

Guia Definitivo!

Adequação à LGPD. Por onde começar?





Passo 1: Conhecer e entender a Lei Geral de Proteção de Dados!

O primeiro e mais importante passo a ser dado rumo à jornada de adequação da sua empresa é a apresentação do tema para os colaboradores.

E como fazer isto?

Apresentando os principais aspectos e impactos da LGPD para todos os colaboradores que realizam suas atividades com base no tratamento de dados.

O ideal é que todos os colaboradores da empresa conheçam e compreendam os objetivos da LGPD, pois assim já estará se construindo a cultura de Privacidade e Proteção de Dados dentro da empresa.



E após essa apresentação do tema. O que fazer na prática?

É recomendável que se faça um relatório minucioso de toda a abordagem feita aos colaboradores, ou seja, descrever todos os pontos referentes à lei que foram mencionados.

Esse documento deverá ser datado e assinado por todos os presentes. E por que isso? Porque não basta só estar em conformidade ou buscando ela, é necessário que a empresa demonstre o seu comprometimento com a conformidade.

Passo 2: Assessment LGPD



Avaliação inicial que objetiva o diagnóstico do cenário atual da empresa em relação à conformidade com a lei.

Neste momento é hora de verificar quais os requisitos da LGPD e demais legislações pertinentes ao seu negócio a empresa já atende. Por meio desta avaliação é que compreenderemos a maturidade dos processos, a adesão e a estratégia adotada pela empresa na busca pela conformidade.

Atividades a serem realizadas no Assessment:

1. Criação do Comitê Multidisciplinar (time que atuará na realização das atividades iniciais).

2. Mapeamento Inicial dos Dados (por áreas e por processos).

3. LIA (Legitimate Interests Assessment) - Caso haja a opção do Legítimo Interesse para fundamentar o tratamento de dados que a empresa realiza.

4. Mapa de Fluxo de Dados para compreender por onde o dado transita dentro da empresa.

5. Elaboração do Relatório de Diagnóstico para fins de análise dos GAP's (brechas) de segurança encontradas.

6. Relatório de Impacto à Proteção de Dados Pessoais ou DPIA (Data Protection Impact Assessment). Seu objetivo é análise, identificação e minimização dos riscos relacionados à incidentes de segurança, objetivando, de igual forma, a indicação da viabilidade ou não para o tratamento de dados pretendido.

7. Plano de Ação. Elaboração do Plano de Ação com cronograma das atividades a serem realizadas, com mapa de calor para as atividades urgentes.

PASSO 3: Mapeamento, Classificação dos Dados e Inventário de Regulamentações

Nesta fase também serão previamente verificados os Princípios aplicáveis ao tratamento e a definição das bases legais aptas a justificar o tratamento de dados que a empresa realiza.

Quem é a empresa? Controladora ou Operadora?

Qual o segmento da empresa?

Qual a área que está realizando o tratamento? Ex: RH, marketing, financeiro, etc..

Qual a categoria dos dados tratados? Ex: dados de empregados, marketing, listas manuais, etc..

Onde a empresa armazena esses dados? Ex:sistemas, e-mails, banco de dados, planilhas etc..



Qual a origem do dado coletado? Ex: cadastro em e-commerce, coleta em meios físicos, etc..



Qual a finalidade da coleta?

Após mapear todos os dados e realizar o inventário das regulamentações, deverá se verificar se o tratamento atende aos princípios da LGPD e quais as bases legais adequadas ao tratamento de dados realizado.





Passo 4: Programa de Governança de Privacidade e Proteção de Dados!



Implementação prática pelo departamento jurídico

Desenvolvimento do Programa de Governança de Privacidade e Proteção de Dados com estabelecimento de Políticas internas, revisão de Política de Privacidade, revisão de contratos, termos, etc..



Implementação prática pela área de Tecnologia da Informação

Adoção das medidas técnicas pela área de TI a fim de atender ao disposto no art. 18 da LGPD.



Implementação dos controles de Segurança da Informação

Execução das principais medidas de Segurança da Informação



Passo 5: Boas Práticas

Manual de Boas Práticas constando as Políticas Internas da empresa sobre Privacidade e Proteção de Dados.

Passo 6: Manutenção do Programa de Governança

Realização da manutenção da cultura de Privacidade e Proteção de Dados, para fins de treinamento e conscientização dos colaboradores acerca da importância de manter a privacidade e a proteção de dados.



Passo 7: Monitoramento do Programa de Governança

- Revisão do Plano de Ação elaborado no Assessment;
- Realização de testes de validação e confiança do Programa;
- Avaliações periódicas.

Lembre-se: não importa o seu ramo de atuação, se em meios digitais ou físicos. Se a sua empresa realiza atividades por meio de operações de tratamento de dados, ela precisa estar em conformidade com a LGPD.



Contatos

contato@implementandoalgpd.com.br

www.implementandoalgpd.com.br

