

JANEIRO/2020

LEI GERAL DE PROTEÇÃO DE DADOS COMO ADEQUAR O SEU NEGÓCIO?



Renata
Rodrigues
Advocacia

LEI GERAL DE PROTEÇÃO DE DADOS COMO ADEQUAR SEU NEGÓCIO?



Introdução

Este material foi produzido por Renata Rodrigues, sócia-fundadora do escritório Renata Rodrigues Advocacia, e tem o objetivo de sugerir, de forma didática e resumida, um passo-a-passo para adequação de sua empresa à Lei Geral de Proteção de Dados (“LGPD”).

O presente documento tem caráter meramente informativo e não busca orientar qualquer pessoa para fins legais, não podendo ser utilizado como opinião legal.

LEI GERAL DE PROTEÇÃO DE DADOS COMO ADEQUAR SEU NEGÓCIO?

Passo-a-Passo

Como você já deve saber, a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (“LGPD”),¹ passará a vigorar em agosto de 2020.² Ela altera, de forma relevante, o tratamento de dados pessoais, que abrange atividades como coleta, arquivamento, utilização, transferência e eliminação de informações relacionadas a pessoas físicas.

Para não sofrer as penalidades previstas na referida lei, pessoas físicas ou jurídicas, dos setores público e privado, que tratem dados pessoais, por meio físico ou digital, no território nacional, independentemente de seu segmento, precisam se adequar ao disposto na LGPD e criar um programa de conformidade.

A seguir sugeriremos os passos a serem observados durante o processo de adaptação das empresas. Consistem em orientações e boas práticas de governança de dados para empreendedores, escolas, varejistas, arquitetos, profissionais de saúde, de marketing, dentre outros.

Cada processo de adequação deverá levar em conta diversos fatores, tais como o tamanho do negócio, o ramo de atividade, a existência de um programa de governança ou de segurança da informação e as necessidades de cada empresa. De todo modo, algumas etapas são imprescindíveis, e, em linhas gerais, consistem em:

- I. Estudo:** análise da LGPD e demais leis que regulamentam o negócio;
- II. Planejamento:** determinação da forma de execução do Projeto;³
- III. Mapeamento:** levantamento dos dados tratados pela empresa e suas características;
- IV. Análise de Risco:** verificação dos pontos de desconformidade com a LGPD;

1 Para entender os principais aspectos da LGPD, acesse o nosso e-book “Lei Geral de Proteção de Dados – Em 5 minutos” e nosso e-book “Lei Geral de Proteção de Dados – Q&A”.

2 Encontra-se em tramitação na Câmara dos Deputados o Projeto de Lei 5762/19, que prorroga por dois anos, de agosto de 2020 para agosto de 2022, a vigência da maior parte da LGPD. Quando da edição deste material, em janeiro/2020, o PL ainda não havia sido votado.

3 Para facilitar a leitura deste material, chamaremos de “Projeto” o processo de adequação de uma empresa à LGPD.

- V. **Plano de Ação:** definição do conjunto de medidas a serem adotadas para implementação do Projeto;
- VI. **Implementação:** adoção das medidas contidas no Plano de Ação;
- VII. **Monitoramento:** acompanhamento das rotinas para manutenção das práticas exigidas na legislação.

A duração de cada etapa de adequação à LGPD variará, principalmente, conforme o tamanho da empresa e seu segmento.

I. Estudo.

Inicialmente, faz-se necessário compreender o que diz a regulamentação. É preciso entender o que a LGPD exige e como ela afeta, concretamente, a empresa, suas rotinas e processos. O desafio para se adaptar pode ser menor, por exemplo, para pequenas empresas. No entanto, como já vimos, a LGPD se aplica de maneira igual para empresas de grande e pequeno portes.

Sua importância e aplicabilidade deve ser claramente compreendida pelos colaboradores e titulares de dados. A cultura de proteção de dados já é uma realidade e traz enormes benefícios para as empresas, especialmente, a vantagem competitiva de se apresentar aos titulares de dados como um negócio que se preocupa com a privacidade e a proteção de seus dados pessoais.

Vale realizar treinamentos para todas as áreas da empresa ou para aquelas que são diretamente afetadas, como TI, Jurídico, Financeiro e RH. Lembre-se de que toda a empresa contribui para a construção da cultura de proteção de dados. É um esforço coletivo no sentido de adequar o processo de negócio e mantê-lo em compliance com a legislação.

Cumpramos ressaltar que a estratégia de comunicação interna pode ser determinante para o sucesso da implementação do programa de conformidade. É importante promover, de forma positiva, a integração e a conscientização de diferentes equipes sobre as exigências da lei.

II. Planejamento.

Após conhecer a lei e entender sua aplicação prática, você precisa promover a mobilização e o alinhamento entre as equipes envolvidas no Projeto. O objetivo desta fase é planejar a forma de execução do Projeto, priorizando as áreas que apresentam um maior risco. Nesta fase é importante detalhar os próximos passos para implementação do Projeto, além de elaborar um cronograma de execução.

Usualmente, são realizadas atividades como: (i) definição da estrutura de responsabilidade do Projeto, incluindo a alocação de responsabilidades internas para execução das ações necessárias; (ii) reuniões

técnicas com os responsáveis para esclarecer eventuais dúvidas; (iii) verificação dos processos que serão alterados; (iv) validação de procedimentos; e (v) elaboração do cronograma que viabilize as transformações antes de agosto de 2020.

III. Mapeamento.

O objetivo desta fase é mapear todos os dados tratados pela empresa para entender como se encontra sua aderência à LGPD. Uma vez terminado o levantamento, a empresa saberá como lidar com os dados em conformidade com as exigências da lei, otimizando o gerenciamento de informações e evitando problemas no processamento.

As atividades realizadas nesta etapa compreendem: (i) levantamento de documentos disponíveis: políticas, normas e procedimentos de tratamento de dados; e (ii) due diligence sobre os dados pessoais tratados (pessoal, sensível, criança, público, anonimizado), meios (físico e/ou digital), operadores internos e externos (áreas da empresa, fornecedores, etc.), pontos de entrada e saída de dados, ciclo de vida dos dados e base legal para tratamento e armazenamento.

IV. Análise de Risco.

Nesta etapa a empresa deve analisar se há discrepâncias entre as obrigações legais e suas atividades, bem como definir quais estratégias adotar para a adequação. Serão identificados os principais pontos de desconformidade com a LGPD, por meio do mapeamento de dados feito anteriormente, e desenhadas as soluções para eliminar ou mitigar os riscos.

Considerando o curto período até a entrada em vigor da lei, pode-se dar prioridade para os bancos de dados mais relevantes, ou seja, buscar primeiramente preservar informações importantes, que possuem maior urgência para serem analisadas e protegidas.

Importante ressaltar que as soluções propostas para o cumprimento da LGPD não podem inviabilizar o modelo de negócio, mas sim possibilitar à empresa eliminar toda situação de desconformidade com a lei.

V. Plano de Ação.

Com base no resultado obtido nas etapas anteriores, é desenvolvido o plano de ação para implementar o Projeto. O plano de ação pode conter as seguintes medidas: (i) classificação de ações prioritárias, com base na sua complexidade e tempo de implantação; (ii) reuniões de acompanhamento de performance; (iii) elaboração e/ou revisão de documentos (contratos, termos de privacidade, políticas de proteção de dados) para uso interno e externo; (iv) concepção de novos produtos com o princípio de *privacy by design*; e (v) ajustes de sistemas, mudanças nos processos, eliminação de dados, revisão de quem pode acessar ou não.

VI. Implementação.

Esta etapa tem por finalidade colocar em prática as atividades definidas no plano de ação. A seguir listamos medidas obrigatórias para que a empresa esteja em conformidade com a LGPD:

- implementar ferramentas que permitam (i) aos titulares de dados pessoais exercerem seus direitos e (ii) gerenciar (ii.i) o consentimento do uso dos dados pessoais existentes no banco de dados e (ii.ii) os pedidos dos órgãos;
- elaborar, revisar, adaptar e aditar contratos que envolvam tratamento e/ou compartilhamento de dados pessoais, tanto nas relações com colaboradores, usuários e consumidores, quanto nas relações com fornecedores, prestadores de serviços e parceiros comerciais, garantindo que todos estão em *compliance*;
- estabelecer um programa de governança em proteção de dados pessoais, o que inclui a criação de regras de boas práticas que estabeleçam procedimentos, normas de segurança, ações educativas e mitigação de riscos no tratamento de dados pessoais;
- elaborar e/ou revisar políticas internas de gestão da informação, segurança e tratamento de dados, planos de comunicação a incidentes e outros documentos sobre privacidade e proteção de dados pessoais;
- adotar medidas de segurança da informação aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas, técnicas e procedimentos de segurança da informação e programas de privacidade desde a concepção e como padrão (*privacy by design/by default*);
- eleger um *Data Protection Officer* ("DPO"), encarregado responsável pela segurança dos dados em nome da empresa, com conhecimentos jurídicos e regulatórios sobre proteção de dados; e
- eliminar todos os dados que não sejam necessários: cópias duplicadas e *backups* que não serão utilizados e elaborar documentos que evidenciem a eliminação.

VII. Monitoramento.

Esta fase tem o objetivo de garantir que a empresa permaneça em conformidade com a LGPD. Esta etapa tem duração indeterminada, pois engloba atividades que devem ser realizadas periodicamente, como forma de assegurar o cumprimento constante do programa de governança de proteção de dados da empresa, suas políticas internas e diretrizes estabelecidas na legislação.

A empresa pode se valer de uma auditoria para verificar se o plano de ação foi implementado em sua totalidade, se as rotinas definidas são obedecidas, além de checar a efetividade das medidas adotadas. A realização de treinamentos periódicos também possibilita maior aderência às exigências da LGPD.

É importante que a empresa seja capaz, a qualquer momento, de atestar que está em *compliance* com as normas de privacidade e proteção de dados, a fim de evitar riscos futuros.

LEI GERAL DE PROTEÇÃO DE DADOS COMO ADEQUAR SEU NEGÓCIO?

Conclusão

Em 2018, a proteção de dados no Brasil ganhou um novo capítulo com a promulgação da LGPD. A partir de agosto de 2020 todas as empresas que tratem dados pessoais, independentemente de seu tamanho e ramo de atividade, deverão respeitar suas diretrizes.

Apesar de toda a complexidade que existe na adequação à LGPD, ainda há tempo para a adoção, pelas empresas, de medidas e providências necessárias à sua adaptação. Acredita-se que o próprio mercado irá cobrar tal adequação e sairá “na frente” aquela empresa que conseguir transmitir ao titular de dados e parceiros comerciais que possui toda a estrutura e competência para a proteção de dados.

O cumprimento da LGPD permitirá uma relação de confiança entre a empresa e titular de dados, o que gera uma relevante vantagem competitiva. Quanto maior a confiança em uma empresa, mais fácil será para a pessoa física aceitar compartilhar seus dados pessoais. Ser transparente no tratamento dos dados e demonstrar comprometimento com a privacidade são atitudes que possibilitarão uma melhor experiência ao titular de dados, podendo aumentar seu nível de satisfação com a empresa e gerar fidelidade à marca.

Sabemos que ter um programa de governança em proteção de dados não assegura que a empresa não terá um incidente de segurança. Entretanto, caso ocorra um incidente, os danos serão mitigados se a empresa estiver em compliance com seu programa de governança e com a LGPD. Outro aspecto positivo é que a lei determina que a ANPD considerará a existência de uma cultura de proteção de dados quando da aplicação de uma penalidade. Então, empresas com um programa efetivo de governança conseguirão controlar seus riscos e exposição a incidentes. Além disso, os passivos oriundos do descumprimento da LGPD também serão fatores determinantes no âmbito da captação de investimentos.

Por todo o exposto, não é apenas a obrigatoriedade que deve motivar a adequação à LGPD, mas sim todos os benefícios decorrentes de se realizar uma proteção de dados eficaz.