LEI GERAL DE PROTEÇÃO DE DADOS

Rony Vainzof
Diretor do Departamento de Segurança e Defesa da FIESP
LinkedIn: Rony Vainzof

FIESP CIESP

LEI GERAL DE PROTEÇÃO DE DADOS

Cartilha – FIESP

https://www.fiesp.com.br/

Eficácia da LGPD

- **Sanção da LGPD:** 14/08/18 - Lei 13.709/18;
- **Criação da ANPD:** 28/12/18 - Medida Provisória 869/18 > Lei 13.853/19;
- **LGPD em vigor:** 18/09/20 - Medida Provisória 959/20 > Lei 14.058/20;
- **Sanções administrativas**: 01/08/21 - Lei 14.010/20.

Segurança jurídica e segurança da informação

- Harmonização e atualização de conceitos;
- A LGPD não impede o tratamento de dados pessoais. Muito pelo contrário, é um “mapa” a ser seguido pelas organizações visando o uso ético, responsável e seguro;
- Benefícios amplos em termos de segurança da informação.

Maior possibilidade de investimentos do exterior

- "GDPR" brasileiro;
- Centenas de países, no mundo inteiro, com legislações correlatas;
- Possibilidade de desburocratizar o fluxo internacional de dados.

Efeito cultural

- Maior conscientização da sociedade sobre privacidade e proteção de dados. Cobrança por um tratamento ético, transparente e seguro;
- Só trocamos informações com quem confiamos;
- PEC 17/19;
- Efeito viral da lei. Empresas cobrando empresas.

Importância da LGPD para o Brasil

Benefícios de se adequar: em pesquisa realizada pela Cisco em Janeiro de 2019, as empresas que se adequaram à GDPR apontaram os principais benefícios identificados a seguir:

- 42% - Ganho em agilidade e inovação por possuir maior controle sobre os dados;
- 41% - Aumento de vantagem competitiva em relação à outras empresas;
- 41% - Alcance de maior eficiência operacional por ter os dados organizados e catalogados;
- 39% - Redução de perdas relacionadas à incidentes de segurança com dados pessoais.

Fonte: Maximizing the value of your data privacy investments – Cisco 2019

Sanções e responsabilidades

Danos reputacionais	**Danos morais e patrimoniais** (individuais e coletivos)	**Sanções Administrativas**

Conceitos relevantes

- Dados pessoais sensíveis
- Dados pessoais diretos
- Dados pessoais indiretos
- Dados pessoais pseudonimizados
- Dados anonimizados (não são considerados dados pessoais)

Conceitos relevantes

- **Titular**: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

- **Tratamento**: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

- **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.

LEI GERAL DE PROTEÇÃO DE DADOS

Autodeterminação informativa

- **Princípios**: finalidade, adequação, necessidade, transparência, não discriminação, livre acesso, qualidade, segurança, prevenção e responsabilização e prestação de contas;

- **Bases legais** para o tratamento;

- **Direitos dos titulares**;

- **Responsabilidade** dos agentes de tratamento.

LEI GERAL DE PROTEÇÃO DE DADOS

Accountability

Responsabilização e prestação de contas:

Demonstrar medidas eficazes e capazes de comprovar a conformidade

O que é dado pessoal?

O que é dado sensível?

O que é dado anonimizado?

Definição de base legal:
Quando aplicável o consentimento?

Quando aplicável o interesse legítimo?

Quando se dá o término do tratamento e a consequente eliminação dos dados pessoais

Quando o relatório de impacto à proteção de dados pessoais será necessário

Escolha do DPO

Escolha dos operadores de dados

Em caso de incidente, decidir se é o caso de informar a ANPD e aos titulares

Medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais

LEI GERAL DE PROTEÇÃO DE DADOS

Governança

- Demonstrar o comprometimento em adotar processos e políticas internas que assegurem o cumprimento de normas e boas práticas
- Ser aplicável a todo o conjunto de dados pessoais que estejam sob seu controle
- Ser adaptado à estrutura, à escala e ao volume de suas operações, 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 estabelecer e aplicar mecanismos de supervisão internos e externos
- Contar com planos de resposta a incidentes e remediação
- Ser atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas
- Demonstrar a efetividade de seu programa

NORMA BRASILEIRA

ABNT NBR ISO/IEC 27701

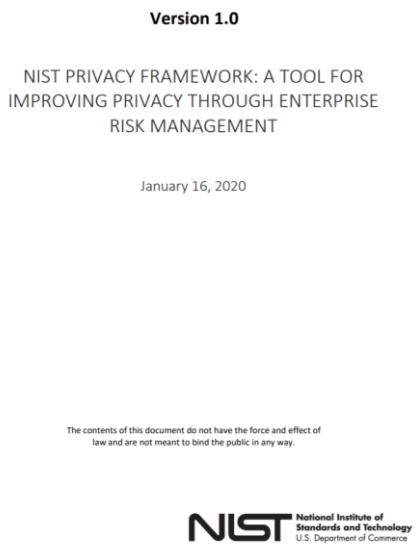
Primeira edição 25.11.2019

Versão corrigida 11.02.2020

Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes

Security techniques — Extension to ABNT NBR ISO/IEC 27001 and ABNT NBR ISO/IEC 27002 for privacy information management — Requirements and guidelines

https://www.abntcatalogo.com.br/norma.aspx?ID=437612



Version 1.0

NIST PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT

January 16, 2020

The contents of this document do not have the force and effect of law and are not meant to bind the public in any way.

NIST National Institute of Standards and Technology U.S. Department of Commerce

https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf

Figure 1 – CIPL "Accountability Wheel" – Universal Elements of Accountability

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/introduction_to_two_new_cipl_papers_on_the_central_role_of_organisational_accountability_in_data_protection.pdf

LEI GERAL DE PROTEÇÃO DE DADOS

O que esperar com a eficácia da LGPD

- Direitos dos titulares.
- Incidentes envolvendo dados pessoais
- Novos projetos que envolvam decisões automatizadas ou dados mais críticos, como sensíveis;
- Que não seja um "novo normal" o aumento de litígios, com a LGPD em vigor, ainda mais pelo fato da ausência da ANPD;
- Diversas questões poderiam já estar regulamentadas, como:
  i. Padrões de medidas técnicas e administrativas de segurança;
  ii. Padrões e técnicas de anonimização de dados pessoais;
  iii. Prazo para atendimento dos requerimentos dos titulares;
  iv. Decisão adequação de outros países e cláusulas-padrão contratuais para facilitar a transferência internacional de dados;
  v. Padrões para portabilidade de dados; e
  vi. Normas complementares para definição e as atribuições do Data Protection Officer, inclusive hipóteses de sua indicação.
  vii. Apreciar petições de titular contra controlador após comprovação de não solução de reclamação no prazo estabelecido em regulamentação;
  viii. Implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com a Lei;
  ix. Estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais; e
  x. Editar orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como startups, possam adequar-se a Lei.
- Ação movida por um estudante em Recife por implantação de biometria facial nos ônibus da Região Metropolitana de Recife.

- Ao invés de inquisição e sanção, dar prioridade ao diálogo, apoio, mútua cooperação, orientação, conscientização e informação;
- Estimule relações abertas e construtivas com negócios que lidem com dados pessoais, primando pela boa-fé das empresas e nos seus esforços em cumprir a lei;
- Crie ambientes para inovações responsáveis, como "Regulatory Sandboxes", nos quais novos projetos são testados de forma controlada visando avaliar eventuais e futuras necessidades regulatórias, conforme o caso, mas a posteriori;
- Edite normas, orientações e procedimentos para que as microempresas e empresas de pequeno porte possam se adequar à Lei;
- As futuras sanções devem ser a ultima ratio, principalmente e somente quando houver alguma violação dolosa, ou práticas exponencialmente negligentes, condutas reiteradas ou extremamente graves.

LEI GERAL DE PROTEÇÃO DE DADOS

Para lembrar

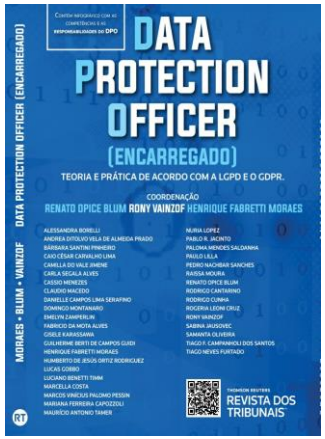
- Coleta massiva de dados para coleta mínima e justificável

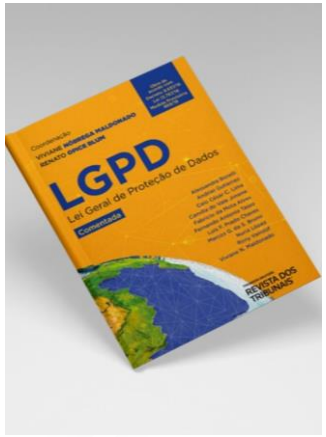
Art. 44. O tratamento de dados pessoais será irregular **quando deixar de observar a legislação ou** **quando não fornecer a segurança que o titular dele pode esperar**, consideradas as circunstâncias relevantes, entre as quais: I - o modo pelo qual é realizado; II - o resultado e os riscos que razoavelmente dele se esperam; III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

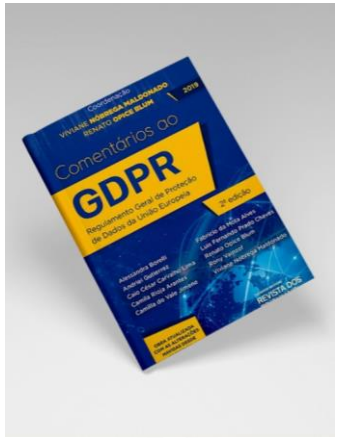
- Binômio: necessidade / proporcionalidade
- Estabelecer uma relação de confiança com o titular
- A Lei vai pegar? Proteção de Dados vai além...
  - "Estamos vivendo uma nova fase do Compliance, que agora, além do combate à corrupção, visa o uso ético e seguro dos dados pelas entidades públicas e privadas" Rony Vainzof

LEI GERAL DE PROTEÇÃO DE DADOS

Recomendações de conteúdo







https://www.portaldaprivacidade.com.br/