(LGPD)

Lei Geral de Proteção de Dados

DID®

Índice

A **Lei Geral de Proteção de Dados (LGPD)**, sancionada em agosto de 2018, estabelece regras sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais, impondo mais proteção aos consumidores e penalidades para empresas que não estejam em compliance, ou seja de acordo com a legislação.

Em 18 de setembro de 2020, a Lei Geral de Proteção de Dados entrou em vigor.

Quais dados a LGPD protege?

A Lei Geral de Proteção de Dados, a LGPD, **protege dados** que identifiquem as pessoas, informação relacionada a uma pessoa natural identificada ou identificável, ou seja, **dados pessoais**, como o seu nome, RG, CPF, CNH, e-mail, Endereço, GPS, cookies, IP, foto etc.

Conceitos:

Dado pessoal: é qualquer informação relacionada à pessoa natural identificada ou identificável.
Dado pessoal sensível: é uma informação 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 a vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural”
Tratamento: se refere a “toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento,

eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

Quem deve cumprir a Lei 13.709/2018?

Todas as empresas, independentemente do porte ou segmento, precisam estar atentas sobre como estão tratando os dados dos seus clientes e se os seus processos estão em conformidade com a nova lei.

Esta Lei se aplica a qualquer operação de tratamento de dados pessoais realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

- Os dados pessoais tenham sido coletados no Brasil ou qualquer outra operação de tratamento seja realizada no território nacional.
- A atividade de tratamento tenha sido feita fora do Brasil, mas ela tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional. Ex: cadastro de sites estrangeiros, mas que utilizem esses dados para vender produtos no Brasil.

Qual o objetivo da Lei Geral de Proteção de Dados?

A Lei Geral de Proteção de Dados Pessoais (LGPD) vem para proteger os direitos fundamentais de liberdade e de privacidade, e a livre formação da personalidade de cada indivíduo.

O que significa proteção de dados?

Como proteção de dados pessoais, entende-se a possibilidade de cada cidadão determinar de forma autônoma, a utilização que é feita de seus próprios dados pessoais, em conjunto com o estabelecimento de uma série de garantias para evitar que estes dados pessoais sejam utilizados de forma a causar discriminação.

O que é tratamento de dados LGPD?

A Lei 13.709/18 dispõe sobre o tratamento de dados pessoais, nos meios físicos e digitais, inclusive por pessoa jurídica de direito público, com o objetivo de proteger os direitos fundamentais da liberdade e de privacidade, e o livre desenvolvimento da personalidade natural

Quem são considerados agentes de tratamento de dados?

A LGPD prevê os seguintes agentes de tratamento de dados pessoais: tem o **controlador,** que é, a quem compete as decisões relativas ao tratamento; e tem o **operador,** que é, quem realiza o tratamento em nome do controlador.

Quem é o controlador de dados?

É ele que decide sobre tratar dados pessoais. Nas palavras da própria lei, o **controlador** pode ser classificado como “pessoa natural ou jurídica, de direito público ou privado, a quem compete as **decisões** referentes ao tratamento de dados pessoais”.

Qual a diferença entre controlador e operador de dados?

O operador vai realizar o tratamento de dados sempre a partir de regras e ordens do controlador. O controlador por sua a vez, apresenta-se como o responsável pelo tratamento desses dados do titular que estão sob sua responsabilidade e pela manipulação dessas informações.

Princípios da LGPD

Os 10 princípios que norteiam a LGPD, e que devem ser respeitados em cada tratamento de dados pessoais, são:

1) Finalidade:

A partir da LGPD não será mais possível tratar dados pessoais com finalidades genéricas ou indeterminadas. O tratamento de cada informação pessoal deve ser feito com fins específicos, legítimos, explícitos e informados. Ou seja, as empresas devem explicar para que usarão cada um dos dados pessoais. Essas finalidades, também devem estar dentro dos limites da lei e devem vir expressamente acompanhadas de todas as informações relevantes para o titular. Além disso, a empresa não está autorizada a modificar a finalidade durante o tratamento.

2) Adequação:

Os dados pessoais tratados, devem ser compatíveis com a finalidade informada pela empresa. Ou seja, sua justificativa deve fazer sentido com o caráter da informação que você pede. Por exemplo: se o seu negócio é um e-commerce de produtos

eletrônicos, dificilmente será justificável pedir dados de saúde aos Usuários. Então, se não é compatível, o tratamento se torna inadequado.

3) Necessidade:

As empresas em geral, devem utilizar apenas os dados estritamente necessários para alcançar as suas finalidades. Procure fazer uma ponderação entre o que é realmente essencial para o seu negócio e o que é apenas conveniente.
Lembre-se que, quanto mais dados você tratar, maior será a sua responsabilidade, inclusive em casos de vazamentos e incidentes de segurança.

4) Livre acesso:

A pessoa física titular dos dados, tem o direito de consultar, de forma simples e gratuita, todos os dados que a empresa detenha a seu respeito. Além disso, devem ser especificadas questões como: o que a empresa faz com as suas informações, de que forma o tratamento é realizado e por quanto tempo.

5) Qualidade dos dados:

Deve ser garantido aos titulares, que as informações que a empresa tenha sobre eles, sejam verdadeiras e atualizadas. É necessário ter atenção à exatidão, clareza e relevância dos dados, de acordo com a necessidade e com a finalidade de seu tratamento.

6) Transparência:

Todas as informações passadas pela empresa, em todos os seus

meios de comunicação, devem ser claras, precisas e verdadeiras. Além disso, a empresa não pode compartilhar dados pessoais com outras pessoas de forma oculta. Se você repassa dados pessoais para terceiros, inclusive para operadores que sejam essenciais para a execução do serviço, o titular precisa saber.

7) Segurança:

É responsabilidade das empresas buscar procedimentos, meios e tecnologias que garantam a proteção dos dados pessoais de acessos por terceiros, ainda que não sejam autorizados, como nos casos de invasões por hackers. Além disso, devem ser tomadas medidas para solucionar situações acidentais, como: destruição, perda, alteração, comunicação ou difusão dos dados pessoais de suas bases.

8) Prevenção:

O princípio da prevenção objetiva, estabelece que as empresas adotem medidas prévias para evitar a ocorrência de danos em virtude do tratamento de dados pessoais. Ou seja, as empresas devem agir antes dos problemas e não somente depois.

9) Não Discriminação:

Os dados pessoais jamais podem ser usados para discriminar ou promover abusos contra os seus titulares. A própria LGPD já criou regras específicas para o tratamento de dados que frequentemente são utilizados para discriminação, os chamados dados pessoais sensíveis, como os que tratam 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 a vida sexual e dado genético ou biométrico.

10) Responsabilização e Prestação de Contas:
Além de se preocuparem em cumprir integralmente a Lei, as empresas devem ter provas e evidências de todas as medidas adotadas, para demonstrarem a sua boa-fé e a sua diligência.

Direitos do Titular de Dados Pessoais:

Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
I - Confirmação da existência de tratamento;
II - Acesso aos dados;
III - Correção de dados incompletos, inexatos ou desatualizados;
IV - Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
V - Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
VI - Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
VII - Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
VIII - Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

IX - Revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

O que é base legal da LGPD?

As bases legais da LGPD, são os requisitos necessários para o tratamento de dados. Em outras palavras, as bases legais constituem as hipóteses de tratamento de dados pessoais. A **LGPD** prevê **dez bases legais** que autorizam o tratamento de dados pessoais. As bases legais não têm dependência ou predominância entre si. Para todo caso de tratamento de dados, a empresa é responsável por definir qual é a base legal mais apropriada.
O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses do artigo 7 da LGPD:
I - Mediante o fornecimento de **consentimento pelo titular**;
II - Para o **cumprimento de obrigação legal** ou **regulatória** pelo controlador;
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 instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
IV - Para a **realização de estudos por órgão de pesquisa**, garantida, 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; esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

VII - Para a **proteção da vida** ou da incolumidade física do titular ou de terceiro;

VIII - Para a **tutela da saúde**, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

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; ou

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

O que é um incidente de segurança com dados pessoais?

Um incidente de segurança com dados pessoais é qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança de dados pessoais, tais como: acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

O art. 47 da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD) determina que os agentes de tratamento de dados pessoais 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.

O que fazer em caso de um incidente de segurança com dados pessoais?

1) Avaliar internamente o incidente, natureza, categoria e quantidade de titulares de dados afetados, categoria e quantidade dos dados afetados, consequências concretas e prováveis.
2) Comunicar ao encarregado (Art. 5º, VIII da LGPD);
3) Comunicar ao controlador, se você for o operador, nos termos da LGPD;
4) Comunicar à ANPD e ao titular de dados, em caso de risco ou dano relevante aos titulares (Art. 48 da LGPD), e:
5) Elaborar documentação com a avaliação interna do incidente, medidas tomadas e análise de risco, para fins de cumprimento do princípio de responsabilização e prestação de contas (Art. 6º, X da LGPD).

*Consulta no site:
https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca

O que acontece com quem descumprir a LGPD?

• As penalidades estão previstas no Artigo 52 da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD) que traz as disposições sobre a fiscalização e as sanções administrativas que incidem sobre quem não cumprir a lei.

O que é Encarregado de Proteção de Dados do art.41 da LGPD ou Data Protection Officer / DPO do RGPD da União Européia?

Chamamos de Data Protection Officer, ou simplesmente DPO, o profissional que, dentro de uma empresa, é encarregado de cuidar das questões referentes à proteção dos dados da organização e de seus clientes.

Em seu trabalho, ele auxilia a empresa a adaptar seus processos para estruturar um programa de compliance com foco em maior segurança das informações que estão sob a sua tutela para atender a Lei .13.709/2018.

Na LGPD, o “DPO” é o chamado “encarregado de proteção de dados”, descrito no artigo 41: ”o controlador deverá indicar encarregado pelo tratamento de dados pessoais. § 1º. A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.”

O encarregado de proteção de dados, é responsável por:

- Iniciar atendimento de requisição de titulares (termo de consentimento, termo de confidencialidade), (atender os Direitos previstos no artigo 18);
- Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- Receber comunicações da autoridade nacional e adotar providências;
- Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;

- Informar e aconselhar a empresa e seus colaboradores que tratem dados pessoais a respeito das suas obrigações;
- Controlar a conformidade com a LGPD e demais normas aplicáveis, incluindo o compartilhamento de responsabilidades, a sensibilização e formação dos profissionais que sejam competentes por operações de tratamento de dados;
- Avaliar e aconselhar, quando pertinente, acerca dos relatórios de impacto;
- Elaborar os termos a serem implementados pelo TI da empresa de acordo com a LGPD;
- Monitoramento de leis e normas;
- Cooperar e ser o ponto de contato com as autoridades competentes.

Nosso Encarregado de Proteção de Dados conforme o artigo 41 da LGPD:

Luís Henrique Ribeiro

e-mail:dpo@daido.com.br

Boas práticas e governança,"estar em compliance" com a Lei Geral de Proteção de Dados Pessoais:

Os gestores, administradores, controladores e operadores, no âmbito de suas competências, nas empresas de qualquer setor ou porte deverão observar pelo tratamento de dados pessoais, individualmente ou por meio de associações, formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento de dados pessoais, fomentar as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos, e outros aspectos relacionados ao tratamento de dados pessoais conforme a Lei 13.709/2018.