LGPD

Lei Geral de Proteção de Dados

FIEG

Federação das Indústrias do Estado de Goiás

PELO FUTURO DA INDÚSTRIA

LGPD

LEI GERAL DE PROTEÇÃO DE DADOS

Uma abordagem concisa e objetiva sobre os principais pontos da Lei Geral de Proteção de dados.

Federação das Indústrias do Estado de Goiás

PELO FUTURO DA INDÚSTRIA

Para que serve a Cartilha da LGPD?

Toda legislação que é criada acaba trazendo diversas dificuldades desde a sua compreensão até a sua aplicação. A cartilha da LGPD foi pensada como ferramenta para introdução dos novos conceitos indicados pela lei e como meio de orientar os empresários nessa nova fase.

Para quem é a Cartilha da LGPD?

Criada pensando em praticidade, a Cartilha da LGPD é dirigida a todas as empresas e colaboradores ligados às áreas jurídica, contábil, de gestão de pessoal, marketing e de vendas que precisam se adequar a nova realidade e a necessidade de proteção de dados, e que, até então, não havia tido contato com qualquer assunto relacionado à segurança da informação, privacidade e LGPD.

ÍNDICE

Dez razões para se preparar para a LGPD

1. Todas as empresas tratam dados pessoais e a lei se aplica a todas elas;
2. Ao contrário do que se pensa, não são apenas as empresas voltadas para a tecnologia que precisam se preparar, pois todas as empresas tratam dados pessoais em seus departamentos de RH, Marketing, Jurídico, Compliance, Comercial e até mesmo em suas redes sociais;
3. Os dados se tornaram a base do desenvolvimento de estratégias comerciais e até mesmo do planejamento de crescimento das empresas, por isso, é preciso compreender a necessidade da proteção deles e como eles podem ser utilizados.
4. O tratamento de dados pessoais somente poderá ser realizado se estiver em conformidade com uma das bases legais previstas na Lei;
5. A transparência e a segurança no tratamento de dados será um diferencial competitivo;
6. A necessidade de adequação à LGPD é uma oportunidade para iniciar ou aprimorar programas de governança corporativa, capacitação contínua ou/e o Compliance nas empresas;
7. A LGPD traz direitos aos titulares dos dados que precisam ser observados. Titulares de dados pessoais passam a ter o direito a: confirmação da existência de tratamento, acesso aos dados, correção de dados incompletos, inexatos ou desatualizados, anonimização; portabilidade, eliminação, informação a respeito do compartilhamento de dados, possibilidade de receber informação sobre não fornecer o consentimento e suas consequências, revogação do consentimento.
8. Será criada uma Autoridade Nacional de Proteção de Dados para fiscalizar o cumprimento da lei e aplicar sanções em caso de violação;
9. A multa pelo descumprimento da lei pode chegar a R$50 MILHÕES de reais;
10. A prevenção e adequação serão sempre mais eficazes para o crescimento e fortalecimento empresarial do que arcar com os custos e prejuízos ocasionados pelas sanções.

Conceitos para compreender a LGPD

A Lei Geral de Proteção de Dados, além de ser uma lei nova, por si só, também traz novidades nos conceitos que utiliza, já que muitas das denominações presentes na LGPD estão ligadas à operações que, até então, não haviam sido abordadas por outros textos normativos.

Por isso, é necessário se familiarizar com alguns conceitos trazidos pela nova lei:

- Banco de dados: conjunto estruturado de dados pessoais estabelecido em um ou em vários locais, em suporte eletrônico ou físico.
- Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.
- Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.
- Operador (Processor): pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.
- Encarregado (DPO): 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 (MP 869).
- Agentes de tratamento: o controlador e o operador.
- Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.
- Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.
- Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.
- Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.
- Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicas no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados. Relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.
- Órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico;

- Autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei.

Por que precisamos de uma lei para a Proteção de Dados?

Além das questões relacionadas a fraudes e crimes que podem resultar em um prejuízo financeiro imediato, os dados precisam de proteção, pois se tornaram uma extensão da personalidade dos indivíduos. A transformação digital do mundo fez com que a maioria das operações realizadas, em todos os âmbitos, estejam fundamentadas na transferência de informações e, por isso, quando os dados são utilizados sem autorização ou com finalidade diversa daquela para qual houve a autorização para uso, existe, então, a violação de direitos.

A proteção de dados no Mundo

Em maio de 2018, entrou em vigor o Regulamento Geral de Proteção de Dados (do inglês, General Data Protection Regulation - GDPR) da União Europeia e, sem dúvida alguma, foi um marco para a proteção de dados no mundo.

A primeira lei de proteção de dados do Japão, a APPI, foi criada em 2003, mas foi recentemente atualizada, em 2015. As novas regras decorrentes da atualização começaram a valer no país em 2017, isto é, um ano antes da GDPR europeia.

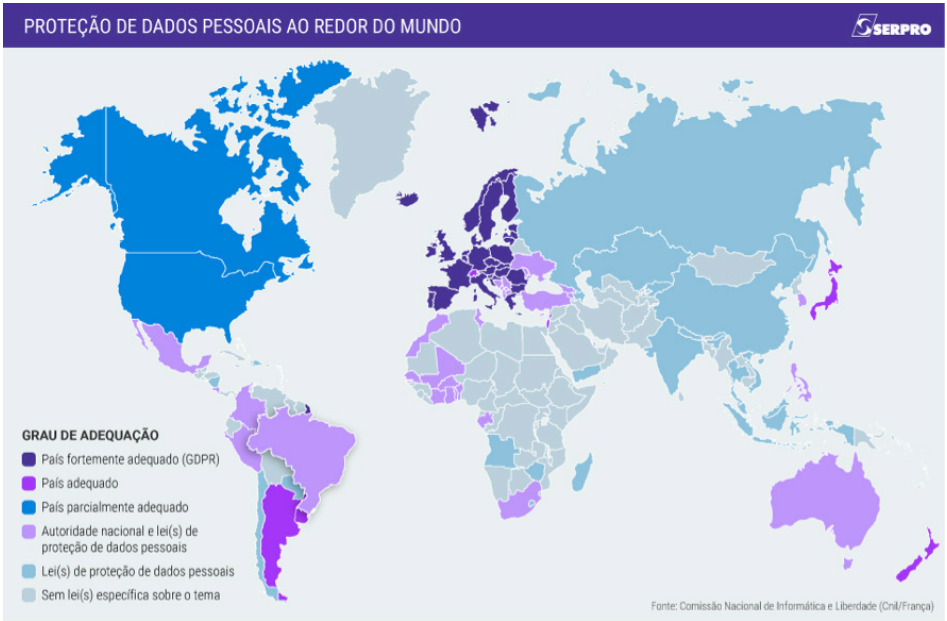
Nos Estados Unidos não existe uma legislação sobre proteção de dados que se aplique ao país inteiro, pois cada estado é responsável pela própria legislação. Nesse cenário se destaca a Lei de Privacidade dos Consumidores da Califórnia (CCPA).

Já na América Latina, a Argentina foi um dos primeiros países a aprovar leis referente à proteção de dados, já em 1994, legislação essa que deve passar por atualizações. O Chile regulamenta a proteção de dados pela Lei nº. 19.628 desde 1999, que possivelmente também sofrerá atualizações após o GDPR.

O México possui a Lei Federal Mexicana de Proteção de Dados Pessoais em Posse de Particulares que está em vigor desde 2010.

Outros países do mundo possuem legislações sobre proteção de dados pessoais, assim como a Rússia e a China.

O mapa abaixo demonstra a situação dos países quanto à leis relacionadas à proteção de dados.



O que é "LGPD"?

Como ficou conhecida, LGPD é abreviação do nome Lei Geral de Proteção de Dados, que é a lei nº 13.709/2018 criada para prever e regulamentar questões relacionadas ao tratamento de dados pessoais nos meios digitais, inclusive, por pessoas físicas ou jurídicas privadas ou públicas. A criação de uma lei com esse tema surge com a finalidade de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Quando a nova Lei Geral de Proteção de Dados Pessoais entra em vigor?

Conforme definição da Lei 13.853/2019, a LGPD entra vigor em agosto de 2020, 24 meses após a publicação original, para possibilitar às entidades públicas e privadas prazo hábil para adequação às regras de usos e tratamento dos dados pessoais.

O que são dados pessoais?

A Lei Geral de Proteção de Dados Pessoais indica que dado pessoal é a "informação relacionada à pessoa natural identificada ou identificável".

Diante dessa definição, podemos entender que dados pessoais não são apenas os nomes, prenomes, endereços e CPF. Dado pessoal é toda informação que pode

identificar um indivíduo, assim os números de Internet Protocol – IP, número de identificação da seguridade social de um funcionário e os dados biométricos utilizados para acesso, por exemplo, se tornam dados pessoais conforme a definição legal.

O que são dados pessoais sensíveis?

São dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde, à vida ou à orientação sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. São aqueles que, se expostos ou compartilhados, podem causar impacto para a vida pessoal e/ou profissional, como por exemplo, os dados relacionados ao histórico de saúde do indivíduo.

O que é tratamento de dados?

Tratamento de dados é toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Em que se aplica a LGPD?

A qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede 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 ou os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

Os dados coletados no território nacional são os dados pessoais dos titulares que se encontrem no território nacional no momento da coleta.

Controladores e Operadores, quem são e o que fazem?

Tanto o Controlador como o Operador são agentes de tratamento por definição legal.

O Controlador é "toda pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais" (art.

5º, VI) e, Operador é a "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (art. 5º VII).

O Operador atua em conformidade com as diretrizes elaboradas pelo Controlador, não interferindo no tratamento dos dados do titular, já que o intuito do tratamento é determinado somente pelo controlador. É o controlador, então, quem vai definir as finalidades do tratamento, se, por exemplo, utilizará os dados pessoais de seus clientes elaborar campanhas de vendas com o envio de comunicações.

É o controlador o responsável por cuidar para que os dados sejam tratados segundo as especificações apresentadas ao titular tem o dever, portanto, de traçar os limites para o operador.

Quem precisa ter Controlador ou/e Operador?

Na verdade, a pergunta não é quem precisa, mas sim quem serão. Controlador e Operador são as definições de agentes de tratamento em decorrência da função que desempenham no tratamento de dados. O Controlador que possuí a prerrogativa quanto à decisão sobre o tratamento poderá ser o dono da empresa, a empresa contratante de prestação de serviços ou um diretor de departamento, a depender de cada caso. O Operador será o responsável pelo tratamento de dados propriamente dito, podendo ser, então, um colaborador da equipe de TI, uma empresa contratada para prestação de serviços e até mesmo um atendente de call center.

Desse modo, fica claro que toda empresa que realiza tratamento de dados já possui pessoas que estão nas funções de Controlador e de Operador, embora não existisse a definição propriamente dita. A partir da vigência da lei o que deverá acontecer é a identificação desses agentes para que se delimite as condutas e as responsabilidades de cada um, conforme a lei prevê.

A LGPD se aplica apenas aos dados digitais?

Não! Quando falamos da LGPD automaticamente acabamos pensando nas operações feitas por meios digitais, transferências eletrônicas e envio de documentos por meio virtual, mas a Lei Geral de Proteção de Dados se aplica aos dados tratados independentemente do meio, por isso, todas as informações tratadas, ainda que estejam armazenadas em meio físico, também devem ser objeto de atenção.

Em quais casos de tratamento de dados pessoais, a LGPD não será aplicada?

São os casos em que o tratamento de dados pessoais for feito: por uma pessoa física, para fins particulares, e não comerciais, para fins exclusivamente jornalísticos, artísticos e acadêmicos, pelo Poder Público - no caso de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais. Podem não estar sujeitos à aplicação da LGPD os dados provenientes e destinados a outros países, que apenas transitem pelo território nacional, sem que aqui seja realizada qualquer operação de tratamento e, desde que o país de origem tenha nível de proteção similar ao previsto na LGPD.

A LGPD prevê multas?

A LGPD implementa a aplicação de severas sanções para empresas que descumprirem as disposições legais e, por isso, é tão relevante a adequação das empresas ao disposto na Lei.

Além das multas pecuniárias, existem outras sanções previstas que podem ser aplicadas, tais como, publicização da infração após devidamente apurada e confirmada a sua ocorrência; bloqueio dos dados pessoais a que se refere a infração até a sua regularização; eliminação dos dados pessoais a que se refere a infração; suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

As sanções seguirão critérios como: gravidade da infração, boa-fé do infrator, possíveis vantagens econômicas auferidas pelo infrator, reincidência, cooperação para esclarecimento do caso, demonstração de evidências de mecanismos, procedimento e adoção de boas práticas de segurança para minimizar possíveis danos causado aos titulares.

Segurança e Boas Práticas

O artigo 46 traz como obrigação tanto a Controladores como a Operadores 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 ou ilícito".

Quando pensamos em segurança da informação, muito se fala sobre recursos tecnológicos que possam evitar ataques ou/e vazamentos, porém, a grande lacuna que existe na atualidade é a ausência da cultura da segurança da informação. Algumas pessoas já se atentaram para o quanto é importante a proteção dos dados, por outro lado, muitas empresas e pessoas não entendem a sua importância e não analisam suas ações diante desse prisma.

De todo modo, a própria LGPD traz em seu texto algumas condutas voltadas justamente para a criação e manutenção dessa cultura, dentre elas estão o Privacy By design, a comunicação em casos de incidente e a Governança em privacidade.

Privacy By design

Por Privacy By design pode se entender que todo "sistema deve ser estruturado de modo a "atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares" previsão essa que está no artigo 49 da Lei Geral de Proteção de Dados .

A adoção do "Privacy by design", segundo a idealizadora da expressão, Ann Cavoukian, deve atender aos seguintes requisitos:

- Ser proativo, não reativo;
- Privacidade como configuração padrão, a opção para tornar algo público deve ser posterior;
- Privacidade incorporada ao design;
- Considerar todos os interesses envolvidos, sobretudo o do titular;
- Segurança de ponta a ponta, durante todo o ciclo de vida do produto ou serviço; Preservação da visibilidade e transparência;
- Respeito à privacidade do titular;
- Comunicação em caso de Incidentes.

Comunicação em casos de incidente

Caberá ao controlador o dever de comunicar à autoridade nacional e também ao titular sempre que ocorrer um incidente de segurança que possa acarretar risco ou dano relevante aos titulares, em prazo razoável, que poderá ser definido pela autoridade nacional e mencionará, 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.

Incidente de segurança não é apenas quando ocorre ataques hackers, um Incidente de segurança é qualquer fato que possa comprometer a integridade dos dados pessoais ou sua utilização por pessoas desautorizadas, como por exemplo, o envio de um arquivo com dados de clientes em um aplicativo de mensagens para o destinatário errado.

Governança em privacidade

Os incisos I e II do artigo 50 da LGPD estabelecem o mínimo que um programa de governança deve conter. Assim, é importante que o Programa:

- Demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
- Seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
- Seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
- Estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
- Tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular; esteja integrado à sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
- Conte com planos de resposta a incidentes e remediação;
- Seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas; seja passível de comprovação (accountability).

A adoção de boas práticas e um programa de governança em privacidade é elemento avaliado quando houver aplicação das sanções, já que a existência dessas medidas tem como finalidade e resultado a criação de uma cultura de proteção à privacidade em uma organização, e de definir os procedimentos internos visando proteger esse valor, que passa a integrar os propósitos da companhia.

E então, por onde começar?

Se você chegou até aqui, o primeiro passo já foi dado, que é saber que em Agosto de 2020 o Brasil passa a contar com uma regulamentação própria quanto à proteção de dados. A partir disso, é preciso, então, avaliar quais são os pontos críticos relacionados à proteção de dados na sua instituição. Política de segurança da informação e a capacitação dos colaboradores serão elementos imprescindíveis para essa nova fase em que o dados exigem proteção. Cada empresa terá necessidades especificas e questões individuais que precisarão de análise e adequação. É o momento de buscar suporte para diagnostico e adequação à LGPD e para inaugurar uma nova fase em sua empresa, em que a segurança e a proteção dos dados refletem o comprometimento com a segurança de todos os consumidores, colaboradores, fornecedores e clientes.

O conteúdo da presente cartilha não esgota o tema e deve, portanto, ser utilizado como material introdutório, não dispensando, ainda, a leitura da legislação na íntegra.

FICHA TÉCNICA

Produção:

LARA MARTINS
ADVOGADOS
www.laramartinsadvogados.com.br

Projeto gráfico e editorial:
FIEG/Ascom

FIEG

Federação das Indústrias do Estado de Goiás

PELO FUTURO DA INDÚSTRIA

Esta cartilha tem caráter orientativo, não substituindo os termos previstos na Lei n.º 13.709/2018, com as alterações introduzidas pela Lei n.º 13.853/2019.