Manual ABA para adequação à LGPD

Orientações e boas práticas de governança de dados para Publicitários

Este guia é uma entrega do GT de LGPD no Marketing, liderado pelo Comitê Jurídico da ABA e composto pelos Comitês de Consumer Experience e de Mídia da Entidade. Foi elaborado em parceria com Pinheiro Neto Advogados.

APOIO

CONAR
Conselho Nacional de Autorregulamentação Publicitária

Sumário

Introdução

O **Manual ABA para adequação à LGPD - orientações e boas práticas de governança de dados - para Publicitários** surge nesse contexto, elaborado pela ABA – Associação Brasileira de Anunciantes, por meio de seu **Grupo de Trabalho de LGPD no Marketing**, em parceria com o escritório Pinheiro Neto Advogados, responsável em conjunto pelo desenvolvimento do seu conteúdo.

Em resposta à relevância do tema "proteção de dados" e à iminente vigência das novas regras, o Grupo de Trabalho de LGPD no Marketing foi formado pelos associados da ABA, liderado pelo **Comitê Jurídico da Entidade**, presidido por **Dra. Vanessa Vilar**, General Counsel Marketing LatAm, Corporate & Transactions Brazil da Unilever e composto por, além deste, os **Comitês de Consumer Experience e de Mídia da ABA**, respectivamente presididos por **Betania Gattai, Latam Consumer engage Centers Manager da Unilever e Marco Frade, Head de Digital, Media & PR da LG**.

> *"É fundamental que as empresas se estruturem para a escolha das tecnologias e processos mais adequados, conforme seus respectivos modelos de negócio, para que atendam às normas e garantam que as informações sejam tratadas com sigilo e transparência, preservando as marcas, respeitando as pessoas e a privacidade do público consumidor."*
>
> **Nelcina Tropardi**, Presidente da ABA e Vice Presidente de Sustentabilidade e Assuntos Corporativos da HEINEKEN

Com o **apoio do CONAR** - Conselho Nacional de Autorregulamentação Publicitária, do qual a ABA é cofundadora, o GT de LGPD no Marketing assumiu em 2019 a responsabilidade do Protagonismo Colaborativo que integra o Plano Estratégico ABA 2020.

Por meio deste manual, a ABA viabilizou uma entrega concreta ao mercado, com o objetivo de difundir e esclarecer as novas regras da LGPD e apoiar os anunciantes a atualizarem suas práticas de Marketing & Comunicação, especialmente no que tange a relação direta com os consumidores e seus dados pessoais.

“As regras do uso, proteção e transferência de dados em sintonia com as políticas de compliance e governança das empresas escreverão um novo capítulo na história das relações de consumo. Empresas terão que se adaptar e buscar inovações para as estratégias de marketing, por outro lado o consumidor se sentirá mais protegido e valorizado, consequentemente buscará produtos e serviços que respeitam essa relação.”

Dra. Vanessa Vilar, General Counsel Marketing LatAm, Corporate & Transactions Brazil da Unilever e Presidente do Comitê Jurídico da ABA

A LGPD é destinada a todas as operações de tratamento de dados pessoais de consumidores no território brasileiro. As atividades de marketing estão entre as mais impactadas pela nova regulamentação, especialmente no ambiente do marketing digital, uma vez que frequentemente analisam e trabalham com dados baseados nos hábitos e comportamentos dos consumidores, oriundos do tratamento de dados pessoais.

“As boas práticas de governança corporativa e compliance constituem a base necessária para a credibilidade dos nossos negócios. Nossa lição de casa é atuar acima de tudo sempre orientados pela ética, pela integridade e pela transparência. Assim, protegemos o maior patrimônio da organização, ou seja, salvaguardamos a reputação das marcas e conquistamos a confiança dos nossos clientes.”

Marco Frade, Head de Digital, Media & PR da LG e Presidente do Comitê de Mídia da ABA

“Adequar-se à nova regulamentação da LGPD representa um importante passo das organizações no compromisso com a integridade e maturidade das relações entre as marcas e consumidores, respeitando a privacidade dos clientes e valorizando o seu papel social junto ao mercado.”

Betania Gattai, Latam Consumer engage Centers Manager da Unilever e Presidente do Comitê de Consumer Experience da ABA

De forma prática e didática, serão encontrados no **Manual ABA para adequação à LGPD - orientações e boas práticas de governança de dados - para Publicitários** os termos e conceitos relevantes para o entendimento da lei, as bases previstas pelas novas diretrizes para o tratamento de dados e os passos a serem observados durante o processo de adequação das organizações.

“Além das sanções administrativas, judiciais e multas onerosas, o descumprimento da Lei pode gerar grandes prejuízos à imagem e reputação das organizações. Portanto, a adoção de políticas de boas práticas e governança corporativa expostas neste manual é essencial não apenas para o cumprimento com as obrigações estabelecidas pela LGPD, como para evidenciar os esforços nesse sentido, fortalecendo as relações dos anunciantes com o mercado.”

Dr. Marcel Leonardi, Consultor do escritório Pinheiro Neto Advogados, parceiro da ABA na elaboração deste guia

“Atender à nova regulamentação da Lei Geral de Proteção de Dados, que entrará em vigor em 2020, vem ao encontro dos principais valores do CONAR, a liberdade de expressão e a ética na publicidade. Buscamos de forma contínua estimular que a publicidade tenha papel construtivo e que trabalhe a favor do consumidor.”

João Luiz Faria Netto, Presidente do CONAR. Conselho Nacional de Autorregulamentação Publicitária

Ciente da importância da relação ética e responsável com o consumidor, a ABA assume o compromisso de pioneirismo pelas melhores práticas do exercício do Marketing & Comunicação no país. O Manual ABA para adequação à LGPD - orientações e boas práticas de governança de dados - para Publicitário corrobora o posicionamento da Entidade de Mobilizar o Marketing para Transformar os Negócios e a Sociedade e integra o calendário de ações em comemoração aos 60 anos da Associação. A criação deste documento, assim como o nascimento da LGPD, representa conquista coletiva para os anunciantes, consumidores e parceiros que ao nosso lado caminham.

Atenciosamente,

Sandra Martinelli
Presidente-Executiva da ABA

Sobre este guia

Este guia foi desenvolvido pela Associação Brasileira de Anunciantes (ABA) em parceria com Pinheiro Neto Advogados e busca apresentar pontos de atenção e aspectos da Lei Geral de Proteção de Dados relevantes aos profissionais de marketing.

Este guia tem um caráter meramente informativo e não substitui nem deve ser entendido como aconselhamento jurídico.

Visão geral da lei

A Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados ("LGPD") passará a ser aplicável em agosto de 2020[1]. Ela traz mudanças profundas nas condições para o tratamento de dados pessoais, o que inclui atividades como coleta, armazenamento, utilização, compartilhamento e eliminação de informações relacionadas a pessoas naturais identificadas ou identificáveis.

O longo período entre a data de publicação da LGPD (agosto/2018) e o início da sua vigência (agosto/2020) deriva da complexidade das ações que precisam ser tomadas pelas empresas para adaptação aos novos parâmetros legais.

No final do ano de 2018, foi criada a Autoridade Nacional de Proteção de Dados ("ANPD"), por meio da Medida Provisória nº 869/2018.

A ANPD terá um papel tríplice de:

(i) fiscalização - poderá editar normas e procedimentos, deliberar sobre a interpretação da LGPD e requisitar informações relacionadas ao tratamento de dados pessoais;

(ii) sanção - terá poderes para instaurar processo administrativo quando houver descumprimento à LGPD e terá competência exclusiva para aplicar as sanções previstas na LGPD; e

(iii) educação - irá difundir o conhecimento sobre a LGPD e medidas de segurança, apresentando diretrizes para interpretação da lei, estimulando padrões para serviços e produtos que facilitem o controle de titulares sobre seus dados pessoais e elaborando estudos sobre melhores práticas nacionais e internacionais de proteção de dados pessoais, entre outros.

1 Esta data poderá ainda sofrer alterações dependendo da votação da MP 869/2018 no Congresso.

Termos e conceitos relevantantes para a continuidade da leitura deste guia

Titular: é a pessoa física a quem um dado pessoal se refere.

Dado pessoal: é qualquer informação relacionada a uma pessoa física identificada ou identificável. RG, CPF, endereço, data de nascimento são alguns exemplos de dados pessoais, mas informações como hábitos de consumo, localização geográfica, perfil comportamental, preferências, históricos de compras e outras informações semelhantes, quando relacionadas a uma pessoa física identificada ou identificável, são considerados "dados pessoais". Da mesma forma, informações sobre navegação na Internet, como endereço IP e cookies, entre outras, são em geral consideradas como dados pessoais sempre que for possível identificar a pessoa relacionada a essas informações.

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 genético ou biométrico, quando vinculado a uma pessoa natural. A lei traz exigências adicionais e impõe algumas restrições para o tratamento de dados sensíveis.

Dado anonimizado e pessoa identificável: dado anonimizado é o oposto de dado pessoal, ou seja, é o dado que não pode ser associado a um indivíduo. É importante notar que ainda que um dado não esteja direta e explicitamente associado a uma pessoa identificada, ele pode ser considerado um dado pessoal (e não anônimo) sempre que for possível associá-lo a um indivíduo utilizando os meios técnicos disponíveis na ocasião.

Meios técnicos razoáveis e disponíveis: A LGPD não estabelece de maneira específica quais padrões, meios técnicos ou processos devem ser aplicados para que os dados sejam considerados suficientemente anonimizados. A interpretação sobre o que deve ser considerado "meio técnico razoável" em cada cenário será feita pela Autoridade Nacional de Proteção de Dados e a LGPD indica apenas que a autoridade deve considerar fatores objetivos, tais como custo e tempo necessários, considerando as tecnologias disponíveis e utilzação exclusiva de meios próprios.

Tratamento de dados: é toda operação realizada com dados pessoais – da coleta ao descarte, incluindo o mero armazenamento. A LGPD menciona expressamente diversos outros exemplos: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Princípios gerais e melhores práticas

A LGPD estabelece alguns princípios que se aplicam a todas as atividades de tratamento de dados. 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.

Entre os princípios mais relevantes aos profissionais de marketing, estão os seguintes:

Princípios da Finalidade, Adequação, Necessidade

De acordo com esses princípios, dados pessoais só devem ser coletados e tratados para os propósitos específicos e legítimos que tenham sido informados ao titular de dados e sejam compatíveis com o contexto do tratamento. O tratamento deve ser limitado ao mínimo necessário para aquelas finalidades que foram informadas aos titulares.

Isso significa que antes de coletar, armazenar ou de qualquer maneira utilizar dados pessoais, é importante verificar:

i. se o titular daqueles dados foi informado de maneira clara e específica sobre como os dados serão tratados e para quais finalidades – o porquê do tratamento;

ii. se o tratamento é adequado ao contexto em que os dados foram coletados, ou seja, às expectativas que o titular de dados tinha ao fornecer os seus dados ou torná-los disponíveis; e

iii. se é realmente necessário tratar aqueles dados para atingir aquela finalidade.

Princípios da Transparência, Livre Acesso

É importante garantir que os titulares de dados pessoais tenham acesso a informações claras e facilmente acessíveis sobre como seus dados são tratados, por quem e para quais finalidades.

Isso pode ser feito de diversas maneiras, conforme a natureza do tratamento. Uma recomendação é sempre utilizar linguagem clara, objetiva, sucinta e específica nas políticas de privacidade ou em outros materiais semelhantes, e facilitar o acesso a esses materiais para os titulares de dados.

Além disso, é também necessário oferecer um canal de comunicação acessível para que os titulares de dados possam esclarecer suas dúvidas e solicitar informações.

Princípios da Segurança e Prevenção

Ao tratar dados pessoais, é importante implementar medidas técnicas e administrativas capazes de proteger esses dados de acessos não autorizados, perda, destruição, alteração, ou divulgação indevida, bem como prevenir quaisquer incidentes que possam causar danos aos titulares de dados. Isso pode incluir, por exemplo, controles de acessos, técnicas de criptografia, revisão de arquitetura de sistemas, separação de bancos de dados, entre outros.

Princípio da Não discriminação

O tratamento de dados pessoais não deve ser realizado para fins discriminatórios, ilícitos ou abusivos.

Melhores práticas: alguns exemplos

Utilize recursos audiovisuais. Para que as informações fiquem mais atrativas e compreensíveis, considere a adoção de vídeos, imagens e infográficos para ilustrar processos e tratamentos de dados pessoais. Recursos interativos também podem ser interessantes.

Clareza e objetividade são essenciais. Procure sempre oferecer informações de forma simples e direta, evitando ambiguidades e termos muito técnicos em seus documentos e políticas.

Seja flexível. Sempre que possível, dê liberdade para o usuário concordar ou não com o fornecimento de seus dados pessoais e gerenciar suas escolhas de privacidade, preferencialmente por meio de painéis de controle (dashboards) ou ferramentas similares. Não deixe as checkboxes pré-marcadas. Não colete dados excessivos ou desnecessários.

Seja disponível. Crie um canal de atendimento e de comunicação para que os usuários entrem em contato de maneira fácil e simplificada para tirar dúvidas sobre o tratamento de dados pessoais.

Por que a LGPD interessa aos profissionais de marketing?

Atividades de marketing frequentemente envolvem tratamento e compartilhamento de dados pessoais. As atividades de marketing estão entre as mais afetadas pela LGPD, especialmente no contexto do marketing digital, uma vez que (i) se baseiam fortemente nos hábitos e comportamentos dos consumidores, derivados do tratamento de dados pessoais; (ii) o compartilhamento de dados no contexto de prospecção e obtenção de leads é comum; (iii) para impactar consumidores interessados na mensagem publicitária e efetuar comunicações são utilizadas informações de contato, que também podem ser consideradas dados pessoais.

A LGPD tem um extenso âmbito de aplicação. A LGPD aplica-se a qualquer operação de tratamento de dados pessoais realizada em território brasileiro ou relacionada a dados pessoais de indivíduos localizados no Brasil no momento em que os dados foram coletados, ou ainda se o tratamento de dados pessoais tem por objetivo oferecer produtos ou serviços no Brasil. Além disso, é importante notar que a LGPD não está restrita ao ambiente digital. Por exemplo, dados pessoais coletados em formulários de pesquisas, eventos, etc. também estão sujeitos à LGPD.

Impactos nas rotinas operacionais. Os direitos e as obrigações estabelecidos pela LGPD requerem a revisão e a adequação de diversas rotinas operacionais das empresas. Por exemplo, a LGPD estabelece que os titulares de dados podem solicitar o acesso aos dados pessoais mantidos pelas empresas, bem como a revisão dos seus respectivos perfis pessoais ou de consumo que tenham sido formados com base em tratamento automatizado de dados (p.ex. por meio de algoritmos). Será necessário criar mecanismos para atender a essas solicitações. Será também necessário estabelecer rotinas para a exclusão de dados mediante revogação do consentimento do titular ou de dados que não servem mais à finalidade para a qual foram originalmente coletados. Ainda, a LGPD determina que o titular de dados pode solicitar a portabilidade de seus dados para outro fornecedor de serviço ou produto, o que também requer o estabelecimento de processos operacionais específicos.

O descumprimento da LGPD tem um custo alto. Além das sanções administrativas e judiciais aplicáveis em caso de descumprimento – a multa pode chegar a 2% do faturamento da empresa no Brasil, até o limite de R$ 50 milhões, por infração – estar em desconformidade com a LGPD pode acarretar danos reputacionais significativos, prejudicando a imagem e as marcas da empresa perante seus consumidores e clientes.

Além disso, a adequação à LGPD será cobrada pelo próprio mercado, tornando-se uma vantagem competitiva importante para a escolha de parceiros de negócio e para o estabelecimento e a manutenção de relacionamento comercial entre empresas. Além disso, os passivos decorrentes de descumprimento das obrigações estabelecidas pela LGPD também serão fatores determinantes no âmbito da captação de investimentos e em operações de fusão e aquisição.

Cuidados com o consentimento

O tratamento de dados pessoais só pode ser realizado em dez hipóteses estabelecidas pela LGPD. Essas hipóteses são conhecidas como **bases legais de tratamento**.

Uma das bases legais de tratamento é o consentimento do titular, ou seja, a concordância com o tratamento de seus dados pessoais para uma finalidade determinada.

O consentimento, no entanto, precisa respeitar alguns requisitos para que seja considerado válido:

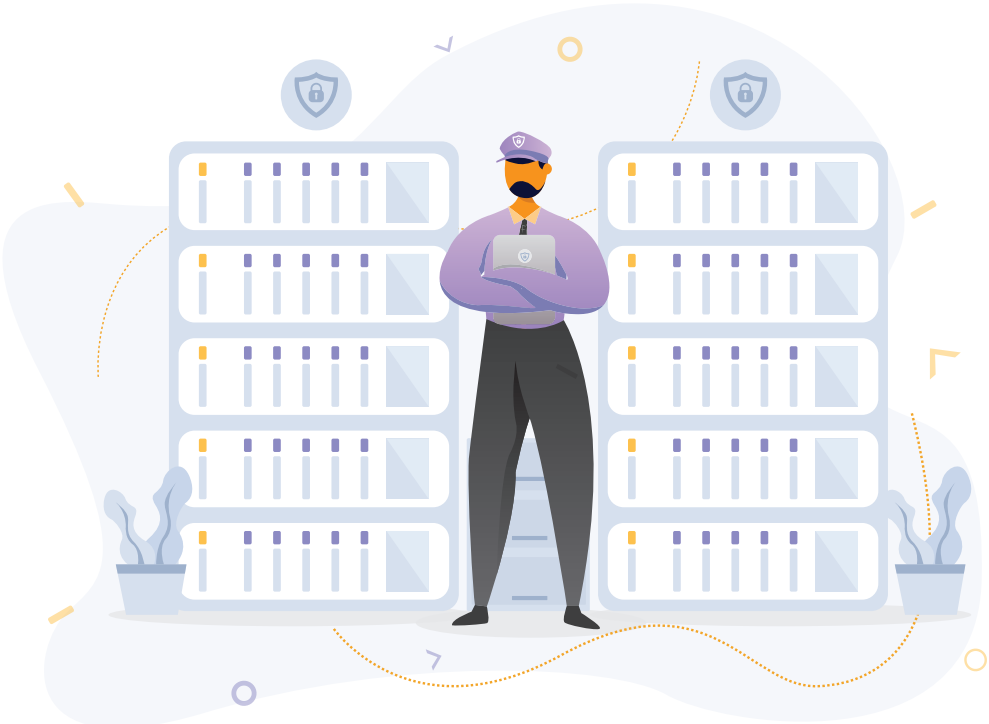
Livre: o consentimento deve refletir uma manifestação livre da vontade do titular. Ou seja, o titular dos dados não pode ser compelido a consentir com o tratamento.

Informado: o titular deve ter recebido informações claras, objetivas e suficientes para decidir de maneira consciente se concorda com o tratamento de seus dados pessoais para as finalidades mencionadas.

Inequívoco: o consentimento deve ser demonstrado de maneira inequívoca. Isso pode ser feito por escrito ou por outros meios que demonstrem a vontade do titular, desde que não deixem dúvidas (por exemplo, gravação de uma ligação telefônica). Consentimentos implícitos, que não tenham sido registrados, ou que deixem por algum motivo dúvidas sobre a vontade do titular, poderão ser desconsiderados.

Relacionado a uma finalidade determinada: o titular de dados deverá autorizar o tratamento de dados para uma finalidade específica. Autorizações genéricas ou vagas podem ser consideradas nulas.

Além de se atentar aos pontos acima, é muito importante que os profissionais se atentem ao fato de que o consentimento é **revogável** a qualquer tempo pelo titular de dados pessoais.



Posso tratar dados sem o consentimento do titular?

A LGPD traz nove hipóteses em que é possível tratar dados pessoais sem obter o consentimento do titular. Entre elas, as que possuem maior relevância aos profissionais de marketing são:

» **Cumprimento de obrigação legal ou regulatória:** se uma lei ou uma regulamentação setorial exige determinada atividade de tratamento de dados, não é preciso solicitar a autorização do titular de dados. É o caso, por exemplo, de registros de acesso a aplicações online para cumprir com as obrigações de retenção previstas no Marco Civil da Internet, legislação que exige que os últimos seis meses de atividade do usuário sejam registrados pelas empresas que oferecem funcionalidades online.

» Para **executar um contrato** ou procedimentos preliminares relacionados a um contrato celebrado com o titular de dados pessoais. Por exemplo, para entregar um produto ou um serviço adquirido após a conclusão da compra, naturalmente é preciso conhecer o nome completo, o endereço e outras informações de contato do consumidor. O tratamento desses dados pessoais é feito justamente para cumprir o contrato celebrado.

» Para o **exercício regular de direitos em processo judicial**, administrativo ou arbitral. Ou seja, o armazenamento ou outra forma de tratamento de dados pessoais para utilização em eventual processo judicial é possível, independente de autorização do titular. Por exemplo, pode ser necessário guardar o histórico de compras e dados de contato de consumidores em casos de litígios pós-venda.

» Para atender aos **interesses legítimos** da empresa responsável pelo tratamento ou aos interesses legítimos de terceiros, desde que o tratamento de dados não ofereça um risco importante aos direitos e liberdades fundamentais dos titulares de dados. Esses pontos são detalhados na seção seguinte, que trata especificamente do legítimo interesse, mas é importante compreender que a LGPD exige a análise do impacto à privacidade do titular de dados e a documentação dessa análise quando se utiliza o legítimo interesse.

As outras hipóteses previstas na LGPD envolvem tratamentos de dados para a proteção da vida ou da incolumidade física do titular dos dados ou de terceiro, para a proteção do crédito, para a tutela da saúde, ou situações específicas de tratamento de dados pela administração pública ou por órgão de pesquisa.

No caso de dados pessoais sensíveis, nem todas essas bases legais estão disponíveis – por exemplo, o legítimo interesse, a execução de contrato e a proteção do crédito não autorizam o tratamento de dados pessoais sensíveis. Nessas hipóteses, é recomendável avaliar se o tratamento de dados sensíveis realmente compensa a necessidade de cumprir com as exigências adicionais previstas na LGPD para esses casos.

Legítimo interesse

O tratamento de dados pessoais com base no legítimo interesse é, certamente, a hipótese mais abrangente e flexível prevista na LGPD. A lei não estabelece em quais situações existe ou não um *legítimo interesse* para tratar dados pessoais, e indica que essa análise deverá ser realizada a partir de situações concretas.

É mais provável que exista um legítimo interesse em situações em que o tratamento a ser realizado esteja dentro das expectativas razoáveis dos titulares de dados e tenham um pequeno impacto à sua privacidade, ou se houver uma justificativa relevante para o tratamento.

Existem três elementos que devem ser considerados:

i. identificar para quais finalidades o tratamento será realizado, e se essas finalidades são legítimas e consideradas a partir de situações concretas;

i. verificar se é realmente necessário realizar o tratamento de dados para atingir aquela finalidade, e

i. balancear o interesse legítimo identificado com os direitos e as liberdades fundamentais dos titulares de dados que sejam impactados por esse tratamento.

A LGPD não apresenta uma lista pré-estabelecida do que constitui ou não legítimo interesse, justamente por esta determinação acontecer de acordo com cada caso concreto específico. A LGPD cita como exemplos o apoio e a promoção de atividades do responsável pelo tratamento dos dados pessoais.

Isso significa que, em tese, o tratamento de dados pessoais para finalidades atreladas a atividades de marketing poderia ser realizado com fundamento no legítimo interesse, desde que observados os requisitos e os elementos indicados acima. Na prática, sempre será necessária uma análise detalhada de cada atividade de marketing e das maneiras e finalidades do tratamento para confirmar se é possível ou não utilizar o legítimo interesse como base legal.

Uma vez verificada a possibilidade de tratar dados pessoais com base no legítimo interesse, é necessário elaborar um relatório de impacto à proteção de dados pessoais (conhecido em inglês como *Data Protection Impact Assessment* – DPIA). Esse relatório deve descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades e aos direitos dos titulares de dados, bem como medidas, salvaguardas e mecanismos de mitigação de risco adotados. A Autoridade Nacional de Proteção de Dados poderá solicitar a apresentação desse relatório.

Dados de crianças e de adolescentes

O tratamento de dados pessoais de crianças (menores de 12 anos) só pode ser realizado com o consentimento específico e destacado de um dos pais ou do responsável legal. As demais hipóteses de tratamento de dados sem consentimento indicadas anteriormente neste guia não se aplicam ao tratamento de dados de crianças.

Já o tratamento de dados de adolescentes (entre 12 e 18 anos) pode ser realizado em qualquer das dez hipóteses previstas na LGPD (inclusive, por exemplo, para execução de um contrato do qual o titular de dados é parte, para cumprimento de obrigação legal ou para atender um interesse legítimo do responsável pelo tratamento). Quando o tratamento de dados de adolescentes for realizado com base no consentimento, é importante observar as regras de capacidade civil do sistema brasileiro: adolescentes entre 12 e 16 anos só podem consentir se representados por um dos seus pais (ou responsável legal), ao passo que adolescentes entre 16 e 18 anos precisam estar assistidos por um de seus pais (ou representante legal).

Em qualquer hipótese de tratamento de dados pessoais de crianças ou adolescentes, as informações sobre o tratamento devem ser fornecidas de maneira simples, clara e acessível, consideradas suas características físicas, perceptivas, sensoriais, intelectuais e mentais, com uso de recursos audiovisuais quando adequado.

As atividades de marketing devem levar em consideração se o tratamento de dados pessoais de crianças e adolescentes realmente compensam a necessidade de cumprir com as exigências adicionais previstas na LGPD para esses casos.

Governança

No contexto de adequação à LGPD e para garantir o efetivo cumprimento das suas disposições, é altamente recomendável que as empresas adotem programas de governança em privacidade.

Esses programas devem estabelecer, por exemplo, condições, regimes e procedimentos internos para o tratamento de dados pessoais, normas de segurança da informação, padrões técnicos, alocação de responsabilidades e obrigações aos diversos colaboradores envolvidos nas atividades de tratamento, ações educativas, mecanismos internos de supervisão e mitigação de riscos, procedimentos de resposta a incidentes de segurança, entre outros.

É também muito importante que todos os processos, decisões, esforços e ações relacionados à governança de dados pessoais na empresa sejam documentados e mantidos em arquivo para apresentação à ANPD, se necessário.

A adoção de políticas de boas práticas e governança não apenas auxilia a empresa a cumprir com as obrigações estabelecidas pela LGPD, como evidencia os esforços nesse sentido e será considerada (como um atenuante) na aplicação de penalidades em caso de descumprimento da LGPD.

Do ponto de vista prático, um programa de governança em privacidade deve:

a. demonstrar o comprometimento da empresa em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b. ser aplicável a todo o conjunto de dados pessoais que estejam sob o controle da empresa, independentemente do modo como se realizou sua coleta;

c. ser adaptado à estrutura, à escala e ao volume das operações da empresa, bem como à sensibilidade dos dados tratados;

d. estabelecer políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

e. ter o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

f. estar integrado a sua estrutura geral de governança de forma a estabelecer e aplicar mecanismos de supervisão internos e externos;

g. contar com planos de resposta a incidentes e remediação; e

h. ser atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

Aspectos internacionais da LGPD

A LGPD foi fortemente inspirada no Regulamento Geral de Proteção de Dados Europeu (*General Data Protection Regulation* – GDPR) que entrou em vigor na Europa em maio de 2018. Assim como o GDPR, a LGPD estabelece limitações à transferência internacional de dados pessoais para países que não ofereçam um grau de proteção de dados pessoais adequados aos previstos na LGPD. Essas limitações se aplicam inclusive às transferências internacionais decorrentes de serviços de cloud e armazenamento em datacenters localizados em outros países.

Esse sistema é conhecido como "adequação", e sua intenção é evitar que dados pessoais protegidos pela LGPD sejam enviados para países que ofereçam risco à privacidade dos seus titulares, sem que a Autoridade Nacional de Proteção de Dados necessite intervir.

Justamente por isso, a Autoridade Nacional de Proteção de Dados deverá indicar quais são os países que ela considera que oferecem grau adequado de proteção aos dados pessoais.

A LGPD estabelece hipóteses em que é possível transferir dados pessoais para outros países mesmo que não tenham sido reconhecidos como adequados pela Autoridade Nacional de Proteção de Dados.

Por exemplo, empresas que efetuam regularmente transferências internacionais deverão oferecer garantias por meio de contratos (que podem ser tanto cláusulas-padrão criadas pela Autoridade Nacional de Proteção de Dados, quanto normas corporativas globais criadas pela empresa e aprovadas pela ANPD).

Em outros casos, as empresas podem se valer do cumprimento de obrigação legal ou regulatória, da execução de contrato ou do exercício regular de direitos para efetuar a transferência internacional, ou podem contar com o consentimento específico e destacado do titular de dados pessoais para a transferência.

Do ponto de vista prático, antes de realizar qualquer transferência internacional de dados pessoais – mesmo que decorrentes da utilização de serviços de cloud – é importante analisar cuidadosamente se a transferência é permitida e qual o mecanismo legal será utilizado para justificá-la.

Além disso, como a LGPD se aplica a qualquer empresa, nacional ou estrangeira, que queira tratar dados pessoais de pessoas localizadas no território brasileiro, inclusive no contexto do oferecimento de produtos ou serviços, é importante que os profissionais de marketing se atentem que eventuais parceiros comerciais estrangeiros também estarão sujeitos à LGPD se efetuarem o tratamento de dados pessoais de titulares nessas condições.

Violações e sanções

Violações à LGPD estão sujeitas a sanções administrativas, a serem aplicadas pela Autoridade Nacional de Proteção de Dados, após processo administrativo, sem prejuízo de outras sanções ou penalidades civis ou criminais.

As duas principais sanções são:

i. multa de até 2% do faturamento do grupo econômico no Brasil no último exercício, até o limite de R$ 50.000.000,00 por infração, e

ii. publicização da infração, ou seja, determinação da Autoridade Nacional de Proteção de Dados para que a violação da LGPD seja amplamente divulgada em meios de comunicação, para conhecimento do público.

Em outras palavras, além de eventual prejuízo financeiro, violar a LGPD pode acarretar danos reputacionais significativos, prejudicando a imagem e as marcas da empresa perante seus consumidores e clientes.

Além disso, a Autoridade Nacional de Proteção de Dados poderá aplicar advertência, com prazo para a adoção de medidas corretivas e, em casos mais graves, determinar o bloqueio temporário ou a eliminação definitiva dos dados pessoais a que se refere a infração.

Pontos de atenção e perguntas frequentes

Quando a LGPD não se aplica?

A LGPD não é aplicável ao tratamento de dados de pessoas jurídicas e nem de dados anonimizados, já que nenhum desses dados é considerado *dado pessoal*.

A LGPD também não se aplica ao tratamento de dados pessoais realizado:

- por pessoa natural para fins exclusivamente particulares e não econômicos;
- para fins exclusivamente jornalísticos, artísticos ou acadêmicos;
- para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais.

Existem dados pessoais que exigem mais proteção do que outros?

Sim, o tratamento de algumas categorias de dados pessoais oferece maiores riscos de danos aos respectivos titulares e por isso são tratados pela LGPD como "dados sensíveis".

São considerados dados sensíveis pela LGPD: 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 genético ou biométrico. É importante observar que a fotografia do rosto de uma pessoa pode ser considerada dado biométrico.

Em boa parte dos casos, profissionais de marketing deverão obter o consentimento dos titulares de maneira específica para poder tratar dados sensíveis.

Posso reaproveitar bases de dados existentes para desenvolver novos produtos/serviços?

Cuidado. Se os dados foram coletados com base no consentimento para um uso específico e esse consentimento não previa o desenvolvimento desses novos produtos ou serviços, provavelmente será necessário obter um novo consentimento dos titulares de dados pessoais.

Alternativamente, é necessário verificar se o tratamento de dados pessoais realizado para o desenvolvimento desses novos produtos ou serviços poderia ser enquadrado em uma das outras nove hipóteses em que é permitido tratar dados pessoais sem consentimento, e se atende aos princípios estabelecidos na LGPD, destacadamente aos da transparência, finalidade, adequação e necessidade.

Posso usar dados públicos à vontade?

Dados pessoais publicamente disponíveis – seja porque foram tornados públicos pelo titular, seja porque encontram-se em bases de acesso público – não deixam de ser dados pessoais. Nesses casos, a LGPD permite que dados pessoais sejam utilizados sem necessidade de obtenção de consentimento do titular, mas continua sendo necessário enquadrar esse tratamento em uma das outras bases legais disponíveis e observar todos os direitos dos titulares de dados e os princípios estabelecidos pela LGPD.

Ou seja, é necessário dar transparência ao tratamento desses dados publicamente disponíveis e às finalidades do tratamento, enquadrar o tratamento em uma base legal, franquear ao titular acesso a informações sobre quais dados pessoais estão sendo tratados, como e porque, entre outras obrigações aplicáveis.

E dados anônimos?

Dados anônimos não são considerados dados pessoais e, a princípio, não estão sujeitos à LGPD. É importante, no entanto, confirmar se os dados podem realmente ser considerados anônimos. Em muitas ocasiões, dados aparentemente anônimos podem ser facilmente re-identificados.

Por exemplo: há situações em que os dados pessoais passam por procedimentos que removem identificadores pessoais (como nome e CPF), os quais são substituídos por números, códigos ou hashes, criando-se uma nova base de dados. Porém, se o detentor dessa base de dados também tiver acesso à base original identificada (como, por exemplo, quando uma mesma empresa cria diferentes bases de dados com informações pessoais removidas para que diferentes áreas de negócio trabalhem com elas), ou possa cruzar informações de outras bases de dados às quais têm acesso para identificar os titulares, essa base de dados supostamente anonimizada será, em verdade, considerada apenas pseudonimizada, aplicando-se normalmente a LGPD.

O que fazer em caso de um incidente de segurança?

Incidentes de segurança que possam acarretar risco ou dano aos titulares de dados devem ser comunicados à Autoridade Nacional de Proteção de Dados e aos respectivos titulares de dados. A LGPD estabelece o conteúdo mínimo que deve constar da notificação.

Além disso, a Autoridade Nacional, ao verificar a gravidade do incidente, poderá determinar providências adicionais, tais como a ampla divulgação do fato em meios de comunicação e medidas para reverter ou mitigar os efeitos do incidente.

Toda empresa deve criar e manter um plano de resposta a incidentes, definindo como agir interna e externamente nessas situações.

Quais os cuidados envolvendo criação de perfis (profiling)?

Em primeiro lugar, o titular dos dados pessoais tem o direito de solicitar a revisão de seus perfis (de comportamento, consumo, dentre outros) formados de maneira automatizada (por exemplo, por algoritmos).

Outro ponto de atenção envolvendo a formação de perfis é a dificuldade em torná-los anônimos. Perfis compostos por um grande volume de informações, ainda que que não estejam atribuídas a um identificador pessoal como nome, CPF ou RG, por vezes possibilitam a identificação da pessoa a quem se referem por meio de inferências. Isso porque, quanto maior o volume e mais específicas as informações acerca de uma pessoa (ainda que não identificada), menor o universo de indivíduos a quem aqueles dados podem ser atribuídos.

Por exemplo, em uma primeira análise, alguém poderia considerar que informações sobre os hábitos de deslocamento de pessoas não identificadas seriam consideradas informações anônimas. No entanto, se esses hábitos forem detalhados ao ponto de se identificar trajetos, rotinas e endereços específicos, a pessoa pode se tornar facilmente identificável e esse perfil não poderá ser considerado anônimo.

Eu posso ser responsabilizado por atos de terceiros?

Sim. Todos os profissionais ou empresas que tomarem decisões e estiverem diretamente envolvidos nas atividades de tratamento de dados pessoais realizadas em violação à lei serão solidariamente responsáveis pelo ressarcimento dos danos causados aos titulares, salvo se puderem provar que (i) não realizaram o tratamento de dados pessoais que lhes é atribuído, ou (ii) embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados, ou (iii) o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros.

Por esses motivos, é bastante importante trabalhar com parceiros comerciais que estejam buscando se adequar à LGPD, já que eventual desconformidade alheia pode, conforme as circunstâncias do caso, acarretar responsabilidade solidária.

A LGPD passa a valer em 2020. E como ficam as regras do Marco Civil da Internet?

O Marco Civil da Internet (Lei 12.965/2014), em vigor desde junho de 2014, estabelece que o usuário da Internet tem direito ao seguinte:

i. não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

ii. informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

iii. consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais, e

iv. exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros.

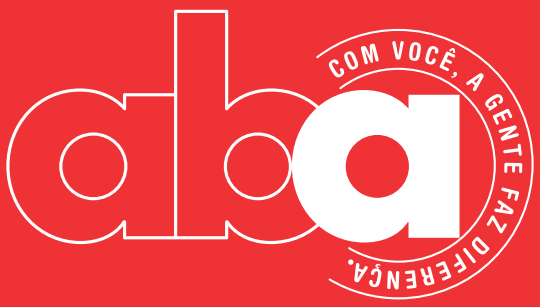
A LGPD, porém, regula todas as atividades de tratamento de dados pessoais, inclusive nos meios digitais.

Isso significa que, até a entrada em vigor da LGPD, continuam válidas as regras do Marco Civil da Internet para atividades de marketing realizadas online. Posteriormente, espera-se que a LGPD substitua as regras do Marco Civil da Internet, de forma a evitar conflitos entre as duas leis.

Checklist

Até agosto de 2020, os profissionais e as empresas de marketing precisam adaptar seus processos à LGPD. As seguintes medidas são os primeiros passos para esse projeto de adequação:

- Realizar um mapeamento geral de todas as atividades que envolvem tratamentos de dados pessoais, incluindo processos de coleta, armazenamento e compartilhamento, verificando, também, se há tratamento de dados pessoais sensíveis.
- Definir as bases legais mais apropriadas para o tratamento de dados, conforme a finalidade específica (consentimento, legítimo interesse, execução de contrato, cumprimento de obrigação legal ou regulatória, etc).
- Analisar se há discrepâncias entre as obrigações legais e as atividades da empresa e definir quais estratégias adotar para adequação.
- Alocar responsabilidades internas para execução das ações necessárias.
- Implementar ferramentas que permitam aos titulares de dados pessoais exercerem seus direitos garantidos pela LGPD.
- Elaborar, revisar, adaptar e aditar contratos que envolvam tratamento e/ou compartilhamento de dados pessoais, tanto nas relações com usuários e consumidores, quanto nas relações com fornecedores e parceiros comerciais.
- Elaborar relatórios de impacto à proteção de dados pessoais nos casos de tratamento baseado em legítimo interesse e em outras situações em que isso seja recomendável.
- Elaborar e revisar políticas internas, planos de resposta a incidentes e outros documentos sobre privacidade e proteção de dados pessoais.
- Revisar e implementar técnicas e procedimentos de segurança da informação e programas de privacidade desde a concepção e como padrão (*privacy by design/by default*).
- Estabelecer um programa de governança em proteção de dados pessoais.



WFA World Federation of Advertisers

Filiada à WFA
World Federation of Advertisers

wfanet.org
info@wfanet.org
+32 2 502 57 40

twitter @wfamarketers
youtube.com/wfamarketers
linkedin.com/company/wfa

ABA
Associação Brasileira de Anunciantes

aba.com.br
contato@aba.com.br
+55 11 3283-4588

bit.ly/facebook-aba
twitter.com/abatransformar/
instagram.com/abatransformar/
bit.ly/linkedin-aba