Guia prático para agentes de tratamento

UM OLHAR SOBRE AS PRINCIPAIS DISPOSIÇÕES DA LEI GERAL DE PROTEÇÃO DE DADOS E AS RECENTES ATIVIDADES REGULATÓRIAS DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

MATTOS FILHO

Panorama geral de proteção de dados no Brasil

A **Lei Geral de Proteção de Dados** (Lei Federal nº 13.709/2018 – LGPD) é a principal lei que regula o tratamento de dados pessoais e de dados pessoais sensíveis por pessoas físicas e jurídicas no Brasil.

A LGPD estabelece regras detalhadas para a coleta, o uso, o tratamento e o armazenamento de dados pessoais. Seus efeitos se estendem por toda a economia, incluindo as relações entre clientes e fornecedores de produtos e serviços, empregados e empregadores, relações comerciais transnacionais e domésticas, bem como outras situações em que dados pessoais são coletados em ambientes físicos e digitais.

Quando a LGPD é aplicável?

A LGPD aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

- A operação de **tratamento seja realizada no território nacional**;
- A atividade de tratamento tenha por objetivo a **oferta ou o fornecimento de bens ou serviços** ou o tratamento de dados de indivíduos localizados no território nacional; ou
- Os **dados pessoais objeto do tratamento tenham sido coletados no território nacional** (enquanto o titular dos dados estava no Brasil no momento da coleta).

A **Autoridade Nacional de Proteção de Dados** (ANPD) é responsável por assegurar o cumprimento da LGPD e garantir a proteção de dados pessoais no Brasil.

Definições-chave da LGPD

Dados pessoais: informações relacionadas à pessoa natural identificada ou identificável.

Dados pessoais sensíveis: dado pessoal 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.

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

Controlador: pessoa física ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

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

Agentes de tratamento: os controladores e operadores, quando referidos em conjunto e indistintamente.

Titular dos dados: pessoa física a quem se referem os dados pessoais que são objeto de tratamento.

Agentes de tratamento

O Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado publicado pela ANPD estabelece a **responsabilidade dos controladores pela definição dos elementos centrais e das características do tratamento de dados** (como a finalidade do tratamento, as categorias de dados a serem tratadas e a duração do tratamento).

A Resolução CD/ANPD nº 2/2022 regulamenta como a LGPD se aplica a agentes de tratamento de pequeno porte, os quais incluem microempresas, empresas de pequeno porte e startups. Os agentes de pequeno porte estão isentos de cumprir determinadas obrigações estabelecidas pela LGPD, conforme detalhado abaixo.

Principais obrigações estabelecidas pela LGPD

De forma geral, os agentes de tratamento devem:

Manter o **registro das suas atividades de tratamento de dados** (RoPA). A ANPD estabeleceu regras simplificadas para agentes de tratamento de pequeno porte em relação à elaboração de RoPA, conforme a **Resolução CD/ANPD nº 2/2022**.

Observar os princípios norteadores das atividades de tratamento de dados (tais como princípio da necessidade, princípio da adequação, princípio da transparência, princípio do livre acesso, princípio da não discriminação etc.).

Assegurar e fazer cumprir com os direitos dos titulares (por exemplo, direito de acesso aos dados, direito de correção de dados incompletos, inexatos ou desatualizados, direito de eliminação, direito de revogar o seu consentimento, direito de portabilidade de dados etc.).

Justificar as **atividades de tratamento de dados pessoais que realizam em uma base legal estabelecida pela LGPD** (tais como, o consentimento do titular dos dados, o cumprimento de obrigações legais e regulatórias, a execução de contrato, o legítimo interesse, entre outros).

O Guia do Legítimo Interesse publicado pela ANPD fornece orientações práticas sobre a interpretação e a aplicação da base legal do legítimo interesse, incluindo o estabelecimento de determinados conceitos e de parâmetros para a elaboração do Avaliação de Interesse Legítimo (LIA) e do Teste de Balanceamento.

Adotar medidas de proteção de dados desde a concepção e desenvolvimento de quaisquer tecnologias, produtos ou serviços (*privacy by design*).

Nomear uma pessoa para atuar como canal de comunicação entre o agente de tratamento, os titulares dos dados e a ANPD (Encarregado). No entanto, esta obrigação é facultativa para agentes de tratamento de pequeno porte.

A Resolução CD/ANPD nº 18/2024 estabelece as funções e obrigações dos Encarregados, a responsabilidade dos agentes de tratamento em caso de não conformidade com a LGPD, bem como situações que podem gerar conflitos de interesse. A ANPD também publicou um guia não vinculativo com boas práticas a serem implementadas por agentes de tratamento em relação aos deveres e obrigações do Encarregado, incluindo modelos de documentos para a nomeação formal do Encarregado.

Incidentes de segurança envolvendo dados pessoais

A LGPD exige que os agentes de tratamento devem adotar medidas de segurança para proteger os dados pessoais de qualquer evento adverso, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais (incidentes de segurança). Se um determinado incidente de segurança expuser os titulares dos dados afetados a risco ou dano material, o controlador deve notificar tanto a ANPD quanto os titulares dos dados afetados.

A Resolução CD/ANPD nº 15/2024 estabelece regras para a comunicação de incidentes de segurança, conforme abaixo:

- **Comunicação à ANPD:** em regra, em até três dias úteis após tomar conhecimento do incidente de segurança.
- **Notificação complementar:** informações adicionais sobre o incidente de segurança podem ser fornecidas de forma fundamentada à ANPD em até 20 dias úteis a partir da data da primeira notificação.
- **Comunicação aos titulares de dados afetados:** em até três dias úteis após tomar conhecimento do incidente de segurança.

Em regra, os controladores de dados devem manter o registro de incidentes de segurança por, no mínimo, cinco anos, sendo que tais registros devem conter informações sobre eventos não comunicados à ANPD e/ou aos titulares dos dados afetados.

Transferências internacionais de dados

De acordo com a LGPD, as transferências internacionais de dados pessoais somente são permitidas nos seguintes casos:

- Para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto na LGPD;
- Quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de cláusulas-padrão contratuais, normas corporativas globais, selos, certificados ou códigos de conduta; ou
- Quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, entre outras circunstâncias.

A ANPD aprovou o Regulamento de Transferência Internacional de Dados, o qual se aplica às transferências de dados pessoais entre agentes de tratamento, do Brasil para outros países ou organismos internacionais. O Regulamento estabelece regras para transferências para países ou organismos internacionais com proteção adequada (conforme reconhecido pela ANPD) ou quando as entidades adotarem cláusulas contratuais ou normas corporativas globais para cumprir os requisitos de transferência elencados na LGPD. Atualmente, a ANPD reconhece a adequação do nível de proteção de dados da União Europeia, entendendo que o Regulamento de Proteção de Dados Europeu assegura um nível equivalente de proteção ao previsto na LGPD.

Enquanto isso, os agentes de tratamento devem confiar em mecanismos alternativos para justificar as transferências internacionais, tais como:

- **Cláusulas-padrão contratuais aprovadas pela ANPD:** essas cláusulas devem ser adotadas integralmente, sem alterações e incorporadas aos contratos. O prazo fixado pela ANPD para implementação das cláusulas pelos agentes de tratamento que optassem por esse mecanismo expirou em agosto de 2025.
- **Cláusulas-padrão contratuais equivalentes:** a ANPD pode reconhecer cláusulas-padrão contratuais de outros países como equivalentes;
- **Cláusulas contratuais específicas:** os agentes de tratamento podem solicitar à ANPD a aprovação de cláusulas personalizadas para transferências quando as cláusulas-padrão não forem viáveis; ou
- **Normas corporativas globais:** os agentes de tratamento podem normas corporativas globais para respaldar as transferências, que são mecanismos vinculativos para transferências internacionais de dados entre entidades do mesmo grupo ou conglomerado econômico.

A ANPD também lançou uma página específica em português e inglês em que os agentes de tratamento podem encontrar orientações detalhadas sobre o assunto, incluindo instruções sobre como enviar solicitações para a análise de mecanismos de transferência internacional de dados.

Responsabilidade da LGPD

Os agentes de tratamento são responsáveis por **danos materiais e morais** que causarem em decorrência de violações à LGPD, conforme abaixo:

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

Os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente.

A LGPD estabelece determinadas **isenções de responsabilidade**.
Os agentes de tratamento não serão responsabilizados quando:

- Provarem que não realizaram o tratamento de dados pessoais que lhes é atribuído;
- Provarem que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à LGPD; ou
- Provarem que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Os titulares dos dados podem defender seus interesses e direitos por meio de processos administrativos ou judiciais, seja individual ou coletivamente. Os titulares também podem propor ações judiciais nos tribunais brasileiros requerendo indenização por danos materiais ou morais decorrentes de violações de seus direitos de privacidade, ou protocolar uma reclamação administrativa junto às autoridades de defesa do consumidor (como os PROCONs) ou à ANPD.

Penalidades impostas pela LGPD

Caso os agentes de tratamento não cumpram a LGPD, eles poderão estar sujeitos à imposição de penalidades administrativas, incluindo:

- Advertência;
- 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;
- Publicização da infração;
- Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
- Eliminação dos dados pessoais a que se refere a infração;
- Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

A Resolução CD/ANPD nº 4/2023, que regulamenta o cálculo e a aplicação de sanções administrativas, define os critérios e parâmetros que a ANPD deve aplicar às sanções pecuniárias e não pecuniárias, bem como as formas e dosimetrias para o cálculo do valor-base das multas.

MATTOS FILHO

SÃO PAULO RIO DE JANEIRO BRASÍLIA NOVA IORQUE

mattosfilho.com.br