ALEXANDRE ATHENIENSE ADVOGADOS
DIREITO DIGITAL
32 anos

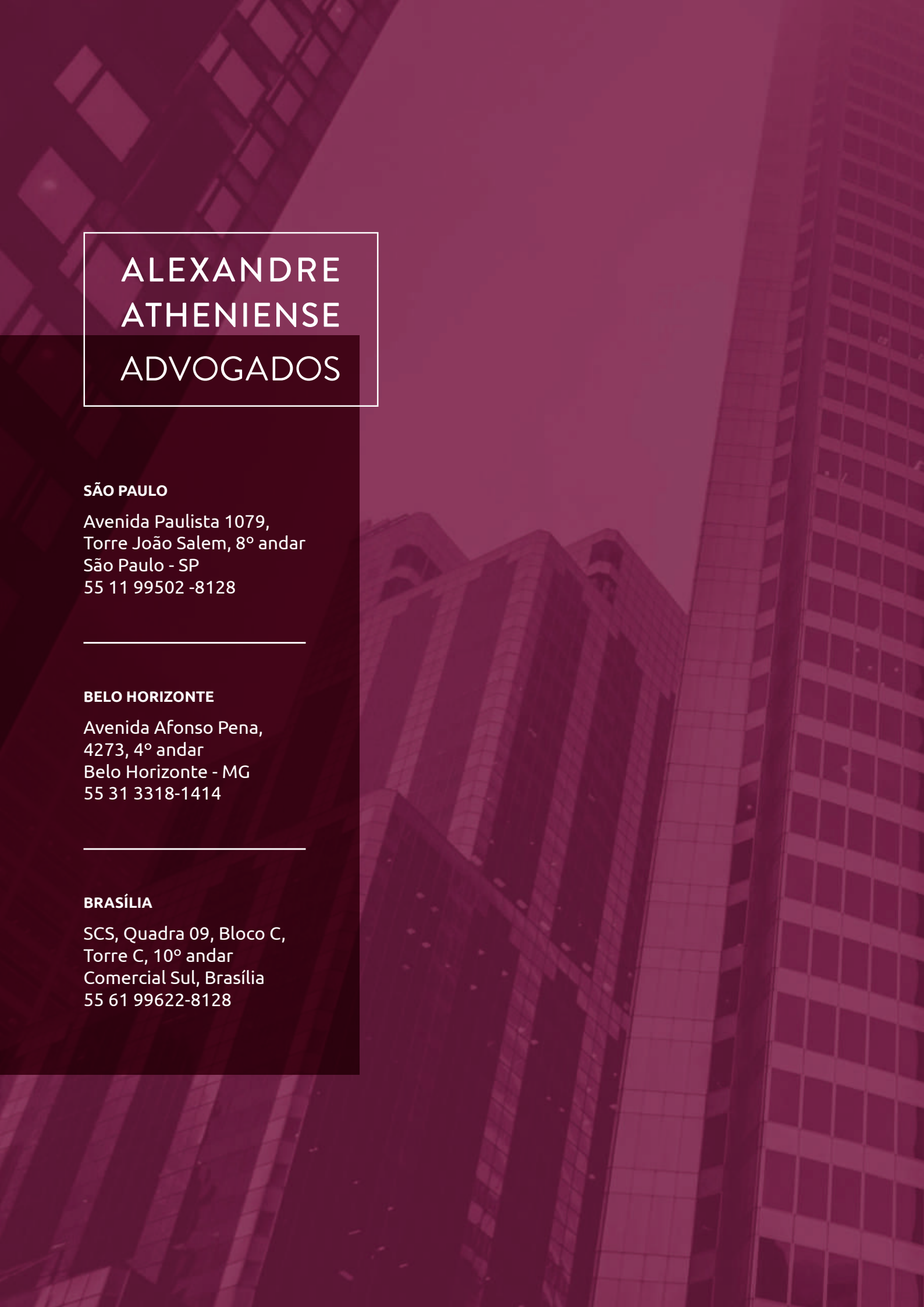
análise ADVOCACIA 500
ADVOGADO MAIS ADMIRADO 2019

RANKED FIRM 2020
LEADERS LEAGUE

JUNHO 2020

LGPD PARA EMPRESAS

www.atheniense.com



ALEXANDRE ATHENIENSE ADVOGADOS

SÃO PAULO

Avenida Paulista 1079,
Torre João Salem, 8º andar
São Paulo - SP
55 11 99502 -8128

BELO HORIZONTE

Avenida Afonso Pena,
4273, 4º andar
Belo Horizonte - MG
55 31 3318-1414

BRASÍLIA

SCS, Quadra 09, Bloco C,
Torre C, 10º andar
Comercial Sul, Brasília
55 61 99622-8128

Alexandre Atheniense é advogado formado pela Universidade Federal de Minas Gerais (UFMG), especializado em Internet Law na Berkman Center – Harvard Law School e sócio-fundador do Alexandre Atheniense Advogados.

Com experiência profissional de 32 anos é um dos precursores do Direito Digital no Brasil. Possui vasta experiência acadêmica e institucional, tendo exercido por oito anos (2002-2010) a presidência da Comissão de Tecnologia da Informação da OAB Federal, representando a entidade na discussão de projetos de lei no Congresso Nacional sobre os temas relacionados a Tecnologia da Informação. Coordenador da Comissão de Direito Digital do CESA - Centro de Estudos das Sociedade de Advogados. Árbitro em questões relacionadas à Propriedade Intelectual e Tecnologia da Informação na Camarb, CAMINAS e ABPI e autor de diversas obras sobre Direito Digital no Brasil e no exterior.

Photo by Essow Kedelina from Pexels

ALEXANDRE ATHENIENSE ADVOGADOS

LGPD Para Empresas

Alexandre Atheniense
Sócio-fundador de Alexandre Atheniense Advogados[1]

Com a sanção da Lei Geral de Proteção de Dados (LGPD), o que antes era considerado boas práticas agora passa a ser obrigação.

O escritório de Alexandre Atheniense Advogados está preparado para guiar as organizações no processo de adequação à LGPD, pois possui uma equipe qualificada para atender à necessidade do cliente. Dentre as competências, estão: Proteção de dados pessoais, Segurança cibernética, *Compliance* e Governança digital corporativa.

Embora este guia abarque inúmeros tópicos da LGPD, o conteúdo não foi esgotado. Os objetivos com este material são informar e mostrar a quem lida diretamente ou indiretamente com proteção de dados que o assunto é contínuo e não se esgota. Cada ramo de atividade tem suas particularidades e, por esse motivo, todos requerem planos de contingência direcionados.

Esperamos que ao final da leitura você tenha uma visão global da LGPD e desenvolva na sua organização uma Governança digital. Conte com a gente.

---

[1] Colaboraram neste guia Valéria E. Alcântara e Alves, Lucas Balsemão, Pedro Resende, Renata Diniz e Giovana Lopes.

Sumário

Introdução

A LGPD não visa barrar o desenvolvimento tecnológico, e sim regulamentar o tratamento de dados pessoais. Ela foi criada com o objetivo de proteger a privacidade, o interesse e a liberdade dos titulares dos dados, além de colocar o Brasil no mesmo nível de regulação de países que prezam pela proteção de dados pessoais de seus integrantes, como os países da União Europeia.

Os termos mais importantes para entender a LGPD

Agentes de tratamento

O *controlador da base de dados*: pessoa física ou jurídica, de direito público ou privado, responsável pelas decisões referentes ao tratamento de dados pessoais; e o *operador da base de dados*: pessoa física ou jurídica que realiza o tratamento de dados pessoais estritamente conforme as obrigações e finalidades definidas pelo controlador.

Anonimização

Consiste na utilização de meios técnicos razoáveis e disponíveis no momento do tratamento do dado pessoal, por meio dos quais um dado pessoal perde a possibilidade de associação, direta ou indireta, a um indivíduo.

Autoridade Nacional de Proteção de Dados (ANDP)

Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento dessa Lei.

Dados pessoais

Segundo a LGPD, é uma "informação relacionada à pessoa natural identificada ou identificável". Tudo que pode identificar direta ou indiretamente uma pessoa, como nome, números de documentos, fotografias, registros biométricos, etc.; ou, indiretamente, dados que podem ser cruzados ou que podem levar a informações, como um e-mail corporativo ou um endereço IP.

Dados anonimizados

São dados relativos ao titular sem sua identificação direta, considerando os meios técnicos disponíveis na ocasião do tratamento. Normalmente, são dados utilizados para pesquisas e políticas públicas.

Dados sensíveis

São aqueles que podem resultar em danos imediatos, caso sejam divulgados indevidamente. O tratamento desses dados requer cuidados especiais, e eles só podem ser solicitados para finalidades específicas. Dentre eles estão os dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato, filiação religiosa, saúde, vida sexual, dados genéticos, informações biométricas.

Dados de crianças e adolescentes

O tratamento de dados de crianças e adolescentes também requer cuidados especiais e somente pode ser realizado com o consentimento específico de um responsável.

Encarregado de tratamento de dados pessoais

Pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados.

Titular dos dados pessoais

O titular dos dados é sempre uma pessoa física. Nos termos da Lei, "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento". (Leia a seguir o significado de "tratamento".)

Tratamento de dados pessoais

Uma das definições mais importantes determinantes na Lei é a do tratamento de dados. Tratamento é o termo usado na Lei que serve como um "guarda-chuva" para uma série de procedimentos envolvendo dados. Exemplos de ações de tratamento: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle, modificação, comunicação transferência, difusão, extração.

O que todos precisam saber sobre a LGPD

A proteção de dados deve ser observada em todas as etapas, desde seu nascimento e por processo, visando garantir ao titular dos dados o tratamento mais protetivo.

Lembrando-se de que:

- a adequação à LGPD não é "somente um problema do pessoal de informática". Como dizem os especialistas, é transversal, envolve todos os níveis de decisão e operação, em todas as áreas da empresa, da base ao topo;

- a LGPD é obrigatória para todas as organizações que lidam com dados pessoais;

- as penalidades são muito pesadas para quem cometer infrações. As multas, conforme a gravidade, podem chegar a 2% do faturamento líquido anual, limitadas a 50 milhões de reais por infração, podendo ser aplicadas cumulativamente;

- o processo de adequação é relativamente complexo e envolve uma ampla revisão das políticas de segurança e adoção de novos procedimentos;

- a Lei foi promulgada em 2018 e - de acordo com o PL 1179/20, ainda pendente de sanção presidencial - entrará em vigor em agosto de 2020. [2]

- a Lei tem uma abrangência ampla, vale para o tratamento de dados realizado no Brasil ou quando os dados forem coletados de pessoas no Brasil;

- a LGPD vale para tratamento de dados digitais ou não, fora ou dentro da internet;

- A Lei abrange apenas dados de pessoas físicas;

- em caso de vazamento, ou quando for solicitado, cabe ao controlador demonstrar que os dados foram obtidos segundo as regras da LGPD;

- o titular tem o direito de ter acesso aos dados, exigir correções e revogar o consentimento de uso;

- em caso de vazamento ou uso indevido dos dados, é obrigação do controlador da base de dados pessoais tomar as medidas para mitigar os danos, informar sobre o vazamento e responder pelo prejuízo causado;

- o objetivo da Lei é assegurar a titularidade de dados pessoais e garantir os direitos fundamentais de liberdade, intimidade e privacidade, além dos demais previstos na LGPD;

- caberá às empresas, ou aos chamados "agentes de tratamento", um inventário detalhado de como a Lei interfere em suas atividades.

---

[2] *Após a apreciação pelas duas casas do Congresso Nacional do PL 1179/20, o qual trata de medidas emergenciais e transitórias para relações de direito privado durante o período de pandemia do Covid-19 e o imbróglio criado pela edição da Medida Provisória 959, publicada em 29/04/2020 ao tratarem concomitantemente, em artigos específicos, sobre a entrada em vigor da LGPD mas, de forma diversa, prevalece, neste momento, a retomada da data inicial da Lei para entrada em vigor em agosto de 2020, sendo que as penalidades (sanções) vigorarão a partir de agosto de 2021 (pendente a sanção presidencial). Independente da solução quanto a data de entrada de vigência é mandatório iniciar as medidas de adequação. O trabalho é complexo pois apurar lacunas quanto ao tratamento de dados na empresa exige esforço e sensibilização de várias lideranças da empresa, alguns eventos presenciais para coleta, análise e revisão dos dados pessoais e das medidas corretivas.*

Direitos do cidadão

Segundo a LGPD (art. 17), toda pessoa "tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade". Diz ainda a Lei, no art. 18: "O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição":

- confirmação da existência de tratamento;
- acesso aos seus dados pessoais;
- correção de dados incompletos, inexatos ou desatualizados;
- anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei;
- opor-se a tratamento realizado;
- portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador;
- revogação do consentimento para tratamento.

Princípios da LGPD

A LGDP preceitua dez princípios aos quais todo empresário deve estar alerta.

Finalidade

Tratamento de dados pessoais para propósitos legítimos, específicos, explícitos e informados ao titular, sem a possibilidade de tratamento posterior de forma incompatível com essas finalidades.

Adequação

Tratamento compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

Necessidade

Tratamento limitado ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

Livre acesso

Garantia aos titulares de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

Qualidade dos dados

Garantir aos titulares exatidão, clareza, relevância e atualização dos dados de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

Transparência

Assegurar aos titulares que as informações sobre a realização do tratamento e sobre os respectivos agentes de tratamento, observados os segredos comerciais e industriais, serão claras, precisas e facilmente acessíveis.

Segurança

Utilizar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Prevenção

Adotar medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Não discriminação

É expressamente proibida a realização do tratamento de dados pessoais para fins discriminatórios ilícitos ou abusivos.

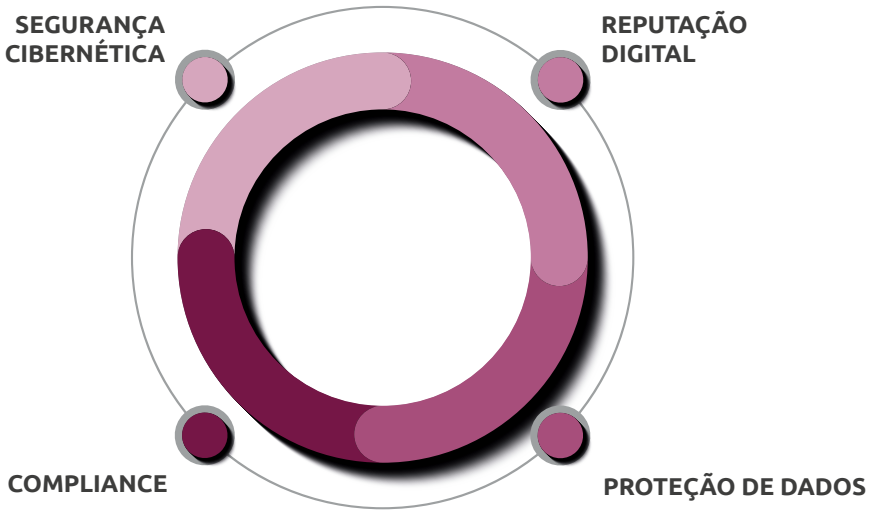
Responsabilização e prestação de contas

Demonstrar, por meio da elaboração de relatórios previstos em lei, a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, bem como a eficiência dessas medidas.

Governança digital

Além da proteção de dados pessoais, a gestão da Governança digital corporativa compreende outros três pilares essenciais para fechar um ciclo virtuoso: Segurança cibernética, Reputação digital e *Compliance*.

Com base na nossa experiência profissional, inovamos ao criar o conceito de Governança digital corporativa para definir um serviço abrangente e de suma relevância estratégica para as empresas. Observamos que tudo o que se lia sobre Governança digital se conectava ao exercício exclusivo do poder estatal de exercer sua atividade de governar. Por outro lado, a expressão "Governança corporativa" não é novidade no meio empresarial, mas as práticas difundidas estavam essencialmente ligadas ao mundo analógico. Ao percebermos essa lacuna, compreendemos a necessidade de levar ao mercado uma solução de consultoria jurídica contextualizada, referente ao exercício do poder decisório corporativo no mundo digital, mitigando os riscos envolvidos.



Cybersecurity

São diversas as medidas para a avaliação de riscos operacionais e a elaboração de um plano de ação para suprir as lacunas jurídicas, sistêmicas e estratégicas quanto à segurança da informação, tais como: elaboração ou revisão de regulamentação interna, obrigações legais, políticas e procedimentos internos quanto ao uso das informações digitais que revelem fatores de risco, análise e preservação de provas dos incidentes em conformidade legal e a necessidade de adoção de medidas jurídicas, ou não, para enfrentamento de incidentes com a maior brevidade possível.

Reputação digital

O perfil de uma empresa no mundo digital não é construído apenas por informações que a própria organização divulga a seu respeito. As informações ou comentários gerados por terceiros possuem, também, grande relevância e riscos. A internet guarda surpresas que precisam ser monitoradas e enfrentadas para que um fato não se transforme numa crise. Por esse motivo, o contingenciamento de problemas para este assunto é mandatório. Será necessário definir atribuições como análise e preservação de provas em conformidade legal dos conteúdos impróprios gerados por terceiros, como: comentários, críticas falsas, *fake news*, perfis falsos e ataques ofensivos que forem divulgados publicamente, alcançando grande relevância nas pesquisas do Google e das redes sociais.

A possível remoção desses conteúdos, judicialmente ou não, ou a adoção de outras estratégias equivalentes devem ser executadas na maior brevidade possível, pois esses conteúdos representam graves fatores de risco quanto à reputação da organização, de seus gestores ou colaboradores,

Compliance

Elaboração e implantação de um conjunto de medidas para fazer cumprir as normas legais, regulamentares e políticas, com a finalidade de evitar a aplicação de sanções anticorrupção, bem como detectar e tratar qualquer desvio ou desconformidade.

Mãos à obra

Sugerimos o uso do ciclo PDCA, uma ferramenta relevante para aplicar a melhoria contínua nos processos da sua organização. Se você nunca utilizou essa ferramenta, apresentaremos, a seguir, um passo a passo para começar.

O PDCA é uma ferramenta de gestão da qualidade com finalidade de proporcionar a melhoria contínua dos processos, por meio de quatro ações: ***Plan*** (**Planejar**), ***Do*** (**Fazer**), ***Check*** (**Verificar**) e ***Act*** (**Agir**). O propósito é entender não somente o problema, que chamaremos de "oportunidade de melhoria", mas, principalmente, suas causas, e não as consequências. Uma vez que a oportunidade de melhoria foi identificada – no nosso caso, a adequação à LGPD –, é hora de colocar em prática o PDCA e atingir o resultado almejado com qualidade e eficiência.

Antes de começar a aplicar esse método, a organização deve definir uma pessoa para liderar o Projeto de Proteção de Dados. Na Lei, essa é a figura do DPO (encarregado de proteção de dados), bem como uma equipe para auxiliar o DPO no desenvolvimento do Projeto de Proteção de Dados e no *Compliance* de proteção de dados da instituição.

Sugestão – É aconselhável uma equipe multidisciplinar com membros da área de Tecnologia da Informação (TI), Jurídico, Marketing, Recursos Humanos (RH), Financeiro, Compras. Um projeto que envolve regulação e *Compliance* só terá sucesso se abranger todas as áreas, e com uma equipe multidisciplinar é possível analisar todas as perspectivas.

A LGPD permite que a governança seja formulada pelos agentes de tratamento, desde que:

- definam o regime de funcionamento do projeto;
- haja normas, padrões técnicos e procedimentos bem definidos;
- haja ações educativas;
- a gestão de risco seja bem executada;
- os envolvidos pelo tratamento tenham obrigações específicas.

Fase 1: Planejar

Identificar a oportunidade de melhoria

Nessa fase, o intuito é conhecer a finalidade e os princípios da LGPD.

Análise do fenômeno

Nessa etapa, devem ser identificados quais dados pessoais são coletados e tratados pela organização.

Análise do processo

Mapear, analisar e identificar as lacunas:

- mapear a categoria de todos dados pessoais coletados (empregados, terceiros, clientes etc.);

- mapear o fluxo dos dados pessoais (como são coletados, por quem, finalidade do tratamento, local de armazenamento – por exemplo, meio físico, e-mail, software –, com quem são compartilhados, quais os meios técnicos e administrativos de segurança dessas informações etc., se há transferência internacional de dados);

- averiguar a localização dos servidores e quem tem acesso a eles– por exemplo, empregados, terceiros, estrangeiro, dentre outros;

- mapear as empresas terceiras que prestam serviço para a organização;

- analisar os contratos vigentes – por exemplo: Há cláusula específica sobre proteção de dados? E sobre confidencialidade e responsabilidade administrativas, civis e/ou criminais no âmbito de proteção de dados?;

- verificar se há políticas, normas, procedimentos relacionados à segurança da informação, armazenamento e descartes de dados, gestão de risco, o que se deve fazer em caso de incidentes como vazamento de dados pessoais;

- quaisquer outras informações relevantes e específicas para a organização desenvolver um Projeto de Governança Digital.

Plano de ação

Criar um plano de ação que deve estar devidamente documentado e estruturado, ou seja, com as ações a tomar, responsável e prazo bem definidos.

Fase 2: Fazer

Executar o plano de ação..

Fase 3: Verificação dos resultados

- A Gestão de Segurança da Informação deve estar em conformidade integral com a LGPD.
- Todos os empregados devem estar treinados para que tenham ciência da importância do Projeto de Proteção de Dados.
- A proteção de dados deve fazer parte da cultura da organização.

Fase 4: Agir

- Padronização das normas e procedimentos.
- Fiscalização: mediante auditorias regulares, a aplicabilidade da LGPD e a eficácia do projeto devem ser monitoradas e relatórios de conformidade podem ser solicitados pela Agência Nacional de Proteção de Dados.

Esse método de análise e mudança de processos parte do pressuposto de que o planejamento não é uma fase esgotada – ou seja, não acontece uma única vez –, muito menos é absoluta. Por isso, no decorrer do projeto, pode ser preciso mudar o planejamento. O Ciclo PDCA ajuda a fazer exatamente esse controle, que é contínuo, contribuindo para que cada processo se desenvolva da melhor maneira possível.

Perguntas e respostas

Os empresários precisam estar atentos aos menores detalhes da sua organização e da vida de seus colaboradores e fornecedores sobre assuntos societários, financeiros, negócios e outros mais.

Nessas atividades, a empresa deve resguardar sigilo. A ética profissional é uma questão de sobrevivência. Qualquer empresa é um grande depósito de informações sensíveis e de grande valor, seja nos e-mails trocados internamente pelos sócios, seja na documentação arquivada: detalhes sobre a esfera privada de clientes e colaboradores, patentes, contratos comerciais, preços e valores, etc.

Selecionamos perguntas e respostas mais relevantes como uma orientação inicial para Instituições de Ensino ao processo de adaptação à nova Lei Geral de Proteção de Dados Pessoais, que passará a vigorar em 14 de agosto de 2020

1. Qual a urgência para começar a adequação da minha instituição à LGPD?

URGÊNCIA IMEDIATA. O prazo atual é de 2 (dois) meses para adequação de todas as medidas legais. A princípio pode parecer muito, mas não é. O trabalho é complexo, pois apurar lacunas quanto ao tratamento de dados na empresa exige esforço e sensibilização de várias lideranças da empresa, alguns eventos presenciais para coleta, análise e revisão dos dados pessoais e das medidas corretivas.

Será necessário que o enfrentamento dessas lacunas seja conduzido por várias pessoas, lideradas por alguém que tenha poder decisório, de modo a cumprir um cronograma de atividades no prazo de um ano. Não é uma tarefa fácil. As mudanças são necessárias, e os empresários têm de estar envolvidos nesse assunto, pois, caso contrário, os prejuízos serão percebidos apenas quando acontecer incidentes futuros.

2. O que a nova Lei determina no que diz respeito às atividades empresariais?

A LGPD define a natureza das informações coletadas nas atividades empresariais, como dados pessoais e sensíveis. Os dados pessoais sensíveis merecem a mais rígida proteção e privacidade, por se relacionarem à esfera íntima da pessoa, trazendo maior risco e potencialização de danos em casos de qualquer incidente relacionado aos dados pessoais,

3. Quais os dados pessoais de pessoas físicas mais usuais nas empresas?

- Informações obtidas pelo RH e/ou outros setores, tanto em papel como on-line, tais como: nome, dados de contato, e-mail, telefone, características físicas, pessoa física e jurídica ou outros.

- Dados necessários para a emissão de documentos fiscais, tais como nota fiscal e cupom fiscal.

- Referências comerciais para limite de crédito.

- Consulta à Serasa, ao Serviço de Proteção ao Crédito (SPC) e a outros.

- Vendas por meio de cheques, boletos bancários, cartão de débito e crédito.

- Força de vendas: por intermédio de representante ou colaborador CLT. Trata-se, na maioria das vezes, de um aplicativo no celular, onde são feitos cadastros e pedidos de vendas, bem como verificada a situação financeira dos clientes, etc. Geralmente esses dados ficam na nuvem e são controlados por terceiros que prestam serviços.

- *E-commerce:* vendas pela internet, onde são feitos cadastros de clientes, pedidos compras, pagamentos por meio de boletos, cartão de crédito e débito.

- Dados pessoais tratados pelos aplicativos visando à fidelização de clientes e descontos promocionais.

- Sistema de roteirização para logística e gestão de entrega, onde são tratados e compartilhados dados de clientes e colaboradores.

- Frente de caixa – autosserviço: o comprador pega a mercadoria e passa diretamente no caixa para finalizar o processo de aquisição.

- Campanhas de marketing.

Tanto as empresas como suas parceiras operam com dados pessoais, por isso é importante ressaltar que a coleta se restringe aos dados necessários para atingir a finalidade.

4. Nenhum dado pessoal poderá ser compartilhado?

Os dados pessoais podem ser compartilhados. O que ocorre com a LGPD é que todo ato de compartilhamento de dados da instituição que receber o consentimento do titular dos dados pessoais e repassar a terceiros precisa ser cuidadosamente documentado e informado ao cedente.

A Lei não visa, de forma alguma, restringir a utilização de dados pessoais para fins econômicos e, em alguns casos, pode-se revelar até mais flexível do que outras legislações setoriais. O que a Lei obriga é que a empresa garanta aos titulares que seus dados pessoais serão tratados com maior transparência, controle e segurança, sob pena de aplicação de sanções severas.

5. Que tipos de cuidado os empresários devem tomar a partir de agora?

O que muda é a forma de tratar os dados pessoais dos associados, que agora se torna obrigação legal, ao contrário das meras boas práticas do passado.

6. Quais operações corriqueiras ocorrem nas empresas que envolvem risco quanto ao tratamento de dados pessoais sujeitas às penalidades da LGPD?

A seguir, alguns exemplos onde os dados pessoais são tratados e merecem atenção redobrada quanto aos riscos envolvidos.

- **Compartilhamento de dados de clientes com terceiros:**
- fornecedores e indústria;
- representantes comerciais;
- empresas de *e-commerce*;
- fornecedores de serviços;
- empresas de cobrança;
- transportadoras;
- dados de cobrança com sistema bancários;
- dados de compra e situação financeira de clientes com os órgãos de proteção ao crédito;
- prestadores de serviços de cobrança;
- empresas que desenvolvem softwares;
- empresas de segurança, como monitoramento por câmeras.

- **Compartilhamento de dados de colaboradores:**
- convênios médicos;
- cartão de benefícios;
- convênios com farmácias, postos de gasolina, supermercados, etc.;
- empresas de transporte.

- **Operação de logística:**
- compartilhar dados de clientes para entrega de produtos;
- compartilhar dados de colaboradores;
- rastreamento por geolocalização ou GPS dos colaboradores na entrega;
- notificação on-line de clientes sobre a situação da entrega.

- **Operação de marketing:**
- envio de e-mail marketing para eleição;
- envio de *folders* promocionais/eleitorais;
- plataforma de envio de e-mails marketing.

- **Interação por Apps.**
- **Informação por WhatsApp.**

7. Qual é a forma correta de obter o consentimento para a coleta de dados pessoais?

De forma geral, o consentimento é uma exigência expressa da Lei, que determina formalizar com o titular quais dados pessoais serão tratados, com quem serão compartilhados e, sobretudo, para qual a finalidade serão utilizados. A LGPD exige alguns requisitos extras, especialmente no que diz respeito a garantir que o titular dos dados estará devidamente informado acerca de como seu dado pessoal será tratado. Essa atividade prevista na Lei é conhecida por "consentimento informado".

8. Existe algum cuidado especial a ser tomado na proteção de dados de menores de 18 anos?

Para os menores de idade, todas as obrigações de informação devem ser prestadas por um de seus representantes legais – pai, mãe ou tutor –, que será o responsável pelo consentimento expresso.
Percebe-se que vários procedimentos operacionais no tocante a dados pessoais devem ser revistos para conformidade legal. Os maiores des-

taques são o consentimento informado, a obrigação de informar a finalidade para a coleta de dados, a possibilidade de o titular revogar seu consentimento e criar uma central de atendimento para que o titular possa, a qualquer tempo, ser informado quanto a quais dados pessoais são tratados pela empresa, corrigir informações erradas ou até mesmo remover seus dados pessoais.

9. Se eu precisar compartilhar as informações pessoais com outras empresas, a quais cuidados devo estar atento?

Muitas empresas compartilham dados pessoais de clientes, perfil de compra e dados de representantes comerciais entre parceiros e terceiros.

Esses dados são utilizados para a avaliação de mercado, produtos, de serviços prestados, dentre outras necessidades. Todavia, essas finalidades não estão expressamente formalizadas com o titular dos dados pessoais, e essa é uma lacuna que precisa ser suprida. Como tratamento de dados pessoais, segundo a LGPD, deve ocorrer lastreado ao consentimento do titular, será necessário, portanto, que a concessão seja específica para as finalidades necessárias,

O compartilhamento das informações pessoais não é limitado ao ato do titular em consentir que a empresa com quem transaciona efetue o tratamento, mas será mandatória a autorização expressa do compartilhamento para outras finalidades.

É necessário avaliar o risco envolvido no compartilhamento, sobretudo quanto à necessidade de repassar informações além daquelas necessárias para o negócio.

A partir de agora, é obrigação das entidades que o tratamento de dados pessoais sempre ocorra da forma mais segura possível – ou seja, usando normas procedimentais previstas na Lei, como adequar contratos de prestação de serviços com fornecedores, revisar processos internos e externos para evitar os riscos de compartilhamento não autorizado com desvio da

finalidade consentida pelo titular.

Para mitigar ou garantir o risco da privacidade dos clientes, um mecanismo que pode ser usado é a omissão de alguns dados pessoais ao compartilhar com terceiros, ou seja, a anonimização total ou parcial dos dados que identificam o titular. Outra opção é a pseudoanimização, que significa a substituição dos dados pessoais que revelam a identidade do titular por outra fictícia.

É importante ter cuidado para que, no ambiente de trabalho, somente tenham acesso aos dados pessoais aqueles que de fato precisam tê-los, respeitando a finalidade do tratamento consentido pelo titular. Essa medida visa evitar casos de negligência ou vazamento proposital que possam vir a ocorrer.

A segurança nos dados passa a ser uma obrigação expressa da Lei, sujeita a penalidades. Por esse motivo, é mandatório que os gestores da organização exerçam a Governança digital – ou seja, conheçam os riscos envolvidos, enxerguem as lacunas atuais e executem as medidas corretivas antes da vigência da LGPD, em agosto de 2020.

10. Possuo serviços de terceiros que lidam com dados pessoais dos meus colaboradores, clientes, etc. Qual cuidado devo ter ao efetuar tais compartilhamentos e qual meu grau de responsabilidade sobre esses dados?

A responsabilidade quanto ao vazamento de dados por parte de empresários é **PLENA**. Certamente a vítima do vazamento vai requerer perdas e danos da empresa a quem ele consentiu o tratamento de dados pessoais. Por esse motivo, é preciso que a empresa esteja legitimamente preparada para agir contra aquele que deu causa ao incidente. Daí a necessidade das revisões imediatas de normas, contratos, processos e sistemas.

Esse risco deve ser avaliado e, se for considerável, recomenda-se a contratação de seguro cibernético para evitar danos potencializados.

Atualmente existe uma lacuna considerável que revela a necessidade de a instituição revisar seus contratos com terceiros relativos às obrigações que devem ter quanto ao tratamento de dados pessoais cuja finalidade for determinada.

A adoção da revisão contratual é uma das medidas que podem dar legitimidade à empresa para agir regressivamente contra terceiros que violarem as condições previstas para o tratamento de dados pessoais.

11. Para automatizar os processos internos e ter maior agilidade neles, utilizo vários serviços de terceiros em que compartilho dados de empregados e clientes. Muitos desses serviços estão em nuvem, e não tenho controle sobre esses dados, como são armazenados, quem tem acesso a eles onde estão hospedados. Como devo lidar com essas questões e o que devo exigir desses prestadores de serviços? A mesma situação se aplica ao *e-commerce*?

Todo terceiro que tratar dados pessoais também será alvo de conformidade no tocante à LGPD. Daí é necessário que este esteja em conformidade quanto a implantar recursos sistêmicos de segurança cibernética, além de se sujeitar às obrigações legais em relação à atividade de tratamento de dados pessoais, sob pena de sanções pesadas.

As mesmas informações se aplicam ao *e-commerce*, que nada mais é do que outra plataforma onde os dados pessoais serão tratados. Possivelmente, em razão de alguns aspectos tecnológicos envolvidos, algumas adequações deverão ser realizadas.

12. Se os dados forem vazados, posso ser considerado responsável por esse incidente de segurança?

Sim. Segundo a Lei, os empresários serão os responsáveis no caso de vazamento de informações.

Na legislação brasileira, todos aqueles que exercem o tratamento dos dados pessoais de terceiros são considerados controladores. Daí, a responsabilidade e o risco de penalidades administrativas, judiciais e reputacionais podem se estender, também, a agentes externos terceirizados que tratam de dados pessoais, caso forem vazados.

A partir de agora, portanto, o vazamento de dados implicará a responsabilização do empresário ou de sua organização pelos danos causados, dadas as vulnerabilidades da segurança da informação.

13. Quais as medidas de enfrentamento devo tomar para reduzir os riscos?

No cenário atual, em que as atividades econômicas são movidas a dados, é necessária a adoção de estratégias de proteção e segurança de dados, assim como de qualquer outro ativo da empresa, para evitar o risco de perdas financeiras,.

É importante perceber que a cada dia os dados, sobretudo aqueles sensíveis que revelam a esfera íntima das pessoas, adquirem valor próprio e se tornam um ativo ainda mais valioso, por isso merecem maior governança ante penalidades potenciais.

Além disso, será necessário colocar em prática um efetivo sistema de contingenciamento com apoio jurídico especializado em Direito Digital, para agir no tempo mais breve possível após o incidente. A potencialização do dano está ligada diretamente ao tempo de resposta para enfrentamento em conformidade legal.

Pela nossa experiência profissional, quando ocorre um vazamento de dados, normalmente a empresa demora, em média, 90 (noventa) dias para identificar o incidente – ou seja, o golpista já vem operando sem ser notado em um período muito superior ao que se imagina.

Com a adoção efetiva de um plano de contingenciamento sistêmico, estratégico e jurídico, será possível abreviar tais medidas corretivas de forma a reduzir os riscos, evitando que um fato se transforme numa crise.

Caso não haja um plano de contingenciamento, o enfrentamento será tardio e desordenado, e o prejuízo pode ser incomensurável. Já que os dirigentes da organização serão os responsáveis, devem se sujeitar às penalidades, inclusive quanto à exposição pública negativa do incidente. A necessidade de indenizar, nesse caso, independe da culpa da empresa, pois ela exerce uma atividade de risco.

Para que o plano de contingenciamento seja efetivo, é fundamental que ocorra a capacitação dos responsáveis para que cada um saiba em que momento correto e o prazo limite para cumprir suas obrigações nesse processo.

A LGPD, embora ainda não esteja em vigor, também dispõe de forma específica sobre o direito de o titular dos dados pessoais ser indenizado em casos de prejuízos decorrentes do vazamento de seus dados pessoais.

Além disso, a legislação obriga que o encarregado da proteção de dados da empresa comunique o fato à Autoridade Nacional de Proteção de Dados (ANPD) e ao "Conselho Nacional de e da Privacidade", órgãos que ainda precisam ser regulamentados, num prazo razoável a partir da data do incidente.

A referida comunicação, conforme exigência legal, deve conter, no mínimo, as seguintes informações: (i) natureza dos dados pessoais afetados; (ii) informações sobre os titulares envolvidos; (iii) indicação de medidas mitigadoras e de segurança utilizadas para a proteção dos dados; (iv) os riscos envolvidos no acidente; e, (v) caso a comunicação não seja imediata, as razões da demora.

14. Como minha equipe precisa atuar para a redução do risco envolvido no tratamento de dados pessoais?

- Manter todos os sistemas com a versão atualizada para reduzir os riscos de segurança da informação.

- Não compartilhar senhas com terceiros não autorizados.

- Consultar sempre os responsáveis pela TI, ou o comitê multidisciplinar que lida com assuntos relativos ao tratamento de dados pessoais, quando não souber realizar alguma atividade relativa a esse tratamento.

- Instalar programas e aplicativos nas máquinas somente quando expressamente autorizada.

- Nunca baixar arquivos sem saber do que se trata.

- Nunca clicar em links sem saber do que se trata.

- Orientar os clientes sobre seus direitos de forma clara e coerente, bem como revelar qual será a finalidade do tratamento de dados em conformidade com a legislação atual.

- Quando ocorrer um incidente, saber como preservar as provas em conformidade legal e quais as orientações da empresa quanto ao contingenciamento.

- Buscar orientação jurídica especializada o mais breve possível, para definir quais medidas extrajudiciais e judiciais serão tomadas, de modo a abreviar o enfrentamento e reduzir o risco.

15. A quais as medidas os colaboradores da minha empresa devem estar atentos?

- Mudar todas as senhas periodicamente.
- Controlar todos os acessos aos bancos de dados, backups e base de teste e homologação.
- Manter todo o sistema atualizado.
- Pesquisar histórico de falhas de segurança de todos os programas que cogitarem usar.
- Fazer um sistema de segurança de acordo com a expectativa legal.
- Fazer um plano de contingenciamento técnico e jurídico.
- Garantir que os processos operacionais relativos aos dados pessoais de terceiros estarão em conformidade legal.
- Manter o registro de todas as medidas que estão sendo tomadas em relação à segurança, como exige a Lei.
- Orientar, de forma clara e coerente, os clientes sobre seus direitos e revelar qual será a finalidade do tratamento de dados em conformidade com a legislação atual.
- Exigir dos prestadores de serviços atuais, com os quais faz compartilhamento de dados, que estejam em conformidade com a LGPD.
- Solicitar sempre orientação jurídica quando for contratar uma nova aplicação ou serviços de terceiros envolvendo dados pessoais.

- Quando ocorrer um incidente, saber como preservar as provas em conformidade legal.

- Buscar orientação jurídica especializada o mais breve possível p,ara definir quais medidas extrajudiciais e judiciais serão tomadas, de modo a abreviar o enfrentamento e reduzir o risco.

16. Mesmo que sejam os colaboradores da empresa que coletam os dados pessoais de terceiros, a empresa será responsável e estará sujeita às penalidades?

Sim. A LGPD atinge qualquer um que colete dados, seja pela internet, seja por outro meio. Quando um colaborador coleta dados para serem usados durante a execução de outras atividades empresariais, ele está agindo em nome da empresa, como subordinado, e a responsabilidade legal será dos gestores.

Isso significa que se sua instituição coleta dados, ou seu atendente os coleta em nome da instituição, a instituição será a responsável pela preservação, tratamento e armazenamento correto desses dados e pode ser obrigada a indenizar em caso de vazamento que gere prejuízo ao titular do dado pessoal.

Ainda que o atendente do nosso exemplo aja sozinho, em nome próprio, gerando o dano, a responsabilidade por proteger os dados pessoais continuará sendo da empresa. Caso a empresa armazene os dados pessoais em locais inseguros e ocorra vazamento ou outro incidente, a responsabilidade também será a mesma.

17. Quais são as medidas essenciais para assegurar a adequação de uma empresa à LGPD?

Ao nos referirmos a dados pessoais, o maior risco em termos financeiros será quando ocorrer vazamento – ou seja, na possibilidade de exposição dos dados pessoais para terceiros que não têm autorização para ter acesso a eles ou desvio de finalidade de tratamento. Para evitar isso, cinco medidas são essenciais para garantir a adequação à Lei:

- utilizar sistema de segurança compatível com os riscos específicos da sua forma de armazená-lo, construído de acordo com as necessidades do seu negócio, que proteja esses dados pessoais e sensíveis;

- adotar plano de contingenciamento sistêmico e jurídico capaz de abreviar o tempo de enfrentamento e reduzir os danos de eventual vazamento;

- verificar se os registros eletrônicos gerados pelos sistemas de segurança são capazes de revelar todas as atividades relativas ao tratamento dos dados, de forma que tais informações possam ser acessadas e preservadas como meio de prova. Essas provas poderão ser decisivas num processo judicial oportunamente;

- dar ampla ciência do incidente aos titulares de dados pessoais envolvidos por meio de comunicação pública, informando quais os dados vazados, o risco de golpes que podem ocorrer a partir desse vazamento, quais medidas jurídicas ou operacionais devem ser adotadas para reduzir o risco.

18. Quais medidas minha empresa deve tomar para estar em conformidade com a LGPD?

- Criar ou revisar a forma pelo qual o colaborador ou cliente vai consentir e tomar ciência da finalidade do tratamento de seus dados pessoais, assegurando a possibilidade da revogação desse consentimento futuramente.

- Adotar medidas de proteção dos dados: contar com a consultoria de especialistas para montar um plano de contingenciamento de segurança digital e medidas legais para abreviar o tempo de resposta ao incidente, reduzindo o alcance dos riscos e prejuízos financeiros.

- Criar um canal de comunicação que permita ao titular dos dados a ciência, a alteração ou a revogação do seu consentimento para tratamento de seus dados pessoais.

- Tornar anônimos ou pseudônimos os dados pessoais compartilhados com terceiros, se possível, como medida de reduzir o risco.

- Capacitar os colaboradores quanto à segurança da informação e proteção de dados, exemplificando os riscos legais e as medidas procedimentais que serão implantadas.

- Manter-se atualizado quanto às melhores práticas operacionais para o tratamento dos dados pessoais de terceiros.

19. Como a minha empresa deve adotar medidas de segurança da informação e um plano de contingenciamento?

A adoção dessas medidas tornou-se obrigação legal, por isso é recomendável que a equipe destacada para executar tais atividades conte com um profissional especializado em Direito Digital, além de um profissional da área de TI, um responsável pela área de Governança, um

representante do setor de Recursos Humanos e de Comunicação, bem como da coordenação de um responsável que tenha poderes decisórios.

Com relação aos procedimentos técnicos, estes devem ser executados por meio de sistemas especialistas de processamento e armazenamento de informações que possam gerar robusta trilha de registros eletrônicos para facilitar o processo investigatório de identificação de autoria do agente que cometeu o ilícito e outros responsáveis.

Quanto à lacuna de capacitação dos colaboradores, é necessário investir em treinamentos e na formalização da sua ciência, no que diz respeito à Política de Segurança da Informação da empresa. Trata-se de um ato normativo necessário de uso interno que define os limites de uso da infraestrutura de tecnologia da informação, os procedimentos a adotar pelos colaboradores e prestadores de serviço, as permissões de acesso, locais ou remotos, e os dados tratados pela empresa.

O plano de contingenciamento envolve respostas jurídicas e tecnológicas para possibilitar a apuração e o enfrentamento com a maior brevidade possível após o incidente, de modo a tomar medidas corretivas em conformidade legal para reduzir os riscos e prejuízos financeiros envolvidos.

O zelo às regras de proteção de dados e privacidade, embora envolva uma série de medidas operacionais complexas e até então inimagináveis, deve ser encarado pelos gestores de atividades de atacado e varejo não apenas como custo, e sim como um diferencial para competitividade no mercado, de modo a potencializar e adequar uma reputação de credibilidade perante seus colaboradores e clientes. Tais medidas se revelam como novos hábitos para combater os riscos da economia digital globalizada, lastreada em dados que se tornaram ativos importantes e regulados pela legislação brasileira e demais atos regulatórios.

Conclusão

A LGPD é uma conquista da sociedade brasileira e coloca o Brasil num patamar alinhado com mais de cem países, onde se valoriza o respeito à privacidade.

Como já relatamos, este é um guia introdutório, criado com o objetivo de guiar os empresários no exercício de seu papel de governança, a fim de executarem a adequação à LGPD, além de sugerir um plano de trabalho para a adoção de medidas exigidas pela Lei.

As empresas terão problemas para se adequar por conta própria à nova Lei. Por isso, dependendo da complexidade do tratamento de dados pessoais, será necessária a ajuda de profissionais especializados.

O cumprimento da Lei não se esgota. É um trabalho contínuo.

É chegada a hora de dar início a esta caminhada!

Bom trabalho. Conte com nossa equipe!

Abril / 2020.

ALEXANDRE ATHENIENSE ADVOGADOS

FALE COM A GENTE

São Paulo • Belo Horizonte • Brasília

- www.atheniense.com
- facebook.com/alexandreathenienseadvogados
- contato@alexandreatheniense.com.br

- Av. Afonso Pena, 4273, 4º andar - Belo Horizonte, MG

Photo by Philipp Birmes from Pexels

ALEXANDRE ATHENIENSE ADVOGADOS
DIREITO DIGITAL
32 anos

JUNHO 2020

SÃO PAULO

Avenida Paulista 1079,
Torre João Salem, 8º andar
São Paulo - SP
55 11 99502-8128

BELO HORIZONTE

Avenida Afonso Pena,
4273, 4º andar
Belo Horizonte - MG
55 31 3318-1414

BRASÍLIA

SCS, Quadra 09, Bloco C,
Torre C, 10º andar
Comercial Sul, Brasília
55 61 99622-8128

www.atheniense.com