



GUIA PARA A LEI GERAL DE PROTEÇÃO DE DADOS

(LEI Nº 13.709, DE 14 DE AGOSTO DE 2018)



CUNHA BUENO,
CASTELLO BRANCO E
F. FERNANDES
ADVOGADOS

1 Intro dução

A **Lei Geral de Proteção de Dados (Lei 13.709/2018 ou “LGPD”)** regulamenta a forma pela qual pessoa físicas, jurídicas e órgãos públicos passarão a utilizar, no Brasil, dados pessoais relacionados a pessoas naturais.

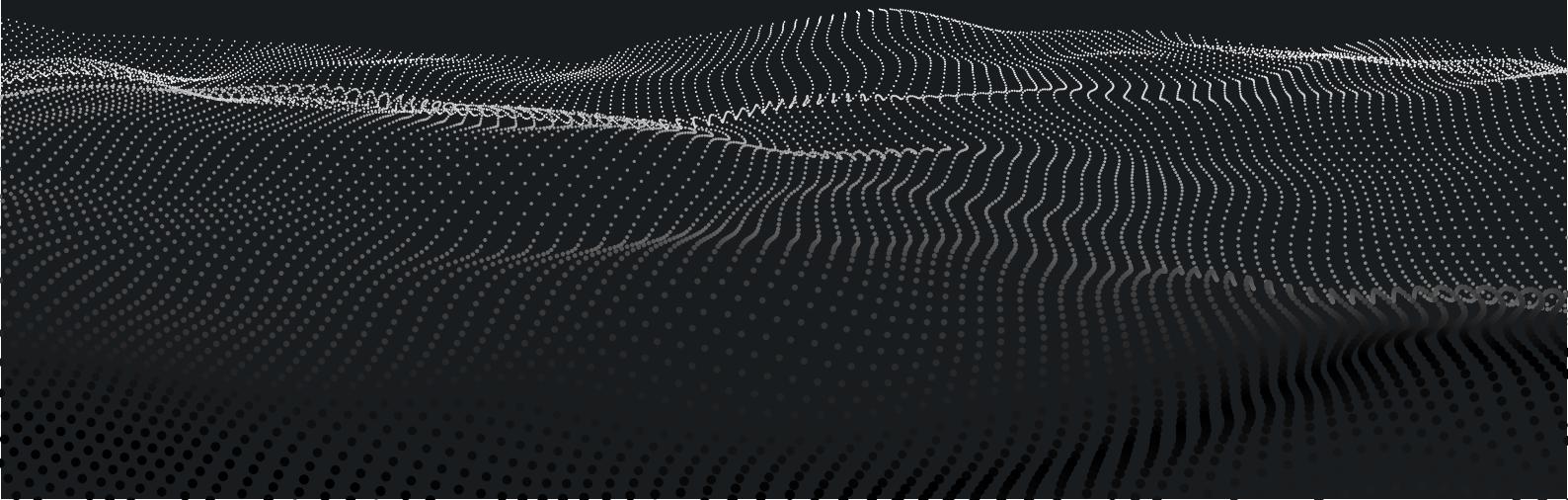
A lei brasileira foi inspirada no General Data Protection Regulation (“GDPR”), o regulamento de proteção de dados da União Europeia e **vigente desde 25 de maio de 2018.**

A LGPD provocará uma mudança radical na forma de tratamento de dados pessoais em todas as empresas brasileiras, das menores às maiores, envolvendo qualquer atividade, inclusive as relações entre clientes e fornecedores de produtos e serviços, empregado e empregador, relações comerciais transnacionais e nacionais, além

de outras relações nas quais dados pessoais sejam coletados tanto no ambiente digital quanto fora dele.

Diante da sua ampla abrangência, a observação das regras dispostas na LGPD é um fator fundamental para que as empresas atendam a referida lei, evitando multas e punições, além, obviamente, de ser um fator fundamental que indica que suas políticas têm o objetivo de zelar pelas informações de todas as pessoas naturais com as quais se relaciona, seja por princípio ético ou por atendimento da lei.

Dada a magnitude da abrangência da LGPD, Cunha Bueno, Castello Branco e F. Fernandes Advogados preparou este guia de modo objetivo e direto para orientar seus clientes e parceiros sobre os impactos no âmbito empresarial e quais providências deverão ser tomadas para que, até 16 de agosto de 2020, as medidas necessárias para a adequação e compliance sejam adotadas de modo planejado e seguro.



2

Definições importantes

Dado pessoal: É qualquer informação relacionada a uma pessoa natural (pessoa física) que possibilite a sua identificação, incluindo, mas não se limitando a: nome, endereço, perfil online, e-mail, contatos, empresa onde trabalha, endereço de IP, CPF, RG, número de telefone, códigos de identificação (Cookies), etc. Esses dados possibilitam individualmente ou em conjunto tornar uma pessoa identificável.

Dado pessoal sensível: Toda informação de uma pessoa natural relacionada à origem racial ou étnica; saúde ou vida sexual; genética e biometria; filiação a sindicato; convicção religiosa; e opinião política

Dado anonimizado: É todo dado que não permite identificar o titular, por ter sido tratado de alguma forma, como criptografia, ou quando são excluídas informações de modo a impedir a associação direta ou indireta a uma pessoa natural.

Tratamento: São todas as etapas que envolvem a operação realizada com o dado pessoal, como, por exemplo: coleta, uso, armazenamento, compartilhamento e exclusão.

Controlador: É a pessoa que decide como, quando e por quê tratar os dados pessoais. Essa pessoa pode ser natural ou jurídica, de direito público ou privado.

Operador: É a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento dos dados pessoais em nome do controlador.

Agentes de tratamento: São o controlador e o operador.

Autoridade Nacional de Proteção de Dados (“ANDP”): Agência reguladora vinculada ao Ministério da Justiça, a qual caberá, dentre outras atribuições, elaborar diretrizes para a Política Nacional de Dados

Pessoais e da Privacidade; emitir normas específicas; fiscalizar; e aplicar as sanções em caso de descumprimento à LGPD.

3

Em quais situações a LGPD é aplicável?

- No tratamento de dados relacionados a pessoas físicas, apenas. Ou seja, não se aplica aos dados de pessoas jurídicas;
- No tratamento de dados pessoais realizado dentro ou fora da internet, utilizando ou não meios digitais como, por exemplo, qualquer formulário em papel, contratos, etc.;
- Às operações de tratamento de dados pessoais que ocorrerem no território brasileiro, mas também às entidades que realizarem tratamento ou tenham coletado dados em território nacional e empresas que tenham como objetivo a oferta ou fornecimento de bens ou serviços a indivíduos localizados no Brasil;
- Terá impacto em diferentes áreas internas das empresas, como setores de marketing, RH, TI, jurídico e de compliance;
- Entrará em vigor em 16 de agosto de 2020. Até lá, todas as empresas deverão ter se adequado para atender aos requisitos da LGPD, sob pena de serem aplicadas sanções prevista na lei.

4

Princípios da LGPD

Finalidade: O tratamento dos dados pessoais deve ser realizado para propósitos legítimos e específicos informados ao titular.

Adequação: O tratamento dos dados pessoais deve ser compatível com as finalidades informadas ao titular.

Necessidade: O tratamento dos dados pessoais deve ser limitado ao mínimo necessário para a realização de suas finalidades.

Livre acesso: Aos titulares é garantida a consulta facilitada e gratuita sobre a forma e duração do tratamento, bem como o acesso à integralidade dos seus dados.

Qualidade dos dados: Deve ser garantido aos titulares a exatidão, clareza, relevância e atualização dos seus dados, de acordo com a necessidade para o cumprimento da finalidade do seu tratamento.

Transparência: Deve ser garantido aos titulares o direito a informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento.

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

Prevenção: Devem ser adotadas medidas para prevenir a ocorrência de danos às pessoas naturais em virtude do tratamento dos seus dados.

Não discriminação: Impossibilidade de realização do tratamento para fins discriminatórios.

Responsabilização e prestação de contas: Os agentes deverão demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais.

Situações nas quais o tratamento de dados é considerado legal

- Mediante o consentimento do titular dos dados pessoais, que deverá ser de forma livre, informada, inequívoca e para uma finalidade determinada. Nesta hipótese, o controlador deverá manter a documentação comprobatória da obtenção do consentimento;
- Para o cumprimento de obrigação legal ou regulatória pelo controlador dos dados;
- Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas;
- Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- Quando necessário para a execução do contrato ou de procedimento contratual preliminar;
- Exercício regular de direitos em processo judicial, administrativo ou arbitral;
- Para a proteção da vida ou da incolumidade física do titular ou de terceiros;
- Para atender interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;
- Para a tutela da saúde, em procedimento realizado por profissionais da área de saúde ou por entidades sanitárias; e
- Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

6

Direitos dos titulares dos dados

Direito à informação e acesso aos dados: o titular dos dados pessoais tratados tem o direito de confirmar o processamento dos seus dados pessoais e tem o direito de, mediante solicitação, obter uma cópia desses dados e demais informações referentes à finalidade específica do tratamento, da forma e duração do tratamento, da identificação e contato do controlador, do uso compartilhado de dados e a respectiva finalidade, da responsabilidade dos agentes de tratamento, etc.

Direito de correção de dados incompletos, inexatos ou desatualizados: trata-se do direito concedido ao titular dos dados pessoais para que haja retificação de dados inexatos e alteração de informações incompletas.

Direito de portabilidade dos dados a outro fornecedor de serviço ou produto: refere-se ao direito de receber as informações pessoais que digam respeito ao titular, bem como a possibilidade de transmitir esses dados diretamente a outro controlador, sem que o último responsável a quem os dados pessoais foram confiados o possa impedir, desde que o tratamento dessas informações esteja legitimado por alguma base legal da LGPD.

Direito de eliminação dos dados pessoais e revogação de consentimento: por meio desse direito, o titular dos dados pessoais também pode obter, por parte do controlador, a eliminação dos seus dados pessoais e a retirada do consentimento para utilização dos seus dados pessoais, exceto para a

hipótese de tratamento necessário ao cumprimento de uma obrigação legal a que o controlador esteja sujeito ou para efeitos de declaração, exercício ou defesa de um direito do controlador em um processo judicial;

Direito de obter informação das entidades públicas e privadas com as quais o controlador realizou o compartilhamento dos dados pessoais: por meio desse direito, o titular pode obter informação sobre as entidades públicas e privadas com as quais o controlador precisou realizar o compartilhamento dos seus dados pessoais.

Direito à anonimização e ao bloqueio: o titular tem o direito de solicitar a perda da possibilidade de associação, direta ou indireta, dos seus dados tratados e, ainda, a suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados, desde que os dados pessoais sejam considerados desnecessários, excessivos ou tratados em desconformidades com as legislações vigentes.

Dados pessoais das crianças e adolescentes: o tratamento de dados pessoais de crianças e adolescentes deverá ser realizado em seu melhor interesse, com o consentimento específico dado por pelo menos um dos pais ou pelo responsável legal. O controlador deverá realizar todos os esforços razoáveis para verificar que o consentimento foi realmente fornecido pelo responsável pela criança.

7

Direitos dos titulares dos dados



Assim como estabeleceu a GDPR, a LGPD autoriza a transferência internacional de dados apenas nos casos previstos na lei, que incluem, dentre outras hipóteses: (i) a transferência para países com grau de proteção considerado adequado pela autoridade competente; e (ii) mediante cláusulas contratuais padrão, em que o Controlador garante o cumprimento da lei.

A União Europeia ainda não considera o Brasil como um país com grau adequado para a proteção de dados, pois a nossa legislação sobre o tema ainda não está vigente e, mesmo após a entrada da LGPD em vigor, a autoridade competente na União Europeia irá avaliar se a nossa legislação está sendo aplicada de forma eficaz para a proteção dos dados pessoais.

8 Sanções

Em caso de descumprimento das normas previstas na LGPD, os agentes de tratamento de dados estarão sujeitos à diversas penalidades a serem aplicadas pela ANPD, dentre elas:

- Recebimento de advertência;
- Publicização da infração;
- Bloqueio ou eliminação dos dados pessoais a que se refere a infração;
- Suspensão do exercício da atividade de tratamento dos dados pessoais.
- Multas diárias, ou multa simples de até 2% (dois por cento) do faturamento do grupo empresarial no Brasil – limitadas a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração.

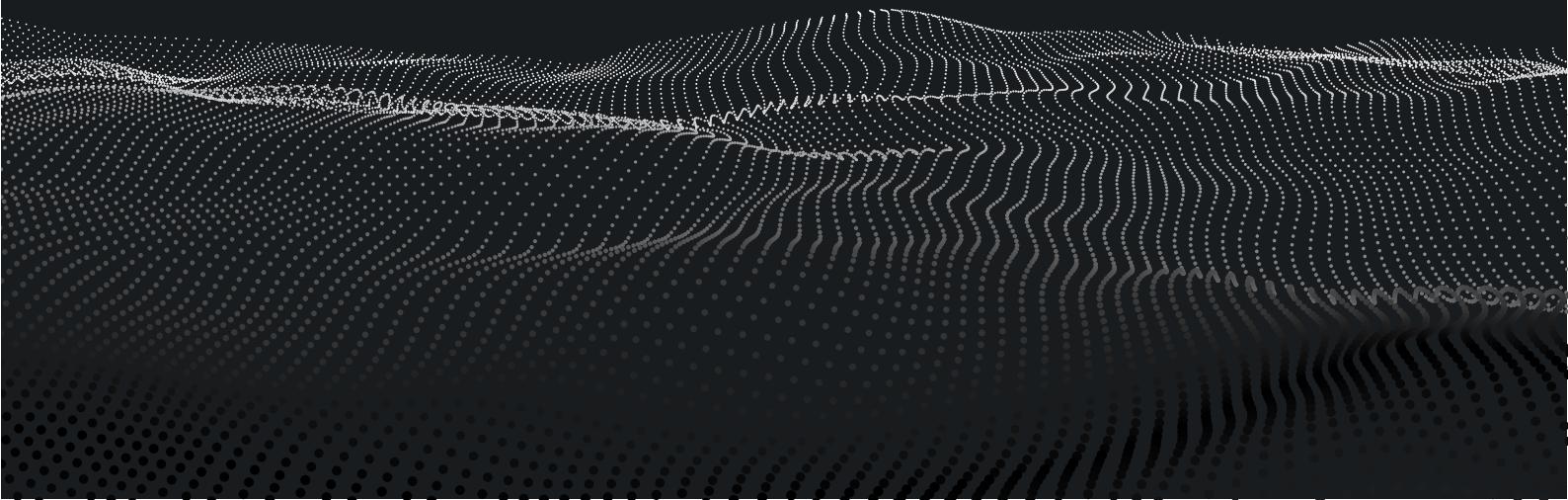
Salientamos que entre o controlador e o operador existirá responsabilidade solidária pelos danos causados aos titulares dos dados pessoais. Nesse sentido, imprescindível ressaltar que as empresas podem, em algum momento, serem controladoras e também operadoras, como, por exemplo, no caso de uma empresa que presta os serviços de nuvem (armazenamento de dados).



Checklist para adequação na empresa em conformidade com a LGPD

A) Inventário dos dados pessoais

- Quais são (é necessário que sejam dados essenciais à atividade e que sejam obtidos a menor quantidade de dados possível) os dados coletados?
- Onde estão (segurança, disponibilidade, acesso à pessoa interessada e à ANPD) os dados coletados? Estamos nos referindo aos dados pessoais de todas as pessoas naturais que disponibilizam essas informações à empresa. São os clientes, os próprios funcionários, dentre outros. Nessa perspectiva, o Data Protection Officer (responsável pela gestão de dados – artigo 5º, VII da LGPD) da empresa deverá tratar todas essas informações como a lei determina (produzir relatórios para as pessoas e órgão regulador, atender aos pedidos de exclusão de informações, descartar as informações por meio de um processo controlado, seguro e comprovado).
- Matriz de tratamento dos dados pessoais (tipos de tratamento e para quais finalidades). Qual a matriz de tratamento dos dados pessoais? Como é feita a colheita, manutenção e descarte dessas informações? Como é feita a gestão do controle de consentimentos (autorização da pessoa natural para que os dados sejam mantidos na empresa)?
- Quais são as finalidades de uso dos dados pessoais (para que a empresa precisa desses dados)?



B) Depois de responder a essas perguntas, será realizado um mapa de risco, que conterá:

- Nível técnico (ferramentas a serem adaptadas);
- Documental (atualizar normas, políticas, contratos); revisão e atualização da política de privacidade; atualização das cláusulas contratuais com cliente/funcionários/parceiros/fornecedores para prever a aplicação da LGPD e da GDPR; atualizar NDA;
- Procedimental (adequar a governança e a gestão dos dados pessoais);
- Cultural (realizar treinamentos e campanhas de conscientização das equipes, dos parceiros, fornecedores e clientes), a saber:
 - i. Criar programa de compliance digital: avaliação de risco, planos de respostas a incidentes, treinamentos e comunicação, due diligence de terceiros;
 - ii. Criar modelo de resposta para a notificação ao Órgão de Controle de Dados (ANPD) sobre o nível de conformidade da empresa e controles auditáveis, para prevenção a aplicação de multas e fiscalizações;

iii. Fornecedores e parceiros deverão estar em conformidade com as novas regulamentações de proteção de dados pessoais (compliance);

iv. Código de Conduta: atualizar com cláusulas que preveem respeito à proteção de dados pessoais;

v. Atualizar a Política de Segurança da Informação.

Importante ressaltarmos que aconselhamos a revisão constante da política de privacidade das empresas e de seus sites, pois ela deve acompanhar as mudanças que ocorrem na empresa. Por isso, sugerimos que a política de privacidade seja revisada, pelo menos, uma vez ao ano.

C) Data Protection Officer e empresa de tecnologia para organizar a captação, tratamento e descarte de dados:

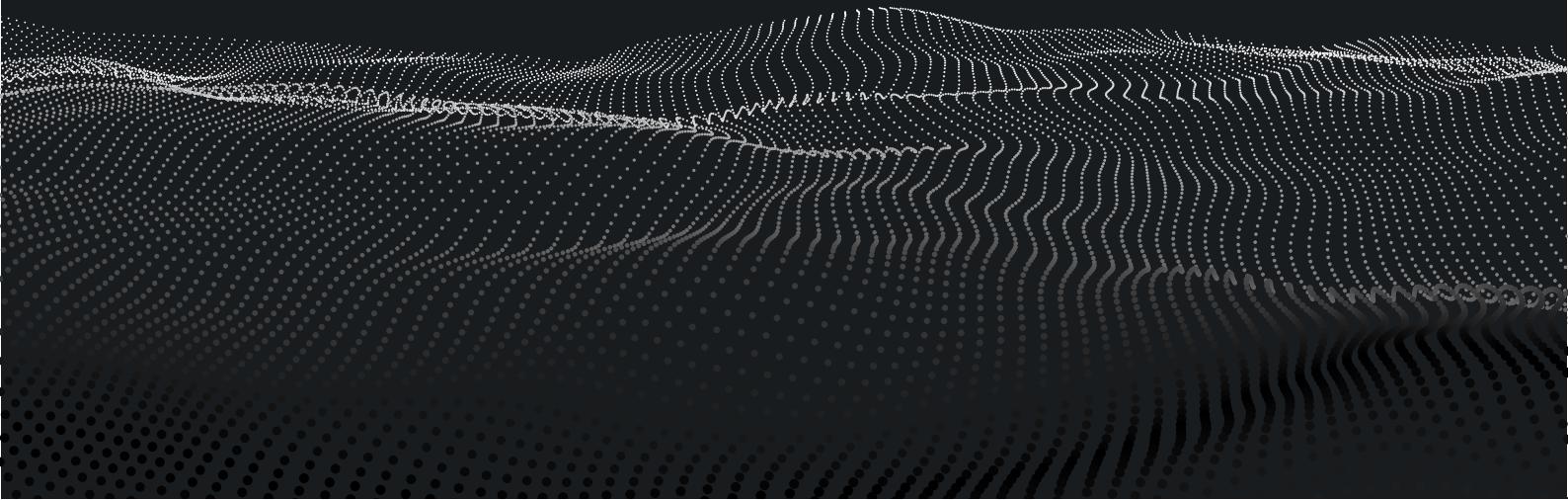
O escritório ainda orientará a empresa sobre como contratar um responsável (pessoa física ou jurídica) pelo tratamento de dados pessoais e a relação desses dados com consumidores/usuários dos serviços e a autoridade regulatória, o que é uma exigência da LGPD (Data Protection Officer), bem como uma empresa capacitada a desenvolver todo fluxo de captação, tratamento e descarte de informações.

10.

Fluxo de gestão de risco

Para que a sua empresa evite qualquer tipo de sanção prevista na LGPD será importante observar os seguintes procedimentos:

- A)** Proteção de dados pessoas: a empresa deverá adotar todas as medidas cabíveis para a proteção dos dados pessoais, desde o seu recebimento até o seu descarte, incluindo a obtenção de softwares para proteção dos dados, como antivírus e criptografia.
- B)** Confirmação do consentimento: a empresa deverá manter os arquivos que comprovem que os titulares dos dados pessoais consentiram com o tratamento dos seus dados, caso esta seja a base legal utilizada pela empresa para o tratamento dos dados pessoais.
- C)** Registro do processamento: a empresa deverá elaborar e manter o registro de todo o processamento de todos os dados pessoais que ela tiver acesso, assim como elaborar relatórios para, em caso de fiscalização, apresentar à ANPD.
- D)** Notificação de violação: a empresa tem o dever de reportar imediatamente à ANPD a ocorrência de algum incidente no tratamento dos dados pessoais. Quanto antes a empresa notificar a ANPD, melhores serão as chances de a sanção ser mais branda (considerando a adoção dos demais procedimentos dispostos acima).





CUNHA BUENO,
CASTELLO BRANCO E
F. FERNANDES

ADVOGADOS

www.bbflaw.com.br

contato@bbflaw.com.br

São Paulo
T: +55 11 4010 9888

Ribeirão Preto
T: +55 16 3075 8888 | +55 16 4141 1565