Documento Oficial CNC
2ª EDIÇÃO | JULHO 2023 | www.portaldocomercio.org.br

LGPD

CARTILHA

Lei Geral de Proteção de Dados Pessoais

CNC
Sesc Senac

LGPD

CARTILHA

Lei Geral de Proteção de Dados Pessoais

LGPD

CARTILHA

Lei Geral de Proteção de Dados Pessoais

Rio de Janeiro, 2023
2° edição

CNC
Sesc Senac

Confederação Nacional do Comércio de Bens, Serviços e Turismo

CARTILHA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Presidente: José Roberto Tadros

Diretora Geral Executiva (DGE): Simone de Souza Guimarães

1ª edição, 2019 | 2ª edição, 2023

Redação técnica: Diretoria Jurídica e Sindical (DJS), Gerência Executiva de Tecnologia da Informação (GETI), Gerência Executiva de Recursos Humanos (GERH) e Gerência Executiva de Comunicação (GECOM).

Revisão e atualização: Diretoria Jurídica e Sindical (DJS).

Projeto gráfico e diagramação: Programação Visual/Gecom-CNC

C748

Confederação Nacional do Comércio de Bens, Serviços e Turismo
Cartilha: Lei Geral de Proteção de Dados Pessoais / Confederação Nacional do Comércio de Bens, Serviços e Turismo. – 2. ed. - Rio de Janeiro : Confederação Nacional do Comércio de Bens, Serviços e Turismo, 2023.

27 p. : il. color. ; 21 cm.

Revisão e atualização: Diretoria Jurídica e Sindical (DJS).

1. Direito Constitucional – Proteção de Dados. 2. Lei Geral de Proteção de Dados (LGPD) I. Título.

CDD 323.4483

Bibliotecário responsável: Bernardo Palma – CRB7: 6479

CNC - Rio de Janeiro
Av. General Justo, 307 – CEP: 20021-130
PABX: (21) 3804-9200

CNC - Brasília
SBN Quadra 1 Bl. B – nº 14 – CEP: 70041-902
PABX: (61) 3329-9500/3329-9501

www.portaldocomercio.org.br

SUMÁRIO

INTRODUÇÃO

Seguindo uma tendência mundial de proteção de dados, que busca garantir a privacidade dos indivíduos e mitigar os riscos do uso indevido de informações pessoais, foi publicada no Diário Oficial da União, em 13 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais, ou simplesmente LGPD (Lei nº 13.709/2018).

A LGPD foi baseada no Regulamento Geral de Proteção de Dados Europeu (GDPR), que trata do mesmo tema e, dessa forma, incluiu o Brasil no grupo de países com Lei de Proteção de Dados única e completa.

Após a edição da Lei nº 13.709/2018, a proteção aos dados pessoais no Brasil ganhou previsão constitucional, sendo elevada a um direito fundamental, por meio da promulgação da Emenda Constitucional nº 115/2022.

Em paralelo, a Autoridade Nacional de Proteção de Dados (ANPD) editou regulamentos importantes para a aplicabilidade da lei, tais como o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador (Resolução CD/ANPD nº 1/2021, o Regulamento de aplicação da LGPD para agentes de tratamento de pequeno porte (Resolução CD/ANPD nº 2/2022) e o Regulamento de Dosimetria e Aplicação de Sanções Administrativas (Resolução CD/ANPD nº 4/2023).

Dessa forma, considerando o estágio atual de amadurecimento da questão e da legislação editada, revisitamos e atualizamos a presente Cartilha, a fim de contribuir no esclarecimento e na propagação dos conceitos e fundamentos da proteção e da privacidade de dados, visando auxiliar as empresas e entidades integrantes do Sistema Comércio em seus processos de conformidade.

OBJETIVOS DA LEI

O objetivo da lei é garantir a proteção aos dados pessoais obtidos, respeitados os direitos fundamentais de liberdade e de privacidade, que possam ser eventualmente violados pela má utilização dessas informações, permitindo maior confiança em relação à coleta e uso de dados, maior segurança jurídica e, em consequência, o fomento ao desenvolvimento econômico e tecnológico da sociedade, à medida que estabelece regras claras sobre proteção de dados pessoais.

FUNDAMENTOS DA PROTEÇÃO DE DADOS

- O respeito à privacidade;
- A autodeterminação informativa;
- A liberdade de expressão, de informação, de comunicação e de opinião;
- A inviolabilidade da intimidade, da honra e da imagem;
- O desenvolvimento econômico e tecnológico e a inovação;
- A livre iniciativa, a livre concorrência e a defesa do consumidor;
- Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

A QUEM SE APLICA

A norma em referência se aplica às pessoas físicas e jurídicas de direito público e privado que venham a realizar qualquer tipo de tratamento de dados, bem como às pessoas físicas que tenham seus dados coletados por meio físico ou digital.

Cabe destacar que a lei não se aplica ao tratamento de dados realizado para fins exclusivamente particulares e não econômicos, para fins exclusivamente jornalísticos, artísticos, acadêmicos, de segurança pública, de defesa nacional, de

segurança do Estado ou de atividade de investigação ou repressão de infrações penais, entre outras, conforme expressamente disposto em seu artigo 4º.

O QUE SÃO DADOS PESSOAIS?

São aquelas informações que possam, de alguma forma, identificar ou tornar identificável uma pessoa natural.

Dado pessoal: informação relacionada a pessoa natural identificada ou identificável, tais como nome, foto, endereço, localização, documentos, e-mail, características pessoais, entre outros.

Dado pessoal sensível: dado 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 a um titular que não possa ser identificado, em razão da perda da possibilidade de associação a um indivíduo, considerando a utilização de meios técnicos razoáveis e disponíveis.

Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

Tratamento de dados pessoais: É toda operação realizada com dados pessoais, tais como a coleta, o acesso, a utilização, a distribuição, a transferência, o processamento, o armazenamento, o arquivamento, até o descarte dos dados.

ATENÇÃO!

LGPD se aplica às operações de tratamento de dados pessoais realizadas tanto em meios físicos, como em meios digitais.

Exemplos: Arquivos em papel, documentos físicos, armazenados em mídias digitais e em nuvem.

HIPÓTESES DE TRATAMENTO DE DADOS

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

I) mediante o fornecimento de consentimento pelo titular;

II) para o cumprimento de obrigação legal ou regulatória pelo controlador;

III) pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;

IV) para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V) quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI) para o exercício regular de direitos em processo judicial, administrativo ou arbitral;

VII) para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII) para a tutela da saúde, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

IX) quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X) para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

A lei também faz a distinção do tratamento de dados e prevê hipóteses para o tratamento de dados pessoais sensíveis. São elas:

I) quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II) sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

- **a)** cumprimento de obrigação legal ou regulatória pelo controlador;
- **b)** tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
- **c)** realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
- **d)** exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;
- **e)** proteção da vida ou da incolumidade física do titular ou de terceiro;
- **f)** tutela da saúde, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
- **g)** garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º da Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

As crianças e adolescentes ganharam destaque no tratamento de seus dados pessoais, que deve ser realizado mediante o consentimento específico e em destaque dado por, pelo menos, um dos pais ou pelo responsável legal. Somente poderão ser coletados dados pessoais de crianças sem o consentimento específico dos pais e/ou responsável legal quando a coleta for necessária para contatar os pais ou o responsável legal, uma única vez e sem seu armazenamento, ou para a proteção da criança.

ATENÇÃO!

O tratamento de dados pessoais nem sempre dependerá do consentimento do titular dos dados, pois o consentimento é apenas uma das hipóteses possíveis, havendo outras previstas na lei. O enquadramento na hipótese legal mais adequada deverá ser analisado em cada caso.

Exemplo 1: No tratamento de dados pessoais de empregados, considerando a finalidade de realização dos serviços, a base legal será a execução do contrato de trabalho e o cumprimento de obrigação legal, na medida em que a lei impõe deveres ao empregador.

Exemplo 2: Ainda no tratamento de dados pessoais de empregados, considerando finalidades que extrapolem a relação trabalhista e a execução do contrato de trabalho, pode ser necessário o enquadramento em outra base legal, como a obtenção de consentimento.

Exemplo 3: Durante o processo seletivo para a contratação de novos empregados, quando ainda não há contrato firmado, é recomendável que se obtenha o consentimento dos candidatos para o tratamento de seus dados pessoais.

AGENTES ENVOLVIDOS NO TRATAMENTO

Estes são os principais agentes envolvidos no tratamento de dados pessoais:

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 compete decidir sobre a utilização e o tratamento de dados pessoais.

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Agentes de Tratamento: o controlador e o operador.

Autoridade Nacional de Proteção de Dados (ANPD): órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da lei em todo o território nacional.

PRINCÍPIOS A SEREM OBSERVADOS

I) **Finalidade:** realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

I) **Adequação:** compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

I) **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.

I) **Livre acesso:** garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

I) **Qualidade dos dados:** 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.

I) **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.

I) **Segurança:** 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.

I) **Prevenção:** adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

I) **Não discriminação:** impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

I) **Responsabilização e prestação de contas:** demonstração 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.

RESPONSABILIDADES, SEGURANÇA E SANÇÕES

Para estar em conformidade com a LGPD, os agentes de tratamento precisam respeitar os direitos dos titulares dos dados, tais como:

- Confirmar a existência de tratamento dos dados pessoais, quando solicitado;
- Garantir o acesso facilitado às informações sobre o tratamento, incluindo sua finalidade, forma e duração, a identificação do controlador, suas informações de contato e suas responsabilidades;
- Corrigir ou atualizar os dados do titular;
- Anonimizar ou eliminar os dados desnecessários, excessivos ou tratados em desconformidade com a lei;
- Disponibilizar a portabilidade dos dados para outras empresas;
- Informar sobre o compartilhamento dos dados com terceiros;
- Possibilitar a revogação do consentimento, com a eliminação dos dados tratados com base neste fundamento.

BOAS PRÁTICAS E GOVERNANÇA

Para melhor se adequarem à Lei Geral de Proteção de Dados Pessoais, as empresas e demais entidades podem adotar uma cultura de compliance (boas práticas de gestão), para evitar riscos que eventualmente possam trazer prejuízos financeiros e impactos negativos à sua imagem e às suas atividades.

Os controladores e operadores podem formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Enumeramos alguns exemplos de medidas de governança e boas práticas que poderão auxiliar as empresas a se adequarem à LGPD:

1) A devida compreensão da lei e como ela irá afetar as atividades da organização.

2) O comprometimento da alta gestão da empresa em destinar esforços e/ou recursos necessários ao processo de conformidade com à LGPD.

3) A nomeação de um encarregado (pessoa física ou jurídica) que será responsável pela estruturação, monitoramento e aprimoramento das boas práticas de gestão.

4) A integração das áreas da empresa, para garantir uma visão global das necessidades de se apoiarem e aprimorarem os projetos de proteção de dados.

5) Realizar a devida análise de riscos, com a apresentação de relatório de impacto à proteção de dados pessoais, apontando eventuais inconformidades que possam ocasionar prejuízos, com o devido mapeamento dos dados e das medidas que possam ser adotadas para mitigar os riscos encontrados, abrangendo cada uma das etapas do tratamento, desde a coleta, a utilização, o compartilhamento e até o descarte.

6) Fazer ajustes por meio da estruturação de regras que garantam uma política de governança, com normas internas voltadas para a proteção dos dados

pessoais, por meio de adequação dos contratos firmados, dos sistemas utilizados, dos processos e procedimentos internos e externos, da limitação dos acessos aos dados protegidos e da criação de um plano de gestão de crise (por meio de manual) para o caso de algum incidente acarretado pelo descumprimento da lei ou até mesmo vazamento de dados, criando com isso não apenas uma capacidade de gerenciamento constante, mas, principalmente, a capacidade de resposta imediata, incluindo notificações à Autoridade Nacional de Proteção de Dados, nos termos exigidos pela Lei.

7) Realização de treinamentos para os empregados, a fim de conscientizá-los sobre suas obrigações e responsabilidades no atendimento das regras e requisitos da LGPD.

8) Enquadramento dos processos nas hipóteses legais que permitem o tratamento de dados pessoais (a exemplo da obtenção de consentimento, cumprimento de obrigação legal, execução de contrato do qual o titular seja parte, entre outras), referentes aos dados já existentes na organização, bem como para os dados coletados daqui para frente.

9) Reavaliação dos dados já coletados, de forma a definir a necessidade de sua manutenção e a eventualidade de seu descarte, primando, desde logo, pela transparência nesses procedimentos.

10) Trabalhar com fornecedores que estejam adequados com a LGPD, de forma a evitar riscos indiretos com relação à utilização indevida de dados.

11) Criar Políticas de Privacidade para os serviços que realizem tratamento de dados pessoais onde fiquem claros os motivos, com finalidade legítima, pelos quais os dados estão sendo coletados e por quanto tempo permanecerão armazenados.

12) Implementar medidas técnicas e administrativas para garantir, por meio de evidências, a segurança de dados pessoais, com a utilização de normas e procedimentos de Gestão de Segurança da Informação e Processos.

ATENÇÃO!

- A coleta de dados pessoais de clientes (pessoas físicas) deve se limitar ao mínimo necessário para o cumprimento das finalidades informadas. As empresas não devem solicitar dados excessivos.
- Dados de pessoas jurídicas não são dados pessoais, mas os dados de seus representantes legais e empregados sim e, dessa forma, são protegidos pela LGPD (por exemplo, dados pessoais dos sócios, presidentes, representantes comerciais, entre outros).
- Quando o tratamento de dados tiver como base o consentimento do titular, este deve ser expresso por meio de manifestação livre, informada e inequívoca do titular das informações, concedido para uma finalidade determinada, não sendo permitidas autorizações genéricas.
- A Autoridade Nacional de Proteção de Dados (ANPD) poderá determinar que o controlador elabore um relatório de impacto à proteção de dados pessoais, documento que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos aos titulares, bem como as medidas e os mecanismos de mitigação desses riscos.

AGENTES DE TRATAMENTO DE PEQUENO PORTE

Em 27 de janeiro de 2022, foi publicado o Regulamento de aplicação da LGPD para agentes de tratamento de pequeno porte (Resolução CD/ANPD nº 2/2022).

De acordo com o mencionado Regulamento, os agentes de tratamento de pequeno porte podem ser beneficiados com um tratamento jurídico diferenciado (simplificado e favorecido), desde que observem os seguintes requisitos:

- Seja microempresa, empresa de pequeno porte, startup, pessoa jurídica de direito privado, inclusive sem fins lucrativos, nos termos da legislação vigente, pessoa física ou ente privado despersonalizado;
- Não realize tratamento de alto risco para os titulares; e

- Aufira receita bruta anual de até R$ 4.800.000,00 (quatro milhões e oitocentos mil reais), ou de até R$ 16.000.000,00 (dezesseis milhões de reais) para startups.

ATENÇÃO!

Entidades sindicais, enquanto pessoas jurídicas de direito privado sem fins lucrativos, podem receber o tratamento destinado aos agentes de pequeno porte, desde que observem os requisitos listados.

O tratamento de dados pessoais de alto risco, que impede a fruição do regime jurídico diferenciado, é aquele que atender cumulativamente a, pelo menos, um critério geral e um critério específico, dentre os a seguir indicados:

I) Critérios gerais:

- **a)** tratamento de dados pessoais em larga escala; ou
- **b)** tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais dos titulares;

II) Critérios específicos:

- **a)** uso de tecnologias emergentes ou inovadoras;
- **b)** vigilância ou controle de zonas acessíveis ao público;
- **c)** decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, inclusive aquelas destinadas a definir o perfil pessoal, profissional, de saúde, de consumo e de crédito ou os aspectos da personalidade do titular; ou
- **d)** utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos.

Entre os benefícios concedidos aos agentes de tratamento de pequeno porte, destacamos os seguintes exemplos:

- Registro das operações de tratamento de dados pessoais de forma simplificada, em modelo fornecido pela ANPD.
- Flexibilização ou procedimento simplificado para comunicação de incidentes de segurança.
- Requisitos mínimos de segurança da informação (medidas administrativas e técnicas).
- Política simplificada de segurança da informação.
- Indicação do encarregado pelo tratamento de dados pessoais é facultativa. Caso não haja a nomeação de um encarregado, o agente de tratamento de pequeno porte deverá disponibilizar um canal de comunicação com o titular.
- Prazos maiores para o atendimento de solicitações dos titulares, para a comunicação sobre incidentes de segurança, para a apresentação de informações à ANPD, para as declarações sobre a existência de dados pessoais e para o pagamento de multas.

Visando orientar os agentes de tratamento de pequeno porte em seus processos de conformidade com a LGPD, a Autoridade Nacional de Proteção de Dados disponibilizou material contendo um checklist de medidas de segurança, abrangendo itens como política de segurança da informação, conscientização e treinamento, gerenciamento de contratos, controle de acesso, segurança dos dados pessoais armazenados, segurança das comunicações, gerenciamento de vulnerabilidades, dispositivos móveis e serviços em nuvem.

O documento pode ser encontrado no sítio eletrônico oficial da ANPD ou acessado diretamente no seguinte endereço eletrônico: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/checklist-vf.pdf.

Entre as medidas de segurança para agentes de tratamento de pequeno porte listadas pela ANPD, separamos alguns exemplos:

- Estabelecer uma política de segurança da informação simplificada, que estabeleça controles relacionados ao tratamento de dados pessoais, como cópias

de segurança, uso de senhas, acesso à informação, compartilhamento de dados, atualização de softwares, uso de correio eletrônico e uso de antivírus.

- Informar os funcionários sobre como evitar de se tornarem vítimas de incidentes de segurança corriqueiros, tais como contaminação por vírus ou ataques de phishing, que podem ocorrer, por exemplo, ao clicar em links recebidos na forma de pop-up de ofertas promocionais ou em links desconhecidos que chegam por e-mail.
- Manter documentos físicos que contenham dados pessoais dentro de gavetas, e não sobre as mesas.
- Não compartilhar logins e senhas de acesso das estações de trabalho.
- Bloquear os computadores quando se afastar das estações de trabalho, para evitar o acesso indevido de terceiros.
- Estabelecer contratos com cláusulas de segurança da informação que assegurem a proteção de dados pessoais, tais como regras para fornecedores e parceiros, regras sobre compartilhamentos, sobre as relações entre controlador-operador, orientações sobre o tratamento a ser realizado com vedação a tratamentos incompatíveis com as orientações do controlador.
- Implementar um sistema de controle de acesso aplicável a todos os usuários, com níveis de permissão na proporção da necessidade de trabalhar com o sistema e de acessar dados pessoais.
- Não permitir o uso de senhas que não respeitem um certo nível de complexidade.
- Adotar e atualizar periodicamente softwares antivírus e antimalwares e realizar varreduras antivírus periódicas nos dispositivos e sistemas utilizados.

RESPONSABILIDADE DOS AGENTES DE TRATAMENTO

O controlador ou o operador que causar dano a alguém, em razão do tratamento de dados pessoais contrário à legislação, pode ser obrigado a repará-lo.

O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança esperada. Dessa forma, o contro-

lador ou o operador respondem pelos danos decorrentes da violação da segurança dos dados, se deixarem de adotar as medidas de segurança necessárias.

O operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador.

O controlador, por sua vez, que estiver diretamente envolvido no tratamento de dados e que, porventura, causar danos ao titular, responde solidariamente.

A obrigação de reparar ou compensar eventuais danos (responsabilidade civil) será apurada mediante processo judicial. A tramitação dos processos judiciais nos Tribunais é independente e não se confunde com a aplicação das sanções administrativas por parte da Autoridade Nacional de Proteção de Dados (ANPD).

SANÇÕES ADMINISTRATIVAS

A Autoridade Nacional de Proteção de Dados (ANPD) foi transformada em uma autarquia de natureza especial, integrante da administração pública, responsável por zelar pela proteção de dados pessoais. Dentre suas inúmeras atribuições, está a de fiscalizar e aplicar sanções em caso de descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso.

A Autoridade Nacional verificará a gravidade de cada incidente e poderá determinar aos agentes de tratamento (controlador e operador) as providências necessárias para eliminar irregularidades, incertezas jurídicas ou situações contenciosas no âmbito de processos administrativos.

Os agentes de tratamento de dados ficam sujeitos às seguintes sanções:

- Advertência, com indicação de prazo para adoção de medidas corretivas.
- Multa de até 2% (dois por cento) do faturamento da empresa, limitada ao total de R$ 50.000.000,00 (cinquenta milhões de reais) por infração.
- Multa diária, observado o valor total acima.
- Publicização da infração após apuração e confirmação da ocorrência.

- Bloqueio dos dados pessoais a que se refere a infração.
- Eliminação dos dados pessoais a que se refere a infração.
- Suspensão parcial do funcionamento do banco de dados a que se refere a infração.
- Suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração.
- Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

E a aplicação das sanções segue os seguintes critérios:

- A gravidade da infração.
- A boa-fé do infrator.
- As vantagens auferidas ou pretendidas pelo infrator.
- A condição econômica do infrator.
- Eventual reincidência.
- O grau do dano.
- A cooperação do infrator.
- A adoção reiterada e demonstrada de mecanismos e procedimentos capazes de minimizar o dano, voltados ao tratamento seguro e adequado dos dados.
- A adoção de política de boas práticas e governança.
- A pronta adoção de medidas corretivas.
- A proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Em 24 de fevereiro de 2023, foi publicado o Regulamento de Dosimetria e Aplicação de Sanções Administrativas (Resolução CD/ANPD nº 4/2023), com o ob-

jetivo de estabelecer parâmetros para a aplicação das sanções, bem como as formas e dosimetrias para o cálculo do valor-base das multas.

A edição do referido Regulamento possibilitou o início da fase sancionadora da ANPD, com a aplicação das sanções administrativas.

O não cumprimento de uma sanção ou a ausência de regularização da conduta, no prazo estipulado, pode ensejar a progressão da atuação da Autoridade Nacional para a aplicação de sanções mais graves.

CONCLUSÃO

O objetivo da cartilha é trazer algumas sugestões e orientações, contribuindo para que as empresas e as entidades integrantes do Sistema Comércio estejam em conformidade com a LGPD, conferindo-se destaque para os seguintes pontos:

- Conheça todos os dados pessoais que estejam sob sua custódia;
- Certifique-se de que possui permissão legal para tratar esses dados, enquadrando-os um uma das hipóteses de tratamento possíveis;
- Gerencie e trate de forma adequada os dados, observando os princípios previstos na lei; e
- Proteja os titulares dos dados, respeitando seus direitos e aplicando as medidas de segurança necessárias.

Quanto mais cedo as organizações implementarem seus processos internos de governança e boas práticas de gestão, menores serão os riscos referentes à violação da lei e à possibilidade de causar danos aos titulares e de sofrer sanções administrativas.

Para dúvidas e esclarecimentos, contate a Encarregada pelo Tratamento de Dados Pessoais da CNC, pelo e-mail encarregadolgpd@cnc.org.br.

Esta cartilha tem caráter orientativo, não substituindo os termos previstos na Lei nº 13.709/2018 e demais legislação aplicável.