CENTRO UNIVERSITÁRIO DE BRASÍLIA

PROJETO DE INTEGRAÇÃO DIRIGIDA E INTERDISCIPLINAR V

JOÃO NILSON DE OLIVEIRA LIMA

SITE E PRÉVIA DO CONTEÚDO

BRASÍLIA

2020

Menus: LGPD; METODOLOGIA DE APLICAÇÃO; SERVIÇOS REALIZADOS; CONTATO.

Título principal: Entenda a LGPD e prepare-se para uma nova era de proteção de dados.

LGPD:

~~**1 - Relógio dinâmico:**~~ Sem relógio dinâmico, a Lei foi sancionada sexta-feira(18).

2- O que é a LGPD?

Antes de tudo, a Lei 13.709/2018 (http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm) é onde se encontra prevista todas as informações referentes à Lei Geral de Proteção de Dados Pessoais (LGPD). Essa lei regula todo o **tratamento** de dados pessoais dos cidadãos brasileiros dentro e fora do país. Nela, há regras de processos de coleta, armazenamento e compartilhamento das informações.

Os principais objetivos na LGPD são: Proteção à privacidade, transparência, desenvolvimento, padronização de normas, segurança jurídica e favorecimento à concorrência.

Este vídeo muito educativo da SERPRO elucida, de forma simples e interativa, o que é a LGPD: https://www.youtube.com/watch?v=Tk-r0GUt1GU

E, para complementar mais ainda, um entendimento prático do funcionamento da LGPD na proteção dos dados pessoais: https://www.camara.leg.br/internet/agencia/videos/repasse_dados_pessoais.mp4

3- Benefícios e impactos ao seu negócio:

A implantação da lei geral de proteção de dados necessita de certos **planejamentos**, os quais trazem à entidade um diferencial frente ao mercado. Percebe-se a imposição de uma **organização** prévia de dados a fim de os gestores compreenderem o cenário atual em que se encontram as informações que serão tratadas e, consequentemente, um **plano de ação** é estruturado.

Também, a **percepção** da importância dos dados e de como estes serão abordados é modificada, portanto, relações mais **transparentes** com o cidadão, empresas e governo serão arranjadas. Por esse motivo, a **infraestrutura** de Tecnologia da Informação deve ser cada vez mais desenvolvida, com uma visão fortemente centrada na segurança cibernética, por conseguinte, o **investimento** nessa área será imprescindível para a

conformidade da sua entidade com legislação atual e, com certeza, uma porta de entrada para novas tecnologias como Internet das Coisas (IoT) e Inteligência Artificial (IA).

A necessidade de um cuidado maior perante os dados de terceiros demanda da entidade possuidora um investimento em **capacitação e conscientização** dos funcionários para uma melhor gestão de informação. Automaticamente, o conhecimento técnico do pessoal cresce e a organização ganha em capacidade de trabalho.

E, por fim, com instauração da LGPD na organização, haverá uma maior **confiabilidade** na empresa em virtude do compliance das normas.

Aqui, a fim de complementar esse tópico, há um vídeo do SEBRAE mostrando os impactos da LGPD para a sua empresa:

https://www.youtube.com/watch?v=-ziciyDjxDI

4- O que sua empresa deve fazer?

Due Diligence sobre dados pessoais: Identificação dos dados (pessoal, sensível, criança, público, anonimizado), departamentos, meios (físico ou digital), operadores internos e externos para mensuração de exposição da empresa à LGPD;

Auditoria sobre o Tratamento: Aderência das 20 atividades de tratamento (art. 5º, X) de dados (coleta, controle, eliminação, etc.) aos princípios gerais previstos no Art. 6º da LGPD, mediante revisão e criação de documentos (contratos, termos, políticas) para uso interno e externo;

Gestão do Consentimento e Anonimização: Controle do consentimento e anonimização para atender possível solicitação do titular e da futura agência;

Gestão dos Pedidos do Titular: Criação de banco de dados para controle dos pedidos dos titulares dos dados (acesso, confirmação, anonimização, consentimento, portabilidade etc.);

Relatório de Impacto: Atendimento à Autoridade Nacional de Proteção de Dados (ANPD) e demais órgãos do Sistema Nacional de Proteção do Consumidor que poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais;

Segurança dos Dados: Adoção das medidas de segurança da informação aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas;

Governança do Tratamento: Criação de regras de boas práticas e de governança que estabeleçam procedimentos, normas de segurança, ações educativas e mitigação de riscos no tratamento de dados pessoais;

Plano de Comunicação – Incidente de Segurança: Comunicação aos órgãos fiscalizatórios (ANPD, Procon, Senacon) e à imprensa sobre incidente de segurança que acarrete risco ou dano;

Validação do término do tratamento: Adoção das providências necessárias à eliminação dos dados tratados e verificação de eventual conservação dos dados com a elaboração de documentos que evidenciem a eliminação;

Certificação: Certificação por auditoria especializada das práticas relacionadas à LGPD;

Data Protection Officer (Encarregado): Identificação do encarregado (Pessoa Física ou Jurídica) e sua capacitação para exercer as atividades previstas na LGPD;

Prevenção de Conflitos: Inclusão de uma cláusula compromissória de mediação vinculada à câmara privada online cadastrada no CNJ para mitigação do contencioso judicial;

https://www.lgpdbrasil.com.br/o-que-muda-com-a-lei/

5- É melhor o investimento

Certamente a implementação da lei na empresa trará impacto nos custos, entretanto, esse investimento de adequação/prevenção é mais conveniente do que multas e penalidades. No artigo 52 da LGPD, são elencadas as sanções cabíveis, como:

1- advertência, com indicação de prazo para adoção de medidas corretivas;

2- multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

3 - multa diária, observado o limite total a que se refere o inciso II;

4 - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

5 - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

6 - eliminação dos dados pessoais a que se refere a infração;

7 - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;

8 - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;

9 - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Dois casos muito importantes que envolveram dados pessoais vazados foram os do **Facebok** e da **Uber**. A rede social teve seu CEO – Mark Zuckerberg – pressionando no Senado dos Estados unidos para explicar o uso indevido dos dados de 87 milhões de usuários da rede social por meio da empresa de consultoria política Cambridge Analytica.

Imagem: https://g1.globo.com/economia/tecnologia/noticia/mark-zuckerberg-depoe-ao-senado-sobre-uso-de-dados-pelo-facebook.ghtml

Já a Uber teve que pagar 148 milhões de dólares pelo vazamento de dados de 57 milhões de clientes.

Imagem logo UBER:

METODOLOGIA:

A consultoria JNC&S prioriza a eficiência e eficácia na produção da sua nova política de segurança de dados. Entendemos a importância da informação dos usuários e o valor que esta apresenta para a entidade. Com isso, a atualização não só trará a conformidade da sua empresa perante a legislação, mas também um olhar atualizado para tecnologias.

Incialmente, a política de proteção e segurança de dados tem que ser **clara**, **concisa**, com uma **linguagem acessível**, para garantir a compreensão e a confiança do cliente.

Também, não adianta somente ter uma política exemplar, há que se investir na proteção desses dados que serão coletados, tornando sua base de dados segura, imune a possíveis violações.

Por fim, seus colaboradores precisam estar atualizados da nova lei e da nova política, a fim de prestarem um serviço completo e seguro aos usuários.

É de suma importância salientar que a JNC&S não se limita somente à atualização da sua política de segurança de dados, mas também presta serviços voltados à **gestão do banco de dados** para controle de pedidos dos titulares dos dados, à **criação do relatório de impacto**, à **adoção de medidas de segurança dos dados**, à **criação de regras de boas práticas e de governança**, à criação de **plano de comunicação de incidente**, à **escolha do Data Protection Officer (Encarregado)** etc.

Com essa pequena introdução, podemos seguir e mostrar como a JNC&S prepara a sua entidade e cria a nova política de segurança de dados.

1- Inicialmente, o entendimento do contexto do tratamento de dados pessoais na organização e como os princípios da LGPD são atendidos no sistema ou serviço é necessário. Para isso, é feita a **identificação dos dados circulantes**, da **estrutura organizacional** e dos demais **operadores internos e externos**. A proteção dos dados não se limita ao ambiente interno, portanto, uma análise do ambiente externo é imprescindível;
2- Em virtude do parágrafo anterior, quando aplicáveis, a política deverá apresentar informações sobre o **compartilhamento dos dados com terceiros** e qual a finalidade, sobre **transferência internacional** e qual

a finalidade, sobre proteção de **dados de menores de idade**, sobre proteção de **dados sensíveis**, dentre outros;

3- A política vigente será analisada, a fim de **acrescentar conceitos** em conformidade com o tratamento de dados, que é 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;
4- O tratamento de dados deverá estar análogo aos princípios presentes no art. 6º da LGPD;
5- Acrescentar-se-á, na política, **informações sobre a organização** responsável pelo tratamento;
6- Também, a consultoria terá acesso às **finalidades dos tratamentos** dos respectivos dados pessoais e, a fim de esclarecer ao usuário o intuito da intervenção, serão inseridas no documento de segurança;
7- Será acrescida à política uma **tabela com prazos de retenção dos dados pessoais**;
8- Há a necessidade de um **Data Protection Officer (DPO)** para a entidade, portanto, na política, terá a informação do encarregado de proteção de dados;
9- É importante estar presente na política as formas como o titular irá acessar, corrigir, solicitar a exclusão de dados, transferir, limitar ou se opor ao tratamento, e retirar o consentimento;

A política criada deve estar disponível ao titular dos dados antes do início do tratamento do dado pessoal dele.

https://www.serpro.gov.br/lgpd/governo/como-se-adequar-lgpd