GUIA PARA A LEI GERAL DE PROTEÇÃO DE DADOS

Thera Compliance

www.theracompliance.com

APENAS UMA NOTA

A LGPD impõe uma profunda transformação no sistema de proteção de dados brasileiro, referindo especificadamente na adoção de medidas de segurança e de boas práticas de tratamento de dados alinhada com a regulação europeia de proteção de dados (GDPR).

É uma lei que estabelece regras detalhadas para a coleta, uso, tratamento e armazenamento de dados pessoais e afetará todos os setores da economia, inclusive as relações entre clientes e fornecedores de produtos e serviços, empregado e empregador, relações comerciais nacionais e internacionais, além de outras relações nas quais dados pessoais sejam coletados, tanto no ambiente digital quanto fora dele.

Os principais pontos tratados pela LGPD são abordados neste guia de modo objetivo e direto para que o leitor possa ter uma ideia clara sobre os impactos no âmbito empresarial e quais providências deverá tomar para que as medidas necessárias para adequação e compliance sejam adotadas de modo planejado e seguro.

Esperamos que as páginas a seguir sirvam como um "guia de navegação" para essa nova realidade. Lembre- se de que nosso escritório está à sua disposição para que você possa enfrentar, com tranquilidade, esse desafio.

Boa leitura!

Thera Compliance

*ESTE GUIA NÃO PODE SER USADO COMO OPINIO LEGAL E NÃO TEM O OBJETIVO DE ORIENTAR QUALQUER PESSOA PARA FINS LEGAIS.

índice

Thera Compliance

Thera Compliance

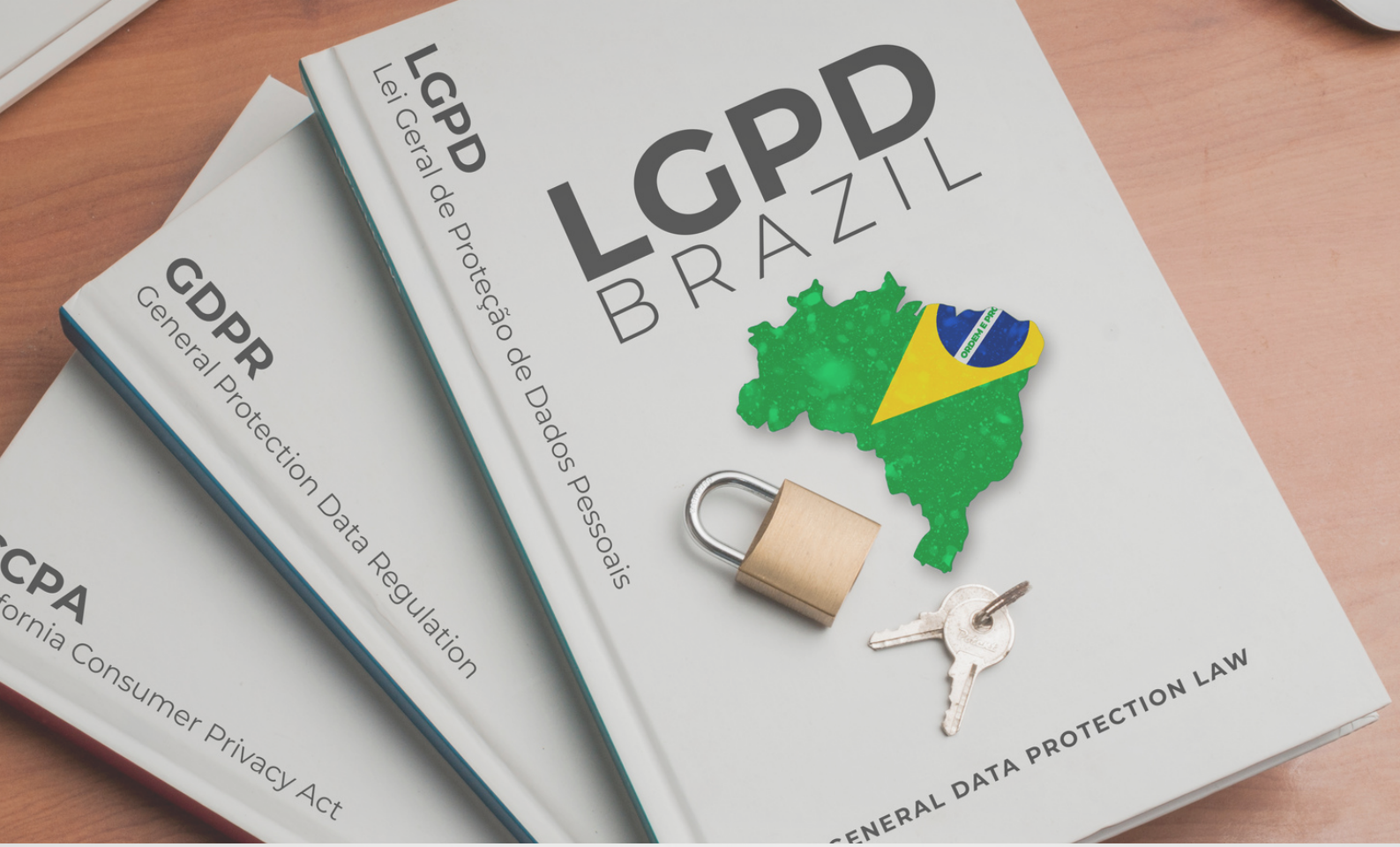
SOBRE NÓS

A Thera Compliance foi fundada por três sócios que atuam profissionalmente como advogados e analistas de TI que também são especialistas em Compliance, Proteção de Dados e DPO (Data Protection Officer).

Temos experiencia internacional na adequação da GDPR (General Data Protection Regulation), lei da União Europeia da qual o Brasil se inspirou para a criação da LGPD (Lei Geral de Proteção de Dados).

Nosso objetivo é proporcionar a proteção dos dados da sua empresa e dos seus clientes, através de treinamentos, cursos, mentorias e materiais didáticos on-line, para a adequação de seus processos de trabalho, no que se refere à proteção de dados pessoais.

Com expertise legal e tecnológica, nos empenhamos em mitigar problemas futuros de sua empresa com a LGPD, aumentando a segurança nas duas pontas de serviço, usuário e fornecedor.



O QUE É LGPD (LEI 13.709/18)?

É uma nova legislação que entrou em vigor em 18 de setembro de 2020 e que trata da proteção dos dados pessoais dos cidadãos brasileiros. Regula o tratamento de dados pessoais, tanto nos meios físicos (analógico) quanto digitais, criando regras sobre os processos de coleta, armazenamento e compartilhamento, findando no descarte dos dados tratados.

Tem como ente fiscalizador e sancionador a ANPD (Autoridade Nacional de Proteção dos Dados), órgão responsável por regulamentar os critérios da LGPD.

DEFINIÇÕES IMPORTANTES

DADO PESSOAL

Qualquer informação relativa à pessoa natural, singular, identificada ou identificável (titular)

DADO PESSOAL SENSÍVEL

Dados 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; dados sobre crianças e adolescentes

TRATAMENTO

Toda e qualquer operação ou conjunto de operações realizadas em dados pessoais ou em conjuntos de dados pessoais, seja ou não por meios automatizados, como 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 natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, por isso é a pessoa à qual a LGPD impõe maior peso jurídico

ENCARREGADO DE DADOS (DPO)

Pessoa indicada pelo controlador e/ou operador como canal de comunicação com os titulare dos dados, a empresa e a ANPD

OPERADOR

Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Sua atuação deve limitar- se as determinações do controlador ou de previsão legal

Thera Compliance

ABRANGÊNCIA

EM QUAIS AS SITUAÇÕES A LGPD É APLICÁVEL?

- Regula o tratamento de dados relacionado às pessoas naturais apenas.
- Aplica-se independentemente do meio e/ou forma de tratamento dos dados; ou seja, impõe regras ao tratamento de dados realizado dentro ou fora da internet, utilizando ou não meios digitais.
- Aplica-se a operações de tratamento que ocorram no território brasileiro, mas também a operações de tratamento que ocorram fora do país, quando:
    - 👉 os dados pessoais forem coletados no Brasil
    - 👉 os dados sejam relacionados a indivíduos localizados no território brasileiro
    - 👉 tiver por objetivo a oferta de produtos e/ou serviços ao público brasileiro
- Não revoga ou impede a aplicação de normas setoriais que também regulamentem dados pessoais

APLICAÇÃO TERRITORIAL E EXTRATERRITORIAL

A LGPD aplica-se a qualquer operação de tratamento realizada no território nacional, ou mesmo fora dele, independentemente de onde os agentes de tratamento estejam sediados ou de onde os dados estejam localizados, desde que:

- A atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços no território brasileiro;
- A atividade de tratamento tenha por objetivo o tratamento de dados de indivíduos localizados no território brasileiro;
- Os dados pessoais objeto do tratamento tenham sido coletados no território brasileiro.

NÃO APLICAÇÃO DA LGPD

A LGPD não se aplica ao tratamento de dados pessoais:

Realizado por pessoa natural para fins exclusivamente particulares e não econômicos

Realizado para fins exclusivamente jornalísticos, artísticos e/ou acadêmicos

Realizado para fins exclusivos de segurança pública, de defesa nacional e/ou de segurança do Estado

Em atividades de investigação e repressão de infrações penais

Provenientes e destinados a outros países, que apenas transitem pelo território nacional, sem que aqui seja realizada qualquer operação de tratamento.

NORMAS SETORIAIS

A LGPD não revoga ou impede a aplicação de normas setoriais que também regulamentam dados pessoais, que devem continuar a ser observadas.

PRINCÍPIOS DA LGPD

É importante que os agentes de tratamento adotem medidas efetivas (e que sejam demonstráveis) para que as operações de tratamento estejam de acordo com os princípios previstos pela LGPD.

1. Boa fé
2. Finalidade
3. Adequação
4. Necessidade
5. Livre Acesso
6. Qualidade dos dados
7. Transparência
8. Segurança
9. Prevenção
10. Não discriminação
11. Responsabilidade e prestação de contas

QUAIS PROVIDÊNCIAS VOCÊ DEVE TOMAR

- Revisar e adequar as políticas (internas e em relação a terceiros), contratos, procedimentos e demais atividades que envolvam tratamento de dados pessoais (tanto de clientes quanto de empregados) aos princípios estabelecidos na LGPD.

- Manter registros, preferencialmente por escrito, que demonstrem a adoção de medidas para adequação das operações de tratamento aos princípios estabelecidos na LGPD, independentemente do tamanho da base de dados existente.

BASE LEGAL

EM QUE SITUAÇÕES O TRATAMENTO DE DADOS PESSOAIS É CONSIDERADO LEGAL?

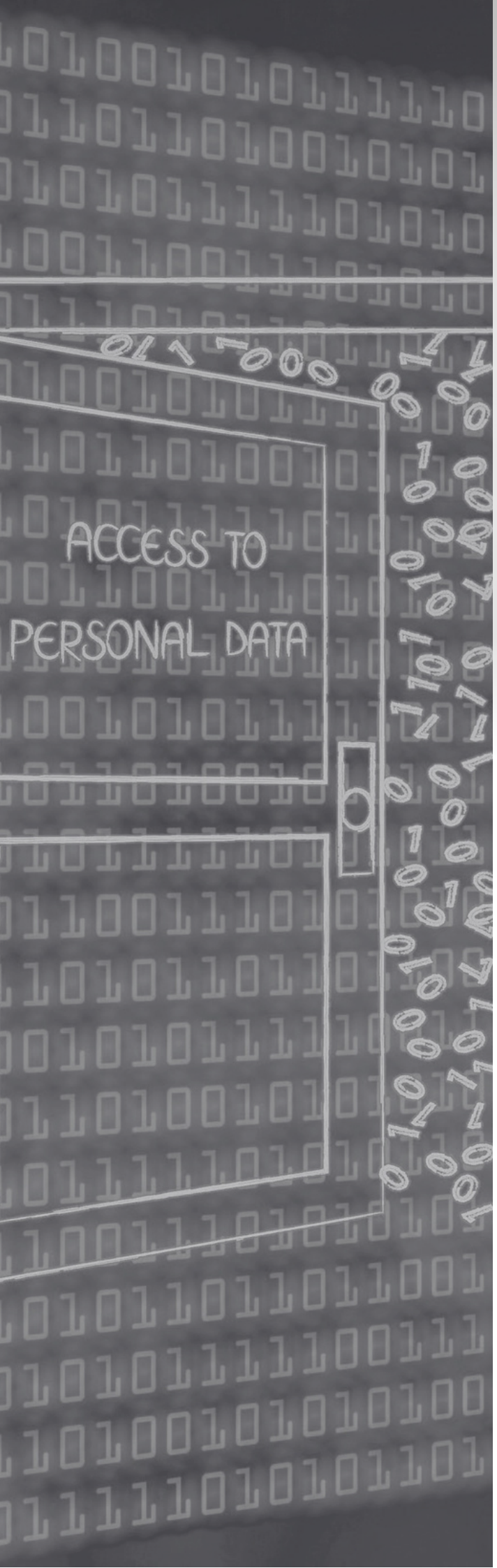
- Enquanto o Marco Civil da Internet apenas permite o tratamento de dados pessoais mediante a obtenção de consentimento do titular dos dados, a LGPD estabelece dez hipóteses para o tratamento de dados, incluindo, além do consentimento, o interesse legítimo do controlador ou de terceiro, a necessidade de cumprimento de contrato e/ou de obrigação legal ou regulatória.

- Exceto a hipótese de consentimento, as hipóteses para o tratamento de dados pessoais sensíveis são mais restritas e não permitem o tratamento com base no legítimo interesse e na proteção do crédito, por exemplo.

- A LGPD estabelece regras específicas para a obtenção do consentimento, que poderá ser nulo caso se trate de uma autorização genérica ou se baseado em informações com conteúdo enganoso ou abusivo.

- Existem regras específicas para o tratamento de dados pessoais de crianças e adolescentes.

- O tratamento de dados pessoais considerados como "públicos" deve considerar a finalidade originária, a boa-fé e o interesse público que justifiquem a disponibilização de tais dados.



HIPÓTESES QUE JUSTIFICAM O TRATAMENTO DE DADOS PESSOAIS

- Mediante o consentimento do titular dos dados pessoais
- Para o cumprimento de obrigação legal ou regulatória pelo controlador dos dados
- Na administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos
- Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, o anonimato dos dados pessoais
- Quando necessário para a execução de contrato ou de procedimentos contratuais preliminares
- Para a proteção da vida ou da incolumidade física do titular ou de terceiro
- Para o exercício regular de direito em processo judicial, administrativo ou arbitral
- Para atendimento de 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
- Para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias
- Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

QUAIS PROVIDÊNCIAS VOCÊ DEVE TOMAR

- Avaliar cuidadosamente qual base legal para tratamento de dados pode ser utilizada no caso concreto.

- Quando o tratamento de dados pessoais for baseado no consentimento, o controlador deve manter documentação comprobatória da sua obtenção em conformidade com a legislação.

- Quando o tratamento de dados pessoais for baseado no legítimo interesse , o controlador deve adotar medidas para garantir a transparência de tal tratamento, que poderá sempre ser revisto pela autoridade nacional de proteção de dados à luz do caso concreto.

- Manter registro e fundamentação das operações de tratamento de dados pessoais, especialmente quando baseado no legítimo interesse.

Como você deve cumprir com os direitos dos titulares dos dados

- Adequar a estrutura operacional e técnica da sua organização para viabilizar e cumprir com todos os direitos que a lei garante ao titular dos dados

- Desenvolver mecanismos para permitir que os titulares de dados exerçam seus direitos, de forma facilitada e gratuita

- Verificar se o conteúdo informativo disponibilizado ao titular dos dados está com uma linguagem clara e adequada.

OBRIGAÇÕES DO CONTROLADOR

- Provar que o consentimento foi obtido em conformidade com a LGPD
- Manter registro das operações de tratamento de dados pessoais que realize
- Mediante solicitação da ANPD, elaborar relatório de impacto à proteção de dados
- Informar o titular caso haja alguma alteração na finalidade ou transferência dos dados coletados para terceiros
- Responder solidariamente, em conjunto com o operador, se causar a terceiros danos por violação à LGPD.

Quais medidas você deve adotar como controlador

- Adotar medidas técnicas que garantam o tratamento de dados de forma segura
- Desenvolver processos internos e criar políticas que permitam realizar a criação e manutenção de registros das operações de tratamento de dados pessoais
- Conservar os dados visando atender a finalidade pela qual foram coletados e para cumprir com obrigações legais e regulatórias
- Nomear o encarregado pelo tratamento dos dados pessoais

MUDANÇAS CONTRATUAIS

CONSTROLADOR - PROCESSADOR

- Os contratos do Controlador-Processador devem incluir informações específicas sobre o processamento de dados pessoais
- Novos termos também devem ser incluídos
- Todos os contratos existentes precisarão ser alterados
- Aplica-se estas regras a todos contratos com fornecedores e com clientes
- Essas alterações são obrigatórias.

TRANSFERÊNCIA INTERNACIONAL DE DADOS

E se os dados forem tratados fora do Brasil?

- É permitida a transferência internacional de dados, desde que as condições previstas na LGPD sejam atendidas. Em linhas gerais, a LGPD somente permite a transferência internacional se os mesmos padrões previstos na lei para a proteção ao titular de dados forem mantidos nos países que receberão os dados pessoais.

- Para receber os dados, o país ou organismo internacional deve oferecer um grau adequado de proteção de dados, o que será avaliado pela ANPD.

Como você deve proceder ao efetuar uma transferência internacional de dados

- Adotar cautela no envio de dados à organizações no exterior e ter a segurança de que elas cumpram com os requisitos estabelecidos na LGPD.

- Adotar procedimentos e elaborar documentos, incluindo contratos e regras corporativas vinculantes, que documentem a adequação do tratamento dos dados segundo a LGPD.

- Informar a ANPD caso haja alteração nas garantias que tenham sido entendidas como suficientes para a realização de transferência internacional de dados.

- Mapeamento e diagnóstico dos dados pessoais
- Estabelecer regras e procedimentos de governança e boas práticas
- Conscientização dos empregados e colaboradores
- Revisão periódica de processos e documentos.

Thera Compliance

AVALIAÇÕES DE IMPACTO DA PROTEÇÃO DE DADOS

Procedimento "chave" exigido pela LGPD, no qual deve indicar como os dados pessoais devem ser tratados.

Pontos necessários para avaliação do impacto da proteção de dados:

- base jurídica do tratamento
- necessidade e proporcionalidade
- riscos para os direitos e liberdades dos titulares dos dados
- controles para tratar riscos existentes
- consulta com os titulares dos dados

Como você deve avaliar o impacto que o seu tratamento de dados traz à proteção dos dados

Organizações que realizam o tratamento de dados pessoais no território brasileiro ou oferecem produtos ou serviços a indivíduos localizados no Brasil devem buscar entender o impacto da LGPD em suas atividades e como se adequar às suas regras. A contratação de consultoria técnica e jurídica especializada para realizar o diagnóstico é uma medida aconselhável.

Ademais, as organizações devem verificar se, além da LGPD, há outras normas setoriais de proteção de dados aplicáveis à sua atividade.

SEGURANÇA E NOTIFICAÇÕES

E SE OCORRER ALGUM INCIDENTE QUE RESULTE EM VAZAMENTO DE DADOS?

Deverão ser adotadas medidas de segurança com a finalidade de garantir a proteção dos dados pessoais contra acessos não autorizados e situações acidentais ou até mesmo ilícitas. O primeiro passo é identificar a natureza dos dados, objeto do incidente. Se forem dados criptografados ou anonimizados, por exemplo, os riscos serão menores.

Casos de incidente de segurança deverão ser comunicados, em até 2 dias úteis, à Autoridade Nacional de Proteção de Dados e ao titular dos dados.

Dependendo da gravidade do incidente, a ANPD poderá determinar a adoção de determinadas providências e eventual comunicação a outros órgãos reguladores, como CVM e BACEN.

O controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas causar algum dano ao titular, responderá pelos danos decorrentes da violação da segurança dos dados. A responsabilidade será subjetiva e solidária.

Como você deve agir em caso de algum incidente de segurança

- Desenvolver sistemas de identificação e combate de incidentes de segurança, bem como treinar uma equipe de TI para garantir a execução destes procedimentos.

- Revisar os acordos de seguros para garantir cobertura em caso de incidentes de segurança.

- Criar políticas e procedimentos internos, bem como parcerias com prestadores de serviços técnicos e de assessoria jurídica, para que a resposta a ser dada a incidentes seja feita de modo a atender os requisitos previstos na LGPD.

SANÇÕES

Além da responsabilidade de indenizar o titular dos dados, a LGPD prevê sanções de caráter administrativo na hipótese de seu descumprimento, como:

- publicação da infração após devidamente apurada e confirmada a sua ocorrência
- bloqueio dos dados pessoais correspondentes à infração até a sua regularização
- eliminação dos dados pessoais correspondentes à infração.

As sanções administrativas aplicáveis pela Autoridade Nacional, em razão das infrações às normas da LGPD, vão desde advertência, suspensão parcial do banco de dados ou da atividade de tratamento, até a imposição de sanções de natureza pecuniária, que podem chegar a 2% do faturamento do grupo no Brasil, limitada a R$ 50 milhões por infração e proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

As sanções podem ser aplicadas cumulativamente, por dia e infração, mas sempre com base na gravidade e extensão da violação.

Todas as sanções serão encabeçadas por um procedimento administrativo que garanta a ampla defesa do infrator. As sanções serão aplicadas considerando as particularidades de cada caso e aos seguintes parâmetros e critérios:

- gravidade e natureza das infrações e dos direitos pessoais afetados
- boa-fé do infrator
- vantagem auferida ou pretendida pelo infrator
- condição econômica do infrator
- reincidência
- grau do dano
- cooperação do infrator
- adoção de política de boas práticas e governança
- pronta adoção de medidas corretivas
- proporcionalidade entre a gravidade da falta e a intensidade da sanção
- adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano.

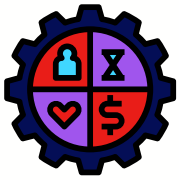
No cálculo do valor da multa, a ANPD poderá considerar o faturamento total da empresa ou do grupo de empresas.

Na aplicação da sanção de multa diária, a ANPD deverá fundamentar a aplicação da sanção observando a gravidade da falta e a extensão do dano ou prejuízo causado. Em casos de incidentes de vazamento internacionais, as multas aplicadas em uma jurisdição não serão compensadas ou abatidas com as aplicadas em outra na qual também foram verificados os efeitos do evento.

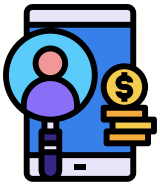
CONCLUSÃO

A coleta e uso de dados pessoais precisam ser devidamente analisadas para se adequar à LGPD.

Políticas, mudanças contratuais, processuais e técnicas podem ser imprescindíveis.



Serão necessários recursos para cumprir as determinações exigidas.



As multas são penosas, caso não haja a devida proteção aos dados pessoais.

A ANPD deverá observar os mecanismos e procedimentos internos adotados preventivamente pela empresa, e a implementação de boas práticas de governança.

CONTATO


+55 (11) 96919-2375


contato@theracompliance.com


/company/theracompliance


@theracompliance


@theracompliance

www.theracompliance.com

Thera Compliance

A LGPD não vai se adequar à sua empresa,
mas nós cuidamos disso pra você.