CHECKLIST PARA SE ADEQUAR À LGPD

CINCO ETAPAS PARA EXECUÇÃO E ADEQUAÇÃO À LGPD.

1. Criação de um Comitê Compliance:

O termo "compliance", diz respeito a "estar em conformidade com".

O comitê compliance vai garantir que toda a sua empresa - colaboradores, diretoria e parceiros - esteja de acordo com a legislação.

Ajustar-se à LGPD não deve ser um assunto somente de TI ou do Jurídico, diz respeito também a dados sensíveis de pessoas físicas, e, em uma empresa muitas áreas lidam com esses dados. Por isso, é importante envolver todas as áreas para entender em cada uma delas, como estão sendo tratados esses dados sensíveis, quem tem acesso a eles, como são armazenados, etc.

Por isso, nesse primeiro passo, deverá ser criado um comitê multidisciplinar, assim você terá maiores condições de entender quais são os riscos reais que a sua empresa pode estar exposta e como resolvê-los.

2. Elaborar um Relatório de levantamento de riscos:

Após criado o Comitê é preciso entender como são tratados e organizados os dados pessoais em sua empresa. Para isso, é necessário incialmente elaborar um **Relatório de Levantamento de Riscos**.

Na elaboração desse relatório você deverá repassar por todos os setores da empresa, descrevendo detalhes sobre todos os dados sensíveis usados em cada atividade da sua empresa.

Esse documento será essencial, pois será usado para priorizar as ações de adequação à lei.

Nessa etapa de levantamento de riscos, no relatório deverá também conter informações sobre terceiros, fornecedores, processos e contratos que podem estar sujeitos a riscos perante a LGPD.

3. Elaborar uma matriz de risco:

Criar uma matriz de riscos priorizando o tratamento que poderá causar maior impacto na empresa e por isso deve ter preferência no Plano de Ação.

Criada a matriz, você irá cruzar a probabilidade daquele risco acontecer e o impacto para seu negócio. Para realizar essa priorização, você dará notas de 1 a 5. Após dado as notas, você terá uma matriz indicando se aquele risco é Extremo, Elevado, Moderado, leve ou Baixo. Assim conseguirá iniciar com segurança o plano de ação após constatado os riscos que mais irão afetar a organização da sua empresa.

Após esses procedimentos iniciais, você poderá dar início ao plano de ação ajustando às normas da LGPD.

4. Plano de ação:

Feito todo o levantamento e a priorização dos riscos é momento de montar o Plano de Ação.

- Inicie pelos Riscos Extremos e Elevados identificados na Matriz de Riscos.

Deve-se fazer uma análise bem detalhada, pois caso algum risco não seja classificado como Extremo ou Elevado, mas tenha impacto grave sobre a empresa, ele também deverá ser considerado no Plano de Ação. Neste momento o Responsável pela Execução entrará em ação para acompanhar o processo de planejamento e execução.

Além dos riscos priorizados no tópico anterior, existem alguns "entregáveis" exigidos pela lei, portanto é importante que estejam no plano.

IMPORTANTE!!

Esses documentos são importantes tanto para guiar as ações internas da empresa, quanto para prestação de contas junto à ANPD (Autoridade Nacional de Proteção de Dados), caso solicitado. Esses entregáveis são:

4. 1. Elaboração de Planilha Data Mapping

- Criar um Mapa de Dados.

Esse mapa se trata de um documento sigiloso, apenas para uso interno.

Nesse documento deve constar todas as atividades do setor que estão sendo avaliadas, se a empresa utiliza dados pessoais ou sensíveis, cargo executante, como são usados, de quem, local, período de armazenamento, base legal e para qual finalidade.

É importante segmentar as atividades para que não se esqueça de nenhum dado.

4. 2. POLÍTICA DE PRIVACIDADE

- Criar uma Política de Privacidade.

Essa política irá orientar todo o público da empresa sobre como os dados serão coletados, armazenados e tratados.

Se sua empresa trata de dados pessoais de forma física, deve-se criar um manual de boas práticas e orientação por exemplo – use a criatividade- existem outras práticas viáveis.

Se ocorrer exclusivamente de forma digital, deve-se criar um portal explicativo das respectivas políticas de privacidade adotadas pela empresa e os direitos dos titulares,

adotando medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais tratados.

Na Política de Privacidade deve conter algumas informações essenciais, como:

*informações sobre a organização responsável pelo tratamento;
*dados pessoais e respectivas finalidades do tratamento;
*termo de consentimento físico ou digital a depender do caso;
* base jurídica do tratamento;
* prazo de retenção dos dados pessoais;
* informações de contato do Data Protection Officer (DPO) ou encarregado de proteção de dados da organização.

Outras que também devem conter na Política de Privacidade:

* Sobre compartilhamento dos dados com terceiros e qual a finalidade, inclusive redes sociais;
* Sobre transferência internacional e qual a finalidade; - Sobre o tratamento por legítimo interesse;
*Sobre o envio de e-mail marketing e como remover o consentimento, quando autorizado inicialmente pelo titular;
* Sobre decisões automatizadas;
* Sobre a proteção de dados de menores de idade;
* Sobre a proteção dos dados sensíveis.

4. 3. DPO

- Nomear um DPO (Data Protection Officer).

Profissional encarregado pelo tratamento de dados pessoais. Ele será o responsável por fiscalizar e manter sua empresa em conformidade com a LGPD.

Ele também será o responsável em divulgar a cultura de proteção de dados na empresa, além de criar normas e procedimentos adequados à lei.

Algumas atividades relacionadas à figura do DPO
- Receber solicitações sobre o assunto;
- Interagir com a autoridade nacional do assunto caso necessário;
- Realizar treinamento sobre a LGPD internamente;
- Informar ao controlador e ANPD sobre Incidente de Segurança.

4. 4. Portal de consentimento

- Criar um "Portal de Consentimento".

Nesse Portal, o público da empresa poderá ter acesso aos seus dados, pedir revisões, exclusões, etc. Isso será necessário, visto que a palavra que resume a LGPD é

"consentimento". A empresa pode conter qualquer dado sensível desde que tenha o consentimento ou alguma base legal que valide essa posse. Após o consentimento, o titular desses dados deve ter transparência sobre qual dado a empresa mantém, se está atualizado e direito de retirar esse consentimento.

Se a empresa trata dados de forma exclusivamente of line deve manter formulário de consentimento acessível ao titular contendo cláusulas em destaque sobre a finalidade para o tratamento, o consentimento e prazo de retenção dos dados pessoais de forma inequívoca e transparente.

4. 5. Revisão

- Revisar constantemente todas as práticas de controle de acessos aos dados.

Essa revisão entra no checklist de segurança da informação. Os dados sensíveis devem estar disponíveis apenas para quem de fato irá precisar daquele dado. Para isso, cada área deve garantir que as informações estejam seguras, deve-se seguir algumas práticas e adotar medidas de segurança técnicas e administrativas aptas a proteger dados de acessos não autorizados e de situações acidentais ou ilícitas.

5. Trabalhar a cultura da empresa:

- Cultura organizacional.

O último e não menos importante passo, é a cultura da empresa. A Privacidade deve se tornar um assunto comum dentro dos negócios.

Para isso, é importante que a empresa conscientize seus colaboradores formulando regras de boas práticas e de governança que estabeleçam condições de organização, o regime de funcionamento, os procedimentos sobre como ela lida com este tema e compartilhe quais são as práticas para garantir a integridade desses dados.

Algumas sugestões:

- Realizar ações educativas com a equipe sobre a LGPD e a política de privacidade da empresa;
- incluir procedimentos que tenham como objetivo adaptar e capacitar os profissionais recém-ingressados em uma empresa na cultura dela), dos novos colaboradores, ou seja, no treinamento e/ou integração dos funcionários recém contratados.
- Criar um manual de boas práticas, normas de segurança e padrões técnicos, incluindo no código de conduta da empresa. A ideia é divulgar essas práticas, utilizando meios de comunicação direto com os colaboradores que garantam o efetivo acompanhamento;
- Realizar treinamentos;
- Fazer campanhas de comunicação interna destacando os principais pontos da LGPD e da política da empresa.

6. CONCLUSÃO:

Manutenção:

Seguindo esses passos sua empresa estará adequada com a LPGD, contudo, é imprescindível garantir a manutenção dessas práticas na empresa, razão porque a figura do DPO será tão importante.

Caso sua empresa tenha um volume de dados muito alto, existem várias empresas de consultoria que estão apoiando as empresas nesse processo, mas seguindo esse checklist tenho certeza que irá facilitar seu entendimento sobre como e onde implementar a LGPD na sua empresa.

Esperamos que seja útil.

Um abraço e até a próxima!

Por
Eleticia Souza de Abreu
Advogada em direito digital