**LGPD em pequenos e médios negócios**

Bruno Seiti, Felipe Leitão, João Pedro Libonati

O Brasil tem muitas empresas, sendo a maioria pequenas e médias empresas (PMEs). Além disso, o entendimento e a execução da aplicação da LGPD é um tema cada vez mais falado. Dessa forma, foi escrito esse documento para esclarecer questões básicas referentes a LGPD às PMEs.

LGPD é a sigla para Lei Geral de Proteção de Dados do Brasil, sancionada em agosto de 2018, que entrará em vigor agosto de 2020. A LGPD regulamenta como qualquer empresa, independente de qual seja, deve utilizar, coletar e armazenar dados de pessoas naturais ou pessoas jurídicas de direito público ou privado.

Os principais objetivos da LGPD é a proteção da liberdade e privacidade do indivíduo. Tendo como princípios:

- **Finalidade**: Propósitos legítimos, específicos, explícitos e informados.

- **Adequação**: Compatível com as finalidades.

- **Necessidade**: Utilização (apenas) de dados estritamente necessários.

- **Livre acesso**: Acesso ao tratamento e à integralidade dos dados.

- **Qualidade dos dados**: Dados exatos, claros, relevantes e atualizados.

- **Transparência**: Informações claras e precisas aos titulares.

- **Segurança**: Medidas técnicas e administrativas aptas a proteger os dados pessoais.

- **Prevenção**: Adoção de medidas para evitar danos aos titulares.

- **Não discriminação**: Não utilização para fins discriminatórios, ilícitos ou abusivos.

- **Responsabilização e prestação de contas**: Demonstração de adoção de medidas eficazes ao cumprimento de normas.

Em relação a sua aplicação, a LGPD regula o tratamento dos dados a pessoas físicas, independentemente do meio utilizado para a coleta dos dados, sendo exclusivamente para o território brasileiros com algumas exceções. Essas exceções sendo: quando os dados são coletados dentro do Brasil, dados com o intuito à venda de produtos ou serviços para o mercado brasileiro e dados pertencentes a brasileiros.

Isso em relação a quando a LGPD se aplica, mas a lei não se aplica quando o tratamento é realizado: por pessoa natural sem fins lucrativos, com fins artísticos, acadêmicos ou jornalísticos, por segurança publica e de estado, com pessoas de outros países que apenas transitem no Brasil.

A fiscalização será feita pela ANPD (Autoridade Nacional de Proteção de Dados), que fará aplicação de sanções e promoverá estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade. Diante disso, o impacto que isso trará a PMEs serão: A adequação do negócio, que é a necessidade de pensar nas políticas necessárias e ver como essas políticas podem ser implementadas. O mapeamento dos dados que é a necessidade de criar uma espécie de fluxograma das informações que passam pela empresa, também mapear todos os dados pessoais que são tratados na empresa para usar processos otimizados e utilizar a menor quantidade de dados para os objetivos da empresa, para correr menos riscos. Custo de implementação e a comunicação interna.

Segundo a LGPD, há a necessdade de que o Data Protection Officer (DPO) seja nomeado. O DPO tem como seu principal papel garantir que a organização processe os dados pessoais (de equipe, clientes, provedores ou de titulares de dados) em conformidade com as regras de proteção de dados aplicáveis. Ele deve treinar e orientar os funcionários da organização, realizar avaliações e auditorias para garantir conformidade com a regulamentação, servir como ponto de contato entre a organização e a autoridade supervisora, manter registros das atividades de processamento de dados realizadas pela organização, responder e informar os titulares de dados pessoais sobre como seus dados estão sendo usados, informar quais as medidas de proteção implementadas pela organização e assegurar que os pedidos de acesso ou apagamento de dados feitos por titulares de dados pessoais, sejam atendidos ou respondidos, quando necessário.

De acordo com o site <https://alvespereiraadv.jusbrasil.com.br/artigos/727340627/data-protection-officer-dpo-papeis-e-responsabilidades>, grandes empresas já estão implementando um compliance em LGPD, enquanto que parte considerável das médias empresas ainda não iniciaram nenhuma ação relacionada ao tema.

Em relação à situação atual da lei, existem partes da LGPD que já estão em vigor desde o dia 28 de dezembro de 2018, sendo esses os Artigos do 55-A até o 55-L,58-A e 58-B. O resto da lei está com data prevista para entrar em vigor em agosto de 2020. Também, a lei não está totalmente regulamentada, como por exemplo o parágrafo único do artigo 27: “Parágrafo único. A informação à autoridade nacional de que trata o caput deste artigo será objeto de regulamentação”.

Caso ainda há dúvidas a respeito de como implementar as novas regras criadas pela a LGPD, levantamos algumas sugestões para auxiliar no processo de implantação da LGPD, sendo essas:

1. Crie um comitê para implementação do LGPD com 1 pessoa de cada área da empresa para repassar as informações.
2. Nomear um encarregado de proteção de dados ou DPO(Data Protection Officer), alguém com conhecimento em segurança da informação e da LGPD
3. Mapeie os dados, ou seja, estabeleça os dados que sua empresa coleta, onde coleta, como e onde armazena.
4. Não guarde dados que desnecessário, ou seja, não guarde informações que não seja necessário para o funcionamento operacional da empresa
5. Separe os dados em categorias, se a sua empresa desenvolve sistemas, também será necessário avaliar a conformidade do seu produto.
6. A LGPD não irá sobrepor as regras já existentes, ou seja, a LGPD deverá ser implementada e deve se obedecer ao marco civil da internet, CDC, CPC, a lei Carolina Dieckmann como outras.
7. Verificar sistemas de terceiros como processadores e controladores de dados para não estar violando a lei indiretamente.
8. Implementar políticas para identificar e controlar quaisquer informações relacionados aos dados da empresa
9. Crie um plano de risco para verificar os riscos e como deter os mesmos
10. Crie uma política de segurança da informação
11. Adequar o armazenamento de dados de modo que fique fluido para quando houver necessidade de transferência de dados fique mais garantido a portabilidade dos dados.
12. Criar uma política de retenção e de destruição de dados (quando os dados terminarem o período de retenção eles possam ser destruídos de uma maneira segura)
13. Treinar o comitê para todos saberem o que constrói os dados pessoais (papeis do controlador, processador, DPO e os princípios da LGPD).
14. Treinar o comitê para identificar violações e manter um registro dessas violações.
15. Criar políticas de resposta ao incidente
16. Alinhar as políticas de resposta ao incidente ao RIPD (relatório de impacto à proteção de dados) se não tiver uma RIPD criar.
17. Fazer o inventário dos equipamentos
18. Verificar se os equipamentos estão criptografados
19. Criar regras para o transporte de equipamentos fora da empresa
20. Revisar e documentar a segurança física dos dados (USB, sistemas de armazenamento de dados)
21. Bloqueie todos os dados pessoais com segurança.
22. Delimitar quais usuários devem ter acesso aos dados de cada dispositivo.
23. Atualize a política de privacidade do seu site (para incluir a identidade do responsável pelo processamento e a base legal, o interesse legítimo, qualquer destinatário ou categorias de destinatários dos dados pessoais, o direito de retirar o consentimento a qualquer momento e o período de retenção de dados). Verifique o uso de cookies do seu website.
24. Realizar auditorias para verificar a conformidade com a LGPD.
25. Fazer testes de intrusão.
26. Use os relatórios do teste de intrusão para verificar vulnerabilidades e potenciais invasões para corrigir as vulnerabilidades e aumentar a segurança do cliente.

Assim, encerramos o artigo sobre a LGPD. Esperamos que isso tenha esclarecido as dúvidas sobre a lei e seus impactos nas pequenas e médias empresas do Brasil.

Seguem as fontes usadas na criação do documento:

http://www.planalto.gov.br/ccivil\_03/\_ato2015-2018/2018/lei/L13709.htm

<https://lgpd.com.br/>

<https://resultadosdigitais.com.br/blog/o-que-e-lgpd/>

<https://www.conjur.com.br/2019-out-31/deputado-propoe-entrada-vigor-lgpd-seja-adiada>

<https://alvespereiraadv.jusbrasil.com.br/artigos/727340627/data-protection-officer-dpo-papeis-e-responsabilidades>

<https://espm.blackboard.com/bbcswebdav/pid-1590891-dt-content-rid-14563281_2/courses/003210-01-1902-GS2-TI5A-02260/Vis%C3%A3o%20geral%20LGPD.pdf>

<https://periciacomputacional.com/guia-para-implementacao-da-lgpd-na-sua-empresa/>