LGPD – O QUE PRECISA SER VISTO

Após termos feito apresentações e dimensionamento do tamanho do problema e definir o envolvimento necessário para atender o descrito pela lei 13.709/18, passamos a olhar o que será preciso para atendê-la.

Alguns aspectos são importantes para entender o processo: responsabilidade e segurança.

RESPONSABILIDADE – dados pedidos e/ou coletados pela empresa precisam ser proporcionais ou adequados para o tipo de ação que a empresa pretende realizar (não faz sentido solicitar dados que não são fundamentais para a realização do serviço ou venda de bens relacionados à transação). Além disso, os dados coletados têm que, necessariamente, ser autorizados (consentidos) pelos donos do mesmo, o cliente. E, por fim, qualquer mudança no cenário do tratamento desses dados, deve ser notificada aos donos dos dados (denominado Titular pela lei).

SEGURANÇA – a empresa precisa providenciar métodos e formatos para que os titulares dos dados possam administrar os mesmos, isto é, as pessoas identificadas por dados devem ter acesso, condições para alterá-los, apagá-los ou mesmo transferi-los de acordo com critério pessoal. Ainda, a empresa é responsável diretamente pelo vazamento ou mau uso dos dados coletados. As pessoas que cuidam desses dados precisam ficar preocupadas, e aptas, a tratar com segurança essas bases de dados.

Agora vamos em frente: por onde começar? Podemos apontar um caminho por onde a empresa poderá seguir:

- Definir uma Análise de Conformidade (Gap Analysis), onde deverá ser levantada a situação de sistema e processos, automatizados ou não;

- Com essa análise, avaliar onde deveremos intervir e ajustar;

- Definido esse caminho, seguimos para uma revisão de contratos (visão jurídica), de processos (visão administrativa) e técnica (sistemas de informação);

- A seguir, desenvolver processos e métricas para acompanhar os ajustes definidos nos passos anteriores; e

- Concluindo o processo, avaliar tecnologias e procedimentos que poderão dar condições para realizar os ajustes necessários à conformidade com a lei.

Agora uma notícia importante: a lei já foi aprovada, sancionada e vai estar valendo a partir de AGOSTO/2020. O orçamento da empresa deverá considerar os valores necessários para a realização de todo esse processo.

A sua empresa pode ficar exposta frente a uma “não conformidade” com a lei e o custo disso é pesado.

Avalie o questionário abaixo. Consegue responder com segurança estas questões?

QUESTIONÁRIO PARA AVALIAÇÃO DE MATURIDADE - LGPD

1. Já foi definido o funcionário responsável pelo tema “privacidade de dados e informações”?
2. Existe uma Política de Segurança de Informação (PSI) formal? Caso sim, abrange os tópicos: privacidade de informações, classificação de informação, controle de acesso à informação, criptografia, política de backup e plano de continuidade de negócios (existem evidencias)?
3. Existe um processo mapeamento do fluxo de dados e informações?
4. Existe um processo formal para controle dos bancos de dados e seu manuseio?
5. Existe documentação sobre a manutenção e controle do processamento de dados pessoais?
6. Existe um código de ética (ou de conduta) formal? Ele possui tópico relativo à privacidade de dados e informações?
7. A empresa já tomou alguma iniciativa sobre a conscientização de privacidade de informações?
8. A empresa já realizou um plano de análise de impacto (PIA- Privacy Impact Analysis)?
9. O risco de privacidade faz parte da gestão de risco corporativo?
10. Quais medidas técnicas existem atualmente para garantir a privacidade (integridade) de dados e informações armazenadas na empresa (Pentest, Firewall, Análise de tráfego, criptografia, outros)?
11. A empresa possui alguma certificação ISO? Qual?
12. Existe um Plano de Resposta para incidentes de TI envolvendo vazamento de informações?
13. Existe um Plano de Crises para minimizar impactos no caso de vazamento de informações privadas?
14. O pessoal da Área Jurídica está habilitado/capacitado a participar de implementação dos requisitos de privacidade no ambiente corporativo da empesa?
15. Preparar um organograma.
16. Descrever uma visão geral da área de TI, com pessoal e funções.

Mãos a obra! O tempo não é nosso aliado, mas podemos ajudar na tarefa.