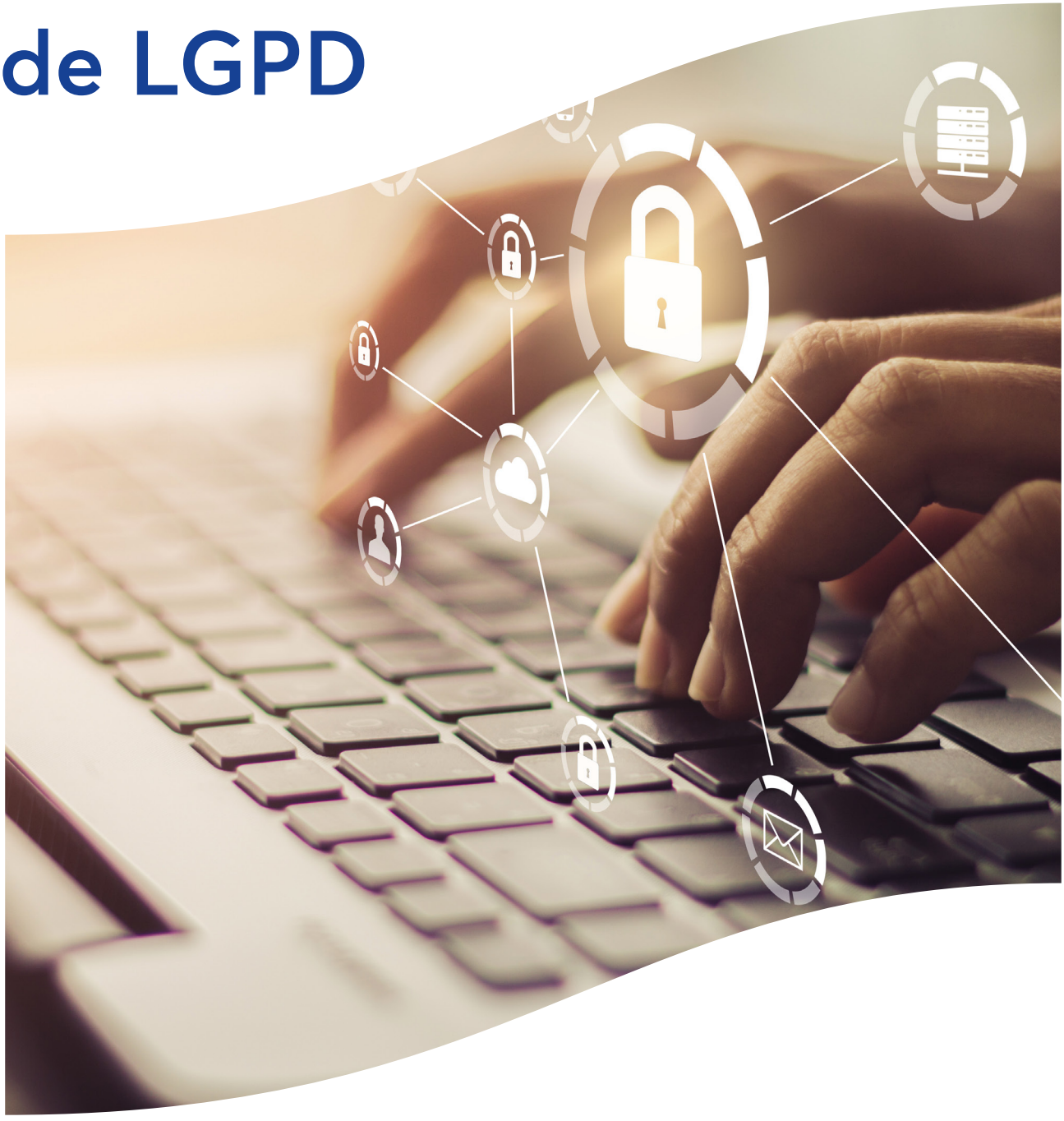
Firjan SENAI SESI IEL CIRJ

# Guia Prático de LGPD



ABR. 2021

Firjan SENAI SESI IEL CIRJ

## Expediente

**Firjan – Federação das Indústrias do Estado do Rio de Janeiro**

Presidente
**Eduardo Eugenio Gouvêa Vieira**

Coordenador do Grupo Empresarial
**Rodrigo Santiago**

Diretora de Compliance, Jurídico e Gestão de Pessoas
**Gisela Pimenta Gadelha**

Diretor de Competitividade Industrial e Comunicação Corporativa
**João Paulo Alcantara Gomes**

Diretor Executivo Firjan SESI SENAI
**Alexandre dos Reis**

Diretora de Pessoas, Finanças e Serviços Corporativos
**Luciana Costa M. de Sá**

### GERÊNCIA DE INTEGRIDADE CORPORATIVA

Gerente de Integridade Corporativa
**Luana Palmieri Franca Pagani**

Coordenadora de Compliance
**Ana Carla Coutinho Torres**

Equipe Técnica
**Cristiana Campos Mamede Maia**

### PROJETO GRÁFICO

Gerente Geral de Comunicação
**Ingrid Buckmann**

Gerente de Comunicação e Marca
**Fernanda Marino**

Equipe Técnica
**Francisco D'Elia Lucchini**
**Luciana Sancho Siqueira de Souza**
**Alessandra do Prado Miranda**
**Amanda Zarife Martins**
**Flávia Rocha Lépori**

**ABR. 2021**

**www.firjan.com.br**
Av. Graça Aranha, 1, 12° andar
Centro, Rio de Janeiro
dpo@firjan.com.br

Este guia foi elaborado com o propósito de conscientizar os empresários fluminenses quanto à importância da adoção da privacidade como norte em todas as etapas de seus negócios, atendendo à Lei Geral de Proteção de Dados.

# Apresentação

Com a vigência da Lei nº 13.079, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), a Firjan identificou a necessidade de criar um Grupo de Trabalho que pudesse auxiliar o empresariado fluminense na missão de implementar a nova legislação.

Para o desenvolvimento desse trabalho, foram convidadas empresas de renome, que, por meio de seus representantes e especialistas no tema, fizeram parte da composição do Grupo de Trabalho Empresarial LGPD.

O presente guia faz parte do legado que os trabalhos desenvolvidos pelo Grupo deixaram para os associados e empresários fluminenses.

A Firjan e o Grupo de Trabalho Empresarial esperam que o conteúdo ora apresentado auxilie os empresários, em especial os pequenos e médios, na caminhada rumo à implementação da referida legislação.

# Sumário

# 1. Da importância da privacidade

A proteção à privacidade não é matéria nova no âmbito global, tendo sido já tratada na Declaração Universal de Direitos Humanos[1], de 1948, e nos *Guidelines* da OCDE[2], de 1980. Assim, pode-se afirmar que desde 1980 há um movimento crescente de regulação do uso de dados a fim de proteger e priorizar a privacidade, tendo em vista o aumento do compartilhamento devido aos avanços tecnológicos.

Conforme estudo realizado pela IBM Securiy[3], o Brasil leva em média 380 dias para mitigar e conter uma violação de dados pessoais, ou seja, 100 dias a mais que a média global. Esse estudo reforça a importância de colocar a privacidade como requisito de qualquer projeto, especialmente hoje, pois vivemos na chamada sociedade da informação e qualquer incidente é amplamente divulgado, podendo acarretar uma imagem negativa para as empresas, além de diversos outros problemas.

Note que empresas que sofrem incidentes de segurança da informação[4] costumam ter não só o prejuízo financeiro, ou da paralização de suas ações, mas também o dano reputacional, ocasionado pela perda da confiança e credibilidade de seus consumidores e parceiros.

O necessário estímulo à valorização da cultura de privacidade, na busca pela adequação legislativa, permite fortalecer e agregar valor à imagem das empresas ante seus clientes e parceiros, além de promover um maior conhecimento do próprio negócio e possibilitar uma tomada de decisão com maior segurança por parte da alta administração.

Neste contexto, o Brasil, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e continuar a fomentar o desenvolvimento da economia digital, editou em 14 de agosto de 2018 a Lei nº 13.709/2018 - Lei Geral de Proteção de Dados (LGPD).

**E por falar em tecnologia, a internet das Coisas (IOT) vem sendo aplicada, cada vez mais, no setor de eletrodomésticos, sendo importante repensar a segurança dos dados pessoais tratados. Ou seja, hoje, é preciso enxergar a privacidade como parte intrínseca de qualquer projeto, e não como um adicional.**



1 Art. 12 da DUDH. Disponível em: https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/por.pdf

2 Disponível em: http://www.oecd.org/digital/ieconomy/privacy-guidelines.htm

3 Vide https://www.somaxi.com.br/post/brasil-%C3%A9-o-pa%C3%ADs-que-mais-tempo-leva-para-identificar-e-conter-incidentes-de-seguran%C3%A7a-diz-estudo

4 Um Incidente de Segurança da Informação, segundo a ABNT (2005), é indicado por um simples evento ou uma série de eventos de segurança da informação indesejados ou inesperados que tenham grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação. https://www.trf3.jus.br/documentos/rget/seguranca/CLRI/GSIC302_Introducao_Gestao_Riscos_Seguranca_Informacao.pdf. Acesso: em 22 set. 2020.

# 2. Da Lei Geral de Proteção de Dados

A LGPD, em resumo, estabelece regras sobre coleta, armazenamento, tratamento e compartilhamento de **dados pessoais**, no âmbito **digital e físico**, impondo diretrizes para proteção dos dados pessoais e penalidades em caso de descumprimento.

## Da aplicação da Lei

A LGPD se aplica a todas as pessoas, físicas ou jurídicas, que efetuem o tratamento de dados pessoais com fins econômicos, e que atendam a um dos seguintes critérios:

a. possuam operação de tratamento que seja realizada por empresa sediada no Brasil;
b. possuam atividade de tratamento com o objetivo de ofertar ou fornecer bens ou serviços a consumidores brasileiros;
c. os dados pessoais objeto do tratamento tenham sido coletados e tratados no Brasil.

Ou seja, essa Lei NÃO SE APLICA para tratamentos que sejam realizados para fins exclusivamente particulares; jornalísticos; artísticos; acadêmicos; de segurança pública; de defesa nacional e segurança do Estado e para atividades de investigação e repressão à infração penal.

**A Autoridade Nacional de Proteção de Dados (ANPD) poderá regular e simplificar as regras da LGPD para as Micro e Pequenas Empresas (MPEs). Neste sentido, a Firjan apresentou em 01/03/2021 à ANPD sugestão de aplicação simplificada da Lei para as MPEs.**



## Dos Conceitos de Tratamento e Dado Pessoal

Para garantir a conformidade com a LGPD é necessário conhecer os principais conceitos da lei, quais sejam:
**Tratamento** – Toda operação realizada com dados pessoais: ver, consultar, armazenar, coletar, produzir, receber, classificar, utilizar, acessar, transmitir, distribuir, processar, arquivar, eliminar, avaliar etc.;

**Cuidado com o armazenamento de documentos em papel, pois a LGPD também se aplica aos dados em meios físicos.**

**Dado Pessoal** – Informação relacionada à pessoa natural, identificada ou identificável, ou seja, é qualquer informação que sozinha ou em conjunto com outros dados ou informações possa identificar uma pessoa natural;

**Dado Pessoal Sensível** – Informação 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 ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
**Dado Anonimizado** – Dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento, como exemplo, dados estatísticos.

**Para um dado ser considerado anonimizado, não pode ser possível sua reversão em nenhuma hipótese, mesmo por quem coletou o dado. Por exemplo, dados como matrícula são pseudonimizados (e não anonimizados), pois podem ser revertidos.**

# Dos Agentes de Tratamento

A LGPD classifica aqueles que efetuam tratamento de dados em duas categorias, Controlador e o Operador, que em conjunto são chamados de **Agentes de Tratamento**. Saber a distinção entre eles é fundamental para compreender o papel da empresa no tratamento de dados pessoais. Vamos ver um pouco desses conceitos:

**Titular –** É o verdadeiro "dono" do dado. É a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

**Controlador** – É a pessoa natural ou jurídica que decide como os dados serão tratados;

**Operador** – É a pessoa natural ou jurídica que trata os dados pessoais em nome do Controlador.

Para melhor exemplificar a diferença entre o Controlador e o Operador, podemos pensar em uma empresa (Controladora), que trata os dados de seus colaboradores (Titular), repassando esses dados para a empresa de ticket refeição (Operadora), a qual deve colocar o saldo nos cartões, conforme orientação da empresa (Controladora).

Note que, mediante os conceitos da lei, os colaboradores **nunca** serão considerados Operadores ou Controladores das empresas em que trabalham, pois ao executarem o tratamento de dados pessoais atuarão em nome da empresa.

**Em certos casos poderá haver dois Controladores simultâneos. É o caso da relação entre as FINANCEIRAS e SEGURADORAS no setor AUTOMOBILÍSTICO, em que ambas atuam mediante contrato direto com o titular/cliente, mesmo que por intermédio de uma concessionária.**

**Por outro lado, o DESPACHANTE da concessionária seria um Operador em relação a ela, que por sua vez é uma Operadora em relação à financeira e a seguradora, mas é Controladora em relação ao despachante.**

# Do Encarregado

Outra figura muito importante, criada pela LGPD, é a do Encarregado, que nas legislações estrangeiras é conhecido como o *Data Protection Officer* (DPO). O Encarregado é a pessoa natural ou jurídica indicada pelo Controlador e pelo Operador (art. 5º VIII da LGPD) para atuar como canal de comunicação entre o Controlador, os Titulares de Dados e a Autoridade Nacional de Proteção de Dados (ANPD).

O Encarregado também possui a responsabilidade de recepcionar, prestar esclarecimentos e atender as demandas dos titulares de dados no prazo de até **15 DIAS** da solicitação, bem como encaminhar – quando necessário – **Relatório de Impacto** e **Notificação de Incidente** para a ANPD.

**CURIOSIDADE: O art. 37, (1) "a" a "c" do Regulamento Geral de Proteção de Dados da União Europeia (GDPR) adota as seguintes condições como regras para a nomeação de DPO, de forma obrigatória: (i) quando o tratamento é realizado por uma autoridade ou organismo público; (ii) quando as atividades principais dos agentes de tratamento consistem em operações que requerem monitoramento regular e sistemático em grande escala; ou (iii) quando as atividades principais dos agentes consistem em grande escala de categorias de dados sensíveis ou dados pessoais, relativos a condenações criminais.**

**O setor de COSMÉTICOS e FARMACÊUTICO, por possuir players de diversos tamanhos, tende a adotar, em alguns casos, a contratação de um Encarregado externo, uma vez que a LGPD não obriga que o Encarregado pertença aos quadros da empresa, podendo haver a terceirização desse profissional.**



# Dos Direitos dos Titulares

A LGPD (art. 18) traz diversos direitos aos titulares de dados pessoais que deverão ser observados pelas empresas. O titular tem o direito de:

- confirmação de existência de tratamento de forma gratuita no prazo de 15 dias;
- acesso aos seus dados;
- informações sobre os tratamentos e compartilhamento efetuados;
- anonimização, bloqueio ou eliminação de seus dados, quando desnecessários ou baseados apenas no consentimento;
- portabilidade, mediante requisição expressa, observados os segredos comerciais e industriais e não incluindo os dados já anonimizados;
- revogação do consentimento e recebimento de informação sobre suas consequências;
- correção de dados incompletos, inexatos ou desatualizados;
- informação sobre seus direitos.

**É obrigatório que o tratamento de dados pessoais seja realizado sempre com o objetivo de atender a finalidade acordada com o Titular e não para usos secundários, de interesse das empresas e sem autorização.**

# Do Tratamento do Dado Pessoal

O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

a. para execução de políticas públicas pela administração pública;
b. mediante fornecimento de consentimento pelo titular, de forma **livre, informada e inequívoca** para uma **finalidade específica e determinada**;
c. para o cumprimento de obrigação legal ou regulatória pelo controlador;
d. para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
e. quando necessário para a execução de contrato ou de procedimentos preliminares relacionados ao contrato do qual o titular é parte, a pedido do titular dos dados;
f. para o exercício regular de direitos em processo judicial, administrativo ou arbitral;
g. para a proteção da vida ou da incolumidade física do titular ou de terceiro;
h. para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
i. quando necessário para atender aos interesses legítimos do controlador ou de terceiro; e
j. para a proteção do crédito.

**É dever do Controlador verificar a AUTENTICIDADE do consentimento dos responsáveis legais. O Controlador, nos casos de revogação do consentimento, precisa informar a todas as empresas às quais realizou o compartilhamento de dados pessoais, para que estas também procedam a exclusão dos dados pessoais.**

Já para os tratamentos de **dados pessoais sensíveis,** cabe destacar que, das hipóteses acima mencionadas, **não** se aplica a base na execução de contrato, interesse legítimo ou proteção ao crédito.
Contudo os **dados pessoais sensíveis** poderão ser tratados, além das hipóteses supramencionadas, para efetuar a garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

**O não cumprimento da legislação poderá implicar multa simples de até 2% do faturamento do grupo no último exercício, limitada a R$50 milhões por infração, entre outras sanções administrativas e judiciais, conforme será mencionado no item Sanções.**

# Do Relatório de Impacto

Em todas as situações de tratamento de **dados pessoais sensíveis**, ou nas hipóteses em que o tratamento de dados pessoais for fundamentado no **legítimo interesse**, poderá ser exigido do Controlador, pela ANPD, a apresentação de um **Relatório de Impacto à Proteção de Dados Pessoais (RIPDP).**

Esse relatório é o documento elaborado pelo Controlador para ajudar **a identificar e minimizar os riscos** na proteção de dados. O documento deverá conter a **descrição dos processos de tratamento de dados pessoais** que podem gerar riscos às liberdades civis e aos direitos fundamentais do titular, bem como indicar as **medidas, salvaguardas e mecanismos de mitigação de risco e tipo de coleta** (metodologia e segurança).

O RIPDP deve apresentar, ao menos, as seguintes informações:

- a natureza, escopo, contexto e finalidade do tratamento;
- avaliação da necessidade, proporcionalidade e medidas de *compliance*;
- identificação e *assessment* dos riscos aos titulares de dados; e
- identificação das medidas para mitigar esses riscos.

# Do Incidente de Segurança

Um incidente de segurança com dados pessoais é qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança, tais como acesso não autorizado, acidental ou ilícito que resulte em destruição, perda, alteração, vazamento. Ainda, pode ser qualquer forma de tratamento de dados inadequada, que possa ocasionar risco aos direitos e liberdades dos titulares dos dados pessoais.

Quando ocorre um incidente de segurança envolvendo dados pessoais, deve-se tomar as seguintes medidas:

- comunicar ao Controlador, se você for o Operador, nos termos da LGPD;
- comunicar ao Encarregado (art. 5°, VIII da LGPD);
- avaliar internamente o incidente: (i) natureza, categoria e quantidade de titulares afetados; (ii) categoria e quantidade dos dados afetados; (iii) consequências concretas e prováveis, tendo por base o formulário disponibilizado pela ANPD;
- comunicar à ANPD e ao titular de dados, em caso de risco ou dano relevante aos titulares (art. 48 da LGPD); e
- elaborar documentação com a avaliação interna do incidente, medidas tomadas e análise de risco, para fins de cumprimento do princípio de responsabilização e prestação de contas (art. 6°, X da LGPD).

**A comunicação à ANPD não será necessária se o responsável pelo tratamento puder demonstrar, de forma irrefutável, que a violação da segurança dos dados pessoais não constitui um risco relevante para os direitos e liberdades do titular dos dados.**

# Das comunicações à ANPD

O art. 48 da LGPD determina que é obrigação do Controlador comunicar incidente de segurança que possa acarretar **risco ou dano relevante aos titulares.** A comunicação precisará ser realizada aos titulares afetados bem como à ANPD, para esta última, em 2 (dois) dias úteis.

Assim, quando ocorre um incidente de segurança envolvendo dados pessoais, ele deverá ser registrado internamente, e em casos graves, ser informado à ANPD por meio da **Notificação de Incidente**, que pode ser feita por meio de formulário eletrônico disponibilizado no site da ANPD[5].

**A ANPD recomenda que os Controladores adotem posição de cautela, de modo que a comunicação seja efetuada mesmo nos casos em que houver dúvida sobre a relevância dos riscos e danos envolvidos, uma vez que, eventual e comprovada subavaliação dos riscos e danos por parte dos Controladores, pode ser considerada descumprimento à legislação de proteção de dados pessoais.**

5 https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca

# Do que constar da Notificação de Incidente

As informações constantes da **Notificação de Incidente** devem ser claras e concisas, e conter as seguintes informações:

- identificação e dados de contato de: (i) entidade ou pessoa responsável pelo tratamento e (ii) Encarregado de dados ou outra pessoa de contato;
- indicação informando se a notificação é completa ou parcial. Em caso de comunicação parcial, mencionar que se trata de uma comunicação preliminar ou de uma comunicação complementar;
- informações sobre o incidente de segurança com dados pessoais: (i) data e hora da detecção; (ii) data e hora do incidente e sua duração; (iii) circunstâncias em que ocorreu a violação de segurança de dados pessoais (por exemplo: perda, roubo, cópia, vazamento, dentre outros);
- descrição dos dados pessoais, natureza e conteúdo dos dados pessoais afetados: (i) descrição da natureza dos dados pessoais afetados; (ii) categoria e quantidade de dados e de titulares afetados; (iii) resumo do incidente de segurança com dados pessoais, com indicação da localização física e meio de armazenamento;
- informações sobre os titulares envolvidos;
- riscos relacionados ao incidente: (i) possíveis consequências e efeitos negativos sobre os titulares dos dados afetados; (ii) possíveis problemas de natureza transfronteiriça; (iii) resumo das medidas implementadas até o momento para controlar os possíveis danos;
- medidas de segurança, técnicas e administrativas preventivas tomadas pelo controlador de acordo com a LGPD; e
- outras informações úteis às pessoas afetadas para proteger seus dados ou prevenir possíveis danos.

Caso **não** seja possível fornecer todas as informações no momento da comunicação preliminar, os dados adicionais poderão ser enviados posteriormente. Contudo é necessário informar, na comunicação preliminar, que maiores esclarecimentos serão fornecidos posteriormente, bem como quais meios estão sendo utilizados para obtê-las.

Vale lembrar que, apesar de ainda não ser regulado o que seria um grave dano, a ANPD já firmou o entendimento de que "a probabilidade de risco ou dano relevante para os titulares será maior sempre que o incidente envolver dados sensíveis ou de indivíduos em situação de vulnerabilidade, incluindo crianças e adolescentes, ou tiver o potencial de ocasionar danos materiais ou morais, tais como discriminação, violação do direito à imagem e à reputação, fraudes financeiras e roubo de identidade".

**A ANPD poderá regular as regras da LGPD sobre a Notificação de Incidentes. A Firjan apresentou em 24/03/2021 à ANPD sugestão de regulamentação da Lei sobre a temática.**

# Das Sanções

A LPGD prevê que poderão ser aplicadas pela ANPD, a partir de agosto de 2021, as seguintes sanções administrativas:

- **advertência**, com indicação de prazo para adoção de medidas corretivas;
- **multa simples,** de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50 milhões por infração, exceto quando não dispuser ou for incompleto o valor de faturamento no ramo;
- **multa diária,** observado o limite total de R$ 50 milhões por infração;
- **publicização da infração** após devidamente apurada e confirmada a sua ocorrência;
- **bloqueio e/ou Eliminação** dos dados pessoais a que se refere à infração; ou
- **bloqueio** da atividade da empresa relacionada à infração.

Conforme previsto na LGPD, para aplicar uma sanção, a ANPD deverá considerar os seguintes critérios:

- gravidade e natureza da Infração;
- boa-fé do Infrator;
- vantagem auferida/pretendida;
- condição econômica do infrator;
- reincidência;
- grau do dano causado;
- cooperação do Infrator;
- pronta adoção de **medidas corretivas**;
- demonstração de adoção reiterada de **mecanismos e procedimentos internos de mitigação de danos**;
- adoção de **Política de boas práticas de governança e segurança da informação**;
- formulação de regras de **boas práticas e de governança** que poderão ser estabelecidas por controladores e operadores; e
- **conciliação** com o titular (52 §7°).

**A implementação de um Programa de Governança e Privacidade EFETIVO, com demonstrações sobre o comprometimento da empresa na adoção de processos e políticas internas que assegurem a devida SEGURANÇA DA INFORMAÇÃO E O CUMPRIMENTO DA LGPD, poderá ser considerada para fins de ATENUAÇÃO DA SANÇÃO.**

# 3. LGPD na prática

A LGPD implica repensar as estratégias de negócios e as atualizações de normas e processos, proporcionando um olhar ético, transparente e atento aos direitos dos titulares.

**Os setores NAVAL e OFFSHORE, apesar de na maioria das vezes não lidarem com dados de clientes pessoas físicas – como ocorre no setor de GÁS –, lidam com dados pessoais de colaboradores, os quais podem ser compartilhados com empresas tomadoras de serviços. Esses e outros processos deverão ser repensados à luz da LGPD.**

## Da implementação da LGPD

Para aplicar a LGPD é necessária a adoção de seus **princípios**, com especial destaque para os seguintes:

- **finalidade** – o tratamento de dados deve ser realizado para **propósitos legítimos, específicos, explícitos e informados ao titular**, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
- **adequação** – compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
- **necessidade** – 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;
- **transparência** – 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; e
- **segurança da informação** – 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.

**Quando o Titular/Cliente utiliza mídia social como meio de autenticação para serviços (para não preencher cadastro), ou quando o primeiro contato da empresa ocorre por meio de redes sociais, o Cliente precisa ser informado sobre todas as finalidades futuras de tratamento, inclusive para novos contatos do mesmo Controlador.**

Também é necessário analisar se as finalidades estão ligadas àquelas descritas nos termos de uso das próprias mídias sociais. Portanto, os dados não poderão ser utilizados para qualquer finalidade que não a expressa quando o dado se tornou público pela mídia social. Certamente a LGPD é, e será, um grande desafio de implementação, não somente por sua complexidade, mas também pela continuidade da conformidade, tendo em vista que **as ações protetivas e preventivas deverão ser, permanentemente, atualizadas**. Como sugestão de implementação, esse Guia traz 3 etapas para o processo de adequação:

## Passo 1: Avaliação e Conscientização

O primeiro passo é **conhecer a empresa e seus principais processos**, a fim de identificar as áreas que possuem tratamento de dados pessoais. As áreas que costumam se destacar com maior volume de dados nas empresas são as áreas de comerciais e de recursos humanos, contudo existem variações.
Nessa etapa é fundamental preparar a empresa e seus colaboradores para as atividades de adequação em proteção de dados, iniciando com a conscientização, pois somente com o engajamento de todos que as demais etapas serão desenvolvidas com sucesso.

**Uma boa dica é definir um GRUPO DE TRABALHO multidisciplinar envolvendo as áreas, como TI, *Compliance*, Negócios, Processos e Comunicação. Planeje as ações de conscientização e de adequação à LGPD em um projeto.**

Outro ponto fundamental é a nomeação de um **Encarregado** – quando exigível – pela empresa. Note que, a LGPD não traz um rol específico sobre os pré-requisitos para assumir a função de Encarregado, contudo é recomendado que a pessoa tenha conhecimentos das temáticas abarcadas na lei e, acima de tudo, seja alguém com acesso à alta administração e tenha independência e autonomia para executar sua função.

**Em alguns setores, como o de ENERGIA, CIGARROS E TABACO, além das normas e exigências trazidas pela LGPD, a empresa deverá atender eventuais exigências de órgãos reguladores, que poderão trazer parâmetros específicos ou maior detalhamento sobre diretrizes de aplicabilidade da legislação.**



## Passo 2: Identificar e Analisar

O segundo passo para a adequação é a preparação de uma análise criteriosa do ciclo de dados pessoais e dos riscos envolvidos na operação da empresa. Assim, sugere-se elaborar uma pesquisa inicial e **mapear a jornada de dados** dentro dos processos da empresa. Com os dados levantados, deve-se categorizar os riscos que envolvem dados pessoais e definir as ações de controle e resposta.

**Lembre-se de que cada empresa pode categorizar os riscos de acordo com seus próprios critérios.**

Por esse motivo, essa segunda etapa é marcada pelo **inventário de tratamento de dados,** uma vez que, apenas por meio do mapeamento, descobre-se onde as informações se encontram e circulam, quem as acessa e por onde estão espalhadas, sendo assim possível adquirir uma ampla compreensão dos fluxos de dados da organização. Este mapeamento também auxiliará na classificação das informações e das hipóteses de tratamentos.

**Na live[6] da Firjan sobre o setor de TECNOLOGIA DA INFORMAÇÃO foi destacada a importância da compreensão ampla e profunda de como os dados dos fornecedores são tratados, além da necessidade de respaldar em contratos eventuais tratamentos remotos que se façam necessários.**

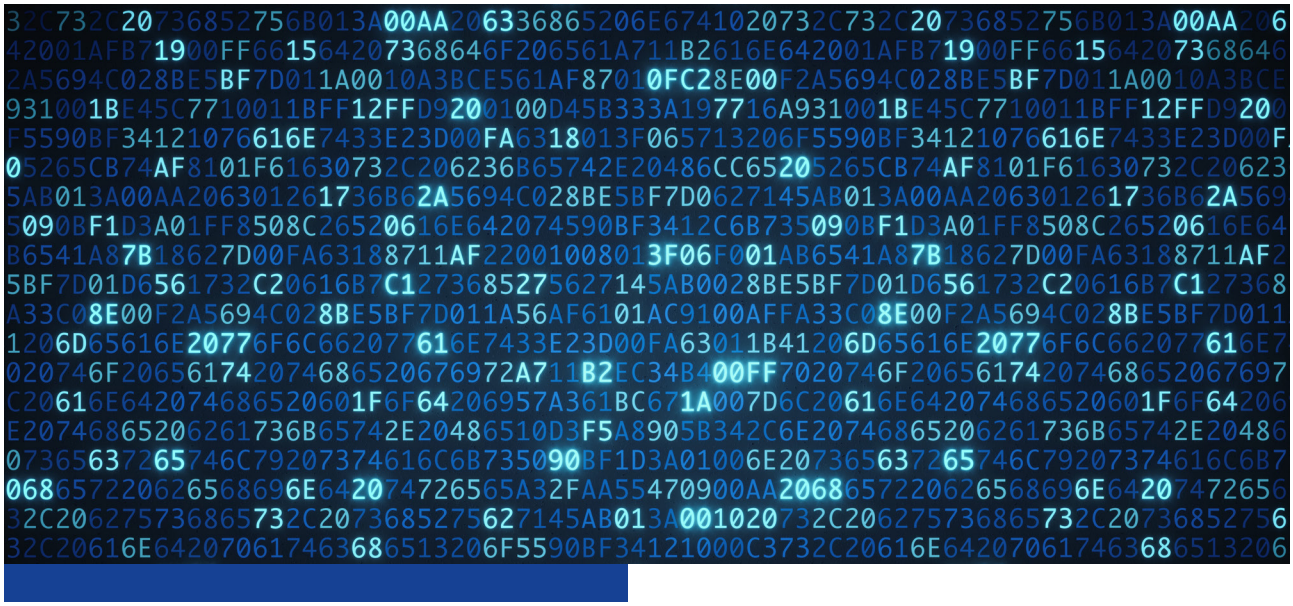


6 Disponível em: https://www.youtube.com/watch?v=Vzks9dJtkjU&list=PLrU28uWBDTQCxEcg6HEPEgGs-zINFOBVN&index=11. Acesso em: 28 fev. 2021.

Após essa etapa você deve ser capaz de responder:

1. Quais dados pessoais são tratados?
2. Quem são os titulares?
3. Há tratamento de dados sensíveis, menores ou idosos?
4. Quais os canais de entrada de dados pessoais?
5. Para qual finalidade específicas são usados?
6. Qual a justificativa (hipótese) para o tratamento?
7. Quais tratamentos precisam de consentimento?
8. Por quanto tempo serão necessários?
9. Onde são armazenados? Há uso de pseudonimização ou anonimização?
10. Quais sistemas são utilizados?
11. Quais os processos e normas existentes? Eles preveem o tratamento e a segurança dos dados?
12. Quem tem acesso aos dados dentro da empresa?
13. Os dados são compartilhados com terceiros? Com quem e para qual finalidade?
14. Há transferência internacional de dados pessoais? Os dados são colocados em sistemas de nuvem?
15. Como é aplicada a segurança dessas informações?
16. Há câmeras de vigilância? Há *Wi-Fi* "Grátis"?
17. Há auditoria de dados e processos periódico de atualização?
18. Os dados são descartados de forma segura? Em quanto tempo?

Os setores de MODA, JOIAS E BIJUTERIAS lidam com bases de dados pessoais, oriundas de diversas fontes para geração de leads, sejam de parceiros ou de fontes públicas, como a Internet. Apesar da Lei permitir o uso dessas informações, é necessário verificar se estas são oriundas de fontes legítimas porque, às vezes, a coleta pode ser lícita. Contudo isso não significa que estes dados estarão disponíveis para o tratamento por terceiros.



## Passo 3: Organizar e Atualizar

Após identificar o ciclo de vida dos dados e os pontos de melhoria, é necessário "colocar a mão na massa" e estabelecer um **cronograma de trabalho** para implementação das medidas que serão adotadas pela sua empresa, indicando os responsáveis por cada tarefa.
Também se torna necessária a **revisão e atualização** das cláusulas contratuais, incluindo, quando necessário, medidas procedimentais e técnicas a fim de mitigar eventuais riscos.

**Algumas orientações quanto à elaboração das cláusulas de LGPD podem ser encontradas no site do Governo Digital[7]. Essa e outras dicas de ferramentas você pode encontrar na sessão Referência desse Guia.**

Além dos contratos, é necessária a **elaboração de documentos com diretrizes e normas** sobre o tema, por exemplo Políticas de Privacidade Dados, de *Cookies*, de Segurança da Informação, de Descarte de dados etc.
As normas internas e os fluxos de dados precisam prever regras claras e suas consequências, a fim de priorizar a privacidade em todos os processos a serem executados.
Cabe lembrar que essas normas deverão prever regras sobre coleta, armazenamento, compartilhamento e descarte das informações, respeitado as diretrizes das legislações vigentes.

**Na terceirização, comumente realizada nos setores de CONSTRUÇÃO CIVIL E MÓVEIS, é necessário estabelecer regras e responsabilidades, por meio de contratos, termos e treinamentos de conscientização – para corretores e despachantes –, especialmente sobre o compartilhamento de dados pessoais. Isso porque, nestes setores, é comum que o tratamento dos dados pessoais dos clientes seja promovido por terceirizados, em nome das imobiliárias e construtoras.**

**Muitos setores, como é o caso do METAL MECÂNICO, possuem um amplo tratamento de dados pessoais em papel. Nesses casos, deve-se lembrar que a LGPD se aplica em qualquer meio que contenha dados pessoais, exigindo que após o tratamento indicado na finalidade seja efetuado o descarte seguro dos dados.**

Logo, no caso de tratamento de currículos e/ou outras fichas impressas, depois do seu uso, é recomendável que seja feita a eliminação dos documentos, picotando os papéis. Ou seja, é importante que cada empresa estabeleça detalhadamente uma tabela de temporalidade, devendo constar o tipo de dado coletado, a finalidade, o tempo de guarda e a hipótese de tratamento, uma vez que os dados podem ser tratados por áreas distintas e finalidades diversas, com embasamentos distintos.

7 Guia de Adequação de Contratos. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaRequisitosdeSIparaContratacoesdeTI.pdf. Acessado em 28 de fev. de 2021.

Cabe lembrar que é necessário proceder com elaboração de modelo de relatório de impacto padrão, manual de contenção de incidente de privacidade, termo de revalidação de dados antigos e, em papel, documento de gerenciamento de crise, de resposta a incidentes, de segurança da informação, de conduta ética, bem como de avisos de privacidade constantes de aplicativos e sites da empresa.

**Lembre-se de que a LGPD também se aplica aos dados coletados antes da vigência da lei, uma vez que armazenar é uma forma de tratar dados pessoais.**

Os documentos elaborados precisam ser fidedignos com a atuação e comunicarem-se com o ambiente externo – na demonstração do comprometimento com a proteção de dados – e com o ambiente interno – prevendo regras para atuação diária de seus colaboradores.

**Após essa etapa você deve ser capaz de responder:**

1. **Existem regras claras sobre registro de tratamento?**
2. **Existe uma verificação de segurança periódica?**
3. **A Política de Privacidade indica a abrangência de tipos de dados coletados; a forma e o objetivo da coleta e tratamento das informações; quem é o Encarregado (DPO) e a forma de contato; os direitos dos titulares; com quem a empresa compartilha os dados pessoais; quais os motivos do compartilhamento e qual o prazo de armazenamento?**
4. **Há controle de acesso com emprego de técnicas de controle lógico e físico?**
5. **Há procedimento instituído para a que permita a gestão do consentimento dos titulares, com registro da justificativa por exceção?**
6. **Foi disponibilizado canal para que os titulares de dados pessoais exerçam seus direitos?**
7. **Há procedimento instituído para responder as solicitações dos titulares de dados no prazo legal?**
8. **Há procedimento instituído para responder as solicitações efetuadas pela ANPD?**
9. **Foi elaborado Relatório de Impacto de Privacidade de Dados para os casos de legítimo interesse?**
10. **Os contratos foram atualizados?**
11. **Existe plano de treinamento e conscientização dos funcionários?**
12. **O acervo de papel e de dados anteriores a LGPD foi revisto?**

**Os setores GRÁFICO E AUDIOVISUAL trabalham com diversos terceirizados. Logo, quando a empresa contratar um terceirizado, deve fornecer apenas a quantidade mínima de dados pessoais necessários para realização do projeto, sempre deixando claro – por meio de contratos e de instruções – quais são as responsabilidades do subcontratado, enquanto estiver em posse das informações/dados pessoais.**

Todas essas ações – dos três passos – podem ser parte de um Programa de Privacidade de Dados, que é um conjunto de ações que auxilia a atuação da empresa quanto à cultura de privacidade de dados.

# 4. Destaques setoriais

As relações *Business to Business* (empresa para empresa) e *Business to Costumer* (empresa para consumidor) se diferem pela finalidade de coleta, mas não pela complexidade. Ou seja, ambas precisam se adequar à LGPD, isto porque as empresas B2B também tratam dados pessoais, seja de seus funcionários, seja de seus fornecedores. Assim, destacamos nos próximos tópicos, algumas peculiaridades setoriais aplicáveis aos diversos setores industriais.

## Automóveis, Reparação e Borracha

Quando falamos de automóveis, muitas vezes não relacionamos a conexão com dados pessoais. Entretanto estamos em uma sociedade de dados, com conectividade, e a indústria automobilística segue essa tendência. Se pensarmos, hoje temos carros autônomos, superconectados, com botões no painel que fazem conexão direta com um atendente que sabe quem é você, qual o modelo do seu carro, onde você está e se o automóvel está com um problema. Toda essa relação, incluindo os dados de geolocalização, são abarcadas pela LGPD.

Caso a empresa presta esse tipo de serviço para o cliente, é necessário ter muita transparência, informando que os dados são 24h monitorados e com quem são compartilhados. São várias informações que podem ser úteis para a empresa e para o cliente, bem como para terceiros, tendo em vista que existe troca de informações entre parceiros comerciais para permitir toda essa conectividade.

**ADOTAR A MINIMIZAÇÃO COMO REGRA SERÁ UM DIFERENCIAL COMPETITIVO.**

**Minimização é saber realmente quais os dados são necessários para desenvolver uma determinada ação. Por exemplo, para o uso da localização do GPS, não é necessário saber o nome da mãe ou o gênero do cliente. Fazer mais com menos informações de dados pessoais será um grande diferencial para as empresas.**

**EU NÃO VOU MAIS PODER FAZER CONTATO COM MEU CLIENTE, VOCÊ ACABOU COM MEU BUSINESS, VOCÊS ESTÃO QUERENDO ME DESTRUIR.**

**Calma! Não é bem isso! Com a LGPD as empresas estarão mais organizadas, com uma base robusta, com bons dados, qualificados e com o consentimento do cliente. Assim sua empresa poderá trabalhar de uma forma muito rica e sem correr riscos.**

Hoje o setor automobilístico possui uma relação vital entre as montadoras, concessionárias, autopeças, e demais fornecedores. Então é necessário ajustar com todos os processos e verificar os papéis de Controlador ou Operador. É necessário deixar os papéis mais definidos entre os parceiros, ter o envolvimento de toda cadeia, e o entendimento sobre a importância da lei.

**Adequar-se à LGPD é um trabalho de duas faces concomitantes: mudança de *mindset* e governança.**

Adequar-se à LGPD é um processo multidisciplinar, que precisa engajar toda empresa e principalmente as concessionárias, as quais, geralmente, captam as informações dos clientes e compartilham com as montadoras. Neste sentido, vale lembrar que a LGPD não é a única lei aplicável ao setor, ou seja, em alguns casos a coleta e repasse de dados se fará necessária para atender a outras legislações, como é o caso da Lei nº6.729, de 28 de novembro de 1979 – Lei Ferrari, que tem como objetivo regulamentar a concessão comercial para o mercado automotivo nacional.

**A coleta de informações no ambiente físico é um grande desafio para o setor, pois muitas vezes as informações são passadas verbalmente para o vendedor durante um teste *drive* ou durante uma visita. Assim, é necessário investir em como passar todas as informações que a LGPD exige ao cliente e como evidenciar essas ações com os controles existentes atualmente no mercado.**

A legislação trouxe uma atenção maior para a transferência internacional de dados. Assim, as pequenas as médias empresas precisam ter esse cuidado, pois hoje é muito difícil ter um *data center* no Brasil, é tudo em nuvem. Então, em uma simples inserção de dados para faturamento em um sistema em nuvem cujo *data center* fique fora do país, a empresa estará realizando uma transferência internacional de dados.



# Moda, Joias e Bijuterias

Em regra, os setores de moda, joias e bijuterias empregam muitas pessoas, incluindo uma forte contratação de prestadores de serviços e de terceirizados para execução de mão de obra. Ao falar de terceirização, é necessário ter em mente que é responsabilidade do contratante garantir o correto tratamento dos dados pessoais. Ou seja, na prática os contratos deverão ser modificados para constarem de cláusulas que tragam as responsabilidades e as formas de tratamentos dos dados.

**Não basta o contrato ter cláusulas, é necessário verificar se essas representam a realidade e permitem a correta fiscalização, pois nem sempre o contrato padrão consegue garantir a conformidade de subcontratados.**

A LGPD traz diversos princípios e exige sua aplicação em harmonia com outros direitos, e por esse motivo considera nula a inserção de cláusulas genéricas e não efetivas em contratos. Assim, não adianta estabelecer que o fornecedor deverá entregar um rol de documentos se a empresa não possuir meios de verificar a validade destes.

**A mudança de cultura é um dos pontos mais importantes e difíceis no processo de implementação da LGPD, pois para ter sucesso é necessário o envolvimento e o apoio da Alta Administração**. Muitas vezes a alta administração entende e patrocina o projeto, mas encontra dificuldade para fazer com que seus colaboradores entendam a importância da adequação. Então é preciso dar informação, desmistificar a legislação e mostrar que a adequação não é só importante para a empresa, mas para toda a sociedade.

**Os empresários não terão que pedir consentimento para todas as atividades executadas no âmbito do relacionamento com os clientes, contudo é necessário estabelecer um processo para que se possa atendê-los rapidamente, seja para uma exclusão, seja para um ajuste dos dados cadastrados.**

É importante compreender que a LGPD não se sobrepõe às demais legislações, então se por exemplo o cliente solicitar a exclusão de um dado e alguma lei impedir isso, os dados não poderão ser excluídos. Como exemplo, pode-se citar a Resolução n° 25/2013, emitida pelo Conselho de Controle de Atividades Financeiras – COAF, que estabelece a obrigatoriedade das pessoas físicas ou jurídicas que comercializem ou intermedeiem bens cujo valor unitário seja igual ou superior a R$ 10.000,00 (dez mil reais) de manterem o cadastro de diversos dados pessoais de seus clientes e dos demais envolvidos na transação.

No âmbito do *e-commerce*, a LGPD trouxe um novo conceito que se chama *privacy by design*, exigindo que as empresas, antes de realizarem qualquer novo projeto, analisem os impactos à privacidade dos titulares de dados destinatários do projeto. Ou seja, para adequar os sites de *e-commerce*, não basta inserir um aviso de *cookies*, é preciso verificar os sistemas e as políticas que regem toda a relação com os clientes.

**Vale lembrar do Decreto n°7.962, de 15 de março de 2013, que regula as contratações no comércio eletrônico, exigindo que as manifestações referentes a informação, dúvida, reclamações por parte do consumidor sejam respondidas no prazo de 5 dias.**

# Construção Civil, Naval e Móveis

Muitas empresas destes setores atuam com serviços B2B, contudo isso não as exime da aplicação da LGPD, uma vez que efetuam tratamento de dados em suas atividades internas como RH, *Marketing*, Negócios, entre outras. Assim, é necessário adequar todos os contratos com cláusulas de LGPD que reflitam o grau e risco da relação. Ou seja, as cláusulas devem ser adequadas ao serviço e ao que se espera do fornecedor.

**O setor de construção civil possui uma extensa cadeia produtiva, assim é natural que o volume de dados seja expressivo. É importante tratar da temática junto aos parceiros comerciais, a fim de estabelecer as responsabilidades de cada um.**

Existem diversas notícias sobre ciberataques em bancos de dados, o que muitas vezes nos leva à falsa sensação de que a segurança da informação seria algo apenas relacionado a informática e sistemas. Contudo, cabe aqui o entendimento de que não é possível garantir a privacidade sem antes garantir a segurança da informação. Assim, é recomendado que todas as empresas elaborem um plano de resposta para incidentes ou contingência.

**É necessário ter em mente que muitas vezes os dados não estão em sistemas, mas em papel, como ocorre com as fichas de interesse preenchidas em estandes de vendas junto aos corretores.**

Os dirigentes das empresas precisam compreender que quando um profissional está executando uma atividade, ele é o responsável pelos dados que estão sob seu poder. Assim, não basta ter sistemas seguros, é preciso que os profissionais entendam e estejam atentos na utilização das ferramentas e tratamento dos dados confiados a eles.



# Energia

Com a chegada da LGPD, a privacidade passou a ser vista como ponto focal de qualquer projeto, especialmente nos setores regulados, como é o caso do setor de Energia, que possui uma ampla capilaridade e trata de dados de quase toda a população do país.

O setor de energia, por ser regulado, possui uma utilização da base de tratamento legal e regulatória. Assim, para que se possa prestar um bom serviço ao cliente, as concessionárias necessariamente precisam tratar dados pessoais.

Muitas vezes as empresas de energia elétrica são obrigadas a efetuar compartilhamento de dados, seja para a agência reguladora, seja para agências de cobrança. Nestes casos não será necessário solicitar o consentimento dos titulares, contudo é preciso ter em mente que a privacidade tem que ser um valor para todos os envolvidos.

**É necessário olhar para quem vai receber os dados, se esta empresa está adequada à LGPD, como faz o tratamento dos dados recebidos. Esse controle pode ser feito por relatório de impacto, capacitação e reuniões constantes com os fornecedores, a fim de comprovar que todos da cadeia estão seguindo fielmente as diretrizes da LGPD.**

Outro ponto de grande importância é o tratamento do histórico dos dados pessoais dentro da empresa. Neste aspecto, deve ser estabelecida regras para o tratamento dos dados pessoais no dia a dia da empresa, elaborando – quando necessário – os relatórios de impactos.

**A LGPD já estabelece os direitos dos titulares de dados, mas no caso da empresa de concessão de energia, existem limitações de outras regulações, como por exemplo a limitação ao direito de exclusão dos dados pessoais, devido à existência de obrigações regulamentares, fiscais, fazendárias e tributárias, que obriga os agentes atuantes no setor de energia a manterem esses dados por um determinado período.**

No setor de energia, pode-se esperar uma atuação da ANPD de forma articulada com os agentes regulatórios específicos, tal qual a ANEEL, TCU, CGU etc. Ou seja, é natural que as próximas regulações da ANEEL passem a incorporar itens da LGPD, uma vez que essa temática de proteção de dados já era demandada ao setor, mesmo antes da legislação nacional, se pode observar da própria redação da **Resolução 414 da ANEEL**, que já exigia um cuidado maior das concessionárias na transmissão de dados para as distribuidoras.

**A LGPD prevê no art. 51 a possibilidade de autorregulação, permitindo que os setores da sociedade formulem códigos de boas práticas e tratamento de dados que poderão ser chancelados pela ANPD.**

# Cosmético e Farmacêutico

Na área de produtos para saúde e farmacêutica, em razão da natureza própria do setor e dos muitos programas de apoio aos pacientes, que as empresas atuantes são obrigadas a desenvolver, são tratados diversos dados pessoais sensíveis. Logo, nesse setor é necessária uma atenção redobrada quanto ao tratamento dos dados pessoais e dados pessoais sensíveis.

**É aconselhado que o setor trabalhe fortemente a temática junto aos colaboradores internos e mantenha em suas bases apenas os dados absolutamente necessários ou exigidos por lei.**

Essa percepção de valor do dado tem se tornado cada vez mais clara no mercado com o avanço tecnológico. Hoje as empresas que utilizam os dados pessoais como seu modelo de negócio, como *commodity digital*, são consideradas mais valiosas no mundo. Assim, é fundamental ter em mente que dados pessoais são ativos da empresa e o correto tratamento é um demonstrativo de confiabilidade no mercado.

**A implantação da LGPD não é um custo, mas sim um investimento. Quanto vale sua empresa em imagem? E sua reputação no mercado?**

Os setores farmacêutico e de cosméticos lidam com diversos dados sensíveis, contudo verifica-se a necessidade de ações mais enérgicas, ações prévias e cuidados maiores no sentido de dissociar esses dados da identificação do titular, sendo salutar aplicar – sempre que possível – técnicas de pseudonimização ou de anonimização total dos dados, uma vez que os dados pessoais sensíveis possuem um maior potencial danoso ao titular, em caso de eventual incidente de dados pessoais.

É importantíssimo que a empresa conheça os seus dados, seus processos, que reveja a quantidade de dados que coletam, a razão e necessidade desta coleta, o entendimento das hipóteses de tratamento nas quais se baseiam essa coleta e o tratamento dos dados e, sem dúvida nenhuma, que tenham uma política de privacidade clara e transparente, ressaltando para o titular exatamente o que será realizado com seus dados. E o mais salutar é o cumprimento das diretrizes constantes da política de privacidade, pois a confiança é tudo no mercado que une o consumidor às empresas com as quais ele se relaciona.

**O Estado de São Paulo, por meio da Lei nº 17.301, de 24 de janeiro de 2020, proibiu farmácias e drogarias de exigir o CPF do consumidor no ato da compra, sem informar de forma adequada e clara sobre a abertura de cadastro ou registro de dados pessoais e de consumo, que condiciona à concessão de promoções[8]. Assim é importante que os empresários tenham bastante atenção com o exercício do direito por parte dos titulares e estabeleçam uma política interna efetiva.**

8 Veja mais em https://www.uol.com.br/tilt/noticias/redacao/2020/12/04/sem-cpf-nova-lei-proibe-farmacias-de-pedir-documento-em-troca-de-desconto.htm?cmpid=copiaecola

# Alimentos e Bebidas

O setor de alimentos lida com dados pessoais de consumidores finais e/ou de seus trabalhadores, por isso é importante adquirir um sistema de gestão de dados pessoais. Isso porque, além da LGPD, aplicam-se outras leis, como o Código de Defesa do Consumidor, que – dentre outras previsões – permite que o consumidor solicite a inversão do ônus da prova.

**Manter um sistema de governança capaz de levantar as informações pessoais de maneira organizada será um diferencial no mercado de alimentos e bebidas.**

No mais, é salutar a elaboração de um processo de *due diligence* de fornecedores, uma vez que os setores de bebidas e alimentos atuam com uma ampla cadeia de fornecedores.

**Os contratos com os fornecedores podem ser revistos em ondas de criticidade e risco quanto ao acesso a dados pessoais.**

É importante elaborar aditivos aos contratos de fornecedores, sempre identificando se estes atuaram como Operadores, Controladores, ou Cocontroladores de dados pessoais. Isso porque essa classificação implicará maior robustez das cláusulas referentes ao tratamento dos dados, segurança dos dados, criptografia, anonimização e regras para encerramento do contrato, incluindo a deleção de dados, comunicado imediato de incidentes, possibilidade de fiscalização e auditoria, sempre que necessário, a serem inseridas nos contratos.

# Plástico, Embalagem e Eletrodomésticos



A LGPD não está só conectada a TI, é preciso que a área de TI converse com *compliance* e jurídico para que a adaptação da empresa possa ser feita.
Fala-se muito sobre a internet das coisas (IOT), pauta que gera uma preocupação a mais com a LGPD, pois essas tecnologias coletam e armazenam diversos dados pessoais. Assim, com o advento das legislações protetivas, vislumbra-se uma tendência a adoção de sistemas embarcados, para evitar que a empresa fornecedora dos eletrodomésticos tenha acesso aos dados pessoais coletados pelas máquinas. Contudo, o fato não exime as empresas de pensarem na privacidade e na segurança da informação em todos os aspectos desses novos projetos.

# Óleo e Gás

Desde o início da pandemia, a quantidade de vazamento de dados aumentou muito. Assim, a segurança da informação tem um papel fundamental na implementação da LGPD. É necessário que sejam redesenhados os perfis de acesso de acordo com o cargo e a necessidade de acessar determinados dados.

**A LGPD é uma possibilidade de melhoria na comunicação com o público de interesse das empresas, especialmente no setor de óleo e gás, no qual os principais tratamentos dos dados pessoais são os programas de fidelização, uma vez que o intuito desses é mapear o consumo e personalizar o atendimento.**

Outro desafio é o momento em que o colaborador sai da empresa, pois existem muitas demandadas de fiscalização que ocorrem após a saída do profissional. Logo, é importante avaliar quais dados a empresa vai manter e por quanto tempo. Então a LGPD deve ser vista como uma oportunidade da empresa rever seus processos, sempre primando pela finalidade da coleta dos dados.

**Para o pequeno empresário o custo da adequação com certeza é um desafio. Contudo, a LGPD distingue micro e pequenas empresas, permitindo que a ANPD adeque a fiscalização e as exigências para esses pequenos e micronegócios.**

# Metal Mecânico

A LGPD não se resume a área de TI, sendo uma responsabilidade da empresa como um todo. Com a chegada dessa nova legislação, o metal mecânico foi atingido tanto quanto os outros setores.
Um dos principais desafios é fechar o mapeamento de dados, visto que essa ação envolve todos os setores da empresa e a alta administração. Outra dificuldade é organizar todos os dados coletados. Já externamente, é preciso estabelecer uma política de governança muito bem definida.
Para a segurança dos dados, as empresas de metal mecânico têm estabelecido regras a serem cumpridas, que incluem a parte de infraestrutura, garantindo que uma eventual invasão não comprometa a captura dos dados.

Com o advento da indústria 4.0, existem as questões de automação e inteligência artificial, que precisam ser contempladas no operacional das empresas. Normalmente as informações de nossos consumidores / fornecedores estão na nuvem (em bancos de dados), contudo, no caso de tecnologia aplicada a fechaduras *hight tech*, por exemplo, essas informações ficam apenas no dispositivo com o consumidor e a empresa não tem acesso aos códigos gerados.
No B2C é necessário tomar ainda mais cuidado, com casas que têm biometria ou reconhecimento facial. Mas, quanto às empresas industriais, o risco maior é o vazamento de informações técnicas (o que não significa que sejam menos importantes).

# Gráfico e Audiovisual

O setor Gráfico e de Audiovisual vem transferindo suas entregas, cada vez mais, para o ambiente virtual. Desse modo, o impacto da LGPD no setor é grande, uma vez que há necessidade de adequar o tratamento de todos os dados fornecidos com pelos titulares. Assim, as empresas que lidam diretamente com o cliente, como TV por assinatura e *streaming*, por exemplo, já estão mais adiantadas na adequação à LGPD do que aquelas ligadas a uma atuação B2B.

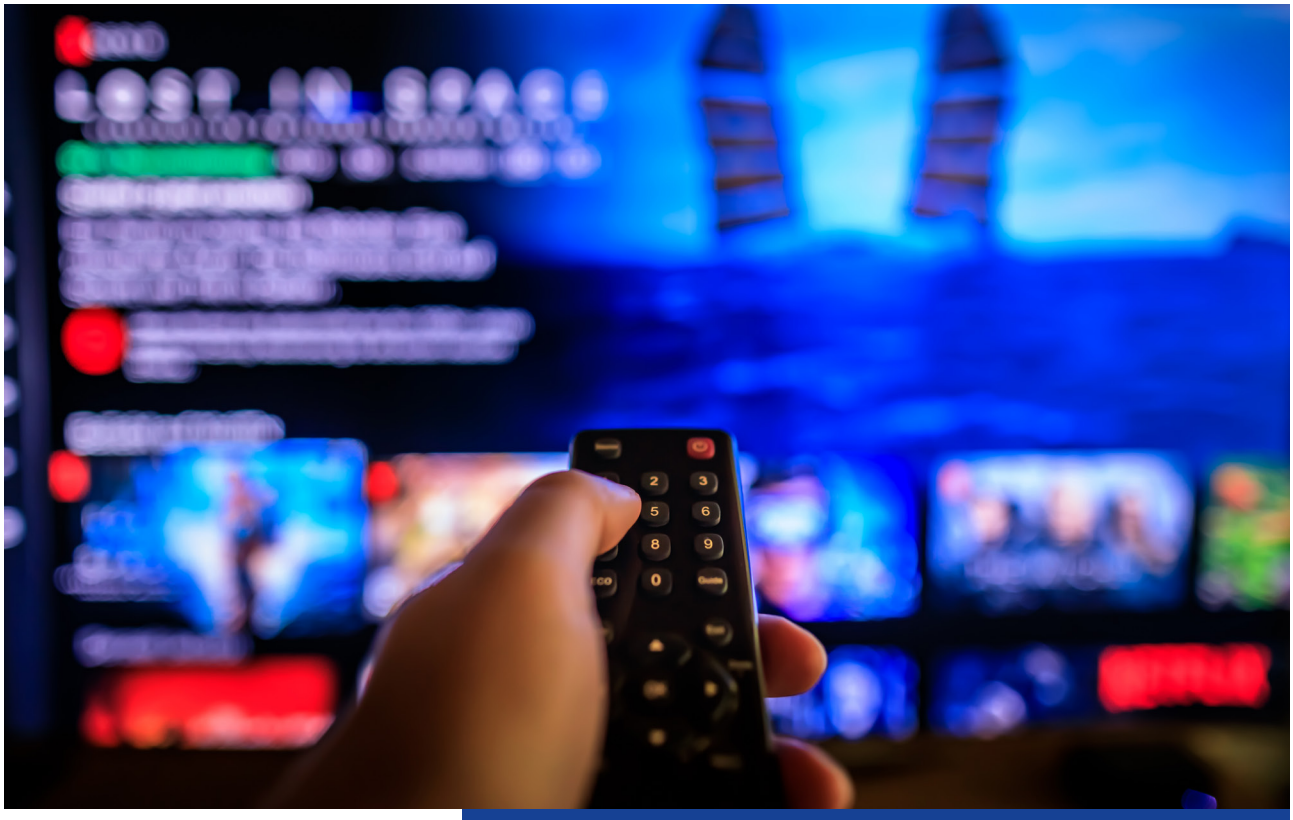
**A LGPD inovou ao exigir o respeito à autodeterminação informativa e exigir que as empresas usem recursos audiovisuais para facilitar a compreensão do titular de dados.**

Dentre os desafios enfrentados pelo setor, pode-se citar a implementação da cultura em si, pois sem a implementação da cultura não há adequação. A implementação passa por duas realidades, física e lógica, da empresa e carece de tecnologia e treinamento. Outro ponto importante é um plano de contingência, uma vez que um cenário de zero risco é impossível.

**Procure ajuda do seu sindicato e da Firjan, pois com as devidas orientações, as empresas podem começar com os passos mais simples, como estudar a lei e permitir que a implementação conte com o total apoio da alta direção.**

Cabe ressaltar a atenção sobre a coleta, como ela se dá e onde os dados são armazenados, de modo que, se um dos dois se derem no Brasil, a ferramenta deverá estar adequada à LGPD. Assim, é fundamental uma análise da documentação dos fornecedores, especialmente os de soluções em nuvem, para se ter ciência de como será o tratamento dos dados fornecidos.





# Tecnologia da Informação

No setor de tecnologia da informação, a adequação à LGPD é dividida em três frentes de trabalho: (i) produtos e hierarquia de acesso às informações; (ii) cultural para conscientizar os membros do time da responsabilidade com o uso dos dados e com a segurança de informação; e (iii) conscientização do cliente quanto à importância da segurança e do cuidado com a privacidade.
A LGPD trouxe a necessidade de adequação dos processos e dos novos projetos à privacidade desde a concepção. Assim, é importante trazer a conscientização da privacidade como um ponto primordial, desde o início, incorporando a segurança como um padrão da empresa.
A segurança da informação está intimamente ligada à proteção de dados pessoais e ao atendimento da LGPD. Assim, é fundamental se cercar de informações sobre o fornecedor e o serviço em si, em relação à privacidade e à segurança, sempre respaldando a atuação em contrato.
A adequação à LGPD é multisetorial, envolvendo diversas temáticas de atuação, como a segurança da informação e o mapeamento de dados. É importante mostrar que adquirir um *software* que possui *cybersecurity* não é adequação à LGPD e isso não tira a responsabilidade de realizar as outras atividades inerentes à adequação.
A demonstração para colaboradores e clientes deve ter como foco a mudança cultural, a qual é implementada de forma gradativa. É importante demonstrar que todas as medidas necessárias foram tomadas minimizando a possibilidade de vazamentos e invasões.

# Cigarro e Tabaco

A indústria do tabaco investe muito em tecnologia, pode-se citar o uso de *drones* para mapear plantações de tabaco, detectores de infravermelho que monitoram insumo nas fábricas e sistemas de logística modernos que são utilizados para acompanhar entregas em tempo real. Além disso, o setor de produção do tabaco gera emprego e renda para muitas pessoas no país.
O setor é voltado para uma dinâmica B2B, de modo que a filosofia minimalista em relação à coleta é perfeita para a política de dados. Não basta inserir cláusulas em contratos, mas realmente compreender o que será feito com os dados coletados, o que é muito bom até mesmo para a transparência.
A proteção de dados independe da natureza deles, se são pessoais ou estratégicos, por exemplo. Assim, é necessário que a análise feita na coleta de dados seja transversal. Após, os dados pessoais deverão ser protegidos de forma proporcional a sua importância.
Na sociedade da informação, o dado possui um valor imenso. A conscientização é fundamental para a implementação da LGPD e isso hoje é tido como um diferencial entre as empresas.
A LGPD, ao trazer a finalidade específica, torna muito mais fácil para a empresa ser transparente. Essa clareza interna é um ponto em que se deve investir muito mais tempo para que apenas os dados realmente necessários sejam coletados.
O setor de tabaco é extremamente regulado, principalmente pela ANVISA, que, embora não tenha determinações específicas sobre coleta de dados, impõe severas limitações em termos de comunicação, em especial com o consumidor.
O consumidor possui uma ampla proteção tanto por parte da ANPD como por parte do Procon, o que permite um olhar mais atento das empresas em relação aos tratamentos de dados empregados. Contudo, o setor de tabaco pouco se relaciona com o consumidor final, tendo por desafio o tratamento de dados pessoais e sensíveis dos produtores rurais, dentre outros terceirizados, uma vez que se trata de um setor muito verticalizado, sendo este seu maior desafio com o advento da LGPD.

# Referências


FAQ da Sascar, Disponível em: <https://www.sascar.com.br/faq-protecao-de-dados/> Acessado em 28 de fev. de 2021.

Ferramenta de Relatório de Legítimo Interesse da CNIL. Disponível em: <https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment> Acessado em 28 de fev. de 2021.

Guia para Pequenas Empresas. Disponível em: <https://www.cnil.fr/fr/la-cnil-et-bpifrance-sassocient-pour-accompagner-les-tpe-et-pme-dans-leur-appropriation-du-reglement> Acessado em 28 de fev. de 2021.

Guias Operacionais Gov.Br. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/guias-operacionais-para-adequacao-a-lgpd> Acessado em 28 de fev. de 2021.

Guia de Programa de Privacidade. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaProgramaGovernanaemPrivacidade.pdf> Acessado em 28 de fev. de 2021.

Guia de Inventário de Dados. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaInventario.pdf> Acessado em 28 de fev. de 2021.

Guia de Boas Práticas. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaLGPD.pdf> Acessado em 28 de fev. de 2021.

Guia para elaboração de Termo de Uso. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaTermoUso.pdf> Acessado em 28 de fev. de 2021.

Guia para elaboração de Avaliação de Riscos. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-avaliacao-de-riscos-de-seguranca-e-privacidade.pdf> Acessado em 28 de fev. de 2021.

Guia de Adequação de Contratos. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaRequisitosdeSIparaContratacoesdeTI.pdf> Acessado em 28 de fev. de 2021.

Guia e Template de Relatório de Impacto. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-template-ripd_v4.docx> Acessado em 28 de fev. de 2021.

Tabela de Registro de Tratamentos da CNPD para controladores. Disponível em: <https://www.cnpd.pt/home/rgpd/docs/templateDocRGPD_sub_v1.xlsx> Acessado em 28 de fev. de 2021.

Tabela para Inventário de Dados. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/arquivos/TemplateInventariodadospessoais.xlsx> Acessado em 28 de fev. de 2021.

Questionário de Diagnóstico de Adequação. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/diagnostico-de-adequacao-a-lgpd> Acessado em 28 de fev. de 2021.

Resolução CMN nº 4.893 de 26 de fevereiro de 2021 do Banco Central, disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=4893> Acessado em 28 de fev. de 2021.

Tabela de Registro de Tratamento da CNPD para subcontroladores (operadores). Disponível em: <https://www.cnpd.pt/home/rgpd/docs/templateDocRGPD_sub_v1.xlsx> Acessado em 28 de fev. de 2021.

Sugestão de Ferramenta de Avaliação de Risco. Disponível em: <https://pesquisa.sisp.gov.br/index.php/468289?lang=pt-BR> Acessado em 28 de fev. de 2021.

A Firjan apoia todas as iniciativas que visam à construção e manutenção de uma cultura ética e de valorização da privacidade nas empresas, em conformidade com a legislação nacional e o direito internacional.


Firjan
SENAI
SESI
IEL
CIRJ