PROGRAMA DE GOVERNANÇA E PRIVACIDADE PARA ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS

FECAM

Federação de Consórcios, Associações e Municípios de Santa Catarina

LGPD E O PODER PÚBLICO

A presente cartilha tem o objetivo de estabelecer orientações gerais para a implementação das exigências e obrigações decorrentes da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD) em órgãos e entidades do setor público.

O Poder Público merece uma atenção especial ao se adequar à essa nova realidade, uma vez que os diversos órgãos da administração direta e indireta lidam diariamente com um grande número de bancos de dados de seus administrados, tratando informações potencialmente sensíveis, como as relativas à saúde e condição econômico-financeira.

Caberá ao Poder Público promover a instrução de seus agentes, aprimorar seus sistemas de proteção de dados com novas tecnologias e adoção de boas práticas por parte de seus servidores, o que pode não ser uma tarefa fácil em boa parte do país. Para cada ente público com plena capacidade de promover mudanças de nível tecnológico e organizacional, há inúmeros outros, em especial em pequenos municípios, que ainda trilham, com dificuldade, por um real processo de digitalização de sua estrutura e serviços.

O QUE VOCÊ PRECISA SABER ?

ALGUNS TERMOS E CONCEITOS IMPORTANTES PARA ENTENDER A LGPD:

DADOS PESSOAIS

Informação relacionada à pessoa natural identificada ou identificável. Todo órgão público trata dados tanto dos administrados quanto de seus servidores, que também são titulares de dados pessoais.

DADOS PESSOAIS SENSIVEIS

É todo dado pessoal que possa gerar algum tipo de discriminação ao seu Titular, como os dados que revelem a origem racial ou étnica, opiniões políticas e convicções religiosas ou filosóficas; filiação sindical; relativos à vida sexual ou orientação sexual da pessoa.

TRATAMENTO DE DADOS

Tratamento é toda e qualquer operação realizada com dados pessoais, seja em meios físicos ou digitais; como o armazenamento, coleta, eliminação, modificação, alteração e transferências de dados pessoais. Toda organização, pública ou privada, irá realizar o tratamento de dados pessoais em um ou mais processos de trabalho.

BASES LEGAIS

A LGPD traz dez hipóteses em que é possível o tratamento de dados pessoais. Todas as operações de tratamento deverão estar de acordo com uma dessas bases. Boa parte dos tratamentos de dados no setor público serão norteados pelo cumprimento de obrigação legal ou execução de políticas públicas.

PRINCIPIOS

São valores gerais que orientam a compreensão, interpretação e aplicação das regras estabelecidas pela LGPD e que devem sempre ser considerados quando uma atividade envolver tratamento de dados pessoais. Dos dez princípios que norteiam a LGPD, os que estarão mais presentes na administração pública são: finalidade e adequação, necessidade, transparência e livre acesso.

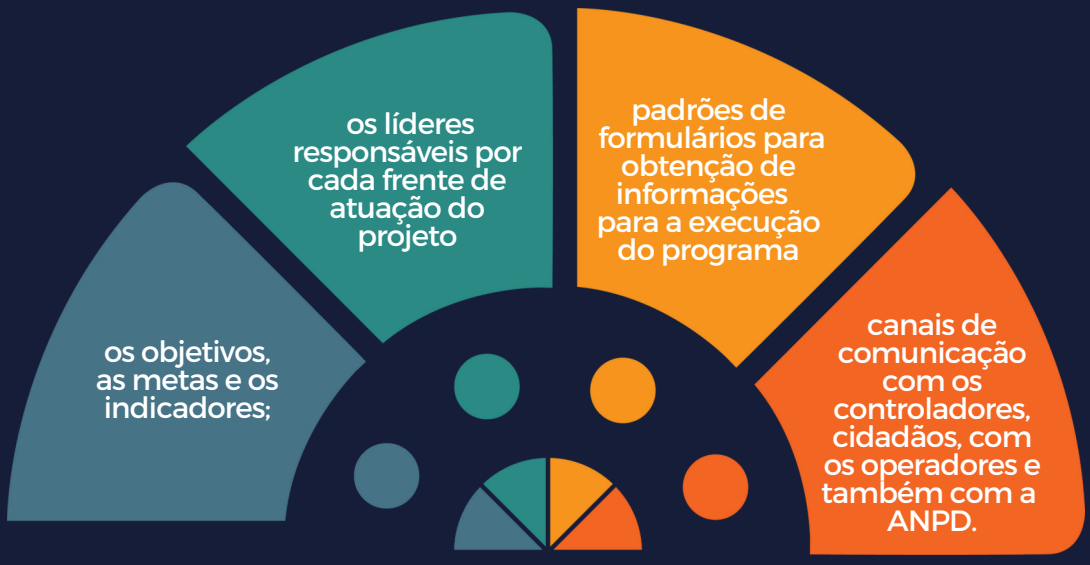
COMO SE ADEQUAR?

O processo de adequação da organização à LGPD passa, primeiro, pela criação de um Programa de Governança e Privacidade. Para isto é necessário que a organização analise a metodologia que melhor se encaixa à realidade do seu dia a dia. Neste documento vamos falar sobre a metodologia apresentada pelo Governo Federal. Contudo, vale ressaltar que esta metodologia não é a única solução disponível, cabendo ao time de privacidade e proteção de dados realizar um estudo para definir qual metodologia deverá ser adotada pela entidade.

PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

A Lei Geral de Proteção de Dados Pessoais, em sua Seção II, (Das Boas Práticas e da Governança), no Art. 50 § 2°, I, determina que o controlador, a quem compete as decisões referentes ao tratamento de dados pessoais, poderá implementar um Programa de Governança em Privacidade (PGP).

Antes ainda do início do programa, é necessário que a alta administração da organização defina alguns pontos que irão nortear a implantação do programa de governança de privacidade. São eles:



IMPORTANTE

Ao contrário de um projeto, que tem início, meio e fim, um programa estabelece uma metodologia abrangente que influenciará permanentemente os processos de tomada de decisão com base em riscos e melhorias contínuas na maturidade.

QUEM É QUEM?

É fundamental saber identificar os principais atores envolvidos no programa de governaça de privacidade

TITULAR DE DADOS PESSOAIS

Pessoa natural a quem se referem os dados pessoais objeto de tratamento. A entidade/organização irá tratar não só os dados pessoais dos seus administrados, mas também dos seus servidores públicos e fornecedores.

CONTROLADOR

Pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais.

OPERADOR

Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

ANPD

Autoridade Nacional de Proteção de Dados, órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD no Brasil.

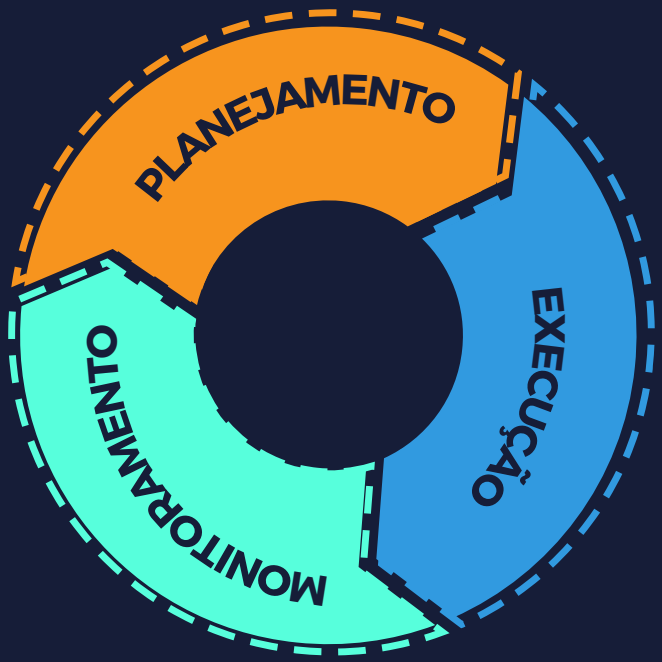
ENCARREGADO (DPO)

Indicado pelo controlador e operador, o Encarregado (DPO) é o profissional responsável pela privacidade e proteção de dados pessoais dentro de uma organização, tendo uma função intermediadora na relação entre controlador, titular de dados pessoais e a ANPD. A LGPD exige (art. 23, III) que todo ente público indique um encarregado.

QUAIS SÃO AS ETAPAS DO PGP ?

O programa tem três etapas:

I - Planejamento;
II - Construção e execução;
III - Monitoramento;



ETAPA I

PLANEJAMENTO

A etapa de Planejamento busca compreender quais são as primeiras informações e os dados importantes que devem ser conhecidos. É nela que serão construídos alguns dos documentos mais importantes e que irão embasar o restante do programa. A etapa é constituída pelas seguintes fases:

NOMEAÇÃO DO ENCARREGADO

A indicação do encarregado deve acontecer no início do programa de governança em privacidade. Além das competências dispostas expressamente na lei (art. 41, da LGPD), são funções do encarregado:

- Apoiar a definição das diretrizes de construção do inventário de dados pessoais, relativas ao registro das operações de tratamento de dados pessoais definidos na LGPD (em seu art. 37);
- Conduzir ou aconselhar a elaboração de relatório de impacto à proteção de dados pessoais, de acordo com casos previstos pela LGPD em que tal documento é necessário;
- Conduzir e aconselhar a implementação de regras de boas práticas e de governança específicas pela LGPD;

ALINHAMENTO DAS EXPECTATIVAS

O Alinhamento das expectativas com a alta administração deve priorizar as ações mais urgentes, sem esquecer de mencionar os projetos e as estruturas da organização envolvida. No setor público a alta administração de um órgão geralmente será os membros da direção.

ANÁLISE DA MATURIDADE

É a análise das ações e boas práticas da entidade em relação à privacidade e proteção de dados, como, por exemplo, se os servidores já foram orientados em relação ao tema, se já foi elaborada alguma política ou relatório exigido pela LGPD.

MEDIDAS DE SEGURANÇA

Ainda que a entidade esteja na fase de planejamento do PGP, é essencial que inicie o quanto antes a adoção de medidas de segurança. Essas medidas, nesse início de projeto, passam pela revisão e aprimoramento das diretrizes e culturas internas da entidade.

ESTRUTURA ORGANIZACIONAL

O próximo passo é estabelecer, dentro da organização, uma estrutura de governança e gestão da proteção de dados pessoais de acordo com o porte da instituição.

INVENTÁRIO DE DADOS PESSOAIS

O inventário de dados é um documento essencial para o mapeamento de dados pessoais da entidade. É nele que ficarão documentadas todas as operações de dados pessoais que ocorrem na instituição e que vai permitir identificar quais os dados pessoais, onde estão e que operações são realizadas com eles.

Atualizado regularmente, o inventário permitirá atender tanto o requisito de manter um registro das operações de tratamento de dados pessoais, quanto o de auxiliar no controle do atendimento aos princípios, ambos estabelecidos pela LGPD.

LEVANTAMENTO DE CONTRATOS

O inventário de dados permite que a instituição identifique todos os serviços onde ocorrem tratamentos de dados. Isso inclui os sistemas, programas, softwares, servidores onde esses dados são tratados. A partir daí a instituição irá realizar o levantamento dos contratos que precisarão ser conferidos e aditados.

ETAPA II

CONSTRUÇÃO E EXECUÇÃO

O objetivo de um programa de governança em privacidade deve ser o de proteger os direitos do titular de dados (cidadão), sendo desenvolvido e implementado seguindo as leis e jurisdição relevantes. Nessa etapa, um programa de gerenciamento da privacidade, devide-se nas seguintes fases:

POLÍTICAS EXTERNAS

A construção das políticas internas e externas em um PGP vai formalizar e garantir que todos os usos de dados pessoais são conhecidos e em conformidade com a lei. Além das políticas e práticas, dentro da Administração Pública devem ser definidos os papéis específicos dos servidores públicos responsáveis pelas operações de tratamento de dados.

- Com a formalização das políticas externas e internas da organização, também é importante que inicie o treinamento dos colaboradores em relação à políticas e práticas de proteção de privacidade.
- É preciso que as políticas internas e externas deixem claro a utilidade e a finalidade das informações tratadas pela entidade, além das bases legais para cada tratamento de dados.

PRIVACIDADE DESDE A CONCEPÇÃO

A LGPD menciona o conceito de privacidade desde a concepção (privacy by design) no seu art. 46, §2°. Esse conceito traduz-se na adoção de medidas de segurança, administrativas e técnicas aptas a proteger dados pessoais desde a concepção (fase inicial) do desenvolvimento de um produto ou serviço.

É uma metodologia que visa a proteção dos dados pessoais – e, por consequência, do cidadão titular de dados – desde o início de um projeto, fazendo com que a proteção à privacidade seja o ponto de partida para o desenvolvimento de qualquer projeto, produto ou serviço realizado por uma organização. Nessa etapa, a entidade promoverá mudanças aptas a incorporar esse conceito dentro de sua estrutura.

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS

Após a etapa de planejamento e a elaboração do Inventário de Dados Pessoais, a organização está apta a produzir o Relatório de Impacto de Dados Pessoais, um dos documentos expressamente exigidos pela LGPD e que pode ser requerido pela ANPD (art. 38).

Instrumento de responsabilidade do controlador (a organização) onde constará uma visão completa do ciclo de vida dos dados pessoais tratados e a descrição formal dos processos para mitigação de riscos (e as responsabilidades) e em qualquer operação que envolva o tratamento de dados pessoais que possa gerar riscos às liberdades civis e aos direitos fundamentais.

POLÍTICAS INTERNAS

Realizada durante a etapa de Construção e Execução, o desenvolvimento e/ou atualização das diretrizes internas de proteção de dados pessoais deverá verificar se não há tratamento excessivo de dados, se os controles de segurança são suficientes para os dados tratados, se é necessário a retenção de determinados dados tratados e se é necessário realizar a revisão de contratos.

Torna-se fundamental o desenvolvimento de uma política de segurança da entidade/organização bem como de uma política de privacidade de dados. Já a Política de Privacidade é um documento informativo pelo qual o controlador transparece ao usuário a forma como o serviço realiza o tratamento dos dados pessoais e como ele fornece privacidade ao usuário.

ADEQUAÇÃO DOS CONTRATOS

Após a elaboração do Inventário de Dados, a entidade terá mapeado todos os contratos, convênios e instrumentos que impliquem no tratamento de dados pessoais. Com o inventário em mãos, é essencial que a organização inicie a revisão e atualização desses instrumentos.

No âmbito dos contratos administrativos, pode ser necessário que a Administração Pública revisite as cláusulas contratuais econômicas firmadas, mesmo após concluído o certame. Pode ser preciso incluir novas cláusulas, conforme os princípios da LGPD.

TERMO DE USO

Termo de Uso é um documento que fornece uma descrição detalhada do serviço, das condições e das regras aplicáveis a ele. Assim como a Política de Privacidade, o Termo de Uso advém da consciência do controlador e do operador em ser transparente com o titular de dados pessoais e comunicar como as atividades de tratamento desses dados observam os princípios dispostos no artigo 6º da LGPD.

ETAPA III

MONITORAMENTO

Acompanhar a conformidade à LGPD é uma atividade contínua e necessária para os órgãos e entidades manterem o PGP a longo prazo. Assim sendo, esta última etapa do PGP aborda aspectos, detalhados nas próximas seções, que incluem, em grande parte, coleta e análise de informações, bem como elaboração de relatórios e apresentações de resultados.

INDICADORES DE PERFORMANCE

Os Indicadores de Performance (Key Performance Indicator - KPI) incluem a análise regular dos principais indicadores de desempenho para verificar lacunas no Programa de Governança em Privacidade, assim como o status de outras iniciativas de privacidade.

GESTÃO DE INCIDENTES

É importante incluir nesta etapa do PGP um processo de Gestão de Incidentes, que registre os incidentes de segurança da informação e de privacidade ocorridos e que armazene informações relevantes desses incidentes.

É recomendado, ainda, que a Gestão de Incidentes possua um Plano de Comunicação orientando a forma que os incidentes de segurança, que acarretem risco ou dano, devem ser informados aos órgãos fiscalizatórios e à imprensa.

ANÁLISE E REPORTE DE RESULTADOS

A análise e divulgação da evolução das ações e resultados obtidos pelo PGP são essenciais para demonstrar o resultado do programa para a alta gestão e o reforço e perpetuação de uma cultura de privacidade e proteção de dados dentro da organização.

ENCARREGADO

O encarregado, dado seu papel de articulação e orientação nos assuntos referentes à proteção de dados na entidade, exerce função fundamental nessa etapa, entre elas:

- Gerenciamento do estabelecimento de métricas para auxiliar o acompanhamento das ações do Programa de Governança em Privacidade;
- Divulgação dos resultados entre as diversas áreas do órgão - estabelecimento de uma estrutura de divulgação de resultados para a alta direção dos órgãos e entidades;
- Interagir e prestar esclarecimento à ANPD, titulares de dados e demais órgãos e entidades públicas;
- Orientar os servidores públicos da entidade a respeito de novas leis, mudanças ou adoção de boas práticas dentro da organização;

EXIGÊNCIAS

DOCUMENTAÇÃO

A LGPD exige do controlador a elaboração de diversos documentos essenciais para comprovar e auxiliar o processo de adequação da organização à lei. Durante o desenvolvimento do PGP, devem ser produzidos (e atualizados) os seguintes documentos:

- NOMEAÇÃO DO ENCARREGADO
- DATA MAPPING
- RELATÓRIO DE IMPACTO
- POLÍTICA DE PRIVACIDADE EXTERNA
- POLÍTICA DE PRIVACIDADE INTERNA
- POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
- CANAL DE COMUNICAÇÃO
- PLANO DE GESTÃO DE INCIDENTES
- TREINAMENTO

AUTORES

Maria Elisa Silva Lemos

Advogada Especialista em Direito Digital. Profissional de Privacidade e Proteção de Dados certificada como DPO (EXIN e IAPP)

Marcelo Tesserolli Abreu

Advogado Especialista em Proteção de Dados e Adequação à Lei Geral de Proteção de Dados

BORNHAUSEN & ZIMMER ADVOGADOS
ABREU & SÍLVIA ADVOGADOS
JORGE LACERDA ADVOGADOS

CONSULTORIA JURÍDICA PARA ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS

CONTATOS

(48) 9 9153-1491

LGPD@BAZ.ADV.BR

FECAM

Federação de Consórcios, Associações e Municípios de Santa Catarina