

Prefeituras e o desafio na implementação à LGPD

por Martha Leal

martha@jpleal.com.br

www.marthaleal.com.br

Sugestão de enfrentamento do tema

Questionamentos a serem enfrentados:

1. A organização se estruturou para a condução das iniciativas de adequação?
2. A organização implementou medidas e controles de proteção de dados pessoais para adequação à LGPD?

O questionamento 1 compreende as seguintes etapas:

Preparação, Liderança, Contexto, Organizacional e Capacitação

O questionamento 2 compreende as seguintes etapas:

Conformidade do tratamento, Compartilhamento de Dados Pessoais, Direitos do Titular, Violação de Dados e Medidas de Proteção.

Fase 1, o que compreende?

A organização deverá adotar medidas para criar um ambiente propício à implementação do projeto de adequação, que consistem em: -

- Implementar um Programa de Governança em Privacidade proporcional a estrutura e o volume de dados pessoais tratados. Por exemplo, a criação de um grupo de trabalho que conte com profissionais de diferentes áreas(SI, TI, Jurídico, RH, Auditoria, etc).
- Elaborar um plano de ação documentado para direcionar a iniciativa do projeto. Esse plano deve conter o que será feito, quais recursos necessários, quem serão os responsáveis, prazo para conclusão das tarefas e como os resultados serão avaliados.

Por que esse plano é importante?

Para guiar os responsáveis na implementação dos controles para adequação à LGPD.

Fase 2, o que compreende?

Nessa fase, a organização começa a executar o projeto e para o seu sucesso e evitar o retrabalho, recomenda-se as seguintes etapas: -

- Identificar os normativos relacionados ao tratamento de dados que a organização está envolvida. O arcabouço jurídico aplicável ao setor público não se restringe à LGPD. A CF, LAI, Lei do Cadastro Positivo, CLT e outros atos normativos devem ser considerados. -
- Identificar a categoria dos dados tratados pelo setor público. Por exemplo, cidadão, cliente, servidor público, representante de fornecedor e terceirizado.

Por que é importante a identificação dessas categorias?

Para auxiliar no planejamento dos controles que serão implementados. Alguns dados requerem controles adicionais.

- Identificar os operadores, seus papéis e responsabilidades.

Fase 2, o que compreende?

- Adequar os contratos firmados com os operadores. Os contratos devem ser adequados para estabelecer as responsabilidades e papéis com relação à Proteção de Dados; -
- Identificar os processos que realizam tratamento de dados pessoais. Necessário haver registro; -
- Mapear estes processos. Essa etapa é fundamental, pois a partir daqui é possível avaliar os riscos inerentes a cada processo, a finalidade e base legal e compartilhamento dos dados; -
- Identificar os responsáveis pelos processos de negócio que realizam tratamento; -
- Identificar onde os dados tratados se encontram (servidor, banco de dados, arquivos físicos e etc);

Por que é importante essa identificação?

Para avaliar os riscos inerentes aos processos de tratamento para direcionar as prioridades dos processos para adequação à LGPD

- Nomear encarregado;
- Formular políticas que busquem assegurar a Proteção de Dados, tais como a Política da Segurança da Informação e implementação dos controles de segurança da informação, nomeação do responsável para Segurança da Informação, definição de processos de gestão de riscos de SI,

Fase 2, o que compreende?

estabelecimento da política de segurança da informação, processo de elaboração de inventário de ativos e implantação de controles de segurança da informação. -

- Formular Política de Proteção de Dados alinhada à Política de Segurança da Informação.

Política de Proteção de Dados e Política de Privacidade são a mesma coisa?

Não. A Política de Proteção de Dados está voltada ao público interno, enquanto a Política de Privacidade ao público externo ao ambiente da organização.

- Capacitar a equipe e treinar colaboradores; Realizar Relatório de Impacto à Proteção de Dados
- RIPD para controle de riscos nos tratamentos que representem riscos;
- Elaborar Política de Privacidade; -
- Estabelecer mecanismo para atendimento dos direitos dos titulares;
- Documentar detalhes relacionados ao compartilhamento dos dados pessoais com terceiros. Observar hipóteses autorizadoras no art. 26, &1º c/c &2º ou consentimento; -
- Transferência internacional, observar art. 33 da LGPD.

Fase 2, o que compreende?



Importante: A Organização deve ser capaz de comprovar que os tratamentos de dados que realiza são lícitos e fundamentados em uma base legal e documentar as finalidades.

Atenção:

- Implementar plano de resposta à incidentes de segurança: Violação de dados requer gerenciamento de incidentes de segurança, registros dos incidentes e plano de notificação à ANPD e Titulares, quando cabível. A organização deve ter um esboço do plano de resposta, quando o incidente ocorrer; -
- Adotar medidas de proteção de segurança da informação, técnicas e administrativas para proteger os dados. Por exemplo, controle de acesso ao sistemas, registros de ventos (LOGS), criptografia, pseudominização e etc..

MATERIAS PUBLICADOS DE APOIO DISPONÍVEIS:

- [GUIA DE BOAS PRÁTICAS DA LGPD – MODELO DE RIPD](#)
- [GUIA DE SEGURANÇA DA INFORMAÇÃO PARA AGENTE DE TRATAMENTO DE PEQUENO PORTE](#)
- [CARTILHA CERT.BR E ANPD QUE APRESENTA INFORMAÇÕES SOBRE ADOÇÃO DE POSTURA PREVENTIVA](#)
- PERGUNTAS E RESPOSTAS SITE OFICIAL DA ANPD
- [GUIA SENACON “COMO PROTEGER SEUS DADOS PESSOAIS”](#)
- [GUIA ORIENTATIVO AGENTES DE TRATAMENTO DE PEQUENO PORTE](#)
- [GUIA ORIENTATIVO TRATAMENTO DE DADOS NO SETOR PÚBLICO](#)
- [TCU AUDITORIA DO GRAU DE IMPLEMENTAÇÃO NO SETOR PÚBLICO](#)