05

Faça o que eu fiz na aula

Faça um check list na sua empresa e avalie o quanto ela está preparada para a LGPD. De acordo com Gustavo Rocha, do site Jus.com.br, para estar em conformidade com a LGPD, a empresa precisa:

1 - Estabelecer uma estrutura de prestação de contas e governança

A conformidade com a LGPD/GDPR exige o suporte da Alta Gestão. Portanto, é essencial que a diretoria entenda as implicações da Lei – tanto positivas quanto negativas – para garantir os recursos necessários para alcançar e manter a conformidade.

O que você precisa fazer

• Apresentar à Alta Gestão os riscos e oportunidades da LGPD/GDPR. • Obter suporte de gerenciamento para um projeto de conformidade com a LGPD/GDPR. • Atribuir a responsabilidade pela LGPD/GDPR a uma pessoa da Diretoria. • Incorporar o risco de proteção de dados na estrutura de gerenciamento de riscos corporativos e controles interno.

2 -Escopo e planejamento do projeto

Depois de obter suporte de nível superior, você precisará descobrir quais áreas de sua organização se enquadram no escopo da LGPD/GDPR e considerar quais processos existentes podem ser afetados, auxiliando em seus esforços de conformidade.

O que você precisa fazer:

• Nomear e capacitar um gerente de projeto e indicar/nomear um Encarregado de Dados ou DPO (oficial de proteção de dados), se necessário. • Identificar quais entidades estarão no escopo: unidades de negócios, filiais, terceirizados, localidades, etc. • Identificar padrões ou sistemas de gerenciamento que possam fornecer uma estrutura para conformidade. Por exemplo: a ISO 27001 demonstra atendimento às melhores práticas de gerenciamento de segurança da informação e proteção de dados. • Avalie o princípio da proteção de dados incorporado e, por padrão, em relação a processos e sistemas, atuais ou novos. • Considere as implicações de regras e Leis anteriores à LGPD/GDPR, no seu planejamento.

Se você trabalhar em uma agência, será importante envolver o pessoal de TI e área de sistemas. Em alguns caso, pode ser interessante terceirizar esse serviço ou contratar alguém para resolver isso.

3 - Realizar um inventário de dados e uma auditoria de fluxo de dados

É impossível cumprir os requisitos de processamento de dados da LGPD/GDPR, se você não entender completamente quais dados processa e como você os processa.

O que você precisa fazer:

• Avalie as categorias de dados mantidos, a origem e a base legal para o processamento. • Mapeie os fluxos de dados de, para, através e da própria organização. • Use o mapa de dados para identificar os riscos em suas atividades de processamento de dados, indicando se um DPIA (análise de impacto na proteção de dados) é necessário. • Criar a documentação do Artigo 30 – o registro de atividades de processamento de dados pessoais, com base na auditoria do fluxo de dados e da análise do inventário.

Ter uma ajuda jurídica de um especilista pode ser útil. Em algumas empresas, cabe tentar contato com o departamento de BI.

4 - Realize uma análise detalhada de brechas

A abordagem sensata da conformidade estabelece o que a sua empresa ainda não faz – avaliar seus fluxos de trabalho, processos e procedimentos atuais – para identificar as lacunas que sua empresa precisa preencher.

O que você precisa fazer

• Auditar sua posição de conformidade atual em relação aos requisitos da LGPD/ GDPR. • Identificar as lacunas de conformidade que exigem correção.

5 - Desenvolver políticas, procedimentos e processos operacionais

Fornecemos uma avaliação no local de suas práticas de gerenciamento de privacidade e processamento de dados, produzindo um relatório resumido das suas lacunas de conformidade e fornecendo recomendações de correção.

O que você precisa fazer

• Garantir que as políticas de proteção de dados e os avisos de privacidade estejam alinhados com a LGPD/GDPR. • Sempre que precisar de consentimento, assegurar que atenda aos requisitos da LGPD/GDPR. • Revise os contratos de funcionários, clientes e fornecedores e atualize, se necessário. • Planejar como reconhecer e lidar com as solicitações de acesso de sujeitos dos dados, fornecendo respostas dentro do prazo estipulado. • Tenha um processo para determinar se é necessária Análise de Impacto de Privacidade. • Analise se os mecanismos para transferências externas de dados são compatíveis com a proteção interna.

Não julgue que "nunca vai acontecer com você ou na sua empresa". Sempre somos surpreendidos e mesmo sendo um roteiro genérico, basta avaliar a forma como os colaboradores lidam com dados internos e externos e conseguirá avaliar o quão perto a sua empresa está das novas regras.

6 - Proteger os dados pessoais através de medidas processuais e técnicas

A LGPD/GDPR exige que as organizações implementem “medidas técnicas e organizacionais apropriadas” para garantir que os dados pessoais sejam processados apropriadamente.

O que você precisa fazer

• Ter uma política de segurança da informação em vigor. • Ter uma política de privacidade em vigor. • Praticar controles técnicos básicos, como os especificados por estruturas estabelecidas como o Cyber Essentials. • Usar criptografia e /ou anonimizacão e /ou pseudonimização, quando apropriado. • Garantir que políticas e procedimentos sejam implementados para detectar, relatar, investigar e responder a violações de dados pessoais.

7 - Comunicações

Manter sua conformidade com a LGPD/GDPR depende muito de sua equipe entender corretamente o que deve fazer e por quê. Todos os envolvidos no processamento de dados devem ser adequadamente capacitados e treinados para seguir processos e procedimentos definidos.

O que você precisa fazer

• A conformidade com o LGPD/GDPR é um projeto de mudança de negócios – comunicações internas eficazes com as partes interessadas e a equipe são essenciais. • Os funcionários precisam entender a importância da proteção de dados e serem treinados nos princípios básicos de LGPD/GDPR e nos procedimentos que estão sendo implementados para garantir a conformidade.

8 - Monitorar e auditar a conformidade

A conformidade com o GDPR é um projeto dinâmico – realizando uma jornada em vez de buscar um destino. Você deve executar auditorias internas periódicas e atualizar seus processos de proteção de dados, incluindo a verificação de seus registros de atividades de processamento (logs), mecanismos de consentimento, testes de controles de segurança de informações e a realização de Análises de Impacto na Privacidade (PIAs).

O que você precisa fazer

• Agendar auditorias regulares de atividades de processamento de dados e controles de segurança. • Manter registros do processamento de dados pessoais atualizados. • Empreender DPIAs e PIAs, quando necessário.