

[3] ENUNCIADO CD/ANPD Nº. 1, DE 22 DE MAIO DE 2023. Conselho Diretor da Agência Nacional de Proteção de Dados (ANPD). Publicado no Diário Oficial da União em 24/05/2023. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-enunciado-sobre-o-tratamento-de-dados-pessoais-de-criancas-e-adolescentes/Enunciado1ANPD.pdf>.

II – O **acesso aos dados** mantidos pelo Controlador;

O acesso aos dados, também decorrente dos princípios do livre acesso e da transparência (artigo 6º, inciso IV e inciso VI), garante aos seus titulares o direito de obter uma cópia de seus dados pessoais, dentre outras informações relacionadas.

O direito de acesso compreende todas as informações constantes do artigo 9º, da LGPD, quais sejam: **(1)** informação sobre a finalidade específica do tratamento; **(2)** informações sobre a forma e a duração do tratamento, observados os segredos comercial e industrial; **(3)** a identificação do controlador; **(4)** informações de contato do controlador; **(5)** informações acerca do uso compartilhado de dados pelo controlador e a finalidade; **(6)** as responsabilidades dos agentes que realizarão o tratamento; e **(7)** os direitos do titular, com menção explícita aos direitos contidos no artigo 18 desta Lei. A consulta quanto à forma e duração do tratamento, assim como em relação à exatidão dos dados pessoais é gratuita, nos termos do artigo 18, § 5º, da LGPD.

Os dados devem ser armazenados em formato que favoreça o acesso pelo titular e poderão ser solicitados aos agentes de tratamento por via eletrônica ou impressa, conforme disposto no artigo 19, § 2º, inciso I e inciso II. Assim como no caso da confirmação do tratamento, o titular pode requisitar o acesso em formato simplificado e imediato ou em formato completo, com o prazo de 15 (quinze) dias para atender à solicitação.

III – A **correção de dados** incompletos, inexatos ou desatualizados;

É garantido ao titular o direito à correção de dados incompletos, inexatos ou desatualizados que consiste no direito de solicitar que os dados tratados sejam corrigidos ou atualizados. Trata-se de um direito que decorre do princípio da qualidade dos dados, previsto no artigo 6º, inciso V, da LGPD.

Nos termos do artigo 18, § 6º, a correção dos dados incompletos deve ser imediatamente realizada pelos agentes de tratamento.

IV – A **anonimização, bloqueio ou eliminação de dados**, desde que sejam considerados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD;

O titular dos dados tem direito à anonimização. Essa prerrogativa, vale lembrar, consiste na "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" (artigo 5º, inciso XI). Cumpre observar que, uma vez anonimizados, os dados deixam de ser regidos pela LGPD, tendo em vista que perdem a qualidade de dados pessoais.

O bloqueio de dados, por sua vez, consiste na "suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados" (art. 5º, XIII). Esse bloqueio, nos termos da LGPD, é tanto um direito do titular (artigo 18, inciso III), quanto uma espécie de sanção a ser imposta pela Agência Nacional, nos termos do artigo 52, inciso X e inciso XI da Lei.

A eliminação dos dados desnecessários, excessivos ou tratados em desconformidade com a legislação, por sua vez, decorre do princípio da necessidade (artigo 6º, inciso III).

V – A **portabilidade de seus dados pessoais** a outro fornecedor de serviço;

A LGPD prevê que o titular dos dados pode solicitar a portabilidade dos dados, ou seja, a transferência das suas informações pessoais a outro fornecedor de produto ou serviços. Para tanto, é necessária a requisição expressa, em conformidade com a regulamentação da agência nacional e observados os segredos comercial e industrial.

O direito do titular é regulamentado pelo § 7º do artigo 18, o qual prevê que a portabilidade não pode incluir os dados já anonimizados do titular.

Em relação aos dados sensíveis, a LGPD autoriza ao titular de dados sensíveis solicitar a portabilidade, possibilitando a comunicação e o uso compartilhado, de forma excepcional à regra contida no artigo 11, § 4º, inciso I, que veda a "comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica".

A portabilidade dos dados trata-se de uma decorrência normativa da essencialidade da "autodeterminação informativa" do titular dos dados prevista no artigo 2º, inciso II, da LGPD.

VI – A **eliminação dos dados pessoais quando retirado o consentimento** dado anteriormente;

Em relação aos dados tratados com consentimento nos termos do artigo 7º, inciso I, a LGPD conferiu ao titular desses dados a prerrogativa de solicitar a eliminação dos dados, ou seja, a "exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado" (artigo 5º, inciso XIV), de forma definitiva e irreversível.

Contudo, a LGPD dispõe que há exceções a essa regra, ou seja, há situações em que o direito de eliminação de dados tratados com o consentimento não pode ser exercido. São elas as hipóteses previstas no artigo 16, da LGPD, vale lembrar: **(I)** cumprimento de obrigação legal ou regulatória pelo controlador; **(II)** estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; **(III)** transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou **(IV)** uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

VII – A **relação de com quem seus dados foram compartilhados**;

Em decorrência do princípio da transparência (artigo 6º, inciso VI), a LGPD incluiu no rol de direitos do titular a garantia de informações sobre o compartilhamento de seus dados, ou seja, é direito do titular saber exatamente com quem, sejam entidades públicas ou privadas, o controlador está compartilhando os seus dados pessoais.

VIII – A **informação de que poderá negar consentimento e quais suas consequências**;

Com fundamento no direito à autodeterminação informativa, aos princípios da boa-fé e da transparência, o titular dos dados pessoais deve ser informado sobre a possibilidade de não fornecer o consentimento e as consequências caso o consentimento seja negado. Esse direito está relacionado à premissa de que o consentimento deve ser pedido e concedido de forma clara, transparente e totalmente livre.

IX – A **revogação do consentimento**.

O consentimento para o tratamento de dados pessoais (artigo 7º, inciso I), pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado, enquanto não houver requerimento de eliminação (artigo 7º, § 5º). Esse direito do titular previsto na LGPD também decorre do direito de autodeterminação informativa.

Cumpre destacar que a revogação do consentimento não implica na eliminação automática de dados coletados valida e licitamente. Para tanto, a revogação do consentimento deve ser acompanhada, de forma expressa, com a requisição da eliminação dos dados, nos termos do artigo 18, inciso III da LGPD.

Além disso, quando uma decisão a respeito de seus dados pessoais é tomada com base em tratamento automatizado, o titular tem direito à **revisão dessa decisão** (artigo 20, da LGPD). Ou seja, o direito à explicação corresponde ao direito do titular de receber informações suficientes para a compreensão da lógica e os critérios utilizados para o tratamento de seus dados. Já o direito à revisão diz respeito ao direito do titular de requisitar a revisão de uma decisão totalmente automatizada que possa ter um impacto nos seus interesses, sobretudo quando relacionados à definição de seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

Além disso, assiste à pessoa física (titular) o direito de que a defesa dos interesses e de seus direitos poderá ser exercida em **juízo**, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumento de tutela individual e coletiva (artigo 22, da LGPD), bem como a **peticionar** contra os agentes de tratamento (controlador e operador) diretamente à Agência Nacional de Proteção de Dados (ANPD), que exerce fiscalização e controle sobre estes agentes de tratamento (artigo 18, § 1º, da LGPD).

12. Incidentes de segurança e sua comunicação.

A ocorrência de um incidente de segurança não encontra definição expressa na LGPD, que se limitou a trazer um rol exemplificativo no *caput* do seu artigo 46, de fatos assim considerados: acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

A partir de tais, pode-se chegar à seguinte definição: incidente de segurança é qualquer evento adverso, confirmado ou sob suspeita, que afete a tríade da segurança da informação: confidencialidade, a integridade ou a disponibilidade dos dados.

Diante da sua ocorrência, uma providência exigida pela LGPD é a comunicação, pelo Controlador, à Agência Nacional – ANPD (artigo 48). No entanto, verifica-se que não é absolutamente todo evento adverso que ensejará tal comunicação, mas apenas aqueles que, no termo do dispositivo citado "possa(m) acarretar risco ou dano relevante aos titulares".

O mesmo raciocínio aplica-se ao prazo para realização de tal comunicação, que não foi fixado pela LGPD (fala-se em "prazo razoável", no artigo 48, § 1º) e se submete, igualmente à razoabilidade aferida no caso concreto. Em relação aos casos em que a comunicação não for imediata, os motivos disso devem ser expostos, conforme previsão do artigo 48, § 1º, inciso V).

Deve-se destacar também que os incidentes que devem ser comunicados à autoridade independem da existência de dolo ou culpa por parte de qualquer agente de tratamento ou se o fato é oriundo de situação acidental ou incidental. Havendo o evento imprevisto e relevante, deve haver a comunicação, independentemente da constatação de elemento subjetivo por parte de qualquer agente.

A comunicação deve ser abrangente e transparente, levando ao conhecimento da Agência Nacional (ANPD) o maior número de informações e as mais aprofundadas tanto quanto possível. Ademais, há um conteúdo mínimo a ser observado, previso nos incisos do artigo 48, § 1º.

Recebida a comunicação, a autoridade nacional avaliará o incidente e poderá impor medidas ao controlador em resposta ao incidente: a ampla divulgação do fato em meios de comunicação; e medidas para reverter ou mitigar os efeitos do incidente (artigo 48, §2º). Tais medidas, não obstantes, devem ser adotadas pelo controlador, operador ou encarregado logo que identificar o incidente, evitando sua perpetuação.

Por fim, a adoção de medidas adequadas será levada em conta pela autoridade no momento em que avaliar a gravidade do incidente. Conforme a previsão do artigo 48, §3º, ele deverá perceber, notadamente, se "foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los".

13. Boas Práticas e da Governança (Artigo 50, da LGPD).

Os Controladores e Operadores podem formular regras de boas práticas para o tratamento de dados pessoais, desenvolver soluções de governança de dados e também implementar programa de governança em privacidade. Para isso, podem estabelecer o regime de funcionamento, os procedimentos – incluindo reclamações e pedidos dos 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 prevenção de riscos.

A implementação da segurança efetiva em relação aos direitos dos titulares é uma tarefa paulatina e que envolve o cultivo de uma cultura institucional de segurança e respeito. As boas práticas e os sistemas de governança são, assim, vetores para a efetivação dos princípios positivados no art. 6º da LGPD, de modo sensível às particularidades de cada caso e primando pela segurança.

Embora não seja obrigatória, a adoção de um programa de governança em privacidade de dados pessoais, assim como de todos os demais instrumentos destinados à prevenção de incidentes e minimização de danos, será levada em consideração quando da aplicação de eventual sanção, pela Agência Nacional de Proteção de Dados, aos agentes de tratamento de dados (artigo 52, §1º, inciso VIII e inciso IX).

14. Segurança (Artigos 46 a 49, da LGPD).

Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas para proteger os dados pessoais. A proteção deve impedir acessos não autorizados e situações - acidentais ou ilícitas - de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilegal. A obrigação de garantir a segurança da informação é dos agentes de tratamento e de qualquer outra pessoa que intervenha em uma das fases do tratamento, durando mesmo após o seu término.

CONFIDENCIALIDADE	somente pessoas devidamente autorizadas devem ter acesso à informação
INTEGRIDADE	a informação deve manter todas as características originalmente estabelecidas para que seja exata, completa e correta
DISPONIBILIDADE	a informação deve estar acessível e disponível para o uso por parte das pessoas autorizadas

15. Quais os Atores e Agentes de Tratamento de Dados?

- Titular de Dados: pessoa natural, a quem se referem os dados pessoais tratados.
- 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 pelo Tratamento de Dados Pessoais (DPO)**:** pessoa indicada pelo Controlador e Operador, para atuar como canal de comunicação entre o Controlador, os Titulares e a Agência Nacional de Proteção de Dados (ANPD).

❖ **As atividades do Encarregado pelo Tratamento de Dados Pessoais (DPO) consistem em**:
a) Aceitar reclamações e comunicações dos titulares;
b) Prestar esclarecimentos;
c) Adotar providências;
d) Receber comunicações da Agência Nacional de Proteção de Dados;
e) Orientar funcionários e terceiros a respeito das práticas em relação à proteção de dados pessoais;
f) Monitorar as atividades de tratamento de dados.

❖ IMPORTANTE:
1. O Controlador e o Operador irão responder pelo dano patrimonial, moral, individual ou coletivo, que vierem a causar em decorrência da violação à legislação de proteção de dados pessoais, cada um por suas ações – conforme artigo 42 da LGPD;
2. Controladores atuando em conjunto serão solidariamente responsáveis;
3. O Operador é solidariamente responsável caso suas atividades sejam contrárias à LGPD ou quando não seguir as instruções do controlador.

16. Quem é o órgão responsável por fiscalizar e zelar pelo cumprimento da LGPD?

A LGPD é fiscalizada e zelada pela **Agência Nacional de Proteção de Dados (ANPD)**[4], a qual foi criada pela Medida Provisória (MP) nº. 869, de 27 de dezembro de 2018, posteriormente convertida na Lei nº. 13.853, de 14 de agosto de 2019, sendo que, a partir de 25/10/2022, transformou-se, definitivamente, em autarquia federal de natureza especial que, embora preserve sua autonomia técnica e decisória, atualmente, se encontra vinculada – mas não subordinada – ao Ministério da Justiça e Segurança Pública.

A partir de setembro/2025 a Autoridade Nacional de Proteção de Dados (ANPD) passou a ser Agência Nacional de Proteção de Dados (ANPD) por meio da Medida Provisória nº. 1.317/2025, que transforma em uma agência reguladora com autonomia e poder de polícia para fiscalizar e sancionar o tratamento de dados pessoais. Essa mudança confere à agência mais poder para aplicar multas, suspender atividades e realizar ações como busca e apreensão, além de fortalecer sua capacidade de atuação com base na Lei das Agências Reguladoras (Lei nº. 3.848/2019), que disciplina sua gestão, organização e processo decisório.

Por isso, a ANPD, além de exigir a proteção de dados pessoais, também possui a responsabilidade de elaborar diretrizes que regulamentam o tratamento de dados pessoais, bem como de fiscalizar e aplicar sanções administrativas em caso do não cumprimento da lei, através de um processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso, com apoio de outros órgãos de proteção aos direitos do cidadão, como Procon e Senacon.

A ANPD também tem a função de avaliar os pedidos dos titulares contra os Controladores, após o titular comprovar que sua reclamação não foi solucionada pelo Controlador no prazo estabelecido, bem como informar e fazer com que a população tenha conhecimento sobre as políticas de proteção de dados pessoais, as práticas exercidas e os direitos existentes, a fim de estimular o entendimento das normas por todos aqueles que tratam e fazem uso destes dados pessoais.

Além disso, e conforme visto anteriormente, o titular de dados pessoais possui uma série de direitos, que devem ser atendidos pelo Controlador. Em um primeiro momento, os pedidos relacionados aos direitos devem ser realizados diretamente à organização responsável pelo tratamento dos dados. Se o pedido não for atendido, o titular de dados pode então apresentar uma reclamação à ANPD, com a comprovação de que a reclamação não foi solucionada pelo Controlador.

ANPD

[4] Site da Agência Nacional de Proteção de Dados (ANPD): https://www.gov.br/anpd/pt-br.

17. Responsabilidades (Artigos 42 e 44, da LGPD).

O Controlador ou o Operador que, em razão da atividade de tratamento de dados pessoais, causar a outra pessoa dano patrimonial, moral, individual ou coletivo, violando assim a legislação de proteção de dados pessoais, tem a obrigação de repará-lo. O tratamento de dados pessoais será irregular quando não observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:

- O modo pelo qual o tratamento é realizado;
- O resultado e os riscos que razoavelmente se esperam do tratamento;
- As técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Também responde pelos danos decorrentes da violação da segurança dos dados o Controlador ou o Operador que, ao deixar de adotar as medidas de segurança necessárias para proteger os dados pessoais, der causa ao dano.

18. Quais são as sanções previstas na LGPD?

Os agentes de tratamento de dados que cometerem infrações às disposições previstas na LGPD ficarão sujeitos às seguintes sanções administrativas, que podem ser aplicadas pela ANPD:

a) Advertência, com prazo para adoção de medidas corretivas;
b) Multa simples, de até 2% (dois por cento) do faturamento, limitada a R$ 50 milhões por infração;
c) Multa diária, observado o limite mencionado acima;
d) Publicização da infração;
e) Bloqueio dos dados pessoais até a regularização;
f) Eliminação dos dados pessoais a que se refere a infração;
g) Suspensão parcial do funcionamento do banco de dados a que se refere a infração;
h) Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Embora o principal responsável pelos dados seja a empresa, os funcionários que tenham contato com esses dados devem estar atentos à segurança dessas informações, devendo respeitar a política de governança de dados que a empresa adotar.

19. Dicas Importantes:

1) Mantenha documentos físicos que contenham dados pessoais e/ou informações sigilosas/confidenciais dentro de gavetas, armários ou arquivos fechados, preferencialmente com trancas, evitando-se deixá-los expostos sobre as mesas de trabalho;

2) Não compartilhe *logins* e senhas de acesso das estações de trabalho e demais sistemas utilizados com outros colaboradores ou terceiros não autorizados;

3) Adote senhas fortes, que não sejam fáceis de ser desvendadas por terceiros e não deixe suas senhas anotadas ou armazenadas em locais de fácil acesso ou visualização;

4) Bloqueie os computadores (clicar nas teclas "*Atl; Ctrl; Del*" – selecionar "Bloquear") todas as vezes que se afastar da mesa de trabalho, para evitar o acesso indevido de terceiros;

5) Mantenha sua mesa e sua tela limpas, isto é, garanta que nenhuma informação sigilosa/confidencial ou dados pessoais de terceiros serão deixados à vista, seja em papel ou em meio eletrônico;

6) Evite conectar *pendrives* e celulares, pois ao conectar um *pendrive* ou até mesmo um telefone no computador, você oferece risco elevado devido à facilidade com que vírus e outros programas maliciosos podem se propagar por esses dispositivos;

7) Não utilize como folha de rascunho os documentos que possuem dados pessoais e/ou informações sigilosas/confidenciais, os quais devem ser descartados de forma correta e segura, a fim de se tornem inutilizáveis (preferencialmente por fragmentadora de papel);

8) Evite o compartilhamento de dados pessoais e informações sigilosas/confidenciais para outros setores, e jamais externalize para terceiros alheios ao negócio que não devem ou não estão autorizados a receber tal dado/informação;

9) Não colete dados pessoais desnecessários ou excessivos para o procedimento de negócio, devendo ser coletado somente o imprescindível para a realização de determinada finalidade, evitando-se, principalmente, a coleta de dados pessoais sensíveis;

10) Tenha cuidado ao preencher cadastros na *internet* para realização de joguinhos, testes de personalidade, mapa astral, aplicativos de envelhecimento, filtros de imagens e outras "brincadeira" aparentemente inofensivas;

11) Não acesse sites desconhecidos e não abra qualquer *link* de *e-mail*. Suspeite e, em caso de dúvida, escolha um site mais confiável ou entre em contato com o remetente do *e-mail*;

12) Não fale sobre assuntos particulares e exclusivos do negócio com terceiros ou até mesmo em local público, com o intuito de evitar vazamento de dados e/ou informações sigilosas/confidenciais;

13) Os espaços físicos – armários, salas ou outros – que contenham informações sigilosas/confidenciais ou dados pessoais deverão estar fechados e protegidos nos períodos de ausência dos responsáveis por seu cuidado;

14) Faça comunicação imediata à equipe responsável e ao Encarregado pelo Tratamento de Dados Pessoais (DPO) quando verificar um incidente de segurança envolvendo os dados pessoais tratados pelo Controlador ou Operador. Isso pode permitir a adoção de medidas capazes de reverter ou diminuir os efeitos do incidente;

15) Todos os cuidados de segurança devem ser observados no trabalho remoto. Mantenha sempre sob sua vigilância dispositivos móveis ou documentos do negócio que estejam em sua guarda.

Qualitec Consult – Versão 3.0.
Outubro de 2025.
www.qualitec.inf.br.
@qualitecconsult.