MANUAL
DA
LEI GERAL DE PROTEÇÃO DE DADOS-LGPD
LEI Nº 13.709/2018.

A Lei n° 13.709, publicada em 15 de agosto de 2018, e que entrou em vigor 18 de setembro de 2020, também conhecida por Lei Geral de Proteção de Dados (LGPD), foi inspirada no modelo da regulação europeia de proteção de dados (GDPR), tem como seus princípios base a proteção à privacidade, a liberdade de expressão e a inviolabilidade da intimidade, honra e imagem, conferindo aos dados pessoais relevância de ativo intangível, na medida em que a sociedade é, cada vez mais, movida por dados.

A nova Lei introduz mudanças muito significativas, que deverão transformar a abordagem da privacidade por parte de empresas e de indivíduos, afetando todos os setores da economia e entes públicos, bem como relações entre clientes e fornecedores de produtos e serviços. E para que o Leitor entenda como a nova Lei poderá impactar seus negócios, iremos abordar neste manual os principais pontos tratados pela LGPD, e quais providências deverão ser tomadas para estar em conformidade com as exigências estabelecidas neste dispositivo legal.

O Grupo Interativa tem como missão apoiar, orientar e capacitar nossos clientes e colaboradores na tomada de decisões relacionadas à proteção de seus negócios dentro desta nova sociedade digital.

ÍNDICE

Revisão: 02 de 19/12/2024.

I - Definições da LGPD

Dado pessoal: Informação relacionada a pessoa natural.

Dados pessoais sensíveis: informações de origem racial/étnica, religiosa, política, filosófica, a vida sexual, à saúde, genética e biométrica.

Titular: Pessoa natural a quem se referem os dados pessoais que são objetos de tratamento.

Anonimização: Meios técnicos utilizados no tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

Consentimento: Manifestação livre, pela qual o titular concorda com o tratamento de seus dados pessoais.

Controlador: Pessoa natural ou jurídica, a quem competem as decisões referentes ao tratamento dos dados pessoais.

Operador: Pessoa natural ou jurídica, que realiza o tratamento de dados pessoais em nome do controlador.

Encarregado: Pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional.

Tratamento: Toda operação realizada com dados pessoais, como as que se referem a coleta, classificação, utilização, reprodução, processamento, arquivamento, armazenamento, eliminação.

Uso compartilhado de dados: Comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de banco de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização especifica, para uma ou

Transferência internacional de dados: Transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

Relatório de impacto à proteção de dados: Documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Autoridade Nacional: Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da lei.

II - Princípios

A Lei traz em seu artigo 6º onze princípios, sendo apontado no *caput* o da boa-fé como primeiro princípio a ser observado, configurando um dever de comportamento leal entre as partes envolvidas.

Nos seguintes princípios abaixo, o legislador trouxe no próprio texto o conteúdo jurídico de cada um, vejamos:

- **Princípio da finalidade:** estabelece a realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

- **Princípio da adequação:** trata-se da compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

- **Princípio da necessidade:** é limitação do tratamento 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;

- **Princípio do livre acesso:** é a 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;

- **Princípio da qualidade dos dados:** é garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

- **Princípio da transparência:** é a garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

- **Princípio da segurança:** é a utilização de 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;

- **Princípio da prevenção:** determina a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
- **Princípio não discriminação:** fixa a impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

- **Princípio da responsabilização e prestação de contas:** é a demonstração, pelo agente, da 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.

III - Âmbito de aplicabilidade

De acordo com o artigo 3º da LGPD, a norma irá ser aplicada para qualquer operação de tratamento de dados pessoais realizada por pessoa natural ou por pessoa jurídica, seja de direito público ou de direito privado, independentemente do meio, do país sede da pessoa física ou jurídica, ou do país onde estejam localizados os dados, desde que:

- a operação de tratamento seja realizada no território nacional;

- a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; e

- os dados pessoais, objeto do tratamento, tenham sido coletados no território nacional, isto é, quando o titular dos dados aqui se encontre no momento da coleta.

Todavia, o artigo 4º da LGPD apresenta hipóteses de quando a Lei não se aplicará ao tratamento de dados pessoais. Vejamos:

- tratamento realizado por pessoa natural para fins particulares e não econômicos;

- tratamento realizado para fins jornalísticos ou artísticos ou acadêmicos;

- tratamento realizado para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (que será objeto de Lei específica); ou

- tratamento provenientes de fora do território nacional e que não seja objeto de comunicação, uso compartilhado com agentes de tratamento brasileiros ou objeto de transferência de dados com outro país que não o de proveniência, desde que este país de proveniência proporcione grau de proteção adequado aos da Lei brasileira.

Medida a ser tomada: Empresas e organizações precisarão contratar consultoria técnica e jurídica especializada para realizar uma avaliação no sistema de funcionamento da empresa, onde serão verificados os possíveis impactos da LGPD em suas atividades.

IV - Atribuições e responsabilidades dos agentes de tratamento

A Lei cria duas figuras para atuarem como agentes de tratamentos de dados, tendo como atribuições:

- **Controlador** - Determina as finalidades, condições e meios do processamento de dados pessoais.

Quem é o controlador?

- ✓ Figura central quando se trata de proteger os direitos dos titulares
- ✓ Principal tomador de decisão em relação aos dados pessoais, e como resultado, a maioria das responsabilidades pela conformidade com a LGPD recai sobre os ombros do controlador de dados.
- ✓ Controla a finalidade e os meios gerais os dados devem ser usados.

O controlador de dados tem a responsabilidade primária de garantir que as atividades de processamento estejam em conformidade com a Lei.

Surge, também, para o controlador a obrigação de indicar um **Encarregado** pelo tratamento de dados, que terá as atribuições de:

- ✓ Aceitar reclamações e comunicações dos titulares, prestando esclarecimentos e adotando providências para solucionar os casos;
- ✓ Receber comunicação da Autoridade Nacional e adotar providência;
- ✓ Orientar funcionários a respeito das práticas a serem tomadas em relação a proteção de dados;
- ✓ Executa as demais atribuições determinadas pelo controlador.

Dispõe a Lei que a Autoridade Nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

- **Operador -** Processar dados pessoais em nome do controlador. O operador de dados não controla os dados e não pode alterar a finalidade ou o uso do conjunto particular de dados, ou seja, está limitado ao processamento dos dados de acordo com as instruções e o propósito dado pelo controlador de dados.

O operador decide...

- ✓ O sistema/método/ferramentas utilizados para coletar os dados;
- ✓ Como armazenar os dados;
- ✓ Como garantir a segurança dos dados;
- ✓ Os meios utilizados para transferir dados de uma organização para outra;
- ✓ Os meios utilizados para recuperar dados pessoais de determinados indivíduos;
- ✓ Como garantir que o método por trás do cronograma de retenção seja respeitado;

O operador de dados tem a responsabilidade de fornecer garantias para implementar "medidas técnicas e organizacionais" adequadas, de modo que o processamento cumpra os requisitos legais e de segurança.

Responsabilidades

Os Agentes de tratamento de dados definidos na Lei como Controlador e Operador estão imputados de grandes responsabilidades, quais sejam:

Registros das operações e sua manutenção - a principal obrigação estabelecida pela Lei referente aos agentes de tratamento de dados foi de que toda a atividade de tratamento de dados pessoais deve ser registrada, indicando quais os tipos de dados serão coletados, a base legal, as suas finalidades, o tempo de retenção, as práticas de segurança de informação.

Adoção de medidas de segurança - Os agentes de tratamento de dados devem adotar medidas de segurança, capazes de proteger os dados pessoais.

Notificação obrigatória a Autoridade Nacional de Proteção de Dados (ANPD) - Todo incidente envolvendo o tratamento de dados que possam vir a acarretar risco ou danos aos seus titulares, deverão ser reportados a ANPD e os titulares envolvidos.

Elaboração do relatório de impacto à privacidade - é a documentação do Controlador que contém a descrição dos processos de tratamento de dados que podem vir a gerar riscos aos direitos dos titulares, bem como as medidas adotadas de mitigação desses riscos. Poderá ser obrigatório em situações já caracterizadas como de risco ou, por solicitação da ANPD.

Ressarcimento dos danos

Responsabilidade solidária - os agentes de tratamento de dados poderão responder solidariamente pelos incidentes ocorridos. Cabe ressaltar que a responsabilidade do

operador, pode ser limitada às suas obrigações contratuais, caso não viole as normas impostas pela LGPD.

A LGPD estende também a responsabilidade aos subcontratantes de uma empresa, como fornecedores e parceiros de tecnologia, ficando sujeitos às obrigações e podem realizar pagamentos de indenização pelos danos causados ao titular do dado

Ônus da prova - a LGPD atribuiu ao Controlador o ônus da prova do consentimento do titular dos dados tratados, vale aqui ressaltar que havendo o vício de vontade, o consentimento deixa de ser valido.

Sendo assim, podem ser solidariamente responsabilizados por incidentes de segurança da informação e/ou o uso indevido e não autorizado dos dados, ou pela não conformidade com a Lei.

V - Tratamento de dados

Faremos a aplicação da LGPD no tratamento de dado pessoal toda e qualquer operação de captura, coleta, recepção, classificação, utilização, processamento, armazenamento, avaliação, transferência, e até mesmo a exclusão de dado pessoal.

A LGPD estabelece em seu artigo 7º, rol taxativo para o processamento válido de dados pessoais.

Assim, de acordo com a Lei, o tratamento somente poderá ser realizado:

- mediante consentimento do titular do dado;
- para cumprimento de obrigação legal ou regulatória pelo controlador;
- pela administração pública, para tratamento de dados necessários a políticas públicas;
- para realização de estudos por órgão de pesquisa, sendo garantida a anonimização dos dados;
- quando necessário para a execução de contrato;
- exercício regular de direitos em processo judicial, administrativo ou arbitral;
- para a proteção da vida ou incolumidade física do titular ou terceiros;
- para a tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
- interesses legítimos do controlador ou de terceiros;
- proteção do crédito.

Consentimento: O consentimento deverá referir-se para as finalidades determinadas, sendo fornecido por escrito ou por meio que demonstre a manifestação da vontade do titular. Aliás, caso ocorra mudança na finalidade para o tratamento de dados pessoais não

compatíveis com o consentimento original, o controlador deverá informar previamente o titular, podendo o titular revogar o consentimento a qualquer momento.

Importante saber: Serão consideradas nulas as autorizações genéricas para o tratamento de dados pessoais, bem como quando as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo, ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

Medidas a serem tomadas: A empresa deverá manter os registros das operações de tratamento de dados realizadas, documentação comprobatória do consentimento do usuário do dado, visando manter a transparência sobre de como o dado foi coletado e tratamento pelo controlador e operador.

Interesse legítimo: O artigo 10 da LGPD apontam situações concretas que legitimam o interesse do controlador, mas não se limitam a:

- Apoio e promoção de atividades do controlador;
- Proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais.

Importante saber que, quando o tratamento do dado for baseado em legítimo interesse, o controlador deverá garantir a transparência do tratamento, registrando e fundamentando a operação adotada. A Autoridade Nacional, poderá solicitar um relatório de avaliação de impacto de dados pessoais quando o tratamento tiver como fundamento o legítimo interesse.

Tratamento de dados pessoais sensíveis

A LGPD prevê requisitos específicos e taxativos para o tratamento de dados sensíveis, tendo em vista que esses dados possibilitam conclusões a respeito de um indivíduo, como por exemplo, a sua orientação sexual, sua religião, saúde e com essas informações, torna-se muito arriscado que as pessoas venham a ser classificadas de forma preconceituosa, interferindo diretamente em seus direitos e liberdades individuais.

A razão da preocupação especial com os dados sensíveis diz respeito a assegurar não apenas a privacidade, mas também que tais dados não possam ser utilizados contra os titulares, trazendo-lhes restrições ao acesso a bens, serviços e mesmo ao exercício de direitos.

Por isso, quem coleta dados sensíveis de seus usuários deve atender às determinações da LGPD, especificadas em seu artigo 11, inciso I e II:

- quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades individualizadas;
- sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
  - ✓ cumprimento de obrigação legal ou regulatória pelo controlador;
  - ✓ tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em Leis ou regulamentos;
  - ✓ realização de estudos por órgão de pesquisa, garantia, sempre que possível, a anonimização dos dados sensíveis;
  - ✓ exercício regular de direitos, inclusivo em contrato e em processo judicial, administrativos e arbitral;
  - ✓ proteção da vida ou da incolumidade física do titular ou de terceiro;
  - ✓ tutela da saúde, em procedimento realizado por profissional da área da saúde por entidades sanitárias;
  - ✓ garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados dos direitos mencionados nessa Lei, e exceto no caso de prevalecerem direitos e liberdade fundamentais do titular que exijam a proteção dos dados pessoais.

A Lei também não permite a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nos casos de portabilidade de dados quando consentido pelo titular.

Tratamento de dados pessoais de crianças e adolescentes

O tratamento dos dados de crianças e adolescentes deverá ser realizado

- no melhor interesse da criança ou adolescente,
- mediante o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal e
- de acordo com a obrigação que os controladores têm de manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos do titular.

A Lei traz exceções ao consentimento dos pais, quais sejam:

- quando a coleta dos dados for necessária para contatar os pais ou o responsável legal e, mesmo nessa hipótese, os dados devem ser utilizados uma única vez e sem armazenamento, e

- para a proteção da criança ou adolescente, sendo que, em qualquer caso, os dados não podem ser repassados a terceiros sem o consentimento de pelo menos um dos pais ou do responsável legal.

Os serviços ofertados pela internet e direcionados ao público infanto-juvenil, como por exemplo, jogos e desenhos animados, não devem ser condicionados ao fornecimento de informações pessoais, salvo as estritamente necessárias à atividade.

A Lei ainda traz que as informações sobre o tratamento e coleta de dados precisa se adequar à capacidade de compreensão das crianças e dos adolescentes, podendo valer-se da utilização de recursos audiovisuais, quando adequado.

Término do tratamento de dados:

Se a finalidade para qual o consentimento foi fornecido restar concluída, os dados deixam de ser necessários, encerrando o tratamento. Também ocorre o término do tratamento quando o prazo acordado para o uso do dado for alcançado.

Outras situações que preveem o término do tratamento são:

- Solicitação do titular de revogação do consentimento, a qualquer momento;
- Determinação da Autoridade Nacional, quando houver violação da Lei;
- Cumprimento de obrigação legal ou regulatória pelo controlador;
- No encerramento de estudo por órgão de pesquisa;
- Na transferência a terceiro - portabilidade de dados quando consentido pelo titular.

Importante saber que toda e qualquer atividade de tratamento de dados pessoais deve ser registrada, desde a sua coleta até a sua exclusão, indicando quais tipos de dados pessoais serão coletados, a base legal que autoriza os seus usos, as suas finalidades, o tempo de retenção, as práticas de segurança de informação implementadas no armazenamento e com quem os dados podem ser eventualmente compartilhados, metodologia conhecida como *data mapping*.

Mas, afinal, o que representa essa proteção?

Os titulares terão informações mais claras sobre a utilização dos seus dados como, por exemplo, saber por qual finalidade está sendo capturados e processados, saber se existiu consentimento para o seu tratamento, a forma e a duração do seu processamento, quem será o responsável pelo tratamento dos dados e como contatá-lo. Além disso, poderá pedir a exclusão do seu dado, preservando a sua privacidade.

VI - Direito do titular do dado

A LGPD demonstra nos seus dispositivos 1º e 17º que tem como finalidade a proteção dos direitos fundamentais da pessoa natural. Portanto, toda pessoa natural tem assegurada a titularidade de seus dados pessoais, garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade.

O titular dos dados pessoais possui os seguintes direitos perante o controlador:

- Confirmação da existência de tratamento;
- Acesso aos dados;
- Correção de dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nessa Lei;
- Portabilidade de 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;
- Eliminação de dados pessoais tratados com o consentimento do titular;
- Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
- Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- Revogação do consentimento.

É bom saber que:

O titular dos dados pode peticionar em relação aos seus dados contra o controlador perante a Autoridade Nacional.

Quando o controlador não puder, imediatamente, dar providência ao requerimento do titular dos dados, deverá este enviar resposta comunicando que não é o agente de tratamento dos dados e se possível indicar o responsável; ou indicar as razões que impedem a adoção imediata da providência.

Em caso de uso compartilhado dos dados, o agente de tratamento deverá informar de maneira imediata os pedidos de correção, eliminação, anonimização ou bloqueio dos dados, para que repitam idêntico procedimento.

Além disso, todo titular pode pedir a revisão de decisões tomadas exclusivamente com base em tratamento automatizado de dados pessoais que definam seu perfil pessoal, profissional, de consumo, de crédito ou sobre sua personalidade.

Para que o titular do dado exerça seu direito **de forma facilitada e gratuita**, as empresas devem adequar sua estrutura operacional, com uma linguagem clara e adequada, para viabilizar e cumprir com todos os direitos que a Lei garante ao indivíduo.

VII - Transferência de dados internacionais

A LGPD permite a transferência internacional de dados pessoais a países ou organismos internacionais que gozem de adequado grau de proteção de dados ou em outras limitadas hipóteses, dentre as quais destacamos:

- a transferência para países/organizações internacionais que assegurem grau de proteção adequado;
- comprovação, pelo controlador, de que certas garantias foram atendidas (cláusulas contratuais específicas ou cláusulas-padrão, normas corporativas globais, certificados regularmente emitidos);
- transferências em casos de cooperação internacional;
- autorização da Autoridade Nacional;
- consentimento específico e destacado do titular.

Mediante garantias oferecidas pelo controlador, a LGPD permite a transferência por meio de adoção de selos, certificados e códigos de conduta regularmente emitidos e autorizados pela Autoridade Nacional.

Assim, o fluxo internacional de dados pessoais dos cidadãos brasileiros deverá estar condicionado a regras que assegurem que os países destinos possuam o mesmo nível de proteção de dados previstos na LGPD, bem como regras que ressaltem a transparência sobre os acordos internacionais ou regionais que tratem do tema.

O tema da transferência internacional de dados pessoais ainda ganhará novos contornos após a criação concreta da Agência Nacional de Proteção de Dados.

VIII - Medidas de segurança e boas práticas

Os princípios gerais da LGPD e os padrões de segurança devem ser observados desde a concepção até a execução e oferecimento do produto e serviço.

O artigo 47 da LGPD prevê que os agentes de tratamento ou qualquer pessoa que intervenha em uma das fases do tratamento obrigam-se a garantir a segurança da informação prevista na Lei em relação aos dados pessoais, mesmo após o seu término.

Em caso de vazamento de dados, o controlador deverá comunicar à Autoridade Nacional e ao titular do dado a ocorrência de segurança que possa acarretar risco ou dano relevante

dono do dado. Tal comunicação deverá ser feita em prazo a ser definido pela Autoridade Nacional, devendo conter os seguintes atributos:

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

Após essa medida por parte do controlador, a Autoridade Nacional irá analisar a gravidade do incidente e poderá determinar ao controlador adoção de providências, como por exemplo, ampla divulgação do fato em meios de comunicação. Ainda, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los. A aplicação das penalidades deverá ser baseada na forma como a empresa conduziu e administrou o vazamento, podendo ser mais brandas ou rígidas, de acordo com os procedimentos adotados para mitigar o vazamento.

Boas práticas

A LGPD claramente incentiva a adoção de códigos de conduta, permitindo que controladores e operadores, individualmente ou por meio de associações, formulem regras de boas práticas e governança para o tratamento dos dados.

Essas regras poderão estabelecer:

- condições de organização;
- regime de funcionamento;
- procedimentos (incluindo reclamações e petições de titulares)
- normas de segurança;
- padrões técnicos;
- obrigações específicas para os envolvidos no tratamento dos dados;
- ações educativas;

- mecanismos internos de supervisão e de mitigação de riscos;
- outros aspectos relacionados ao tratamento de dados pessoais;
- seguros contra-ataques cibernéticos.

As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela Autoridade Nacional.

Importante saber que, as empresas que estiverem em conformidade com as exigências da Lei de Proteção de Dados, poderão ter suas penas atenuadas em caso de vazamento de dados.

IX - O seguro contra-ataques cibernéticos

Uma modalidade nova de seguro foi criada no Brasil, tendo em vista os recorrentes incidentes cibernéticos ocorridos às empresas. Assim sendo, a contratação de uma apólice visa não só garantir ao segurado a recomposição das perdas sofridas em razão de um ataque, bem como a indenização pelas perdas causadas a terceiros.

Além disso, as seguradoras também poderão prover um serviço de resposta a incidentes cibernéticos, mediante o oferecimento de serviços jurídicos, regulatórios, investigação forense, recuperação e restauração de dados, relações públicas, comunicação de crise, notificação às autoridades e centro de atendimento, consulta de fraude, monitoramento de roubo de identidade e soluções de monitoramento de crédito.

Essas apólices poderão estabelecer seguros para defender as empresas em razão das seguintes ocorrências:

(i) Perdas Causadas a Terceiros

- Responsabilidade pela Privacidade - Cobre danos e as despesas decorrentes de reclamações de terceiros por violação de privacidade
- Responsabilidade pela Segurança da Rede - Cobre danos e as despesas decorrentes de reclamações de terceiros por falhas de segurança da rede.
- Responsabilidade por Conteúdos Eletrônicos - Cobre danos e as despesas decorrentes de reclamações de terceiros acerca de conteúdos eletrônicos.

(II) Perdas do Próprio Segurado:

- Ciberextorsão - Cobertura para danos e despesas por Ciberextorsão pagas pelo Segurado em razão de um evento de Ciberextorsão.

- Perdas de Ativos Digitais - Cobertura para despesas de recuperação em razão de um incidente de perda de ativos digitais.
- Lucros Cessantes /Interrupção de Negócios - Cobertura para redução do lucro líquido que ocorra durante o período de indenização, resultante de um incidente de interrupção do negócio, e despesas de recuperação que surjam, decorrentes de um risco cibernético.

Importante saber que, em muitos casos, as empresas estão contratando antes o seguro contra-ataques cibernéticos e, na sequência, realizam o que se denomina assessment, que seria uma auditoria tecnológica a fim de analisar a vulnerabilidade do parque tecnológico da empresa. Assim, é possível fazer a auditoria com um certo amparo de segurança.

X - Fiscalização e sanções

O artigo 52 da LGPD elenca os tipos de sanções aplicáveis em caso de infração, quais sejam: advertência, multa de até 2% do faturamento (limitada a R$ 50.000.000,00) por infração, multa diária, publicização da infração, bloqueio dos dados pessoais e eliminação dos dados pessoais do banco de dados do infrator.

O texto da Lei prevê alguns parâmetros que devem ser observados pela Autoridade Nacional para escolha do tipo de sanção que deverá ser aplicada ao caso concreto, a fim de que não se inviabilize o próprio negócio do infrator em caso de aplicação de multa.

Importante saber que: É preciso ter consciência de que o descumprimento não está apenas relacionado em pagar a multa de até 2% do faturamento das empresas (com valor máximo de até R$ 50 milhões), mas relacionado também com à reputação da marca da empresa e o que ela significa para os clientes, visto que a Lei exige a publicização da infração e do infrator, além do bloqueio e até a eliminação de dados. Isto pode ser muito mais danoso para a empresa, em virtude da quebra de confiança, segurança e credibilidade com os seus consumidores e usuários, já que garantir a transparência e a confiança entre os envolvidos deve ser contínuo.

Importante saber que: O Ministério do Público do Distrito Federal criou a Comissão de Proteção de Dados, onde poderá receber comunicações sobre a ocorrência de qualquer incidente de segurança que possa acarretar risco ou prejuízo relevante aos titulares dos dados. E, ainda, podendo ingressar com Ação Coletiva pleiteando indenizações em nome dos titulares dos dados contra a empresa que negligenciou a proteção dos dados.

Portanto, o quanto antes as empresas adotarem as medidas impostas pela LGPD, adequando-se aos seus comandos, poderão evitar esse tipo de aborrecimento e prejuízo, uma vez que já estarão em conformidade da Lei.

XI - Como a LGPD impacta seus negócios

Ao garantir às pessoas maior privacidade e controle de suas informações, a LGPD afetará todos os setores da economia e companhias de todos os tamanhos. É importante salientar que a nova Lei se aplica também a todos os subcontratantes da empresa de posse dos dados, como fornecedores, prestadores de serviço, agências e parceiros de tecnologia.

As organizações devem adaptar seus processos e produtos, já que o não cumprimento da Lei pode afetar drasticamente a saúde econômica do negócio.

Além disso, é preciso entender que, mais do que prejuízos financeiros no caso de descumprimento da Lei, a empresa que não respeitar a LGPD pode ter sua imagem arranhada. Afinal, em tempos tão sensíveis no compartilhamento de dados, o cliente pode preferir fazer negócio com a empresa que tenha mais credibilidade e for mais confiável.

A Lei atinge todos os setores da economia, além de ter aplicação extraterritorial. Ou seja, toda empresa que tiver negócios no Brasil deve se adequar a ela.

XII - Como se preparar

A principal meta da LGPD é garantir a privacidade dos dados pessoais dos cidadãos e permitir um maior controle sobre eles, e para tanto criou regras claras sobre os processos de coleta, armazenamento e compartilhamento dessas informações, ajudando a promover o desenvolvimento tecnológico na sociedade e a própria defesa do consumidor.

Antes de embarcar em um projeto para atingir a conformidade com a LGPD é muito importante garantir o compromisso da alta administração. Este é, provavelmente, o fator mais significativo que poderá conduzir as entidades a um projeto de operação (e posterior implementação) bem-sucedido.

As primeiras questões que a alta gerência fará sobre o projeto provavelmente serão:

- quais requisitos deverão ser cumpridos,
- quanto irá custar; e
- quando deverá estar pronto?

O ponto mais importante é que **a conformidade à LGPD não é opcional** e as multas previstas em caso de descumprimento são altas. Os requisitos a serem observados e os custos de adequação irão depender da avaliação de cada negócio, mas todos deverão estar em conformidade com a norma até meados de agosto de 2020.

Segue alguns *insights* destinados a fornecer um ponto de partida razoável para iniciar um projeto de conformidade à Lei:

Estabelecer as necessidades e o contexto - Reunir as equipes e mapear a situação interna no que se refere às operações de processamento de dados, a fim de compreender em que medida a LGPD se aplica a seu negócio. Para tanto, é necessário criar comissões multidisciplinares, a fim de que todos os colaboradores da empresa possam apresentar as suas demandas e preocupações no que se refere a proteção de dados.

Identificar os riscos - Realizar um *gap assessment* (parte legal e técnica) para identificar as providências a serem adotadas.

Analisar e avaliar os riscos - Analisar e definir as bases legais para tratamento; avaliar os mecanismos de segurança das bases de dados.

Definir o projeto de acordo com os riscos - Definir responsabilidades; nomear um DPO (*Data Protection Officer*); readequar e documentar os processos internos de tratamento de dados.

Educar - Incentivar a adoção de boas práticas e a mudança na cultura interna (através de treinamentos periódicos, por exemplo) e externa.

Implementar o projeto desenvolvido - Elaborar ou revisar (i) políticas de privacidade (internas e externas) e (ii) contratos com colaboradores e terceiros que impliquem no processamento de dados (operadores), assegurando-se dos meios para garantir sua execução.

Registrar o processo - Documentar as análises e procedimentos e implementar o registro de processamento de dados.

Implantar Plano de Contingência, Monitorar e notificar - Organizar uma política de tratamento dos incidentes para garantir o cumprimento de requisitos de comunicação às autoridades em caso de vazamentos ou uso indevido de dados pessoais.

Com a nova Lei Geral de Proteção de Dados brasileira, todas as empresas de pequeno, médio e grande porte terão que investir em cibersegurança e implementar sistemas de *compliance* efetivos para prevenir, detectar e remediar violações de dados pessoais, notadamente porque a Lei prevê que a adoção de política de boas práticas será considerada como critério atenuante das penas.

Brasília-D.F., 19 de dezembro de 2024.

GRUPO INTERATIVA
Viviane Rodrigues Paes – DPO.

Revisão: 02 de 19/12/2024.

Autores:

Paulo Salvador Ribeiro Perrotti: Advogado LGPDSolution, Presidente da Câmara de Comércio Brasil-Canadá, Professor de Pós Graduação de Cybersecurity da Faculdade de Engenharia de Sorocaba (FACENS), membro da Comissão Especial de Relações Internacionais da OAB/SP, Certified Secure Computer User (CSCU) pela EC-Council, com especialização em Direito Canadense e de Québec pela Université de Québec à Montreal - UQÀM, possuindo Pós Graduação em Administração de Empresas pela Fundação Getúlio Vargas de São Paulo, especialização em Direito de Informática (LLM) pelo IBMEC/SP, Mercado Financeiro pelo Instituto Finance e Responsabilidade Social pela ESPM/SP - paulo@lgpdsolution.com.br

Aline Figueiredo: Advogada LGPDSolution, formada pela Fundação Educacional do Município de Assis/SP - FEMA/IMESA. Pós-graduada em Direito Processual Cível pelo Damásio Educacional. Pós-graduada em Direito Empresarial pela EPD - Escola Paulista de Direito. Pós-graduando em Direito Digital e Compliance pelo Damásio Educacional. Extensão Universitária em “Contratos e Negociações” pela FGV - Fundação Getúlio Vargas. Extensão universitária em “Direito das Start Ups” pela ESA - Escola Superior de Advocacia. Participante de palestras e cursos na área de Direito Empresarial, Direito Societário e Direito Digital - aline@lgpdsolution.com.br

Revisão: 02 de 19/12/2024.