CARTILHA LGPD
PARA IBAPEs

Versão 1.0
Novembro 2023

Comissão:
Amarilio Mattos Jr – Presidente IBAPE Nacional
Eduardo Rottmann – IBAPE Nacional
Edson Haluch – IBAPE/PR
Maria Teresa Cerqueira – IBAPE/BA
Paulo Magri – IBAPE/SP
Valéria das Graças Vasconcelos – IBAPE/MG

ENTIDADE FEDERATIVA NACIONAL
Filiado a UPAV • Unión Panamericana de Asociaciones de Valuación
IVSC • International Valuation Standards Council

secretaria@ibape-nacional.com • (11) **3115-3784**
Rua Maria Paula, 122 • cj 109/110 • 1º andar
São Paulo/ SP • Brasil • CEP 01319-907

Sumário

INTRODUÇÃO

Esta cartilha tem o objetivo de apresentar a Lei Geral de Proteção de Dados conhecida como LGPD.

A Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece diretrizes importantes e obrigatórias para a coleta, processamento e armazenamento de dados pessoais. Ela foi inspirada na GDPR (*General Data Protection Regulation*), que entrou em vigência em 2018 na União Europeia, trazendo grandes impactos para empresas e consumidores.

No Brasil, a LGPD (Lei nº 13.709, de 14/8/2018) entrou em vigor em 18 de setembro de 2020. Com isso, passamos a fazer parte de um grupo de países que contam com uma legislação específica para a proteção de dados dos seus cidadãos. Diante dos atuais casos de uso indevido, comercialização e vazamento de dados, as novas regras garantem a privacidade dos brasileiros, além de evitar entraves comerciais com outros países.

Existem muitas matérias que discorrem sobre o tema que disponibilizamos abaixo alguns links ou arquivos, de forma que todos possam se educar e divulgar no seu Ibape, com associados e diretoria.

Referências:

Confea:
https://www.confea.org.br/funcionamento/lgpd

Crea/SP:
https://www.creasp.org.br/lgpd/

FUNDAMENTAÇÃO DA LEGISLAÇÃO

A legislação se fundamenta em diversos valores e tem como principais objetivos:

- Assegurar o direito à privacidade e à proteção de dados pessoais dos usuários, por meio de práticas transparentes e seguras, garantindo direitos fundamentais.
- Estabelecer regras claras sobre o tratamento de dados pessoais.
- Fortalecer a segurança das relações jurídicas e a confiança do titular no tratamento de dados pessoais, garantindo a livre iniciativa, a livre concorrência e a defesa das relações comerciais e de consumo.
- Promover a concorrência e a livre atividade econômica, inclusive com portabilidade de dados.

DEFINIÇÕES DIRIGIDAS PARA INICIAR A IMPLEMENTAÇÃO

A legislação da LGPD é bastante complexa e engloba todos os negócios de uma organização, como:

- Treinamentos;
- Elaboração do Mapa de Risco à Proteção de Dados Pessoais;
- Elaboração da documentação que será submetida à validação da Companhia;
- Identificação dos riscos críticos a serem tratados e medidas de mitigação ou tratamento de dados de equipes e comunicação do projeto;
- Implantação de Mecanismo de Reporte (Canal de Denúncias ou Comunicação disponível aos Titulares de Dados);
- Elaboração dos planos de resposta aos titulares dos dados e autoridades;
- Elaboração do plano de contingenciamento de crises e continuidade de negócios (em caso de eventuais ocorrências de vazamentos ou violações de dados pessoais);
- Outras atividades identificadas de acordo com as características do negócio da Organização.

A LGPD regula como organizações devem tratar dados pessoais e fornece uma série de direitos aos titulares dos dados.

Praticamente toda organização trata dados pessoais, tais como: dados de seus associados e funcionários, fornecedores, dados de inscritos em eventos, entre outros.

O tratamento de dados pessoais é regulado pela LGPD tanto no formato físico como no digital, quer estejam em um computador ou em uma sala de arquivos.

O setor de atuação de cada empresa ou instituição, exerce influência nas medidas que cada uma terá que adotar para se adequar a LGPD, ou seja, como a lei será aplicada, mas não altera a necessidade de adequação.

A LGPD pode ser entendida como um PROGRAMA VIVO, que estará em constante necessidade de avaliação e revisão, o que não pode ser negligenciado pela organização, tanto a Alta Direção, como o Encarregado de Proteção de Dados (DPO), que precisa ser identificado e nomeado, e também, todos os coordenadores e colaboradores envolvidos nos processos em que há impacto da LGPD.

Abaixo, então, passamos a apresentar as MEDIDAS DE CONFORMIDADE, as MEDIDAS DE MITIGAÇÃO DE RISCOS e eventuais MEDIDAS TÉCNICAS necessárias a garantir conformidade e, ainda, assegurar o cumprimento de PRINCÍPIOS e DIRETRIZES da LGPD para os Agentes de Tratamento de Dados, bem como assegurar os direitos dos titulares dos dados.

DADOS SENSÍVEIS E NÃO SENSÍVEIS

O que precisa ser compreendido com a LGPD é como devem ser tratados os DADOS PESSOAIS, classificados em três categorias:

DADO PESSOAL: É qualquer dado que possa vir a ser usado para identificar, direta ou indiretamente, uma pessoa, chamada de “titular” desse dado, tais como nome, RG, CPF, e-mail, dados genéricos etc.

DADO PESSOAL SENSÍVEL: É o dado pessoal 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 genérico ou biométrico, quando vinculados a uma pessoa natural, que podem ser utilizados de forma discriminatória e, portanto, carecem de proteção especial. Qualquer dado que esteja na categoria de dados sensíveis, só poderá ser fornecido com a permissão do Titular.

DADOS NÃO SENSÍVEIS: É todo aquele que não seja considerado sensível, aplicando-se, a ele, embora a lei tenha selecionado um rol de dados que entende ser de natureza sensível, existe um profundo debate se esse rol é fechado (apenas os dados neles existentes são considerados sensíveis) ou meramente exemplificativo. Então, por via das dúvidas, considere como dado sensível todo aquele passível de gerar conduta discriminatória.

Assim, ao associar um profissional, criar um formulário para inscrição em evento, elaborar uma pesquisa de opinião, entre outros, deve-se selecionar o menor número possível de dados dos Titulares, ou seja, aqueles fundamentais para reconhecimento e contato, como por exemplo, Nome Completo, CPF, E-mail, Celular, Formação Profissional, Cidade e Estado.

Os dados devem permitir que a instituição consiga, através deles, emitir um certificado, recibo ou nota fiscal (precisa do endereço).

Outras informações, tais como: endereço completo, foto, dados bancários, gênero, entre outras, devem ser solicitados apenas em situações específicas.

DEFINIÇÕES DE PARCEIROS, COLABORADORES E FORNECEDORES

Todos os contratos (PF ou PJ) com empresas, entidades, funcionários, colaboradores e fornecedores, devem ter no seu texto uma cláusula ou um termo de confidencialidade.

O principal fornecedor (ou fornecedores), e o mais sensível por lidar com os dados dos "clientes" são as empresas de TI, site, marketing, multimidia, backup dos servidores e manutenção de informática (software e hardware).

Nesse termo ou cláusula, a empresa e funcionários devem assinar dizendo que não irão usar, divulgar nem distribuir os dados dos nossos "clientes" para ninguém e nem dar acesso a terceiros.

Se houver manutenção em computadores ou servidores, e for um novo fornecedor, este deverá assinar um documento onde garante que não irá copiar, nem usar, nem divulgar, nem distribuir os dados dos nossos "clientes".

POLÍTICA DE PRIVACIDADE

A Política de Privacidade é um dever de toda empresa que coleta dados de seus usuários ou colaboradores.

Esse documento é fundamental para que todos os clientes, usuários e/ou colaboradores que utilizem a sua página na internet, tenham o conhecimento sobre a forma como a sua empresa recolhe os seus dados pessoais, permitindo-lhes ver como são utilizados. Ela deve estar em local de fácil acesso na sua página da internet.

É muito importante que os clientes ou usuários possam ler a sua política de privacidade para que possam cumprir as suas obrigações de proteção de dados. Para isso, é recomendável:

- Incluir a sua política de privacidade em local visível no seu website por exemplo, na sua página inicial;

- Fornecer e assegurar um endereço de e-mail aos clientes ou usuários para o qual possam enviar as suas dúvidas sobre a sua política de proteção de dados;

- Resolver pedidos de clientes ou usuários o mais breve possível.

POLÍTICA DE COOKIES

Cookies são pequenos arquivos de texto armazenados no computador do usuário por um site, e que permitem ao site lembrar informações específicas sobre o usuário, tais como suas preferências e histórico de navegação. Eles são amplamente utilizados em páginas web para melhorar a experiência do usuário, permitindo que os sites personalizem a apresentação com base no histórico de navegação e nas preferências do usuário, além de manter o usuário conectado em sua conta. Adicionalmente, os cookies são usados para coletar dados sobre o comportamento do usuário, como informações de navegação e preferências de compras, que podem ser usados por empresas para personalizar anúncios e oferecer ofertas relevantes.

Se desejar incluir ou ativar cookies no seu website, deve informar aos seus clientes de forma clara acerca do consentimento que deve ser manifestado de maneira expressa. Este é o caso, por exemplo, se tiver incorporado o YouTube no seu website, se tiver utilizado um botão do Facebook ou processado dados com o Google Analytics.

Os clientes ou usuários devem aceitar a política de cookies, nas configurações do site, antes de descarregarem qualquer serviço ou conteúdo, ou indicando na política de cookies o que acontece se o utilizador continuar a utilizar o site etc.

Na LGPD, não são encontrados termos como “cookie”, “arquivo”, “browser” e “navegador”. O que acontece é que, na medida em que cookies se caracterizam como identificadores de indivíduos e repositórios de informações pessoais, eles devem estar sujeitos aos tratamentos previstos na regulação.

O banner de cookie deve incluir informações claras e simples sobre o tipo de cookies usados pelo site e para que finalidade eles são usados. Além disso, o usuário deve ser capaz de escolher se aceita ou não o uso de cookies antes de continuar a navegar no site. O banner de primeiro nível é exibido assim que o usuário acessa o site e contém informações básicas sobre o uso de cookies. Ele deve incluir um aviso claro e simples sobre o uso de cookies pelo site, bem como um link para a política de privacidade do site. O banner de segundo nível, por outro lado, é mais detalhado e só é exibido depois que o usuário concorda em permitir o uso de cookies. Ele deve fornecer informações mais específicas sobre cada tipo de cookie usado pelo site, bem como permitir que o usuário escolha os tipos de cookie que deseja utilizar. O banner de segundo nível pode incluir botões de "Aceitar todos" e “Rejeitar não-necessários”, além de permitir ao usuário selecionar os tipos de cookies que deseja utilizar.

O Guia Orientativo sobre cookies da Autoridade Nacional de Proteção de Dados apresenta uma lista de práticas desaconselhadas quando da elaboração de banners de cookies:

- Utilizar um único botão no banner de primeiro nível, sem opção de gerenciamento no caso de utilizar a hipótese legal do consentimento (“concordo”, “aceito”, “ciente” etc.);

- Dificultar a visualização ou compreensão dos botões de rejeitar cookies ou de configurar cookies, e conferir maior destaque apenas ao botão de aceite; impossibilitar ou dificultar a rejeição de todos os cookies não-necessários;

- Apresentar cookies não-necessários ativados por padrão, exigindo a desativação manual pelo titular; não disponibilizar banner de segundo nível;

- Não disponibilizar informações e mecanismo direto, simplificado e próprio para o exercício dos direitos de revogação do consentimento e de oposição ao tratamento pelo titular (além das configurações de bloqueio do navegador);

- Dificultar o gerenciamento de cookies (exemplo: não disponibilizar opções específicas de gerenciamento para cookies que possuem finalidades distintas); informações sobre a política de cookies apenas em idioma estrangeiro;

- Apresentar lista de cookies demasiadamente dividido, gerando uma quantidade excessiva de informações, o que dificulta a compreensão e pode levar ao efeito de fadiga, não permitindo a manifestação de vontade clara e positiva do titular;

- Ao utilizar o consentimento como hipótese legal, vincular a sua obtenção ao aceite integral das condições de uso de cookies, sem o fornecimento de opções efetivas ao titular.

AUDITORIA

Após a conclusão de todos os requerimentos do Plano de Ação Mínimo, o Ibape deve então contratar um especialista local para fazer uma auditoria e identificar os pontos ainda carentes e as oportunidades de melhoria do processo de implementação de LGPD.

Como sugestão, o Ibape Regional pode pedir referência de empresas de auditoria ao Crea do seu estado.

Pode também ser um colega advogado que possa fazer uma auditoria inicial e depois uma formal com empresa especializada.

Ibape Nacional
Revisão 01 - Data: 20/abril/2023
Revisão 02 - Data: 14/junho/2023
Revisão 03 - Data: 19/julho/2023
Revisão 04 - Data: 23/agosto/2023