Associação Nacional dos Profissionais de Privacidade de Dados

ARTIGO TÉCNICO

LGPD
Medidas emergenciais para iniciar a adequação

Resumo:

O conteúdo a seguir sugere medidas emergenciais para que as empresas que iniciaram apenas as etapas iniciais ou não iniciaram suas atividades relacionadas à LGPD, para esses casos elaboramos um checklist sobre medidas emergenciais de rápida e fácil aplicabilidade para que as empresas possam iniciar seus projetos imediatamente no caminho à conformidade.

Com o objetivo de garantir privacidade, controle e segurança no uso dos dados de pessoas físicas nos mais diversos meios, o Brasil criou a Lei Geral de Proteção de Dados Pessoais (LGPD), que entrou em vigorar no dia 18/09/2020, trazendo o desafio de adequar a política de tratamento dessas informações sensíveis por meio da adaptação de processos e sistemas em conformidade com a lei. A LGPD permeia sua aplicação em uma extensão extraterritorial, ou seja, tratando de dados de cidadãos brasileiros ou estrangeiros residentes no Brasil, a organização deve se comprometer com a regularização e transparência em todas as etapas do processo, incluindo empresas parceiras.

A privacidade de dados pessoais vem a cada dia sendo um fator mais relevante para as empresas, um relatório global, encomendado pela IBM Security e conduzido pelo Instituto Ponemon em 2019, revela que o custo de uma invasão de dados aumentou 12% nos últimos cinco anos, passando para um custo médio de US$ 3,92 milhões.

No Brasil, o relatório aponta que o custo médio de uma violação de dados é de US$ 1,35 milhão (R$ 5,4 milhões), um aumento de 18,93% em relação a 2018. O estudo também observou um aumento no número de dias para identificar a violação de dados, que subiu de 240 para 250, e para conter a violação, que cresceu de 100 para 111 dias, em comparação a 2018[1].

A LGPD obstina-se a tutelar a governança de dados pessoais, privilegiando o compliance, a transparência e a segurança da informação, bem como a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, direitos estes que se encontram amparados na nossa Constituição Federal.

A partir da entrada da LGPD em vigor, empresas públicas e privadas deverão adotar uma série de medidas para evitar que titulares de dados pessoais tenham seus dados vazados. Além disso, as empresas têm que estar preparadas para informar aos titulares, quando solicitado, sobre a finalidade de uso de seus dados, bem com o tempo de uso.

Mesmo sendo previsto na lei sanções apenas para agosto de 2021, a inobservância de tais direitos por parte das organizações pode originar ações judiciais (tanto individuais ou coletivas) em desfavor da empresa (fazendo-as dispender recursos para defender-se judicialmente e para arcar com eventuais condenações que lhe venham a ser aplicadas).

Diante do novo contexto podemos afirmar que as empresas que não iniciaram a adequação para LGPD, já estão vulneráveis, pois a jornada de adequação é longa. Dessa forma, elas precisarão adotar medidas emergenciais para mitigar maiores vulnerabilidades e assim, realmente, iniciar sua trajetória no processo de conformidade exigida pela lei, o qual pode demorar entre 8 a 12 meses para completarem todas as etapas necessárias para a adequação às inúmeras exigências previstas pela LGPD.

[1] https://www.ibm.com/security/data-breach

A ANPPD vem apresentar medidas emergenciais a serem adotadas pelas empresas, são elas:

1. **Aviso de Privacidade de Dados**: elaborar um aviso de Privacidade e Proteção de Dados para ser divulgado em todos os seus canais de comunicação externos.
2. **Aviso de uso de cookies**: a empresa deverá elaborar um aviso de uso de cookies utilizados em seu site externo.
3. **Política de Privacidade:** elaborar e publicar política de privacidade de dados pessoais com o objetivo de direcionar a conduta dos funcionários, fornecedores e prestadores de serviços envolvidos nas atividades com dados pessoais.
4. **Nomeação do DPO (Data Protection Officer - art. 41, §1º:** a identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador, para que essa nomeação tenha comprovação a empresa deverá:
    a. Elaborar uma carta de formalização da nomeação do DPO;
    b. Definir um canal de comunicação da empresa com os titulares de dados; e
    c. Definir um fluxo para atendimento das solicitações dos titulares ao DPO.

Diante da necessidade iminente da nomeação do DPO, as empresas, em primeiro momento, podem terceirizar os serviços para avaliar os custos e perfil para internalização.

5. **Definição das atividades do DPO (Data Protection Officer - art. 41, §2º:** além da carta de nomeação do DPO a empresa deverá elaborar documentos internos definindo quais são as atividades. Em caso de terceirização esse documento também deverá conter direitos e deveres do DPO.
6. **Estabelecer canal de comunicação:** após a nomeação do DPO, deverá ser definido um canal de comunicação entre a empresa (controlador), os Titulares dos Dados (clientes, empregados e demais grupos cujos dados são informados a empresa) e a Autoridade Nacional de Proteção de Dados (ANPD).
7. **Revisão e ajuste contratuais:** elaborar padrões em seus contratos para abarcar disposições que tragam uma maior proteção para a empresa perante terceiros que realizem o tratamento de dados em seu nome.
8. **Órgãos Reguladores:** elencar todos os órgãos, legislações e regulações as quais são obrigados a responder ou informar dados; esse levantamento ajudará num primeiro momento a responder aos titulares sobre o uso de seus dados na empresa.
9. **Comunicação com Operadores:** elaborar comunicação formal para os fornecedores, prestadores e parceiros sobre a necessidade de adequação para conformidade com a LGPD no que tange ao escopo dos serviços prestados para a empresa.
10. **Política do setor de RH**: avaliar políticas para cumprir princípio da transparência e ciência. Nessa atividade deverão ser avaliado os compartilhamentos dos dados, uso de banco de talentos, política de benefícios, folha de pagamento e de ponto, bem como dados de dependentes menores.
11. **Aviso de privacidade em ambientes internos**: elaborar placas informativas sobre tratamento de dados, bem como a base legal que ampara essa atividade:
    a. Monitoramento do ambiente;
    b. Locais de grande acesso (portaria, recepção, sala de espera, etc.); e

c. Locais de acesso exclusivo.

12. **Gestão dos consentimentos:** definir plano e formulário para obtenção de consentimento dos titulares de dados, inclusive de dados atualmente utilizado sem autorização documentada.
13. **Requisição de titulares - art.18:** elaborar o fluxo, formulário e procedimento de atendimento das requisições dos titulares de dados sobre o uso na empresa (atender os direitos previstos art. 18 da Lei);
14. **Infraestrutura Crítica:** avaliar junto à equipe de tecnologia quais são os ativos críticos que trabalham ou armazenam dados pessoais e sua respectiva localização (Brasil ou exterior).
15. **Infraestrutura Física:** avaliar sobre a guarda de documentação física que contém dados pessoais e definir processos de guarda, acesso e utilização.
16. **Política sobre Incidentes art.48:**
    a. Formulário de Comunicação de Incidente: deverá ser criado um modelo formal para que toda a empresa utilize, em caso necessário, para informar sobre incidentes que envolvam violação de dados pessoais, independentemente de ser vazamento externo ou acessos internos indevidos, perda de backup etc.; e
    b. Formulário de aviso de vazamento à ANPD: deverá ser criado um modelo formal para que toda para que o DPO possa formalizar qualquer tipo de violação de dados pessoais que traga risco aos titulares de dados. Outra hipótese de uso desse formulário é por solicitação da ANPD ou para usar como defesa para apresentação aos órgãos reguladores ou fiscalizadores.
17. **Treinamentos:** deverão existir dois tipos de treinamentos sobre LGPD.
    a. Conscientização inicial das equipes sobre os principais pontos trazidos pela LGPD;
    b. Normas, fluxos e políticas a serem seguidas para atendimento da conformidade à LGPD; e
    c. Uso das documentações elaboradas.

Depois de implementada a etapa emergencial, a empresa poderá seguir com os demais passos para adequação e aderência à LGPD que são:

1. Análise

a. Conhecer a estrutura, processos e fluxos da empresa;
b. Mapeamento do ciclo de vida dos dados;
c. Avaliação Técnica e Jurídica dos Processos frente à LGPD;
d. Avaliação de maturidade da segurança da informação – ISO 27001 e ISO 27002;
e. Avaliação de risco de segurança da informação para empresa – ISO 27005;
f. Análise de aderência ao Sistema de Gerenciamento de Informações de Privacidade – ISO 27701; e
g. Elaboração de plano de ação para aumentar a maturidade e aderência necessária.

2. **Implementação:**
    a. Analisar o plano de ação recebido na etapa anterior e elencar os projetos a serem executados, avaliando custo, tempo e risco;
    b. Especificação das Tecnologias e Processos a serem adotados;
    c. Definir plano de execução dos projetos, cronograma, bem como os riscos aceitáveis;
    d. Programas de Treinamento e reciclagem; e
    e. Elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD) para atividades que gerem risco ao titular.
3. **Gestão**
    a. Operação dos serviços e projetos executados para aderência à LGPD;
    b. Manutenção e Análise Crítica dos Processos;
    c. Criar sistema de Gestão de Crises como forma de mitigar riscos inerentes aos negócios; e
    d. Manutenção dos processos e fluxos Técnico e Jurídico;

4. **Melhoria Contínua**
    a. Auditoria interna para acompanhamento – Privacy by default;
    b. Correção de erros e/ou sugestões de melhoria encontrados na auditoria; e
    c. Revisão e adequação de conteúdo conforme atualizações ou reformulações nas legislações do setor.

Além de todas essas etapas explanadas acima, recomendamos que as empresas também tenham conhecimento sobre os seguintes tópicos:

a. ISO/IEC 38500: está fundamentada em 6 princípios aplicáveis a qualquer porte de organização, oferecendo as diretrizes básicas para a implementação e manutenção de uma eficaz governança de TI

b. ISO/IEC 27003 : contém um conjunto de diretrizes para a implementação do SGSI. Enquanto a ISO/IEC 27001 disponibiliza apenas requisitos, aqui obtemos uma orientação detalhada.

c. ISO/IEC 27004: define métricas de medição para a gestão da segurança da informação. Pode ser uma importante aliada no momento de definir metas de níveis de serviço para a segurança da informação, ou mesmo executar as etapas check e act do SGSI;

d. Legislações que falam sobre privacidade e conformidade:

- Crimes Eletrônicos – Lei n.º 12.737, de 30 de novembro de 2012;
- Decreto 10.474 de 26 de agosto de 2020;
- Lei Anticorrupção – Lei n.º 12.846, de 1º de agosto de 2013;

- Lei de Acesso à Informação – Lei n.º 12.527, de 18 de novembro de 2011;
- Marco Civil da Internet – Lei n.º 12.965, de 23 de abril de 2014; e
- MP 2.200/2001 Medida Provisória n.º 2.00-2, de 24 de agosto de 2001.

CLASSIFICAÇÃO DESTE DOCUMENTO – PÚBLICO

Elaborado por:

Mirian Esquarcio Jabur
Membro do Comitê de Conteúdo da ANPPD

Revisado por:

Luciene Rosa
Coordenadora do Comitê de Conteúdo da ANPPD

Anielle Martinelli, DPO
Diretora do Comitê de Conteúdo da ANPPD

Davis Alves, Ph.D
Presidente da ANPPD

Outubro de 2020