SILVA SANTANA & TESTON
ADVOGADOS

ACATE ASSOCIAÇÃO CATARINENSE DE TECNOLOGIA

Governança em Privacidade e Proteção de Dados

Orientações Práticas para atendimento à Lei Geral de Proteção de Dados

LEI N. 13.709/2018

Introdução

A LGPD tem sido muito discutida e como se trata de uma lei multi-disciplinar você já deve ter ouvido recomendações com enfoques distintos sobre o que você tem que fazer para adequar sua empresa. Há quem se concentre nos esforços de segurança da informação. Há quem aborde exclusivamente os direitos dos titulares. Outros abordam apenas a questão da legalidade. A verdade é que a lei exige um pouco de tudo: segurança, legitimidade, gerenciamento de pessoas, cultura organizacional e atendimento de direitos de titulares. Não adianta você ter dados seguros, se estes dados nem deveriam estar sob sua posse, se seus dados foram coletados ou estão sendo tratados de forma ilegítima. Também não adianta ter uma base de dados absolutamente legítima, mas vulnerável, sem atender a requisitos de segurança.

Ainda que suas operações contemplem dados seguros e legítimos, sua empresa não estará regular se não tiver capacidade de atender solicitações e direitos de titulares. A questão, portanto, é instituir "Governança de Dados." Ter processos e controles internos que assegurem gerenciamento, legitimidade e segurança de dados.

Proteção de Dados, Desenvolvimento e Inovação

Um equívoco muito comum quando se trata da Lei Geral de Proteção de Dados é falar que as novas regras acabam barrando o progresso tecnológico, o investimento em novos negócios ou desenvolvimento de novas soluções. Isso não é verdade.

Em primeiro lugar, é importante lembrar que além da privacidade e proteção de direitos de personalidade, a LGPD tem outros fundamentos, por exemplo, o tratamento de dados como ferramenta para o desenvolvimento econômico e tecnológico. Além disso, não é intenção do legislador criar qualquer tipo de barreira aos negócios.

O que existe, na verdade, é uma preocupação em exigir de cada negócio atenção cuidadosa aos princípios de proteção de dados em cada uma de suas atividades que envolva tratamento de dados pessoais.

Se determinada inovação ou determinada nova ferramenta envolve tratamento de dados pessoais com uma finalidade bem identificada e legítima, e observando princípios da proteção de dados como transparência, segurança e minimização, é provável que essa inovação seja lícita. A questão, portanto, não é deixar de fazer ou deixar de inovar. É conciliar novos negócios, novas ferramentas, com os princípios de proteção de dados pessoais que, afinal, são de interesse de todos nós.

Hipóteses de Legitimidade

Com a edição da LGPD, cada operação de tratamento de dados precisa ter uma finalidade legítima de acordo com as hipóteses permitidas em lei. No que diz respeito à proteção de dados pessoais, o princípio de legalidade se traduz em tudo o que não for expressamente permitido pela lei é presumidamente proibido.

As permissões para tratamento de dados pessoais constam do art. 7º da Lei. São 10 as hipóteses de legitimidade que podem validar as operações de tratamento. A mais conhecida e comentada com a edição da LGPD é a hipótese do processamento de dados sob o consentimento do titular.

Consentimento é a modalidade que (em tese) menos invade a esfera de privacidade dos titulares, mas não é a única finalidade legítima de acordo com o legislador. Existem outras 9 finalidades permitidas em lei, todas contemplando a operação de tratamento de dados sem consentimento, mas que buscam efetivação de outros direitos e obrigações. Por exemplo, o tratamento de dados para cumprimento de dever legal, para execução de contrato, para defesa de interesses em processos judiciais e ou administrativos, para a garantia da segurança ou saúde do titular e de terceiros dentre outras.

É importante, repito, que a empresa cuide de identificar, para cada operação que envolva tratamento de dados pessoais, uma base legal dentre as que constam do art. 7°. Esse é um ponto de elevada atenção na lei.

Dados Pessoais e Riscos

A Lei Geral de Proteção de Dado Pessoais atribui aos processadores de dados, em meio eletrônico ou não, o ônus de avaliar suas atividades negociais, entender seus processos, analisar as medidas de segurança de informação empregados e, ao fim, interromper tratamentos que não tenham amparo legal (falta de legitimidade), assegurar que os dados tratados estejam seguros e planejar ações de correção, ajuste e melhoria nos processos de governança, em especial aqueles voltados ao atendimento de direitos dos titulares.

Em outros termos, a Lei exige que se implemente processos de avaliação e gerenciamento de riscos.

Na tarefa de dimensionar, avaliar e mitigar riscos, compreender as distinções entre os diversos tipos de dados pessoais de acordo com a lei é um primeiro passo crucial.

Tipo de Dado Pessoal	Exemplos	Impacto em caso de exposição
Dado Sensível	Dado médico; Exame de saúde; material genético; orientação sexual; origem étnica; filiação partidária; etc	Máximo
Dado Pessoal Direto	Nome; CPF; Foto; Vídeo; Documento de Identidade	Moderado
Dado Pessoal Indireto	Endereço de IP; Endereço de e-mail; placa do automóvel; registro de navegação; número de telefone	Baixo
Dado Pseudonimizado	Dados submetidos a Criptografia reversível ou submetidos a medidas como desagregação ou obscurecimento;	Muito Baixo
Dado Anonimizado	Dado que não pode ser acessado sem emprego dos mellhores esforços técnicos; dados mascarados e obscurecidos que não permitem reversão de anonimização	Inexistente

Numa escala de riscos, os dados pessoais sensíveis importam cuidados superiores aos dados pessoais diretos ou indiretos em razão da maior criticidade dos impactos.

Daí porque a lei exime de proteção os dados anonimizados, aqueles que não permitem identificação. A intenção é estimular métodos de anonimização ou, quando não possível, pseudonimização. São dados que envolvem menos riscos quando tratados.Ao avaliar riscos e endereçar medidas de salvaguardas em relatórios de impacto, identificar os dados que são tratados e o tipo de risco envolvido é fundamental para justificar a legitimidade de tratamentos.

Programa de Governança da Privacidade

Para que possam efetivamente alegar que observam a proteção de dados pessoais na forma da lei, além de validar as questões de segurança, gerenciamento e legitimidade de dados, os controladores e operadores deverão evidenciar o desenvolvimento e implementação de um programa de governança em privacidade.

Este programa contemplará processos e controles internos voltados a assegurar a adoção das melhores práticas de gestão de dados e de monitoramento do uso seguro e legítimo de dados pessoais. **Todas as áreas e todos os colaboradores das empresas devem ser engajados nesse compromisso.** É preciso, portanto, comunicar e fazer cumprir essas políticas internas.

Além disso, as empresas terão que adotar mecanismos de monitoramento, auditoria, revisão e constantes revisões. **Não existe um programa específico que atenda a todas as infinitas realidades corporativas. Cabe a cada empresa avaliar que tipo de processos e controles são adequados às características de seus negócios.** O importante é que estabeleça processos de avaliação de legitimidade das operações de

tratamento de dados, mecanismos técnicos e gerenciais de segurança e planos de monitoramento e resposta a incidentes.

O programa, portanto, deve levar em consideração o grau de risco e a estimativa de impacto potencialmente causadas pelas operações de tratamento de dados de cada empresa.

Por onde começar?

Não existem receitas ou estradas únicas para alcançar algum grau de adequação e para desenvolver um programa de privacidade e proteção de dados. Cada empresa deve adotar os mecanismos, avaliações e trabalhos de desenvolvimento proporcionais aos riscos que assume.

O que é crucial, de imediato, é a compreensão da lei. Sugerimos a leitura do texto legal e que, passo a passo busque compreensão com apoio de comentários ou conteúdo relacionado a cada disposição em específico.

Quando iniciar a parte prática, a ideia é começar por avaliar riscos, identificar os processos que envolvem dados pessoais, mapear as bases de dados e traçar um plano de ação. Considerando a quantidade de trabalho, é importante que cada empresa, controladora ou operadora de dados, institua uma equipe ou um profissional para se dedicar a esse programa. Solicitar apoio de especialistas é altamente recomen-

dável.

Existem algumas metodologias disponíveis e diferentes abordagens de concepção de um programa. Novamente, cabe a cada empresa entender que tipo de esforço supre o risco envolvido em seus negócios.

Acreditamos que ter uma boa visão sobre o que compõe e pra que serve o programa a ser desenvolvido, ajudará nos trabalhos de apuração e avaliação de riscos e de mapeamento dos dados pessoais tratados. Na prática temos acompanhado vários projetos de mapeamento travados pela dificuldade de compreender a importância de cada informação que é levantada.

Por fim, insisto que troca de experiências é fundamental, pois tudo é muito novo. Além da lei contemplar exigências até então inexistentes, as formas como tratamos dados se renovam com muita rapidez. Nesse cenário, é importante ter em mente que sempre haverá pontos de melhoria, por isso o compartilhamento de experiências e a colaboração é uma melhor prática de quem se esforça para estar em conformidade.

Avaliação de Operações e Bases

Uma atividade importante e que toda empresa deve desenvolver é avaliar cada uma de suas atividades de tratamento de dados. Nesse caso, a recomendação é listar as atividades que cada área da empresa

executa envolvendo tratamento de dados pessoais. Cada uma dessas atividades será identificada como "Operação".

Para cada operação, deveremos levantar informações sobre quais dados pessoais são tratados, quando e como são obtidos, por quanto tempo são armazenados, para que finalidade são necessários, com quem são compartilhadas e atribuir uma base legal (hipótese de legitimidade). Esses são os critérios mínimos que um mapeamento de operações exige para que a legitimidade do processamento seja avaliada.

Sugerimos que essa avaliação seja executada em todas as áreas. Apresentamos uma relação de atividades a serem mapeadas e um exemplo de como fazer essa avaliação com algumas operações no setor de RH em apêndice.

Essa etapa é bem trabalhosa e costuma levar tempo, pois as pessoas envolvidas já estão sobrecarregadas por suas atividades negociais. É importante impor um prazo limite. Sugerimos pelo menos 30 dias para que as atividades não prejudiquem o andamento regular da empresa.

Ao fim desses trabalhos, a empresa terá capacidade de identificar, dentre outros pontos:

(i) se não a totalidade, a parte mais significativa de suas "operações de tratamento de dados pessoais", cujo registro é uma exigência da LGPD;

(ii) se não a totalidade, a parte mais significativa dos sistemas e ferramentas utilizados para gestão de dados pessoais, os quais deverão ser validados pela área de TI e terão termos de privacidade e contratos revisados pelo jurídico;

(iii) e quais operações envolvem tratamento de dados pessoais sensíveis, que serão objeto de uma avaliação de segurança urgente;

(iv) quem são os terceiros com os quais a empresa compartilha dados pessoais, e com os quais serão celebrados ou revisados contratos para estabelecer a forma de compartilhamento legítimo;

(v) as bases legais e as finalidades para as quais a empresa trata dados pessoais, podendo assegurar a boa-fé e legitimidade de suas atividades de processamento de dados.

Estruturando o Programa de Privacidade e Proteção de Dados

Não há uma estrutura pré-concebida do que seja um Programa de Governança em Privacidade e Proteção de Dados, uma exigência expressa da lei.

Quando falamos em um Programa de Governança em Privacidade e Proteção de Dados, estamos tratando da expectativa de que as empresas construam formalmente uma estrutura de esforços para desenvolver e

manter uma cultura de privacidade e proteção de dados corporativa. Nesse caso, estamos falando de uma visão empresarial sobre como a estrutura de tecnologia da informação, de instrumentos jurídicos, de organização negocial, de gestão de pessoas e processos e de concepção de negócios, leva em consideração a preocupação com privacidade em seu dia a dia.

Entendemos que o desenvolvimento de um Programa de Governança em Privacidade e Proteção de Dados contemple:

(a) **A estruturação organizacional de responsáveis pela Privacidade e Proteção de Dados.**

Além da figura do encarregado de tratamento de dados, exigida pela lei, a empresa deverá instituir um comitê de proteção de dados formado por profissionais de diversos segmentos e necessariamente por alguém da alta direção. Outros comitês relacionados são importantes, como o de Gestão de Incidentes de Segurança e de Ética e Disciplina. Logicamente esses comitês são dispensáveis em empresas com pequena quantidade de empregados/colaboradores.

(b) **Respaldo Financeiro aos Esforços em Privacidade e Proteção de Dados**

A empresa deverá demonstrar apoio efetivo aos esforços constantes de aprimoramento de maturidade em privacidade e melhorias em segurança da informação. Uma forma de executar esse objetivo é

fazer registrar que investimentos em governança de dados (segurança e gerenciamento de TI) constarão dos orçamentos anuais.

(c) **Conscientização e Gerenciamento de cultura em Privacidade**

Instituição de atribuições, treinamentos, reforços institucionais de cuidados, divulgação de políticas e de recomendações de segurança e responsabilidades, engajamento, desenvolvimento e manutenção de cultura.

(d) **Formalização de Políticas e Procedimentos**

Instrumentalização de políticas de proteção de dados, de segurança da informação, de desenvolvimento seguro, procedimentos de denúncias, de sugestões, de questionamentos, procedimentos de prevenção, etc.

(e) **Instituição de Ferramentas Técnicas e Gerenciais**

Adoção de procedimentos de revisão e monitoramento de uso de dados, monitoramento investigativo de ferramentas corporativas, adoção de soluções de compartilhamento seguro e controlado de informações, soluções de data loss prevention, etc.

(f) **Planejar Enfrentamento de Incidentes**

Desenvolvimento, teste e revisão de plano de resposta a incidentes, plano de continuidade de negócios, estruturação de comunicação

com titulares, parceiros, clientes e terceiros interessados.

(g) **Gerenciamento de Direitos de Titulares**

Revisão e atualização de procedimentos para recebimento e resposta a solicitações de titulares (direitos de informação, de edição, de oposição, de exclusão), e de gestão de consentimento.

Levantamento de Operações de Tratamento de Dados Pessoais

Embora cada organização deva elaborar o levantamento de suas operações com nível de detalhamento adequado ao volume e impacto de suas atividades, sugerimos que esse mapeamento leve em consideração no mínimo a avaliação abrangente dos dados tratados setorialmente na empresa: RH; financeiro; comercial; marketing; administrativo/patrimonial; jurídico; T.I.; produto.

Cada área terá sua especificidade, portanto é importante que o time de privacidade leve em conta quais operações cada departamento realiza e que, obviamente, envolvam o tratamento de dados pessoais. No mapa de levantamento abaixo propomos um esquema de como colher as informações que poderão auxiliar a descrever o ciclo de vida dos dados pessoais tratados em algumas operações promovidas pela pela área de RH:

SETOR DE RH										
Operação	**Finalidade**	**Base Legal**	**Quais dados são tratados?**	**Qual a forma de coleta?**	**Quem disponibiliza os dados?**	**Por quanto tempo os dados são tratados?**	**Onde os dados são armazenados?**	**Quais as medidas de segurança?**	**É compartilhado externamente? Se sim, como?**	**Estimativa de titulares alcançados**
Recrutamento e Seleção										
Contrato de Trabalho										
Benefícios (Saúde, Alimentação, Transporte)										

É importante que seja considerado o tratamento dos dados pessoais relacionados à cada operação para entender as peculiaridades de cada atividade do setor. Com o mapeamento de todas as áreas, será formado o registro de operações (art. 37), exigência expressa da LGPD.

O papel do Encarregado pelo Tratamento de Dados Pessoais

A Lei prevê a criação do cargo de Encarregado. O profissional nomeado, além de garantir que a organização faça tratamento de dados pessoais em conformidade com a LGPD, atuará como canal de comunicação entre o controlador, os titulares dos dados e a ANPD.

É importante que a nomeação esteja baseada em qualidades pessoais e profissionais, mas atenção especial deve ser dada ao conhecimento especializado em proteção de dados. Algumas organizações atribuem

a responsabilidade de Encarregado a alguém da área de TI, segurança da informação ou recursos humanos. Ainda, é possível atribuir responsabilidades de Encarregado a uma empresa contratada.

As atividades do Encarregado incluem:

(i) Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

(ii) Receber comunicações da autoridade nacional e adotar providências;

(iii) Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;

(iv) Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Além dessas atividades, a autoridade nacional poderá definir outras atribuições do encarregado, bem como hipóteses de dispensa da necessidade da sua indicação, a depender da natureza e do porte da sua organização ou do volume de operações de tratamento de dados pessoais.

Por fim, a organização deverá disponibilizar publicamente um canal para tratar sobre privacidade e proteção de dados, preferencialmente

nos sites e plataformas de contato com o público e mercado, sendo este gerenciado pelo encarregado para atendimento às solicitações de titulares (Exemplo: privacidade@empresa.com.br)

Relatório de Impacto de Proteção de Dados

Nos casos em que um tratamento de dados pessoais possa resultar em alto risco às liberdades civis e aos direitos fundamentais, a sua organização, na posição de controladora de dados, deverá elaborar um relatório de impacto à proteção de dados pessoais. Este documento deverá conter a descrição dos processos de tratamento de dados pessoais, bem como as medidas, salvaguardas e mecanismos de mitigação de riscos, mapeamentos, treinamentos, auditorias e políticas de proteção de dados.

O Encarregado de Proteção de Dados ou um especialistas em privacidade e proteção de dados deve ser consultado para ajudá-lo na confecção do documento, ajudando a identificar as bases legais de tratamento, bem como identificar e avaliar os riscos.

A identificação e avaliação de riscos consistem em elencar as ameaças, a probabilidade, o impacto e o nível de risco para que sejam mitigados com a adoção de medidas de segurança 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 qualquer forma de tratamento inadequado.

Nem sempre, importa anotar, a sua organização necessitará eliminar todos os riscos. Alguns riscos podem ser entendidos como aceitáveis, tendo em vista os benefícios do tratamento dos dados pessoais e as dificuldades de mitigação. De todo modo, é recomendável consultar a ANPD antes de prosseguir com as operações de tratamento de dados pessoais se após a adoção de medidas de controle ou mitigação seja identificado um risco residual de nível alto ou crítico.

Por fim, sempre que o tratamento tiver como fundamento exclusivo a promoção de um interesse legítimo (art. 7º, inciso IX da LGPD), a autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais.

Boas Práticas em Segurança da Informação

A Lei alçou a segurança de dados ao patamar de princípio da proteção de dados. Isto significa que a adoção de medidas de segurança deve estar no centro da sua abordagem de tratamento de dados pessoais,

obrigando todos os agentes de tratamento ou qualquer outra pessoa que participe das fases do ciclo de vida do tratamento de dados pessoais a assegurar a segurança da informação para proteção dos dados pessoais.

As medidas de segurança incluem, dentre outras:

(a) Proteção de perímetro. Um firewall bem configurado protege sua organização contra acesso não autorizado e intrusões a partir da Internet.

(b) Controle de Acesso e Identidade. Os funcionários da sua organização precisam ter permissões de acesso na medida do necessário para cumprir suas funções. Além disso, no caso de uma violação de segurança, você terá uma referência para detalhar seus logs e encontrar a causa raiz.

(c) Complexidade de Senhas. É preciso adotar uma política de complexidade de senhas para mitigar os riscos de acesso não autorizado e evitar ataques de força-bruta bem-sucedidos.

(d) Segurança dos terminais. Os terminais devem ser verificados regularmente contra softwares maliciosos. Além da verificação, é importante revisar os avisos de alerta e seguir as recomendações de uso e de atualização de versões dos licenciadores de sistemas.

(e) Criptografia de dados. É recomendável o uso de criptografia de

dados pessoais em repouso e/ou em trânsito.

(f) Gerenciamento de patches e vulnerabilidades. Manter os softwares atualizados para evitar que suas vulnerabilidades sejam exploradas. Considere também a realização de testes de segurança, como pentests.

(g) Gerenciamento de backup. Se os dados forem comprometidos, um dos pilares da segurança da informação, que é a disponibilidade, estará comprometido. A indisponibilidade dos dados pessoais viola o princípio da segurança.

(h) Programas de conscientização. A conscientização dos funcionários é essencial para a segurança dos dados. Fomentar uma cultura de segurança e proteção de dados garante que os funcionários e os parceiros saibam o que é esperado deles. Sessões regulares e contínuas de treinamento garantirão que as informações, orientações, legislações e regulamentações mais recentes sejam conhecidas e compreendidas.

Riscos de não cumprimento da LGPD

Como toda norma jurídica que impõe condutas, a LGPD estabelece sanções para a hipótese de descumprimento. Deste modo, os agentes de tratamento de dados, em razão das infrações cometidas à previ-

são normativa, ficam sujeitos a sanções administrativas aplicáveis pela autoridade nacional, que vão desde advertências, multas à proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Além dessas penalidades, é preciso levar em consideração a perda de negócios e da confiança da marca, bem como perdas financeiras relacionadas a eventuais processos administrativos e judiciais.

Muitas organizações, conscientes dos riscos que corre, estão exigindo dos seus parceiros que estejam em conformidade com a LGPD, como condição para fazer negócios. Portanto, é importante que a sua organização esteja preparada para receber solicitações de documentos capazes de demonstrar suas iniciativas de proteção de dados.

O não cumprimento dessas solicitações pode resultar em perdas de negócios para os concorrentes que são capazes de demonstrar sua conformidade.

Esteja preparado para as violações de dados pessoais

Diante de um incidente, não é incomum que advogados especialistas e outros profissionais sejam acionados para conter o incidente, realizar investigações forenses e orientar, do ponto de vista jurídico, como a organização deve proceder.

De todo modo, isso não significa que a sua organização não possa se preparar minimamente para agir diante de uma eventual violação de dados. Há muitas coisas que podem e devem ser feitas antes que um incidente de segurança ocorra.

É importante lembrar que a LGPD estabelece que o controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. A comunicação deverá ser feita em prazo razoável, conforme definido pela autoridade nacional, mencionando, no mínimo:

- A descrição da natureza dos dados pessoais afetados;
- As informações sobre os titulares envolvidos;
- A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- Os riscos relacionados ao incidente;
- Os motivos da demora, no caso de a comunicação não ter sido imediata; e
- As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Portanto, você deve considerar a elaboração de um plano de resposta a violações de dados pessoais que englobam, além dos pro-

cedimentos relacionadas à comunicação, as medidas para reverter ou mitigar os efeitos do incidente. Para que o plano seja bem-sucedido, é crucial que a alta gerência o valide e esteja envolvida em todas as etapas do ciclo de gerenciamento de incidentes de segurança.

Pense nisso: se a sua organização sofrer uma violação de dados, você sabe quais devem ser os procedimentos adotados diante da autoridade nacional e dos titulares?

Responsabilização e prestação de contas

Por mais que as organizações brasileiras, de maneira geral, ainda não tenham uma boa cultura de proteção de dados e privacidade bem consolidadas em seus ambientes de negócios, é preciso entender que o princípio de responsabilização e prestação de contas estabelecido pela LGPD obriga as organizações a demonstrarem a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Será preciso, portanto, passar da teoria para a prática, transformando os requisitos legais da nova legislação em comportamentos operacio-

nais compatíveis e sustentáveis.

A esse respeito, entendemos que, minimamente, para atender ao princípio de responsabilização e prestação de contas, sua organização deverá:

- Desenvolver políticas internas de proteção de dados, aprovadas e endossadas pelo mais alto nível de gestão da organização.

- Informar e treinar colaboradores e funcionários sobre como implementar as políticas.

- Atribuir a responsabilidade ao mais alto nível da organização para o acompanhamento do Programa de Governança de Privacidade, avaliando e demonstrando às partes externas interessadas e à ANPD a qualidade do programa.

- Estabelecer procedimentos para correções de não conformidade e violações de dados.

Due diligence: verificação da conformidade de operações de tratamento de dados pessoais de operadores e terceiros

Um aspecto muito importante tratado pela LGPD refere-se ao regime de responsabilidade civil e ressarcimento de danos aplicável aos agen-

tes de tratamento de dados caso violem a referida lei, resultando em danos a outrem. Para a Lei, o tratamento será considerado irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular de dados dele poderia esperar.

Caso o controlador ou o operador de dados pessoais, em razão do exercício da atividade irregular de tratamento de dados causar a outrem dano patrimonial, moral, individual ou coletivo, está sujeito a reparar o dano. Dessa forma, os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados, mesmo que o responsável direto pelo dano tenha sido o operador, responderão solidariamente. De igual modo, o operador responderá solidariamente pelos danos causados pelo tratamento, caso descumpra as obrigações estabelecidas pela lei ou quando não seguir as instruções lícitas do controlador.

Esta é a importância de a empresa implementar um processo de due diligence com o fim de verificar se operadores e terceiros, como fornecedores e prestadores de serviços, estão em consonância com os acordos contratuais e se representam algum risco.

Para aqueles riscos considerados altos, uma verificação mais minuciosa será de fundamental importância, demandando um profissional que entenda como os requisitos da LGPD se aplicam à relação que está sendo verificada.

Ao realizar essas verificações, sua organização oferecerá mais evidências de que agiu com responsabilidade. Avaliações regulares também demonstram compromisso com a melhoria contínua. Estes são pontos que, certamente, serão levados em consideração no juízo de gravidade de eventual incidente de segurança ou tratamento irregular de dados pessoais.

Autores

Norival Raulino da Silva Junior

Gestor da Área de Direito Digital da SST. Graduado em Direito pela UFSC, pós-graduado em Direito da Comunicação Digital pela FMU, com especialização em Direito Digital pelo INSPER e em Direito da Propriedade Intelectual pela PENNLAW. MBA em Tecnologia para Negócios (PUCRS). Certificações Internacionais em Gestão da Privacidade (CIPP/E; CIPM - IAPP) e em Segurança da Informação e Proteção de Dados (EXIN).

Maria Paula Ferreira

Advogada na área de Direito Digital da SST. Graduada em Direito pela UNIVILLE. Pós-Graduada em Direito Empresarial pela FGV e em Direito Digital, Inovação e Novas Tecnologias pela Católica-SC. Certificação Internacional em Privacidade e Proteção de Dados Pessoais e em Gerenciamento de Segurança da Informação. DPO (EXIN).

Ricardo Cordoba Baptista

Advogado na Área de Direito Digita na SST. Consultor em Segurança da Informação, com mais de 15 anos de experiência em soluções de segurança de dados. Pós-Graduado em Segurança da Informação pela Estácio e em Direito Digital e Compliance pelo Instituto Damásio. Certificação Internacional em Privacidade e Proteção de Dados Pessoais e em Gerenciamento de Segurança da Informação. DPO (EXIN).

SILVA SANTANA & TESTON
ADVOGADOS

Rua Orestes Guimarães, 786,
1º Andar América, Joinville/SC
(47) 2101-3600
contato@sst.adv.br

ACATE ASSOCIAÇÃO CATARINENSE DE TECNOLOGIA

Rod. José Carlos Daux - SC 401,
4120 - km 4, Bairro Saco Grande,
Florianópolis/SC
(48) 2107-2700
contato@acate.com.br