1. O que é a Lei Geral de Proteção de Dados?

A Lei Geral de Proteção de Dados (LGPD) é uma legislação brasileira que regula o tratamento de dados pessoais por pessoa natural (pessoa física) ou pessoa jurídica (pública e privada), dispondo de princípios e requisitos autorizadores dos tratamentos de dados.

2. Como isso se dá na prática?

No dia a dia há contato com dados pessoais de colaboradores, representantes de fornecedores, clientes ou terceiros. Com a definição do que é dado pessoal e do que é um tratamento de dados, ao analisarmos a nossa rotina percebemos a quantidade de dados pessoais que são tratados em nosso cotidiano.

3. Mas o que é um "tratamento" de dados pessoais?

É, basicamente, toda operação realizada com dados pessoais. Desde sua coleta, passando por sua classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, até sua eliminação, abrangendo todo o ciclo de vida do dado dentro da organização, de modo que a simples guarda ou consulta a dados pessoais já é considerada tratamento e está sujeita à legislação.

4. E o que é um dado pessoal?

Dado pessoal é toda informação sobre pessoa natural que permita sua identificação em um único passo ou, em conjunto com outros dados, que possa identificar, em um certo contexto, uma pessoa natural.

Por exemplo, o CPF é um dado pessoal que permite a precisa identificação de uma pessoa natural (relacionado a pessoa identificada). De outro lado, a profissão, embora não identifique, por si só, com precisão uma pessoa natural, pode, se contextualizada com outros dados, como nome do Empregador, idade e gênero, tornar-se uma informação capaz de tornar um indivíduo identificável.

5. O que não é considerado dado pessoal?

Dados de pessoas jurídicas e dados anonimizados (que não permitem identificação de uma pessoa) não serão considerados dados pessoais para fins da legislação. Dados sobre produtos ou serviços também são exemplos de informações que não estão sujeitas à LGPD por não serem consideradas dados pessoais.

6. O que se compreende por dados pessoais sensíveis?

Há um conceito legal para dados pessoais sensíveis que não se confunde com o valor estratégico da informação para a empresa ou Titular. A preocupação da Lei foi proteger especialmente os dados cujo tratamento possam ensejar a discriminação em face do titular. A legislação não proíbe o tratamento destes dados, apenas estabelece regras mais protetivas.

São considerados sensíveis aqueles sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, referente à saúde ou à vida sexual, bem como dado genético ou biométrico.

Vale observar que dados de imagem, financeiros, bancários, CPF e outros que à primeira vista seriam considerados "sensíveis" pelo grau de afetação a diretos do Titular não são considerados sensíveis pela legislação.

7. Quem é o Titular de Dados Pessoais?

É a pessoa natural (física) a quem se referem os dados pessoais que são objeto de tratamento.

8. A Lei Geral de Proteção de Dados se aplica somente aos dados em formatos digitais?

Não. A lei abrange quaisquer dados pessoais, seja os dados presentes em suportes físicos ou digitais.

9. O que devo saber sobre os princípios da Lei Geral de Proteção de Dados e como eles poderão me ajudar?

A LGPD elenca 10 (dez) princípios que devem ser respeitados em um tratamento de dados pessoais e servirão de guia para a atuação da empresa em conformidade com a legislação.

Dentre eles, destacam-se os princípios da finalidade, necessidade e transparência. Este trinômio pode ser sintetizado na exigência de que os dados pessoais tratados sejam utilizados apenas para as finalidades específicas para as quais foram coletados, dentro do limite do necessário para estas finalidades, garantindo-se aos titulares informações claras, precisas e facilmente acessíveis sobre a realização do tratamento.

Os demais princípios a serem observados são o da adequação, livre acesso, qualidade dos dados, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

10. O que é o Mapeamento ou Registro de Operações de Tratamento de Dados Pessoais?

Todas as operações de tratamento de dados pessoais realizadas pela **GESTAMP** precisam ser registradas. Para tanto, **será desenvolvido um Registro de Operações de Tratamento de Dados Pessoais**, elemento primordial de nosso Programa de Governança em Privacidade e Proteção de Dados.

É importante que você preste auxílio à consultoria, aos seus superiores e/ou ao Encarregado de Dados (DPO) na identificação das operações que se utilizem de dados pessoais a fim de que o Registro de Operações de Tratamento de Dados Pessoais (Mapeamento) seja o mais fiel possível à realidade da organização.

11. Quem é o Encarregado de Proteção de Dados (DPO)?

O Encarregado de Dados ou DPO (*Data Protection Officer*) é a pessoa indicada pela **GESTAMP** para ser o ponto focal do Programa de Governança em Privacidade e Proteção de Dados.

A função do Encarregado (DPO) é apoiar e orientar todas as equipes da empresa a atuarem de forma a respeitar as normas de Proteção de Dados. Além de acompanhar a execução e atualização do Programa de Governança em Privacidade e Proteção de Dados, é o responsável por receber as demandas de titulares e tomar as providências cabíveis, conforme o caso.

12. Como a Lei Geral de Proteção de Dados afetará o meu trabalho?

Antes de mais nada, a proteção de dados pessoais passará a fazer parte da cultura da **GESTAMP**. É imprescindível que você leia participe do comitê e leia atentamente todas as políticas de privacidade e de segurança da informação que serão criadas e esteja atento a todas as orientações voltadas ao cumprimento da legislação.

Isso implica, principalmente, em utilizar apenas os dados pessoais imprescindíveis para o exercício das suas funções, não podendo realizar o tratamento de dados excessivos ou desnecessários para atingir a finalidade daquela operação, bem como noticiar ao membro do Comitê de Proteção de Dados representante do seu setor, o qual reportará ao Encarregado (DPO), sempre que tiver acesso franqueado a dados que não sejam necessários para a execução de suas atividades.

13. Quais as penalidades pelo descumprimento das normas de Proteção de Dados?

As penalidades para a Empresa vão desde a aplicação de advertências com indicação de prazo para adoção de medidas corretivas, multas de até 2% do faturamento líquido da empresa, com limite de R$ 50 milhões por infração, até a obrigatoriedade de retratação pública, que afeta diretamente a imagem da companhia.

O descumprimento de qualquer norma de conduta poderá ensejar advertência ou, a depender de sua gravidade, o desligamento da empresa, sem prejuízo de arcar com as perdas e danos que tiver dado causa, restando assegurado **GESTAMP** o direito de regresso, nos termos da lei.

14. O que é um incidente de segurança de dados pessoais?

Um incidente de segurança de dados pessoais é qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

15. Como devo agir diante de um incidente de segurança relacionado a dados pessoais?

Toda vez que houver suspeita de ocorrência de um incidente de segurança de dados pessoais, este deve ser, imediatamente, reportado ao Encarregado de Dados Pessoais (DPO).

A **GESTAMP** desenvolverá um Plano de Resposta a Incidentes e o Encarregado, conjuntamente com os demais membros do Comitê de Resposta a Incidentes, poderá direcionar as melhores condutas para evitar ou minimizar danos.