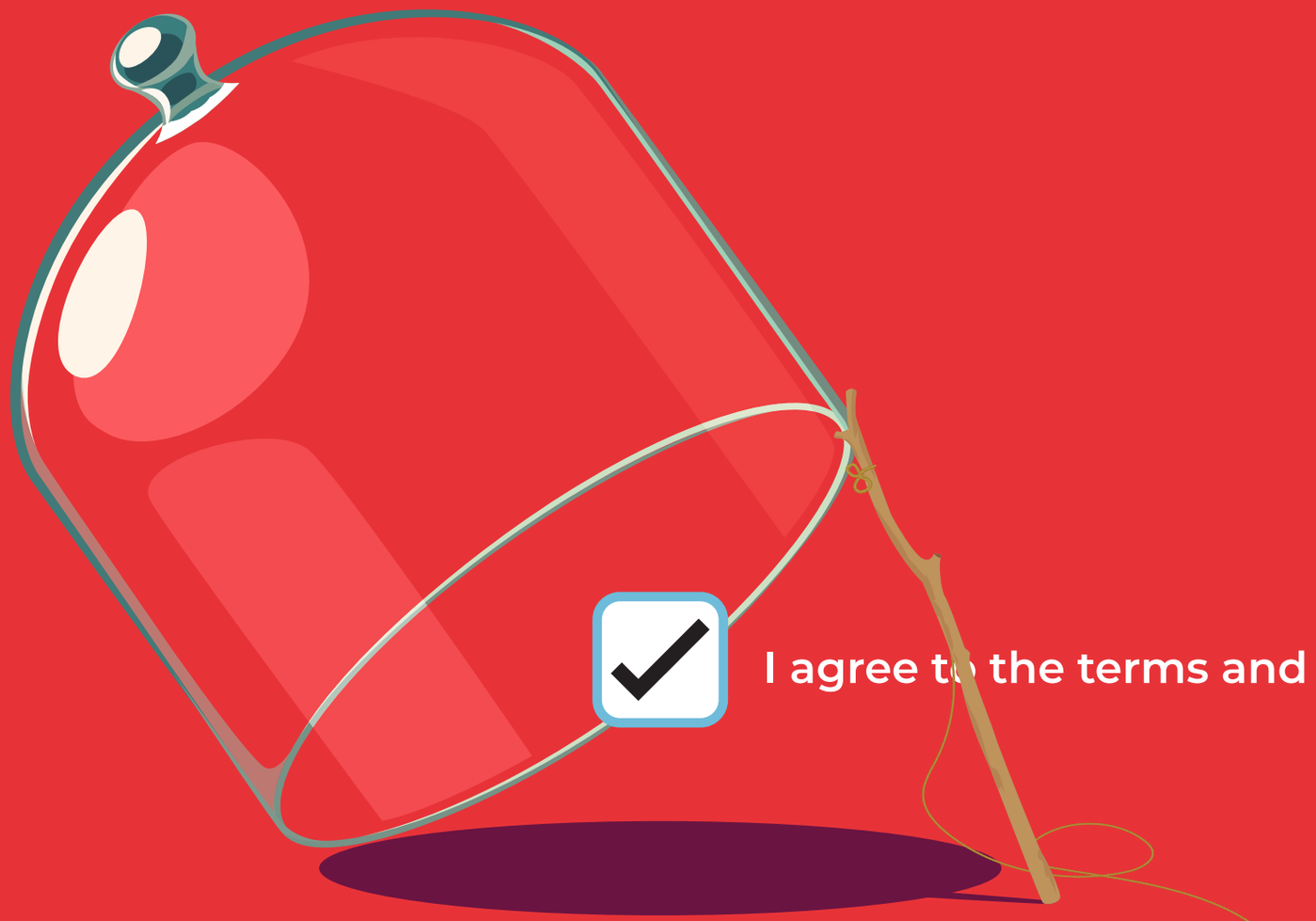
AMCHAM CONNECT

6 pontos de atenção

na hora de se adequar à

Lei de Proteção de Dados

segundo o **PK Advogados**



PK PINHÃO E KOIFFMAN ADVOGADOS

Conteúdo patrocinado

AMCHAM Brasil

Conteúdo

Empresas têm até fevereiro de 2020 para entrar em conformidade com as exigências da lei

Comprar produtos, buscar informações e compartilhar experiências na internet são, hoje, hábitos naturais na vida das pessoas. Mas essas comodidades têm um preço, avisa o Escritório Pinhão e Koiffman Advogados (PK). Em troca dos serviços, muitas vezes gratuitos, as empresas passaram a coletar informações dos usuários de maneira ampla e sem a devida transparência sobre como esses dados eram utilizados.

“Diversos casos de vazamento de dados foram relatados nos últimos anos e as pessoas passaram a sentir que sua privacidade estava em risco. Era necessário, então, definir certas regras para balancear a inovação e a comodidade dos novos serviços, com a proteção de direitos fundamentais como a privacidade, intimidade, liberdade de expressão, dentre outros.”

O Brasil aprovou este ano a Lei Geral de Proteção de Dados (LGPD) para regulamentar o tratamento de dados pessoais. A lei, que começa para valer em fevereiro de 2020, foi inspirada no GDPR (*General Data Protection Regulation* – Regulamento Geral de Proteção de Dados) da EU (União Europeia). O novo marco regulatório brasileiro reúne, em uma lei abrangente e específica, todo o regramento de proteção de dados pessoais que antes estava espalhado em diversas legislações, bem como adiciona novos conceitos trazidos de legislações estrangeiras.

De modo geral, os cuidados no uso e tratamento de dados terão que ser redobrados, segundo o PK. Para ajudar as empresas a se adaptar à nova realidade, o escritório recomenda seis pontos de atenção:

1.

Registre todos os passos do tratamento de dados pessoais e sensíveis

As empresas deverão registrar todas as operações de tratamento de dados pessoais realizadas, com especial atenção àquelas fundamentadas no seu legítimo interesse comercial.

A Lei regulamenta o tratamento de dados pessoais, que são os dados referentes a informações relacionadas ao usuário que o identifique como pessoa física. Entre elas estão nome, endereço, e-mail, idade, estado civil e situação patrimonial, obtidos em qualquer tipo de suporte (papel ou meio eletrônico, informático, som, imagem, etc.)

"A LGPD optou por um conceito amplo dos dados pessoais sem uma lista taxativa. Isso dá maior longevidade à lei e deixa a definição da sua amplitude para o regulador ou os operadores do Direito", opina o PK.

1.

Registre todos os passos do tratamento de dados pessoais e sensíveis

Os dados pessoais sensíveis são aqueles sobre origem racial ou étnica, convicções religiosas, opiniões políticas e filiação a sindicatos. Também incluem a participação em organizações de caráter religioso, filosófico ou político e dados referentes à saúde ou vida sexual. Além deles, a lista considera dados genéticos ou biométricos vinculados a uma pessoa física.

E sobre esse tipo de dado a lei é bem mais criteriosa.

"O tratamento destes dados é abordado com maior rigor pela LGPD, sendo vedado o seu tratamento, exceto em hipóteses específicas trazidas pela lei", afirma o PK.

2. Documente processos, controles e riscos

Outro cuidado que a empresa deve tomar é documentar os processos que envolvem tratamento de dados pessoais que podem gerar riscos às liberdades civis e direitos fundamentais dos clientes. Isso inclui os tipos de dados coletados, a metodologia de coleta e as garantias de segurança das informações. Também é importante ter análises do controlador (responsável pelas decisões sobre o tratamento dos dados) em relação às medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Deve haver especial atenção com o processo de obtenção do consentimento do usuário (titular dos dados pessoais), que deve ser feito através de manifestação livre, informada e inequívoca. É importante documentar que o usuário concordou com o tratamento dos seus dados pessoais para a finalidade informada.

Também devem ser adotados processos para que os titulares exerçam seus direitos, que são: (i) confirmação da existência de tratamento; (ii) acesso aos dados; (iii) correção de dados incompletos, inexatos ou desatualizados; (iv) anonimização, bloqueio ou eliminação; (v) portabilidade; (vi) eliminação dos dados; (vii) informação sobre uso compartilhado; (viii) informação sobre não fornecimento do consentimento e (x) revogação do consentimento .

3.

Defina o Encarregado

As informações sobre o Encarregado do Tratamento de Dados devem ser divulgadas pela empresa, de acordo com o PK.

"Ela deverá fornecer publicamente a identidade e informações de contato, preferencialmente no website corporativo."

O Encarregado, informa o PK, terá a função de interagir com os titulares de dados pessoais e será o ponto de contato para receber reclamações, solicitações e comunicações. Também será o canal de prestação de informações e esclarecimentos para as autoridades.

O Encarregado também tem o papel de orientar funcionários e contratados sobre as normas de proteção de dados pessoais adotadas pela empresa, além de outras atribuições corporativas. Muita responsabilidade? Depende da comparação, na opinião do escritório. "A LGPD não concedeu a esse agente um papel de tanta autonomia e destaque, como na UE."

4. Segurança é prioridade

Outra obrigação das empresas é verificar se o tratamento de dados pessoais está sendo realizado de maneira segura, acrescenta o PK.

"É importante verificar o modo pelo qual o processo é realizado, o resultado da ação e os riscos que razoavelmente se esperam, bem como das técnicas de tratamento de dados pessoais disponíveis à época em que o procedimento foi realizado."

Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de modo a atender aos requisitos de segurança, boas práticas, governança e princípios gerais previstos na lei (*privacy by default*). Além dos processos internos, a segurança no uso de dados tem que estar desde a concepção do produto ou serviço até a execução (*privacy by design*).

No que se refere à operacionalização da segurança, os agentes de tratamento têm papel importante nas medidas técnicas e administrativas.

5. Comunicação de vazamento de dados

Está na lei: todo incidente de segurança que possa acarretar risco ou dano relevante aos titulares deve ser comunicado pelo controlador às autoridades.

"A divulgação pública do fato em meios de comunicação poderá ser determinada pela autoridade nacional, de acordo com a gravidade do incidente. Ela pode ainda determinar medidas para reverter ou mitigar os efeitos do incidente", detalha o PK.

6. Adote boas-práticas e implemente uma governança de proteção de dados

A empresa também deve formalizar regras e boas práticas de governança. Elas devem estabelecer condições de organização, regime de funcionamento e procedimentos – incluindo reclamações e petições de titulares.

As regras internas também devem abranger normas de segurança, padrões técnicos, obrigações específicas aos envolvidos no tratamento de dados, ações educativas, mecanismos internos de supervisão e mitigação de riscos.

Dica bônus:

Lei brasileira vale para o exterior e vice-versa

Como explica o PK, a LGPD tem aplicação internacional, assim como a GDPR. Ou seja, uma empresa estrangeira que coletar e tratar dados no Brasil poderá estar submetida à LGPD – tendo operações ou não em território nacional.

A recíproca é mútua. “Até mesmo uma pequena empresa brasileira pode coletar, armazenar e utilizar informações pessoais de uma pessoa que está localizada na UE (União Europeia). Dessa forma, como o GDPR se refere exatamente aos dados de pessoas localizadas na UE, qualquer empresa que vier a lidar com essas informações poderá estar sujeita a essa regulamentação”, de acordo com o PK.

Ou seja, estar em conformidade com a lei de dados no Brasil equipara as empresas brasileiras às estrangeiras. Nesse contexto, o Brasil oferece um nível de proteção similar ao de países desenvolvidos.

Expediente

| *PK Advogados* |

Hélio Ferreira Moraes

Sócio

55 11 3054-1020

hfmoraes@pk.adv.br

Linkedin
www.linkedin.com/company/pinh-o-e-koiffman-advogados/

| *Amcham Brasil* |

Deborah Vieitas

CEO da Amcham Brasil

Camila Moura

Diretora de Produtos & Serviços

Dirceu Pinto

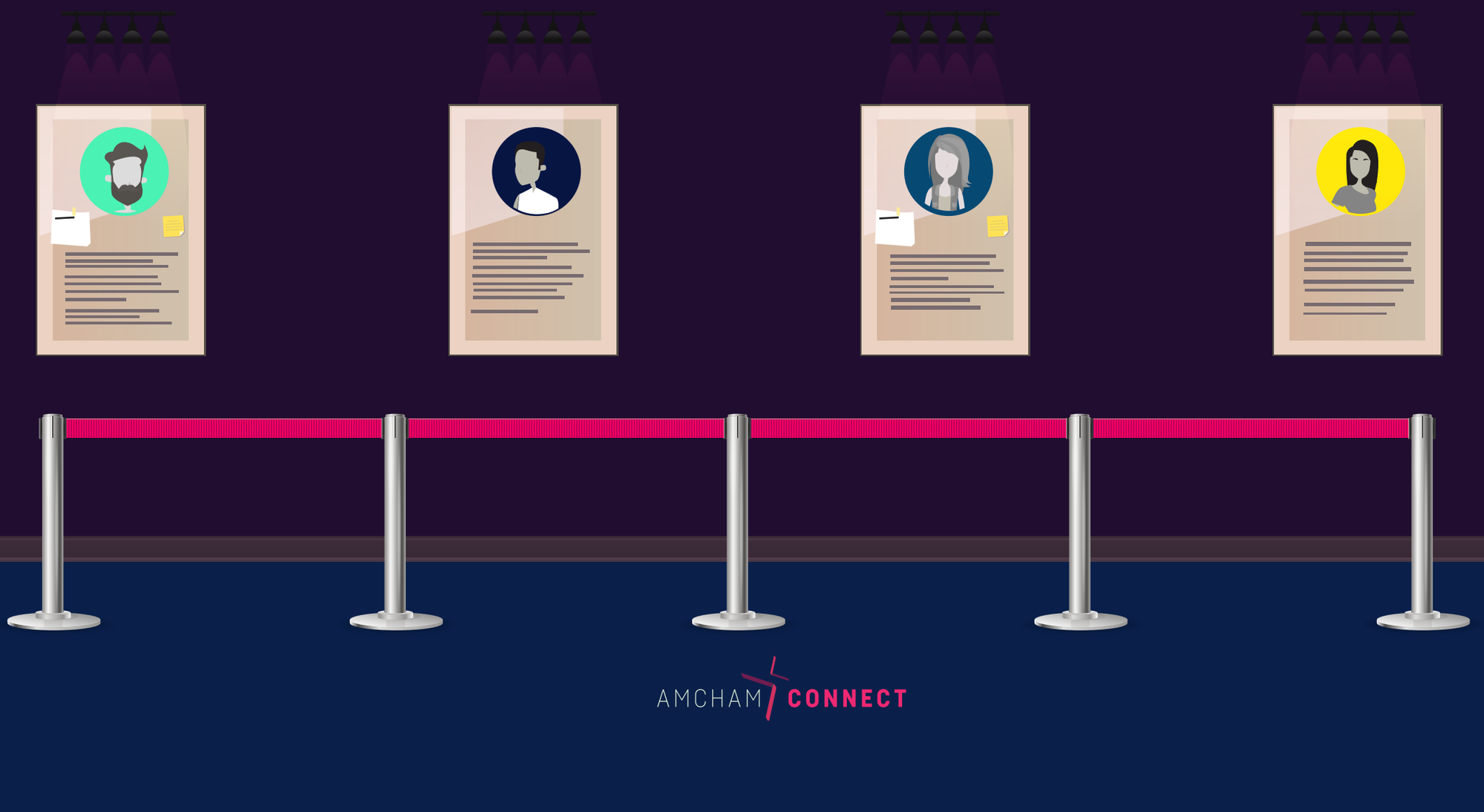
Superintendente de Comunicação & Marketing

André Inohara

Repórter

Projeto Gráfico
Renato Orlandini Santos | *ist*

AMCHAM Brasil



AMCHAM CONNECT