Lei Geral de Proteção de Dados

Marcos para implementação da LGPD no Brasil

2010

Consulta Pública no Brasil sobre um anteprojeto de lei para proteção de dados

2013

Escândalo Snowden Espionagem de líderes de governos através de um software pelos EUA

Marco civil da internet (MCI)

2014

2016-2018

GDPR *(General Data Protection Regulation)* - **surgiu em 2016, na União Europeia e passou a vigorar em maio de 2018**

Escândalo Cambridge Analytica - Eleições Donald Trump

2018

LGPD no Brasil Aprovação em 2018, com entrada em vigor em maio/2021

2018

Notícias envolvendo vazamento de dados

Home › Segurança

Natura tinha brecha de segurança que expôs mais de 250 mil clientes

Por Felipe Demartini | 19 de Maio de 2020 às 15h51

Dados pessoais e sensíveis de mais de 250 mil clientes da Natura foram expostos na internet a partir de uma falha em dois servidores da empresa de cosméticos, que está entre as mais reconhecidas do segmento no Brasil. Além de registros identificáveis dos clientes, os volumes também traziam 40 mil tokens de acesso ao Wirecard, sistema de gestão financeira utilizado pela empresa em seu e-commerce, junto com informações de seus usuários, entre consumidores e vendedores de produtos da marca.

MENU G1 ECONOMIA BUSCAR

TECNOLOGIA

Rede social Google+ é encerrada após vazamentos de dados de usuários

Ferramenta foi criada para rivalizar com o Facebook, mas nunca teve o sucesso esperado.

Notícias envolvendo vazamento de dados

Hosts do Airbnb expõem fotos e dados de hóspedes em grupos de Facebook

01/11/2019 às 15:30 • 2 min de leitura

Vazamento expõe dados de 267 milhões de usuários do Facebook

Guilherme Preta, editado por Cesar Schaeffer 20/12/2019 09h17

LGPD (Lei n.° 13.709/2018)

Dispõe sobre o **tratamento de dados pessoais**, por pessoa natural ou jurídica de direito público ou privado.

Objetivo: proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Operações de tratamento realizadas no **território nacional**, para fins de oferta ou fornecimento de bens ou serviços.

LGPD (Lei n.° 13.709/2018)

A LGPD impõe regras sobre:

- **Coleta**
- **Armazenamento**
- **Tratamento** *(uso de dados com finalidade econômica)*
- **Compartilhamento de dados pessoais**

Essa norma objetiva a proteção de dados das pessoas naturais (físicas) e prevê a aplicação de penalidades pelo não cumprimento.

LGPD (Lei n.° 13.709/2018)

- Foi inspirada na lei europeia (GDPR)

- É uma lei de **governança** e ***compliance***
(políticas internas, normas, padrões – código de conduta e/ou regulamento interno)

LGPD (Lei n.° 13.709/2018)

A LGPD não busca proteção dados:

- ✓ **Empresariais**
- ✓ **Financeiros**
- ✓ **De propriedade industrial ou intelectual da empresa**

A proteção é somente aos dados das **pessoas físicas**.

Dados pessoais

- São informações que **identificam** *(nome, título de eleitor, CPF, RG, etc.)* **ou podem identificar** uma **pessoa** *(conjunto de dados)*:

Apresentador → **Jornal Nacional** → **Globo**

Dados sensíveis

- São dados que, pela **<u>sensibilidade natural</u>**, podem levar a uma situação de discriminação. *Ex.: saúde, raça, cor, partido político, biometria, gênero, etc.*

Dado de geolocalização que identifica religião = DADO SENSÍVEL

Personagens da Lei

DPO (*Data Protection Officer*) = **ENCARREGADO**

Consumidores = **TITULARES DOS DADOS**

EMPRESA

Empregados = **OPERADORES**

Empregador = **CONTROLADOR**

Bases Legais para utilização/armazenamento de dados

- Para tratar de dados é necessário uma **base legal**.

- "Tratar" dados envolve: coleta, armazenamento, exclusão, transferência, etc.

Bases Legais para utilização/armazenamento de dados

<u>Consentimento</u>: merece especial atenção e, para ser considerado válido, possui requisitos obrigatórios e cumulativos:

- Prévio
- Livre
- Informado
- Inequívoco
- Revogável

Ex.: Consentimento/autorização do empregado para transmitir dados ao Plano de Saúde.

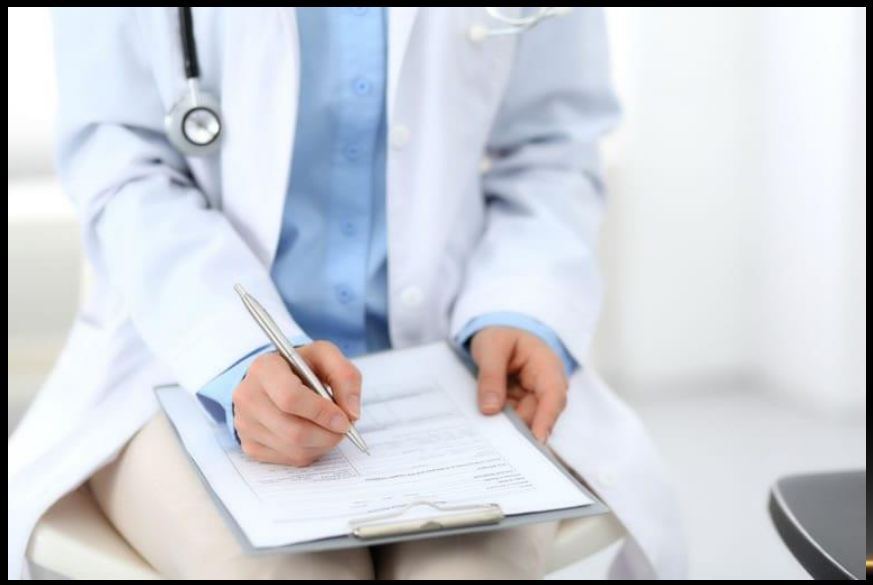
Bases Legais para utilização/armazenamento de dados

<u>Obrigação Legal</u>: É quando existe uma lei ou regulação que obriga o controlador a tratar aquele dado pessoal.

Ex.: Na legislação trabalhista é preciso que o empregador colete determinados dados do empregado, a fim de perfectibilizar o Contrato de Trabalho (RG, CPF, CTPS).

Bases Legais para utilização/armazenamento de dados

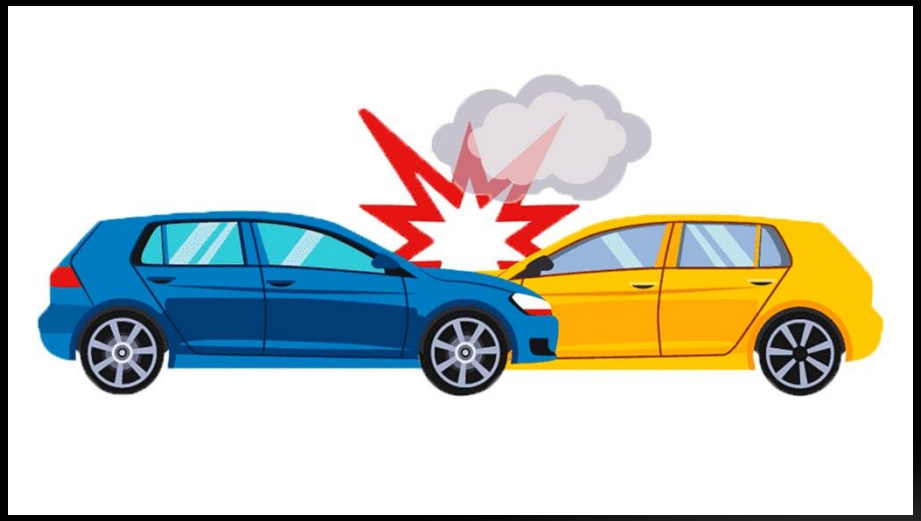
<u>Tutela da Saúde</u>: Legitima o tratamento de dados pessoais essenciais para prestação de serviços ligados à saúde.



Ex.: Fornecer dados pré-cirúrgicos ao médico

Bases Legais para utilização/armazenamento de dados

<u>Exercício regular de um direito</u>: A lei autoriza o tratamento de dados pessoais para atuação em processos judiciais, administrativos ou arbitrais.



Ex.: Há uma colisão de veículos e determinada pessoa não quer pagar o conserto. Para entrar com ação judicial não precisa do consentimento para uso dos dados.

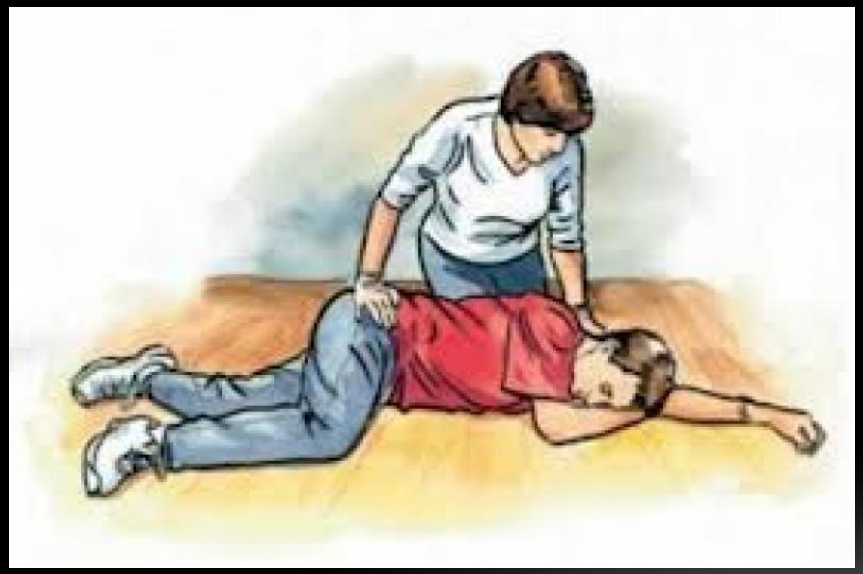
Bases Legais para utilização/armazenamento de dados

<u>Execução de um contrato</u>: É permitido o tratamento de dados pessoais para garantir a eficácia de um contrato, ou seja, para cumprir uma obrigação.

Ex.: Pede um lanche, via app, e compartilham dados com motoboy *(nome, pedido e endereço)*. A base legal é o contrato - não seria possível a entrega sem fornecer esses dados.

Bases Legais para utilização/armazenamento de dados

Proteção da Vida: quando identificado estado de perigo ou risco de vida do titular ou de terceiro, para que seja prestado socorro.



Ex.: Verificar na carteira o plano de saúde e identificação de alguém que passa mal na rua, para salvar sua vida.

Bases Legais para utilização/armazenamento de dados

<u>Políticas Públicas</u>: Base legal utilizada pelos órgãos públicos que legitima o tratamento de dados pessoais para execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres.

Ex.: Tragédia em Brumadinho = a administração pública precisou coletar dados para identificação das pessoas que moravam nas casas, para retirá-las.

Bases Legais para utilização/armazenamento de dados

<u>Finalidade de Pesquisa</u>: Utilização de dados pessoais para realização de pesquisas, mas somente por órgãos de pesquisa.

Ex.: Pesquisa do Censo (IBGE).

Bases Legais para utilização/armazenamento de dados

<u>Proteção ao crédito</u>: objetiva diminuir o risco de inadimplência

Ex.: Pontuação, Score, SERASA.

Bases Legais para utilização/armazenamento de dados

<u>Legítimo Interesse</u>: o controlador precisa ter legítimo interesse na coleta e armazenamento de dados, **estritamente necessários** para a finalidade pretendida.

Ex.:Autorização para envio de material de marketing.

Riscos da não-adequação à LGPD?

Risco financeiro: as multas para empresas que não estão em conformidade podem variar de 2% do faturamento do ano anterior chegando até a R$ 50 milhões por infração, passando por penalidades diárias. Além disso, titulares de dados poderão mover ações indenizatórias em decorrência de vazamento e desvio de finalidade.

Risco de perda reputação, de mercado e de clientes: empresas em desconformidade com a LGPD podem perder mercado para a concorrência, parcerias e consumidores. O abalo da confiabilidade reflete diretamente na reputação e nos negócios.

Como adequar empresas à LGPD?

<u>Mas, por onde começar</u>?

O ideal é estabelecer um projeto (jurídico + TI) de conformidade em proteção de dados. Esse projeto deverá ter, no mínimo, cinco etapas, podendo haver adaptações de acordo com o porte da organização e suas especificidades.

Etapa 1
MAPEAMENTO

Etapa 2
GAP ANALYSIS

Etapa 3
PLANEJAMENTO

Etapa 4
IMPLEMENTAÇÃO

Etapa 5
MONITORAMENTO

Etapa 1
MAPEAMENTO

Mapear por completo os dados que a empresa armazena, distinguindo a categoria deles: dados pessoais ou sensíveis

Averiguar o tratamento que os dados recebem, por exemplo, se estão apenas sendo armazenados ou são repassados para terceiros.

Identificar a necessidade de consentimento ou não para armazenamento e repasse dos dados.

Etapa 1
MAPEAMENTO

Assim, é preciso verificar:

- Qual o **fluxo** de dados pessoais nos setores?
- **De onde vem** esses dados e **para onde vão**?
- Com qual **finalidade?**
- **Onde ficam armazenados**?
- São **compartilhados** com **terceiros**?

Etapa 2
GAP ANALYSIS
(Análise de Lacunas)

Através do mapeamento de dados feito na etapa anterior, **identificam-se** os principais pontos em desconformidade com a legislação, apontando soluções para **mitigar ou minimizar os riscos**.

Ex.: O problema da empresa é nos procedimentos X, Y e Z. A partir do mapeamento de dados é possível demarcar as soluções.

Etapa 3
PLANEJAMENTO

O objetivo dessa fase é **planejar** a forma de execução das soluções propostas na fase anterior, criando um **plano de ação e um cronograma de execução**, **priorizando as áreas que contém maior risco**.

Nessa etapa é importante fazer o relatório do projeto de conformidade, detalhando os próximos passos para implementação do programa de governança em proteção de dados.

Etapa 4
IMPLEMENTAÇÃO

O objetivo é colocar em prática o **plano de ação** estabelecido na fase anterior, incluindo a elaboração de todos os **documentos** que se fizerem necessários:

- criação de políticas internas
- elaboração de termos de consentimento específicos para as finalidades de cada tratamento
- revisão dos procedimentos adotados.

Etapa 5
MONITORAMENTO

O monitoramento do cumprimento das diretrizes estabelecidas no **programa de governança em proteção de dados** deve ser constante, com as atualizações necessárias, garantindo que a organização se mantenha em conformidade.

É realizado pelo **DPO** (*Data Protection Officer*), ou seja, o profissional responsável pela proteção de dados.

Penalidades da LGPD

A **NÃO** observância da LGPD implica em sanções de ordem Administrativa a serem aplicadas pela ANPD (Autoridade Nacional de Proteção de Dados), por exemplo:

- Advertência e indicação de medidas corretivas, dentre elas a adoção de aspectos de segurança da informação

- Multa de até 2% do faturamento ou até 50 milhões de reais, por infração

- Obrigação de divulgar a infração ao mercado

- Bloqueio dos dados pessoais

- Eliminação dos dados pessoais

Penalidades da LGPD

Vale destacar o prejuízo à marca da empresa autuada pela não conformidade à LGPD. A obrigação de divulgar a infração faz com que os agentes sem a maturidade organizacional, exigida pela LGPD tenham sua imagem prejudicada.

Além disso, o não cumprimento da norma pode levar à perda de clientes e impactar na avaliação das empresas.

O papel da TI no processo de mudança

Encarregado: pessoa indicada pelo controlador. É o DPO (*Data Protection Officer*).

- Responsável pela comunicação entre o controlador, os titulares dos dados e a ANPD
- Atua no gerenciamento do programa de proteção de dados dentro de uma empresa
- Elabora a interface interna com colaboradores da empresa e relacionamento externo com clientes, fornecedores ou qualquer empresa que possa ter relação
- Fiscaliza o gerenciamento de dados

O papel da TI no processo de mudança

A área de TI tem um papel regulador essencial no processo de adequação à LGPD:

- Revisão da estrutura da empresa (pastas compartilhadas, permissões de acesso, arquivos)

- Revisão de processos (físicos e digitais)

- Contratação de fornecedores adequados à LGPD

O papel da TI no processo de mudança

Ao fazer a verificação, os profissionais vão incluir a própria área. E é nesse ponto que a TI se apresenta como um desafio, pois, por menor que seja, haverá a necessidade de mudanças para que todas as ferramentas utilizadas, de hardwares a softwares, de banco de dados à infraestrutura para backup, estejam preparadas para garantir o tratamento adequado dos dados e sua segurança.

Qualquer dúvida, estamos à disposição pelo e-mail: gilcelerneradvogada@gmail.com e Fone: (54) 99710-4004