ABRAVA
ASSOCIAÇÃO BRASILEIRA DE REFRIGERAÇÃO, AR CONDICIONADO, VENTILAÇÃO E AQUECIMENTO

Lei Geral de Proteção de Dados Pessoais (LGPD)

Lei nº 13.709, de 14 de agosto de 2018.

Elaborado em outubro de 2020.

A Rosenthal Advogados é o escritório responsável pelo Departamento Jurídico da ABRAVA , contato pelo email juridico@abrava.com.br

I – RAZÕES PARA ADEQUAÇÃO À LGPD

(A) estar de acordo com a legislação vigente;

(B) evitar prejuízos financeiros com eventuais violações aos direitos de titulares de dados;

(C) viabilizar a contratação de seus serviços no mercado, afinal, com a entrada em vigor da LGPD, tomadores serão responsabilizados por atos de seus prestadores de serviços, sendo certo que o mercado irá procurar empresas e instituições que estejam adequadas à nova lei para contratações mais seguras;

(D) assegurar um diferencial competitivo no mercado.

II – VIGÊNCIA DA LEI

Primeiramente, a lei entraria em vigor 24 meses após sua publicação no Diário Oficial, ou seja, em 15.08.20.

No entanto, vários adiamentos ocorreram, sendo que o último deles foi derrubado pelo Senado, fazendo com que a LGPD entrasse em vigor no dia 18.09.20, sem, contudo, vigência das sanções administrativas previstas na lei, que ficaram prorrogadas para agosto de 2.021.

III – CARACTERÍSTICAS E FUNDAMENTOS DA LGPD

(A) como o próprio nome diz, a lei é **GERAL**, ou seja, destinada a todos os setores econômicos.

(B) aplicação a qualquer operação de tratamento de dado, independente do meio em que seja realizada a operação (físico ou virtual).

(C) aplicação extraterritorial da Lei, uma vez que é possível sua aplicação mesmo para operadores de dados sediados fora do território nacional.

(D) obrigação das empresas observarem princípios legais no tratamento de dados pessoais, sendo eles finalidade, adequação, necessidade, livre acesso de dados pelos titulares, integridade dos dados, transparência, prevenção de danos, proibição de discriminação ilícita ou abusiva, responsabilização e prestação de contas.

(E) as empresas só poderão tratar dados pessoais se houver base legal para o tratamento dos dados, sendo que as duas bases legais que se destacam é o consentimento do titular e o cumprimento de obrigação legal ou regulatória.

(F) tratamento específico para Dados Pessoais Sensíveis e Dados Pessoais de Crianças e Adolescentes.

(G) atribuição de Direitos aos Titulares dos Dados Pessoais – a pessoa natural, a quem se referem os dados pessoais que são objeto de tratamento, tem assegurada a titularidade de seus dados pessoais, sendo-lhe conferido o direito de acesso aos dados, a portabilidade dos dados a outro fornecedor de produtos ou serviços, a eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a Lei, bem como daqueles dados tratados com seu consentimento, a revogação do consentimento, entre outros direitos.

(H) São fundamentos da LGPS o respeito à privacidade, a autodeterminação informativa, a inviolabilidade da intimidade, da honra e da imagem, a livre iniciativa, concorrência e defesa do consumidor e o livre desenvolvimento da personalidade, dignidade e exercício da cidadania pelas pessoas naturais.

IV – PRINCIPIOS GERAIS

Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

Livre Acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

Qualidade dos Dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Não Discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

Responsabilização e Prestação de Contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

V – CONCEITOS DA LGPD

5.1. Dado pessoal

É a informação relacionada a pessoa natural identificada ou identificável, como por exemplo, nome, telefone, endereço, RG, CPF, data de nascimento, profissão, nacionalidade, e-mail, digitais, imagem, gostos, interesses, hábitos de consumo, entre outros.

5.2. Tratamento de dados

É toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

5.3. Titular

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

5.4. Controlador

É a pessoa física ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

5.5. Operador

É a pessoa física ou jurídica, de direito público ou privado, que efetivamente realiza o tratamento de dados pessoais em nome do controlador. Tanto o operador quanto o controlador também são chamados de agentes de tratamento.

5.6. Eliminação

É a exclusão de um dado ou de conjuntos de dados armazenados em bancos de dados.

5.7. Dado pessoal sensível

É um dado que, devido ao seu maior potencial de trazer problemas pessoais ao titular em caso de tratamento inadequado, recebem tratamento diferenciado pela LGPD.
São dados sensíveis aquele sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

5.8. Autoridade Nacional de Proteção de Dados

Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD. Apesar de já ter sido criada pelo Governo Federal, ainda não está estruturada, com todos os seus cargos ainda vagos.

5.9. Dado anonimizado

É o dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. Esses dados não são considerados pessoais. Em virtude da lei ser um pouco genérica sobre a questão, este tema certamente será objeto de regulamentação pela Autoridade Nacional de Proteção de Dados.

VI – APLICAÇÂO DA LGPD

A LGPD se aplica a qualquer operação de tratamento de dados, seja ela realizada por pessoal física ou pessoa jurídica (de direito público ou privado).

O meio no qual são tratados os dados, físico ou digital, é irrelevante, assim como a localização dos agentes de tratamento (controlador e operador) ou dos dados, desde que atendidos um dos seguintes critérios:

- A operação de tratamento seja realizada no território nacional;

- A atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;

- Os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

Portanto, atendido qualquer dos critérios acima, a LGPD será aplicada para regular o tratamento dos dados.

VII - NÂO APLICAÇÃO DA LGPD

A LGPD não será aplicada no tratamento de dados realizado por pessoa física para fins exclusivamente particulares e não econômicos.
Também não será aplicada para fins exclusivamente artísticos, jornalísticos, de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais.

VIII – REQUISITOS (BASES LEGAIS) PARA TRATAMENTO DE DADOS

Os interessados em tratar os dados deverão comprovar ao menos uma das bases legais abaixo para realizar o tratamento de dados pessoais. São elas:

- Fornecimento de consentimento pelo titular;

- Cumprimento de obrigação legal ou regulatória pelo controlador;

- Para fins de proteção do crédito;

- Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

- Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

- Para o exercício regular de direitos em processo judicial, administrativo ou arbitral;

- Para a proteção da vida ou da incolumidade física do titular ou de terceiros;

IX – CONSENTIMENTO PARA O TRATAMENTO DE DADOS

O consentimento é a principal base legal da LGPD, devendo sempre ser buscado por aquele que pretende ou precisar tratar dados pessoais em sua rotina de trabalho.

Deve ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular, devendo, em contratos, estar em cláusula destacada das demais cláusulas contratuais.

Vale destacar que o ônus de provar que o consentimento foi obtido em conformidade com a Lei é do controlador.

Outra questão importante é que o consentimento deverá ser conferido para fins específicos. Autorizações e cláusulas genéricas são consideradas nulas.

X – DIREITO DOS TITULARES

São direitos dos titulares de dados o acesso aos dados, a confirmação da existência de tratamento, a correção de dados incompletos, inexatos ou desatualizados, a portabilidade dos dados para outro fornecedor, o bloqueio ou eliminação de dados desnecessários, a revogação do consentimento a qualquer momento e a anonimização dos dados.

XI – OBRIGAÇÕES DOS AGENTES

Manter registros das operações de tratamento de dados, especialmente quando a base legal para o tratamento for o legítimo interesse.

O controlador deverá indicar encarregado pelo tratamento de dados pessoais, com atribuição para atuar como canal de comunicação entre a empresa, de um lado, e os titulares e a autoridade nacional, de outro lado – a identidade e as informações de contato do encarregado deverão ser divulgadas publicamente

O controlador e o operador deverão adotar medidas de segurança, técnicas e administrativas para proteção dos dados.

Obrigação de comunicação de incidentes de segurança que possa acarretar risco ou dano relevante aos titulares.

XII – ENCARREGADO PELO TRATAMENTO DE DADOS

É a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados.

Todas as empresas, associações e afins são obrigadas a ter essa figura dentro da organização. Vale destacar que não necessariamente uma pessoa deverá ser contratada exclusivamente para isso, podendo um funcionário da organização assumir este papel, desde que devidamente treinado para tal.

O controlador deve indicar o encarregado pelo tratamento de dados pessoais, informando publicamente a identidade e as informações de contato do encarregado, de forma clara e objetiva, preferencialmente no website (assim como ocorre com responsável químico em alguns produtos).

São atividades do encarregado:

- aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

- receber comunicações da autoridade nacional e adotar providências;

- orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;

- executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

XIII – SANÇOES

Conforme destacamos no começo, as sanções administrativas serão aplicadas somente a partir de agosto de 2021, sendo elas:
- Advertência, com indicação de prazo para adoção de medidas corretivas;

- Multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

- Multa diária, observado o limite total acima indicado;

- Publicação da infração após devidamente apurada e confirmada a sua ocorrência;

- Bloqueio dos dados pessoais a que se refere a infração até sua regularização;

- Eliminação dos dados pessoais a que se refere a infração;

- Suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;

- Suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;

- Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Vale destacar que embora as sanções administrativas estejam adiadas, titulares de dados que se sentirem afetados por dados tratados indevidamente poderão buscar o judiciário para pleitear indenizações, assim como órgãos de competência concorrente, como o PROCON.

Daí a importância de efetuar as adequações necessárias no fluxo de trabalho.

XIV – ROTEIRO DE ADEQUAÇÕES

Visando a adequação da legislação, sugerimos três ações básicas:

- Buscar o envolvimento dos executivos desde o início do plano de adequação para que a proteção de dados pessoais esteja incorporada aos valores da organização e assim o tema ganhe o engajamento e a força necessária;

- Estabelecer as ações e um líder para o plano, identificando os principais projetos e áreas da organização afetadas pela LGPD;

- Criar um programa de treinamento envolvendo todos os funcionários e prestadores de serviços da organização.

Recomendamos o seguinte roteiro para identificação dos riscos e adequação à legislação:

- Mapeamento de processos e diagnóstico de riscos;

- Análise de tecnologias utilizadas pela organização;

- Identificação dos dados tratados (sensíveis e não sensíveis) e alocação dos dados (área jurídica, CLT, terceiros e clientes);

- Análise da finalidade e necessidade de uso de tais dados;

- Análise do tempo necessário de armazenamento dos dados pessoais e aplicação dos princípios legais;

- Definição das bases legais de tratamento de dados pela organização;

- Definição do encarregado de Proteção de Dados Pessoais (DPO) – escolha e capacitação;

- Atualização de cláusulas contratuais;

- Atualização de políticas (Política de Proteção de Dados, Políticas de Uso de Equipamentos, Segurança de Informação, Códigos de Conduta de Fornecedores, etc.);

- Atualização de políticas de cookies no website da empresa;

- Atualização de mailings, sobretudo verificando a existência do consentimento para recebimento de informações;

- Alinhamento de fluxos e procedimentos;

- Due Diligence de terceiros fornecedores (capacidade financeira/seguro);

- Avaliação de Seguro;

- Treinamento de colaboradores – Políticas, procedimentos, riscos e etc;

- Assegurar o exercício dos titulares de dados e fluxo de atendimento;

- Criação de Programa de Governança em Privacidade;

- Criação de um Comitê de Gestão de Risco e de Crise, para atuar prontamente em caso de um vazamento de dados.

XV – CONCLUSÃO

Como visto anteriormente, organizações de todos os setores e de todos os portes estão obrigados a se adequar à nova legislação.

É muito importante que as empresas façam as devidas alterações em seus sites, redes sociais, atualizem seus mailings, bem como definam quem será o Encarregado de Proteção de Dados e treine-o para tanto.

Vale destacar que ao fazer o mapeamento de riscos e identificação dos dados tratados, certamente serão identificados dados desnecessários para as atividades, estes dados deverão ser imediatamente descartados e não mais solicitados.
Como não tínhamos uma legislação sobre a questão, não é incomum que as organizações tratassem dados desnecessários. Focando somente no que é realmente essencial, diminui-se o risco de problemas com eventual vazamento de dados ou mesmo uso inadequado de tais informações.

Vale destacar que certamente virão alterações e novas regulamentações, afinal, a Autoridade Nacional de Proteção de Dados ainda não implementada. Após sua implementação espera-se uma maior regulamentação e maiores definições sobre a aplicabilidade da LGPD à microempresas, associações, dentre outras, afinal, não é correto que uma ME ou associação sem fins lucrativos tenha o mesmo tratamento de uma multinacional que trata milhões de dados por dia.

Estamos à disposição para eventuais dúvidas e para auxiliar a associação na atualização de documentos e implantação efetiva das medidas trazidas pela LGPD.

Thiago Giovanni Rodrigues
OAB/SP 286.787