

# Guia GDPR para Profissionais de Marketing

Cinco conceitos que todo profissional de marketing deve saber sobre a Regulamentação Geral de Proteção de Dados.



No dia 25 de maio de 2018, a Regulamentação Geral de Proteção de Dados (GDPR, da sigla em inglês) passou a ser aplicada a qualquer empresa que ofereça bens ou serviços a consumidores na União Europeia, ou monitore o comportamento de pessoas no continente. Porém, mesmo se tratando de uma legislação para proteger dados da população que está na Europa, as companhias que estão fora do território e coletam, processam ou armazenam essas informações, também são impactadas pela nova lei.

A criação destas novas normas é encarada como importante ferramenta de proteção à privacidade das pessoas que fornecem dados às empresas, permitindo, por exemplo, identificar um usuário (nome, endereço, e-mail, geolocalização, endereço de IP etc.), crenças filosóficas ou religiosas, opinião política, origem étnica ou racial, orientação sexual, dados biométricos ou de saúde, associação sindical, entre outros pontos.

Além disso, a GDPR demanda das empresas a transparência. As companhias deverão sempre deixar o público informado, de forma clara e objetiva, qual a finalidade de seus dados estarem sendo coletados. E ainda exige a exclusão de tais informações logo após a utilização das mesmas. O descumprimento da regulamentação pode gerar penalidades rigorosas.

“A importância da privacidade de dados, na era digital que vivenciamos, reflete-se no impacto que gera na comunicação das marcas via *web*, especialmente com a entrada em vigor da Lei de Proteção de Dados Pessoais (GDPR) na União Europeia, o que determinou uma atenção especial do Comitê Jurídico da ABA. Seus integrantes passaram a trabalhar no desenvolvimento de alternativas que pudessem facilitar a compreensão dessas mudanças pelos profissionais das empresas associadas, pois, mesmo sendo uma regulação estrangeira, pode impactar empresas que fazem negócios na Europa”, ressalta Vanessa Vilar, Legal Director LATAM – Cluster Category Counsel da Unilever e Presidente do Comitê Jurídico.

Ciente da importância da privacidade e das relações entre marcas e consumidores em bases transparentes, a ABA vem orientando seus associados a lidar com a nova lei, que impacta empresas com operações globais e, em especial, a atividade dos profissionais de marketing, cada vez mais orientada pelo uso de dados.

Através da atuação do seu Comitê Jurídico, a entidade tem debatido a nova legislação em seus fóruns, lançou o infográfico “GDPR – 10 Coisas que Você Precisa Saber” e traduziu o vídeo disponibilizado pela WFA sobre o assunto.

Neste momento, apresentamos ao mercado brasileiro o “Guia GDPR para Profissionais de Marketing”, desenvolvido pela World Federation of Advertisers (WFA), com apoio da Hunton & Williams, e adotado pelo Comitê Jurídico.

“A atuação baseada em ética e marketing responsável está no nosso DNA e é um compromisso de todas as empresas associadas. Nesse sentido, não medimos esforços para que os gestores de marcas estejam preparados para lidar com as mudanças necessárias dentro das suas organizações, bem como de seus parceiros, para proteger os dados de seus consumidores. Em um momento no qual a confiança é um fator primordial no relacionamento entre marcas e pessoas, este “Guia GDPR para Profissionais de Marketing” está alinhado com nosso propósito de mobilizar o marketing para transformar os negócios e a sociedade”. – João Branco, Diretor de Marketing do McDonald’s e Presidente da ABA.

Atenciosamente,

Sandra Martinelli  
Presidente Executiva

## Resumo Executivo

A partir de maio de 2018, a Regulamentação Geral de Proteção de Dados (GDPR) exigirá que todas as empresas façam mudanças expressivas na forma como coletam e processam dados de consumidores. Isso deve ter um impacto significativo nos profissionais que usam dados de consumidores para executar campanhas publicitárias direcionadas.

A GDPR aplica-se a qualquer empresa que ofereça bens ou serviços a consumidores na União Europeia ou monitore<sup>1</sup> o comportamento de pessoas na Europa. Isso significa que a maioria das empresas globais será afetada, mesmo as que não são sediadas na Europa. As empresas podem enfrentar multas elevadas caso não cumpram. Essas multas podem atingir até 4% do faturamento global anual da empresa, o que, para as empresas da Global 500, poderia significar multas variando de US\$ 800 milhões a até US\$ 19,2 bilhões.

Em uma pesquisa de 2017 com membros da WFA, 94% das empresas, que representam mais de US\$ 20 bilhões em gastos com anúncios globais disseram que a GDPR era importante para sua organização. No entanto, 70% disseram que os profissionais de

marketing em sua organização não estavam totalmente cientes das implicações da GDPR para futuras campanhas de marketing.

Este guia, desenvolvido com o apoio da Hunton & Williams LLP, visa ajudar a resolver essa lacuna, destacando cinco áreas-chave do GDPR que os profissionais de marketing devem estar cientes a fim de se preparar.

*“A GDPR é extremamente importante para a nossa empresa, pois afetará nossas operações globais em todo o mundo. A Philips está investindo recursos significativos para atender aos requisitos da GDPR e ajudar os profissionais de marketing a entender as implicações para o seu dia-a-dia de trabalho”*

**Blake Cahill**  
SVP de Global Digital  
Marketing & Media, PHILIPS

# Conteúdo

<b>Resumo Executivo</b>	2
<b>Sobre esse Guia</b>	3
<b>Por que a GDPR é importante para profissionais de marketing?</b>	3
	4 Consentimento
	5 E se o consentimento não for uma opção?
	5 Transparência
	7 Processando dados de crianças
	7 Reutilizando dados para outros fins
<b>Checklist</b>	8
<b>Considerações adicionais</b>	8

## Sobre esse Guia

A Regulamentação Geral de Proteção de Dados (GDPR) é uma importante norma de privacidade. Será aplicável a partir de 25 de maio de 2018. É provável que ela tenha um impacto significativo em quase todas as grandes multinacionais, uma vez que se aplica a qualquer empresa que ofereça bens ou serviços a consumidores na UE ou monitore o comportamento de consumidores na Europa. Essas empresas podem ser obrigadas a alterar substancialmente a maneira como coletam e usam os dados de consumidores. Do ponto de vista de proprietários de marcas, a GDPR exigirá um foco maior em como as marcas se comunicam com os consumidores sobre sua privacidade e pode limitar a forma como alguns dados de consumidores podem ser usados para desenvolver o marketing personalizado.

O Guia GDPR para profissionais de marketing da WFA destaca alguns dos elementos-chave do GDPR que provavelmente afetarão os proprietários de marcas e fornece sugestões concretas sobre como os profissionais de marketing devem pensar sobre sua abordagem à privacidade no contexto da GDPR. Embora este guia não seja exaustivo, o objetivo é destacar algumas áreas em que os profissionais de marketing podem começar a pensar em novas abordagens e iniciar discussões com os especialistas técnicos relevantes em suas organizações (por exemplo, conformidade, jurídico e governança digital) para saber mais sobre a abordagem da sua empresa à GDPR. **Este guia destina-se a complementar, em vez de substituir ou constituir aconselhamento jurídico.**

## Por que a GDPR é importante para profissionais de marketing?

### 1. A GDPR vai mudar significativamente como e quando empresas podem usar dados de consumidores

A Europa é frequentemente vista como uma região com algumas das mais rígidas regras de proteção de dados do mundo e a GDPR confirma essa imagem fortalecendo as proteções de privacidade existentes para os consumidores. Isso inclui um foco muito mais forte na obtenção de consentimento significativo dos consumidores para o uso de seus dados pessoais, incluindo requisitos rigorosos para as empresas melhorarem a maneira como explicam aos consumidores como seus dados serão usados.

### 2. A GDPR afetará a maioria das grandes empresas multinacionais.

A GDPR aplica-se a qualquer empresa que ofereça bens ou serviços a consumidores na UE ou monitore o comportamento de pessoas

na Europa. Isso significa que a maioria das empresas globais será afetada, mesmo que sua sede global não esteja na Europa.

### 3. Empresas correm o risco de pagar multas pesadas pelo descumprimento.

As sanções pelo não cumprimento da GDPR incluem multas que podem chegar a 4% do faturamento global anual de uma empresa. Para as empresas da Global 500, isso pode significar multas variando de US\$ 836 milhões até US\$ 19,2 bilhões. Além das multas regulamentares, a GDPR também abre a possibilidade de os consumidores e organizações sem fins lucrativos apresentarem processos judiciais para compensação no caso de processamento de dados em violação à GDPR.

## Consentimento

A GDPR dá um foco especial ao empoderamento de consumidores, deixando-os decidir como seus dados pessoais podem ser usados pelas empresas. O consentimento já é um dos fundamentos legais em que as empresas podem se apoiar para justificar o processamento de dados pessoais. Entretanto, a GDPR possui condições novas e extensivas para que o consentimento seja válido.

Com isso, é provável que consumidores sejam cada vez mais consultados a respeito de seu consentimento, já que este será necessário para cada propósito no qual a empresa queira processar os dados pessoais coletados. Além disso, será necessário dar aos

consumidores a possibilidade de cancelar seu consentimento a qualquer momento. Esses requisitos podem atrapalhar a experiência *online* dos consumidores, causar irritação ou, em alguns casos, levar à recusa do consentimento.

Em muitos casos, entretanto, uma permissão genérica dada por um “*check*” em um “*opt-in*” no ato da inscrição para receber um serviço pode não ser mais suficiente. De acordo com as novas regras, o consentimento deve ser **livre, específico, informado e inequívoco**, dada por meio de uma declaração ou ação afirmativa clara.

### Livre

Consumidores não podem ser forçados a dar seu consentimento para a coleta e o processamento de seus dados para assinar um serviço, a não ser que esses dados sejam necessários à prestação do serviço.

### Específico

Em muitos casos, não será mais suficiente a permissão dada pelo “*check*” em uma caixa que cubra de forma genérica o uso de dados relacionado a uma política de privacidade. Consumidores também precisarão aceitar especificamente o uso de seus dados para determinadas finalidades.

### Informado

Empresas precisarão detalhar para os consumidores como seus dados serão usados. Para mais informações, leia o **Capítulo 3: Transparência**.

### Inequívoco

O consentimento deve ser uma indicação clara de que um consumidor está de acordo com o uso de seus dados. É improvável que métodos “passivos” de consentimento (ex.: continuar usando um site sem ler o aviso de privacidade) sejam considerados inequívocos e suficientes.

As marcas anunciantes deverão estar aptas a demonstrar que o consentimento foi dado conforme essas condições, ainda que tenham sido coletados por um terceiro. É importante que os times de Marketing e Jurídico trabalhem com parceiros de agências e outros terceiros para assegurar que isso seja possível.

Na maioria dos casos, será necessário obter **consentimento expresso** para executar qualquer tipo de “perfilamento” (*profiling*). Consentimento expresso significa que os consumidores devem ter a possibilidade de concordar ou discordar com o uso de seus dados pessoais para determinada finalidade específica por meio de uma declaração afirmativa clara.

O consentimento expresso também será necessário para o processamento do que o GDPR chama de “categorias especiais” de dados, os quais são considerados particularmente sensíveis. Isso inclui:

- Dados pessoais que revelem a origem étnica ou racial, opiniões políticas, crenças religiosas, filosóficas ou filiação sindical, em uma larga escala.
- Dados genéticos<sup>2</sup> ou biométricos<sup>3</sup> que identifiquem unicamente a pessoa.
- Dados relacionados a saúde<sup>4</sup>, vida sexual ou orientação sexual.
- Dados relacionados a condenações e infrações penais.

### Próximos passos:

- Revise os acervos digitais com o departamento jurídico e, quando necessário, atualize o que for necessário para se adaptar às novas regras sobre consentimento.
- Revise as práticas das agências e outros terceiros para verificar se estão de acordo com o GDPR.

## E se o consentimento não for uma opção?

O consentimento não é o único fundamento legal que pode ser usado para o processamento de dados pessoais. A GDPR também permite que dados pessoais sejam processados, quando necessário, para atender a determinado “interesse legítimo” da empresa sem precisar de um consentimento.

Isso pode ser muito relevante em casos onde conseguir o consentimento do consumidor não seria uma opção viável (ex.: a empresa não possui um contato direto com o consumidor para pedir o seu consentimento).

Por exemplo, em alguns casos, a empresa pode argumentar que há um interesse legítimo em processar os dados de um cliente, desde que haja uma relação relevante e apropriada entre eles.

Entretanto, para se apoiar no “interesse legítimo”, o Marketing deve

trabalhar em conjunto com o jurídico para avaliar o risco envolvido, levando em consideração:

- Um balanço entre o legítimo interesse da empresa e o direito à privacidade do consumidor (ou outros direitos fundamentais).
- Se um consumidor esperaria que seus dados pessoais fossem processados nessa situação, com base em seu relacionamento com a empresa.

Em casos de dados processados com base no “interesse legítimo”, tais interesses deverão ser explicados aos consumidores (ex: na política de privacidade da empresa).

O Departamento de Marketing deve trabalhar com o jurídico para descobrir se o interesse legítimo é um fundamento legal possível para o processamento de dados em cada situação.<sup>5</sup>

### Próximos passos:



Revise caso a caso com o departamento legal quando que é necessário ter o consentimento para usar dados coletados em campanhas de marketing.

## Transparência

A transparência é um dos princípios-chave da lei de proteção de dados da União Europeia e a GDPR introduz obrigações de transparência adicionais para as empresas. Ela requer que as empresas forneçam aos consumidores informações sobre diversos elementos acerca de como seus dados estão sendo usados (ou planejando usá-los). A GDPR também define que a informação sobre como os dados estão sendo processados seja provida de uma forma concisa e inteligível, usando uma linguagem clara e concisa.

Esses requisitos criam um equilíbrio difícil para os profissionais do Marketing. De um lado, as informações precisam ser fornecidas com detalhes aos consumidores, porém isto deve ser feito de uma maneira que não seja de difícil entendimento. Os departamentos de Marketing precisarão explorar maneiras criativas para colocar isso em prática em suas campanhas Digitais.

Em fevereiro de 2017, a WFA conduziu um workshop, Digital Governance Exchange (DGX), para compartilhar ideias e melhores práticas de como, onde e quando o consentimento deve ser coletado, criando as melhores condições para que os consumidores tenham transparência, poder de escolha e controle sobre seus dados pessoais. Foram levantados seis pontos principais durante a sessão, que podem ser úteis na implantação da Transparência.

## FAÇA ALGO VISUAL

- A ideia do “*emoji*”: usar símbolos para fácil entendimento para explicar políticas de privacidade.
- Conte uma história/vídeos curtos em vez de utilizar um texto.

## DEIXE CURTO E SIMPLES

- Use apenas uma linguagem que poderia ser compreendida por uma pessoa de 13 anos de idade.
- Seja relevante.
- Destaque o que é importante e habilite atalhos para “Saiba mais”.

## NÃO ME PERTUBE

- Apenas peça por consentimento quando for necessário.
- Não seja intrusivo - não entre no caminho da experiência de uso.

## QUERO MUDAR DE IDEIA

- Crie sistemas de uso fácil para deixar que os usuários controlem todas as configurações de privacidade em um único lugar. Exemplos: planilhas, centros de notificações e “*task bars*”.
- Botão ‘Eu me arrependo’ - dê aos usuários a chance de cancelar seu consentimento sempre que ele desejar.

## DEIXE FÁCIL

- Faça com que seja mais fácil sair de determinada base de dados do que entrar.
- “*Opt-in*” e “*Opt-out*” de forma simples (exemplo: deslizar em vez de clicar).

## DIGA-ME O QUE VOCÊ VAI FAZER

- Explique aos usuários porque você quer seus dados sempre que você pedir.
- Explique as consequências/implicações de dizer “sim” ou “não”.
- Explique as consequências/implicações de dizer “sim” ou “não”. Explique claramente a “moeda de troca”. Exemplo: 1 vídeo de música = 10 segundos de anúncio.

### Próximos passos:

- Explore formas criativas de falar sobre privacidade em conteúdo digital.

## Processando dados de crianças

Para processar dados pessoais de crianças, o consentimento dos pais será requerido<sup>6</sup>. A GDPR estabelece a idade de uma criança em ‘abaixo de 16 anos de idade’, contudo reguladores nacionais em países da UE podem optar por baixar este limite para algo entre 13 e 16 anos de idade.

Isto significa que as empresas precisarão adotar mecanismos para pedir e verificar o consentimento dos pais. Mesmo que reguladores nacionais em alguns países da UE possam decidir baixar o limite de idade de modo que o consentimento dos pais seja necessário, as empresas devem estar preparadas para implementar estes mecanismos para crianças de até 16 anos de idade.

A GDPR não estabelece detalhes específicos sobre como verificar que o consentimento dos pais seja válido. Inicialmente, empresas que têm serviços ou produtos que apelam primariamente às crianças podem querer mobilizar seus departamentos legais ou de assuntos públicos para contatar a autoridade de proteção de dados em sua jurisdição para solicitar orientação sobre como implementar estas medidas.

### Próximos passos:

- Revisar todas as campanhas e/ou ativos digitais que possam envolver o uso de dados de crianças (com menos de 16 anos) na medida em que o consentimento dos pais seja necessário.

## Reutilizando dados para outros propósitos

Em muitos casos, dados pessoais são coletados com um propósito específico em mente, como a assinatura para recebimento de uma *newsletter*. Contudo, profissionais de marketing podem ter interesse em usar esses dados para desenvolver *insights* que podem ser usados em outras campanhas de marketing ou para direcionar mensagens similares sobre outros produtos ou serviços. A GDPR permite isso apenas sob circunstâncias específicas.

Se não for possível (ou apropriado) pedir o consentimento do consumidor novamente, profissionais de marketing precisarão trabalhar com seus times jurídicos para fazer uma análise sobre

se os dados podem ser usados para outros propósitos sem consentimento. Esta análise precisará levar em consideração:

- Qualquer ligação entre os propósitos para os quais os dados foram originalmente coletados e os usos futuros que os profissionais de marketing possam vislumbrar.
- O contexto no qual os dados foram originalmente coletados.
- As expectativas razoáveis dos consumidores, baseadas em sua relação com a empresa.
- Se os dados são ‘críticos’.
- As possíveis consequências de uso destes dados para novos propósitos.
- Se os dados foram anonimizados, criptografados ou protegidos de outras formas.

### Próximos passos:

- Quando pretender reutilizar dados coletados de campanhas históricas, discuta com sua equipe jurídica para checar se isso ainda é possível.

## ✓ Checklist

Quando a GDPR for aplicada em todos os países da UE, em 25 de maio de 2018, profissionais de marketing deverão estar preparados para as mudanças destacadas neste guia. Para se prepararem, profissionais de marketing devem pensar em tomar, ao menos, as seguintes medidas:

- Explorar formas criativas de integrar informações sobre privacidade em campanhas de marketing *online* e ativos digitais.
- Revisar os ativos digitais com o jurídico e, onde necessário, atualizar todos os pontos de contato com o consumidor para refletirem as novas regras sobre consentimento.
- Revisar todas as campanhas e/ou ativos digitais que possam envolver o uso de dados de crianças (abaixo de 16 anos) na medida em que o consentimento dos pais for necessário.
- Revisar, caso a caso, com a equipe jurídica se o consentimento é necessário para usar dados coletados via campanhas de marketing.
- Quando pretender reutilizar dados coletados de campanhas históricas, discutir com sua equipe jurídica para checar se isso ainda é possível.
- Revisar práticas de coleta de dados de agências e outros terceiros para verificar o cumprimento da GDPR.

## Considerações adicionais

A próxima seção aborda diversos outros elementos da GDPR que, apesar de provavelmente terem menos impacto direto sobre profissionais de marketing, são úteis como conhecimento sob a

perspectiva da empresa. Para mais informações sobre como sua organização está se preparando para implementar os seguintes requerimentos, sugerimos que contatem suas equipes jurídicas.

## Responsabilidade

A GDPR requer que as empresas implementem várias medidas para demonstrar conformidade, incluindo as seguintes:

**Algumas empresas serão obrigadas a apontar um responsável pela proteção de dados (Data Protection Officer - DPO)** para supervisionar todas as atividades de processamento de dados. Este requerimento se aplica apenas a empresas cujas atividades-fim envolvem:

- Monitorar pessoas regularmente de uma forma sistemática ou em ‘grande escala’.  
OU
- Processar dados pessoais que revelem origens étnicas ou raciais, opiniões políticas, crenças religiosas ou filosóficas, ou associações a sindicatos ‘em grande escala’.  
OU

- Processar dados genéticos<sup>7</sup> ou biométricos<sup>8</sup> para identificar ou individualizar uma pessoa, ‘em grande escala’.  
OU
- Processar dados relacionados à saúde<sup>9</sup>, vida sexual ou orientação sexual, ‘em grande escala’.  
OU
- Processar dados relativos a condenações e ofensas criminais, ‘em grande escala’.

As empresas precisarão verificar se elas se encaixam em alguma das categorias acima para decidir se são legalmente obrigadas a apontarem um *Data Protection Officer*<sup>10</sup>.



**As empresas deverão implementar um Sistema interno para realizar análises de impacto de proteção de dados** antes de fazer qualquer processamento de dados que possa resultar em alto risco de privacidade para os indivíduos<sup>11</sup>. Profissionais de marketing devem trabalhar com suas equipes jurídicas para entender como e quando acionar uma análise de impacto de proteção de dados para projetos futuros.

**As empresas terão que manter registros internos de suas atividades de processamento por escrito,**

contudo, empresas com menos de 250 funcionários podem ser dispensadas desta prática (sob certas condições). A GDPR oferece uma lista de informações que precisarão ser incluídas nestes registros.

**As empresas sem uma base na UE precisarão apontar um representante em um único país da UE** que atuará como ponto de contato para as autoridades de proteção de dados.

## Direitos dos consumidores

**As empresas deverão assegurar que sistemas sejam implementados para responder a pedidos de consumidores sobre seus dados pessoais.** Consumidores terão direito de pedir às empresas a que lhes deem acesso aos seus dados, e a pedir que estes sejam deletados, corrigidos ou lhes devolvido (sob certas condições). Os consumidores também poderão,

sob certas condições, opor-se ao processamento de seus dados pessoais e terem seus dados pessoais devolvidos a eles. Eles também podem solicitar que seus dados sejam transferidos para outra empresa. As empresas deverão estar preparadas para responder a estes pedidos ‘sem atraso indevido’ e atualizar seus sistemas de TI de acordo.

## Notificações de violações de dados

**Quaisquer incidentes de segurança relacionados a dados pessoais (como invasão ou vazamento)<sup>12</sup> deverá ser notificado dentro de 72 horas** à respectiva autoridade de proteção de dados. Em alguns casos, será necessário notificar consumidores diretamente.

O curto prazo para notificação irá requerer que as empresas respondam muito rápido a quaisquer suspeitas de incidentes de segurança relacionados a dados pessoais e pode ter implicações sobre a reputação de uma marca.

Profissionais de marketing devem considerar trabalhar com o jurídico, TI e outras partes do negócio para desenvolver uma estratégia de comunicação-padrão para responder a incidentes de segurança relacionados a dados pessoais. Isso pode envolver o desenvolvimento de técnicas e ideias sobre como notificar consumidores diretamente com o mínimo prejuízo à reputação da marca.

## Sanções

**Empresas enfrentarão multas de até 4% do faturamento global anual<sup>13</sup> ou €20 milhões<sup>14</sup>** pelo descumprimento da GDPR, qual destes seja o mais alto.

Consumidores e organizações sem fins lucrativos também poderão apresentar processos judiciais contra empresas pela violação à GDPR.

## Contato

Por favor, contate **Catherine Armitage, Senior Public Affairs Manager**, para maiores informações (c.armitage@wfanet.org, +32 470 367677)

# Notas

<sup>1</sup>“Monitorar” significa, por exemplo, o rastreamento de indivíduos *online*.

<sup>2</sup>Os dados genéticos são definidos na GDPR como “todos os dados pessoais relativos às características genéticas de um indivíduo [...] que fornecem informações exclusivas sobre a fisiologia ou a saúde desse indivíduo”.

<sup>3</sup>Os dados biométricos são definidos na GDPR como “quaisquer dados pessoais relativos às características físicas, fisiológicas ou comportamentais de um indivíduo que permitem ou confirmam a identificação única desse indivíduo”, por ex., imagens faciais ou dados datiloscópicos (impressões digitais).

<sup>4</sup>Os dados referentes à saúde são definidos na GDPR como “dados pessoais relacionados à saúde física ou mental de um indivíduo que revelam informações sobre seu estado de saúde”. Isso inclui informações sobre a prestação de serviços de saúde.

<sup>5</sup> Para obter mais informações sobre o conceito de “interesse legítimo”, consulte o artigo 29. Parecer do Grupo de Trabalho de Proteção de Dados 06/2014 sobre a noção de interesses legítimos do responsável pelo tratamento de dados.

<sup>6</sup> A menos que outros fundamentos legais possam ser usados, consulte o Capítulo 2: E se o consentimento não for uma opção?

<sup>7</sup>Os dados genéticos são definidos na GDPR como “todos os dados pessoais relativos às características genéticas de um indivíduo [...] que fornecem informações exclusivas sobre a fisiologia ou a saúde desse indivíduo”.

<sup>8</sup> Os dados biométricos são definidos na GDPR como “quaisquer dados pessoais relativos às características físicas, fisiológicas ou comportamentais de um indivíduo que permitem ou confirmam a identificação única desse indivíduo”, por ex. imagens faciais ou dados datiloscópicos (impressões digitais).

<sup>9</sup> Os dados referentes à saúde são definidos na GDPR como “dados pessoais relacionados à saúde física ou mental de um indivíduo que revelam informações sobre seu estado de saúde”. Isso inclui informações sobre a prestação de serviços de saúde.

<sup>10</sup> Além disso, as empresas deverão também avaliar os requisitos específicos para o DPO que se aplicam aos Estados-Membro da UE. As empresas que não se enquadram nos critérios descritos neste documento não são obrigadas a nomear um DPO específico para a GDPR, mas podem, ainda assim, querer nomear um DPO de forma voluntária para facilitar o cumprimento de seus requisitos. Este tipo de DPO ‘voluntário’ estará sujeito aos mesmos requisitos da GDPR que se aplicam quando da designação de um DPO obrigatório.

<sup>11</sup> Avaliações de impacto de proteção de dados serão necessárias para qualquer processamento de dados que possa resultar em um alto risco para os direitos e liberdades dos indivíduos.

<sup>12</sup> A GDPR define incidentes de segurança relacionados a dados pessoais como “violações de dados”, ou seja, violação de segurança levando à destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso a dados pessoais, transmitidos, armazenados ou processados de qualquer outra forma.

<sup>13</sup> Do ano imediatamente anterior.

<sup>14</sup> Equivalente a aproximadamente USD 22.5 milhões.

The logo for Hogan Lovells, featuring the name in a serif font on a yellow rectangular background.

Nota: Todas as pesquisas comparativas, resultados, agendas e minutas da WFA são revisadas pelo Hogan Lovells International LLP, nosso escritório de advocacia de direito concorrencial.

#### **Política de cumprimento da lei concorrencial da WFA**

O objetivo da WFA é representar os interesses dos anunciantes e atuar como um fórum para contatos legítimos entre os membros da indústria da publicidade. É, obviamente, política da WFA que não deverá ser utilizada por nenhuma empresa para promover qualquer conduta anticoncorrencial ou conivente, ou para o envolvimento em outras atividades que possam violar qualquer lei antitruste ou de concorrência, regulamento, regra ou diretivas de qualquer país ou de qualquer outra forma prejudicar a concorrência plena e justa. A WFA realiza verificações regulares para garantir que esta política

seja rigorosamente cumprida. Como condição para a associação, os membros da WFA reconhecem que sua participação na WFA está sujeita às regras da lei de proteção à concorrência e concordam em cumprir integralmente essas leis. Os membros concordam que não utilizarão a WFA, direta ou indiretamente, (a) para alcançar ou tentar chegar a acordos ou entendimentos com um ou mais de seus concorrentes; (b) para obter ou tentar obter, ou trocar ou tentar trocar informações confidenciais ou proprietárias sobre qualquer outra empresa que não seja no contexto de um negócio de boa-fé; ou (c) para promover qualquer conduta anticoncorrencial ou colusiva, ou para se envolver em outras atividades que possam violar qualquer lei antitruste ou de concorrência, regulamentação, regra ou diretivas de qualquer país ou prejudicar a concorrência plena e justa.



**ABA - Associação Brasileira de Anunciantes**  
Av. Paulista, 2073 - Horsa II - 14º andar - Cj. 1403  
01311-940 - São Paulo-SP - Brasil  
55 11 3283-4588

[www.aba.com.br](http://www.aba.com.br)



**ABA** - Associação Brasileira de Anunciantes



@abatransformar



@abatransformar



**ABA** - Associação Brasileira de Anunciantes



[aba.com.br](http://aba.com.br)

**World Federation of Advertisers**  
Londres, Bruxelas, Cingapura

[wfanet.org](http://wfanet.org)  
[info@wfanet.org](mailto:info@wfanet.org)  
+32 2 502 57 40

[twitter@wfamarketers](https://twitter.com/wfamarketers)  
[youtube.com/wfamarketers](https://youtube.com/wfamarketers)  
[linkedin.com/company/wfa](https://linkedin.com/company/wfa)