APOSTILA EPISÓDIO-5
A LGPD NAS EMPRESAS

A Lei é muito clara quanto ao tratamento de dados pessoais pelas empresas.

Sejam dados de seus colaboradores, clientes, prospects ou parceiros de negócios.

Como já vimos nos episódios passados, a Lei não veio para que as empresas não tenham dados pessoais mas, principalmente, para regular como deve ser o tratamento destes dados.

A **LGPD** determina os cuidados e controles que as empresas devem possuir nos dados pessoais que possuem e tratam.

Relembrando alguns pontos importantes:

1. Coleta dos dados: No momento da coleta dos dados, deve estar explícita para qual finalidade serão tratados os dados.
2. Base Legal para o tratamento: A atividade com o dado pessoal deverá estar abaixo de uma da 10 bases legais que a Lei determina. Se o Consentimento for a base legal utilizada, lembrar que este deve ser livre, explícito e inequívoco e não poderá ter vícios de autorização.
3. Adequação e necessidade do tratamento: Limitação do tratamento ao mínimo necessário e compatibilidade do tratamento com as finalidades informadas ao titular.
4. Transparência: Garantia, aos titulares, de informações claras, precisas e facilmente acessíveis.
5. Compartilhamento: Auditoria e cuidado com as empresas que compartilhamos os dados pessoais.
6. Dados pessoais sensíveis: Para aqueles dados pessoais que possam discriminar o titular, deverá ser observados cuidados extras e processos mais estruturados e seguros.
7. Processo de adequação das empresas: As empresas deverão possuir o processo de adequação plenamente documentado, com os levantamentos das atividades com dados pessoais, seus riscos e vulnerabilidade atribuídos, as ações para minimizar e/ou eliminar estes risco, comprovação de capacitação dos colaboradores, analise de risco dos fornecedores e parceiros comerciais que compartilham dados pessoais entre outros.
8. Canal do Titular: A empresa deverá ter um canal de comunicação exclusivo para o titular, informando sua Politica de Privacidade, o Termo de Conduta assinado com os colaboradores, as Políticas de Cookies utilizadas e como o Titular pode solicitar seus direitos.

PROCESSO DE ADEQUAÇÃO

Praticamente todos os departamentos de uma empresa, em algum momento, tratam dados pessoais e devem ser envolvidos no processo de adequação.

O processo de adequação à LGPD é um processo moroso, porém inevitável e deverá ter a participação de todos. É um processo que denominamos TOP DOW (de cima para baixo) onde os principais executivos da empresa deverão participar ativamente.

Os passos que devem ser seguidos:

- Definição do Comitê Gestor LGPD: Normalmente um profissional de cada área da empresa com poder de decisão (Diretor e/ou gerente)
- Contratação de uma ferramenta (sistema) de gestão e documentação LGPD: O processo de adequação gera uma quantidade muito grande de informações. É necessário a utilização de um sistema especialista para que todo o processo seja documentado adequadamente desde o início dos trabalhos.
- Inventário de dados: Levantamento de todas as atividades com dados pessoais, por cada departamento da empresa, definindo o responsável pelas informações coletadas.
- Equalização de conhecimento: Treinamento e capacitação da equipe de trabalho, expansível a todos os colaboradores.
- Enquadramento base legal: Enquadramento de cada atividade relacionada a uma ou mais das 10 Bases Legais perante a Lei (Art. 7º).
- Analise dos processos: Analise dos índices de risco e vulnerabilidade de cada atividade mapeada com dado pessoal gerando o relatório de risco (ROPA).
- Analise de contratos: Analise de cada contrato que possa ter compartilhamento de dados e reformular com clausulas LGPD especificas a cada caso.
- Implementar Politicas de Conformidade: Criar e colocar em prática as Politicas de Privacidade, Politica de atendimento ao titular, Termos de Conduta, Política de segurança da informação entre outras.

- Definir o Encarregado de Dados (DPO): Definir, se for o caso de ser uma empresa que se enquadre em tal situação, o Encarregado de dados (DPO) ou contratação de DPO As-A-Service.
- Geração do Relatório Geral de Proteção de Dados (RGAPD): Gerar, conforme evolução dos processos, os RGAPDs que deverão conter todas as atividade mapeadas, seus riscos, ações para minimizar e/ou eliminar os risco e índice de conformidade alcançado em cada etapa e o atual.

O processo de adequação LGPD tem início mas não tem fim. Deverá sempre ser auditado e estudado para implementações que melhorem o índice de risco.

ÁREAS AFETADAS E CUIDADOS A SEREM TOMADOS

Administração:

Área que normalmente trata dados de vários tipos de titulares. Pode ser colaboradores, fornecedores, clientes, parceiros de negócio, prestadores de serviços, entre outros.

Como todas as áreas que, em algum momento tratam dados pessoais, as atividades que envolvam tais tratamentos deverão ser mapeadas e adequadas ao mínimo risco possível.

Atenção especial a guarda de documentos físicos. Devem ser armazenados em ambiente de acesso restrito e controlado. Papéis infligem um alto risco de incidentes.

Marketing:

Área que coleta muitos dados pessoais, via formulários físicos e/ou eletrônicos, Cookies ou outras ações de captação de interessados.

Deverá tomar o cuidado de informar o titular sobre como serão tratados os seus dados que estão sendo coletados. Para qual finalidade específica; se serão compartilhados e, se sim, com quem e, se possível e viável, coletar o consentimento formal para tal tratamento.

Comercial:

Os mesmos cuidados que devem ser tomados pelo marketing, se aplicam a área comercial, adicionando no contexto que, em muitos casos, os dados serão de clientes já conquistados e, portanto, deverão ter maior cuidado no tratamento destes dados.

Recursos Humanos:

Esta é uma área que demanda muita atenção, pois tratam uma grande quantidade de dados pessoais, bem como compartilham com outras empresas.

Tão importante, que nosso Episódio – 4, trata exclusivamente deste tema.

Financeiro/contabilidade:

Normalmente muito ligado ao administrativo, no âmbito de tratamento de dados pessoais. Deve-se tomar os mesmos cuidados, principalmente na guarda e compartilhamento dos dados em meios físicos.

Jurídico:

Todos os contratos devem ser cuidadosamente revistos, especialmente aqueles que envolvem o compartilhamento de dados pessoais de terceiros ou em larga escala.

Evite o uso de cláusulas padrão da LGPD, pois cada contrato deve ser analisado com base nas especificidades do negócio, considerando os riscos e vulnerabilidades para ambas as partes.

Além disso, é importante evitar contratos "leoninos" que atribuam responsabilidades unilaterais.

A Lei é clara sobre a responsabilidade solidária de toda a cadeia envolvida no tratamento de dados pessoais, tornando fundamental que todas as partes assumam suas respectivas responsabilidades.

TI e SI:

Tecnologia da Informação e Segurança da Informação são áreas de grande preocupação.

Faz-se necessário disseminar orientações interdepartamentais, dando suporte às áreas envolvidas, de forma a privilegiar e ter como ponto de partida a revisão sistêmica dos processos e procedimentos internos, que levem ao pleno atendimento da lei quanto à garantia da segurança das informações, com o especial cuidado voltado para que estas estejam protegidas a ataques de hacker e/ou a compartilhamento não permitido, assegurando assim que a organização esteja em conformidade com o atendimento da legislação, livre de incidentes e isenta de penalidades.

A Segurança da Informação é alcançada através da implementação ou revisão do conjunto de controles, rotinas e procedimentos, em especial voltados a: *Políticas*, *Processos*, *Procedimentos*, *Estrutura organizacional*, *Funções de software*, *hardware*, *backup's*, entre outros.

TECNOLOGIA DA INFORMAÇÃO ≠ SISTEMA DE INFORMAÇÃO

Tecnologia da Informação (TI) é usada para: **COLETAR** - **TRANSFERIR** - **ARMAZENAR** - **PROCESSAR**

Sistema da Informação (SI) é a preservação da **CONFIDENCIALIDADE**, da **INTEGRIDADE** e da **DISPONIBILIDADE** das informações.

Algumas funções do TI/SI:

1. Disseminar informações sobre segurança da informação aos dirigentes e colaboradores,
2. Implementar processos de segurança que minimizem riscos de incidentes, entre eles:
    - Politica de criação de senhas de acesso (não pode, por exemplo, ser a data de nascimento ou nome....)
    - Politica de troca de senhas periodicamente,
    - Controle de acesso e rastreabilidade, pelos usuários, em pastas e arquivos da rede e equipamentos interconectados a rede,
    - Implementação de anti-virús e firewalls na rede e em equipamentos interconectados,
    - Testes de intrusão e pentests regulares, entre outros.
3. Gerar relatórios periódicos a direção e colaboradores alertando sobre os resultados dos testes e propondo melhorias.
4. Auxiliar no programa de segurança dos meios de armazenamento fisicos.

Diretoria e alta gestão:

Como já colocamos, o processo deve ser TOP DOW. Do mais alto escalão, envolvendo todas as áreas e colaboradores da empresa.

É primordial o envolvimento pleno da alta direção da empresa em todo o processo, fazendo-se presente em cada etapa da implementação e cobrando continuidade nos processos implementados.

Encarregado de dados (DPO):

A Resolução CD/ANPD 18 estabelece o regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais nas empresas.

A LGPD define o "encarregado" como a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD. Nos termos do art. 41 da LGPD as atividades a serem desenvolvidas pelo encarregado incluem: aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; receber comunicações da ANPD e adotar providências; orientar os colaboradores a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares. Além disso, a LGPD prevê que a ANPD pode estabelecer normas complementares sobre a definição e as atribuições do encarregado, bem como hipóteses de dispensa de indicação.

Alguns pontos importantes:

Indicação do encarregado: a nova resolução estabelece que a indicação do encarregado deve ser realizada por ato formal do agente de tratamento, detalhando que esse ato deve dispor sobre as formas de atuação e as atividades a serem desempenhadas pelo encarregado, bem como ser um documento escrito, datado e assinado. Quando solicitado, o ato de nomeação deve ser apresentado à ANPD. Essa exigência de formalização é uma medida que traz mais seriedade e clareza ao processo de indicação do encarregado, embora possa ser vista como um ônus administrativo adicional para os agentes de tratamento;

Divulgação da identidade e contato do encarregado: como regra geral, a Resolução nº 18 exige que a identidade e as informações de contato do encarregado sejam divulgadas publicamente, de forma clara e objetiva, em local de destaque e de fácil acesso, no site do agente de tratamento que o indicou. A divulgação da identidade do encarregado depende se este último é uma pessoa natural ou pessoa jurídica: se for pessoa natural, a identidade do encarregado abrange, no mínimo, o seu nome completo; ou se for pessoa jurídica, a identidade do encarregado abrange, no mínimo, o nome empresarial ou o título do estabelecimento, bem como o nome completo da pessoa natural responsável. A divulgação das informações de contato do encarregado, por sua vez, deverá abranger, no mínimo, os dados referentes aos meios de comunicação que viabilizem o exercício dos direitos dos titulares junto ao controlador e possibilitem o recebimento de comunicações da ANPD.

A exigência de maior transparência é positiva, mas é importante resguardar a privacidade do próprio encarregado;

Atribuições e deveres do encarregado: estão ampliadas e detalhadas na resolução, de forma a incluir as atividades de assistência e orientação ao agente de tratamento na elaboração de registros, comunicação de incidentes de segurança, relatório de impacto, e implementação de medidas de segurança, entre outras. O encarregado deve ser capaz de comunicar-se com os titulares e com a ANPD em língua portuguesa, o que é visto como essencial para a eficácia do papel e função do encarregado um país com diversidades regionais e linguísticas como o Brasil;

Deveres dos agentes de tratamento e responsabilidade: Prover os meios necessários para o exercício das atribuições do encarregado e garantir a autonomia técnica necessária para suas atividades, livre de interferências indevidas. Essa autonomia é vital para assegurar a independência e eficácia da atuação do encarregado;

Conflito de interesse: Qualquer situação que possa comprometer, influenciar ou afetar, de maneira imprópria, a objetividade e o julgamento técnico do encarregado no desempenho de suas atribuições. É de responsabilidade do agente de tratamento se atentar para que o encarregado não exerça atribuições que acarretem conflito de interesse;

Cumulação de funções: O encarregado pode acumular funções e exercer as suas atividades para mais de um agente de tratamento, desde que seja possível o pleno atendimento de suas atribuições relacionadas a cada agente de tratamento e inexista conflito de interesse. Essa possibilidade é positiva, especialmente para organizações que podem ter dificuldades em manter um encarregado exclusivo, mas requer uma gestão cuidadosa para evitar sobrecargas de trabalhos e conflitos de interesse.

A possibilidade de que o encarregado seja uma pessoa natural ou jurídica, interna ou externa à organização (DPO As-A-Service);

O exercício da atividade de encarregado não pressupõe a inscrição em qualquer entidade nem qualquer certificação ou formação profissional específica;

O agente de tratamento permanece responsável por garantir os recursos necessários para que o encarregado possa desempenhar suas funções adequadamente;

Cabe ao agente de tratamento estabelecer as qualificações profissionais necessárias para o desempenho das atribuições do encarregado, considerando aspectos como: conhecimento sobre a legislação de proteção de dados pessoais, segurança da informação, processos bem como o contexto, o volume e o risco das operações de tratamento realizadas;

A responsabilidade pela conformidade do tratamento de dados pessoais continua sendo do agente de tratamento, não do encarregado.

CAPACITAÇÃO GRATUITA

No intuito e democratizar as informações sobre a Lei 13.709/18 – LGPD, disponibilizamos, **SEM NENHUM CUSTO**, aos colaboradores da sua empresa, nosso "*Curso Básico Passo a Passo Adequação LGPD*", inclusive com avaliação final e emissão de Certificado de Participação.

Este curso, On-Line e disponível em plataforma profissional, já formou algumas centenas de profissionais nas mais diversas áreas.

Para maiores detalhes e inscrição de seus colaboradores, entre em contato por qualquer um dos canais abaixo.

contato@lgpd13709.com.br
www.lgpd13709.com.br
www.lgpd4me.net
1144850215 (voz e WhatsApp)

PROGRAMA
LGPD 13.709
CONSULTORIA ESPECIALIZADA