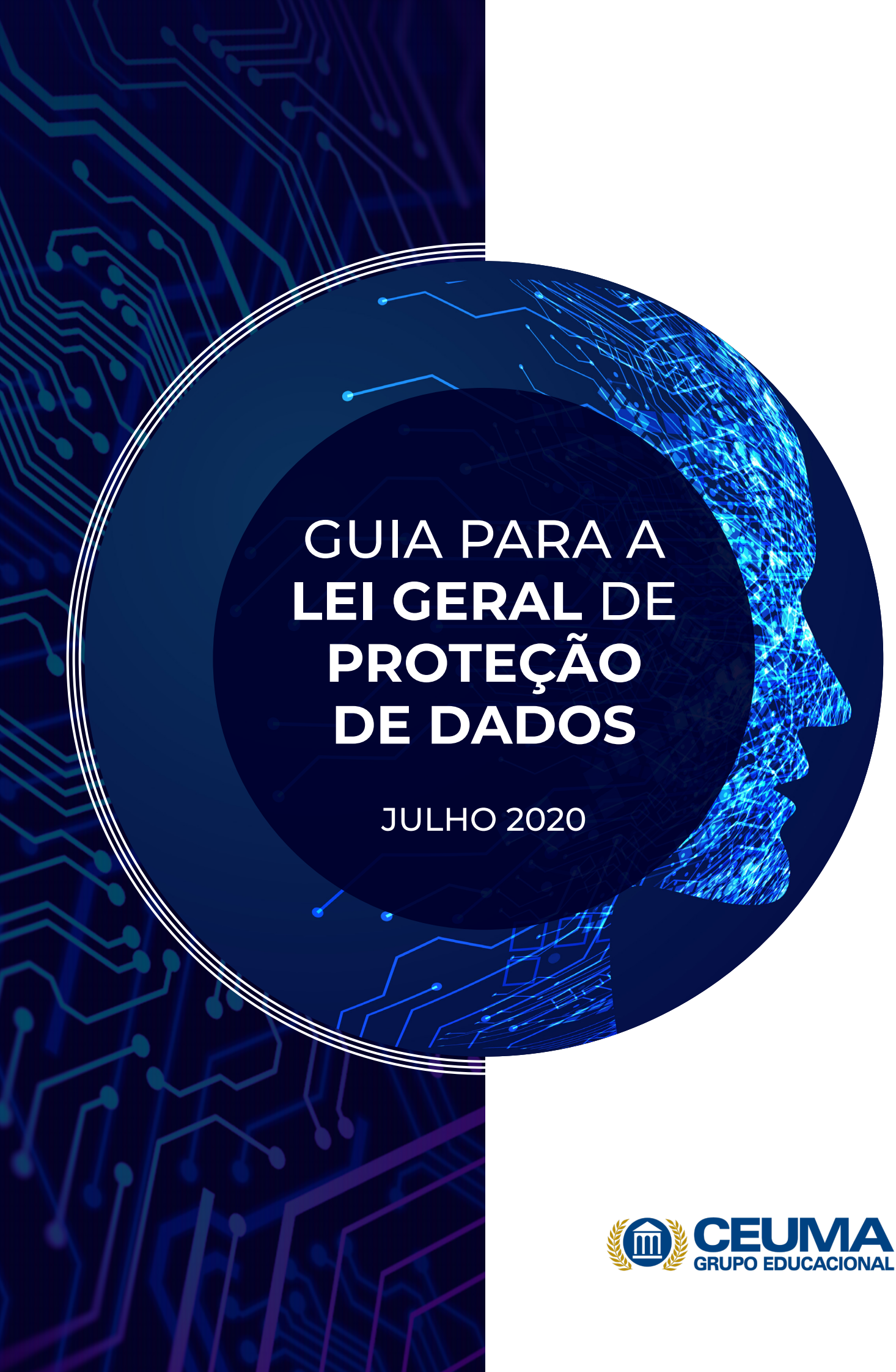


GUIA PARA A **LEI GERAL** DE **PROTEÇÃO DE DADOS**

JULHO 2020

CEUMA
GRUPO EDUCACIONAL

GUIA PARA A LEI GERAL DE PROTEÇÃO DE DADOS

A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LEI 13.709/18 OU "LGPD") REGULAMENTA A FORMA PELA QUAL AS ORGANIZAÇÕES PASSARÃO A UTILIZAR, NO BRASIL, DADOS PESSOAIS ENQUANTO INFORMAÇÃO RELACIONADA À PESSOA NATURAL IDENTIFICADA OU IDENTIFICÁVEL.

A LGPD impõe uma profunda transformação no sistema de proteção de dados brasileiro, em boa medida 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 transnacionais e nacionais, 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, durante o prazo de 18 (dezoito) meses previstos para que a LGPD entre em vigor, as medidas necessárias para adequação e compliance sejam adotadas de modo planejado e seguro.

ÍNDICE

04 - Definições Importantes

05 - Abrangência

07 - Princípios

09 - Base legal

13 - Direitos do titular

17 - Obrigações ao controlador

20 - Transferência internacional

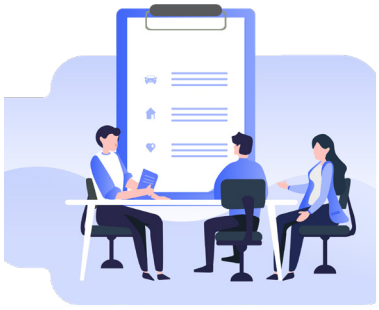
22 - Segurança e notificações

24 - Sanções

DEFINIÇÕES IMPORTANTES

Dado pessoal

É a informação relacionada a uma pessoa natural identificada ou identificável, ou seja, qualquer informação que identifique ou possa identificar uma pessoa, tais como nomes, números, códigos de identificação, endereços.



Dado pessoal sensível

É o dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião pública, 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.

Agentes de tratamen

São o controlador e o operador.

Tratamento

É toda a operação realizada com o dado pessoal. Por exemplo: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle da informação, comunicação, transferência, difusão ou extração.

Operador

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

Controlador

É a pessoa que tem competência para tomar decisões referentes ao tratamento de dados pessoais. Essa pessoa pode ser natural ou jurídica, de direito público ou privado.

ABRANGÊNCIA

Em quais as situações a LGPD é aplicável?

O QUE VOCÊ PRECISA SABER

- Regula o tratamento de dados relacionados a pessoas físicas 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 ocorrem no território brasileiro, mas também a operações de tratamento que ocorrem 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 regulamentam dados pessoais.

- Entrará em vigor em fevereiro de 2020, mas ainda será objeto de regulamentação por meio de decreto em relação a alguns temas.

- Teve vetados os dispositivos que criavam a Autoridade Nacional de Proteção de Dados, o que deverá ser feito posteriormente pelo Poder Executivo (via medida provisória ou projeto de lei).

SAIBA MAIS

A LGPD regulamenta o tratamento de informações relacionadas a pessoas físicas apenas, de modo que não se aplica aos dados de pessoas falecidas e de pessoas jurídicas. Organizações do setor público e privado estão sujeitas à lei. Além disso, a LGPD regulamenta o tratamento de dados pessoais realizado por qualquer meio, dentro ou fora da internet, utilizando ou não meios digitais.

ONDE POSSO ENCONTRAR ESTE TEMA NA LGPD? Artigos 1º, 3º e 4º

QUE PROVIDÊNCIAS VOCÊ DEVE TOMAR?

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.

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

ABRANGÊNCIA

Em quais as situações a LGPD é aplicável?

Aplicação territorial e extraterritorial:

A LGPD aplica-se a qualquer operação de tratamento realizada no território nacional, ou mesmo fora do território nacional, independentemente de onde os agentes de tratamento estão sediados ou os dados estão 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, acadêmicos;

• Realizado para fins exclusivos de segurança pública, de defesa nacional, 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.

Vigência:

A LGPD entrará em vigor em fevereiro de 2020, mas ainda será objeto de regulamentação em relação a alguns temas.

PRINCÍPIOS

Quais são e o que dizem os princípios da LGPD?

O QUE VOCÊ PRECISA SABER

Os princípios estabelecidos na LGPD impõem novas diretrizes e limitações sobre como os dados pessoais poderão ser tratados. São eles:

PRINCÍPIOS

- Finalidade;
- Adequação;
- Necessidade;
- Livre acesso;
- Qualidade dos dados;
- Transparência;
- Segurança;
- Prevenção;
- Não discriminação;
- Responsabilização e prestação de contas.

É importante que os agentes de tratamento adotem medidas efetivas (e que sejam demonstráveis) para que as operações de tratamento estejam aderentes aos princípios previstos da LGPD.

SAIBA MAIS

Os princípios estabelecidos pela LGPD, relacionados ao lado, trazem novas diretrizes e limitações sobre como os dados pessoais poderão ser tratados no Brasil. Assim, as atividades de tratamento de dados pessoais passarão a observar, além da boa-fé, os seguintes princípios: **Finalidade, Adequação, Necessidade, Livre acesso, Qualidade dos dados, Transparência, Segurança, Prevenção, Não discriminação, Responsabilização e prestação de contas.**

ONDE POSSO ENCONTRAR ESTE TEMA NA LGPD? Artigos 6°

QUE 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.

Princípios

1. FINALIDADE:

O tratamento de dados pessoais deve ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular, observadas as finalidades originárias.

2. ADEQUAÇÃO:

O tratamento de dados pessoais deve ser compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

3. NECESSIDADE:

O tratamento de dados pessoais deve ser limitado 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.

4. LIVRE ACESSO:

É garantida aos titulares a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

5. QUALIDADE DOS DADOS:

É garantido aos titulares que seus dados sejam exatos, claros, relevantes e atualizados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

6. TRANSPARÊNCIA:

É garantido aos titulares o direito a informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

7. SEGURANÇA:

Devem ser utilizadas 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.

8. PREVENÇÃO:

Devem ser adotadas medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

9. NÃO DISCRIMINAÇÃO:

Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

10. RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS:

Demonstração, pelo agente, 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.

BASE LEGAL

Em quais situações o tratamento de dados pessoais é considerado legal?

O QUE VOCÊ PRECISA SABER

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 ou de obrigação legal ou regulatória.

Afora 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 justificaram a disponibilização de tais dados.

ONDE POSSO ENCONTRAR ESTE TEMA NA LGPD? Arts. 5º, XII, 7º a 16 c/c art. 37

QUE 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 interesse legítimo, 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.

SAIBA MAIS

A LGPD estabelece um rol taxativo de 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;

• Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas emleis e regulamentos;

• Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização 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.

Consentimento:

A LGPD estabelece que o consentimento é uma manifestação livre, informada e inequívoca que autoriza o tratamento de dados pessoais para uma finalidade determinada. Autorizações genéricas, isto é, autorizações que não têm como escopo uma finalidade específica, explícita e informada serão nulas.

O consentimento deverá ser fornecido por escrito em cláusula destacada ou por qualquer outra ação afirmativa que demonstre a vontade do titular dos dados. Não se admite em hipótese alguma o consentimento implícito.

O consentimento será sempre considerado uma autorização temporária porque pode ser revogado a qualquer momento pelo titular dos dados pessoais, por procedimento gratuito e facilitado.

Caso haja mudança na finalidade para o tratamento de dados pessoais para a qual o consentimento do titular foi obtido e desde que essa mudança não seja compatível com o consentimento originalmente dado, o controlador deverá informar previamente o titular sobre tal mudança.

Em caso de dados tornados manifestamente públicos pelo próprio titular dos dados, o agente fica desobrigado de obter o consentimento para tratamento de dados, observada a finalidade originária do tratamento, de modo que permanecem vigentes os demais direitos do titular e princípios estabelecidos na LGPD.

SAIBA MAIS

Interesse legítimo:

O tratamento de dados pessoais necessário para atender ao interesse legítimo do controlador ou de terceiro é permitido pela LGPD, desde que tal tratamento não viole os direitos e liberdades fundamentais do titular dos dados e que medidas para garantir a transparência de tal tratamento sejam adotadas.

O interesse legítimo deverá ser verificado a partir da análise da situação concreta e com base nos princípios da LGPD e poderá ser revisto pela autoridade nacional de proteção de dados. A título de exemplo, a LGPD estabelece um rol de finalidades que podem vir a justificar o interesse legítimo do controlador ou de terceiro, a depender da situação concreta:

• Apoio e promoção de atividades do controlador;

• Proteção, em relação ao titular dos dados, do exercício regular dos direitos ou prestação de serviços que beneficiem o titular, desde que respeitadas as legítimas expectativas do titular dos dados.

No caso de tratamento de dados pessoais com fundamento no interesse legítimo do controlador, somente os dados estritamente necessários, considerando a finalidade pretendida, poderão ser utilizados.

Tratamento de Dados Pessoais Sensíveis:

Considerando a natureza de dados pessoais sensíveis, a LGPD se preocupou em diminuir as hipóteses para tratamento desses dados e impor um consentimento mais rigoroso.

O consentimento para o tratamento de dados pessoais sensíveis deve ser fornecido de forma específica e destacada. Isto é, o agente de tratamento responsável por obter o consentimento deve se preocupar em obter uma autorização especial para o tratamento de dados pessoais sensíveis.

Além disso, a LGPD não permite o tratamento de dados pessoais sensíveis para atender ao interesse legítimo do controlador ou de terceiros ou proteção do crédito. Por outro lado, permanece a possibilidade de tratar os dados pessoais sensíveis quando for indispensável para o cumprimento de obrigação legal ou regulatória pelo controlador dos dados, para o exercício regular de direitos em processo judicial, administrativo ou arbitral ou necessário para a execução de contrato.

Tratamento de Dados Pessoais de Crianças e de Adolescentes:

O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse. O tratamento de dados pessoais de crianças deve ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal. Os controladores deverão realizar todos os esforços razoáveis para verificar que o consentimento foi realmente fornecido pelo responsável pela criança.

SAIBA MAIS

A única hipótese em que a LGPD permite a coleta de dados pessoais sem o consentimento de pais ou responsável legal é no caso da coleta necessária para realizar contato com os pais ou responsável legal. Neste caso, os dados pessoais coletados sem o consentimento somente poderão ser utilizados uma vez e não poderão ser armazenados em hipótese alguma, dado que sua única finalidade é a realização do referido contato.

Término do tratamento:

O término do tratamento de dados pessoais ocorrerá quando:

• For verificado que a finalidade para a qual o consentimento foi obtido foi alcançada ou que os dados pessoais coletados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;

- Decorrer o fim do período de tratamento;
- Ocorrer uma manifestação do titular dos dados pessoais nesse sentido;
- Houver uma determinação legal.

Nos casos de término de tratamento de dados pessoais, os dados pessoais devem ser eliminados, salvo se de outra forma a sua guarda for autorizada pela LGPD, tal como o emprego de anonimização.

DIREITOS DO TITULAR

Quais os direitos que o titular dos dados pode exigir dos agentes de tratamento?

O QUE VOCÊ PRECISA SABER

O titular dos dados tem direito ao acesso facilitado a informações sobre o tratamento de seus dados pessoais e a exigir correção de dados incompletos, inexatos ou desatualizados.

Também poderá, mediante requisição expressa, solicitar a transferência de seus dados pessoais a outro fornecedor de serviço ou produto.

Quando o tratamento dos dados for baseado exclusivamente em decisões automatizadas, o titular dos dados tem o direito de solicitar a revisão de tal tratamento por pessoa natural.

Quando verificado o descumprimento de disposições da LGPD, o titular dos dados poderá se opor ao tratamento de seus dados pessoais, se realizado com base em uma das hipóteses de dispensa de consentimento.

O titular dos dados também poderá revogar o consentimento dado anteriormente para o tratamento de seus dados pessoais.

Arts. 8°, § 5°; 9°, caput; e §3°; art. 14, § 6° e 17 a 22

QUE PROVIDÊNCIAS VOCÊ DEVE TOMAR?

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 proporcionado ao titular dos dados está com uma linguagem clara e adequada.

SAIBA MAIS

A LGPD impõe como seu principal objetivo a proteção dos direitos fundamentais de liberdade e de privacidade dos indivíduos. Para tanto, apresenta um rol de princípios e direitos especialmente voltados à garantia de informações claras ao titular dos dados e imposição de limitações ao seu tratamento.

Além de ter o direito a informações claras acerca do tratamento de dados, o titular tem o direito a obter gratuitamente as seguintes providências, mediante requisição expressa ao controlador:

• Confirmação da existência de tratamento e acesso aos dados pessoais;

• Correção de dados incompletos, inexatos ou desatualizados;

• Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a legislação;

• Portabilidade dos dados a outro fornecedor de serviço ou produto;

• Eliminação dos dados pessoais tratados com o consentimento do titular, ressalvadas as hipóteses de guarda para cumprimento de obrigação legal ou regulatória;

• Informação a respeito do uso compartilhado de dados pessoais;

• Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

• Possibilidade de revogação do consentimento, por procedimento gratuito e facilitado.

Direito à informação:

O titular dos dados tem direito a ter acesso facilitado a informações relacionadas ao tratamento de dados pessoais, incluindo, mas não se limitando a informações a respeito:

• Da finalidade específica do tratamento;

• Da forma e duração do tratamento;

• Da identificação e contato do controlador;

• Do uso compartilhado de dados e a respectiva finalidade;

• Da responsabilidade dos agentes de tratamento;

• De tratamento de dados pessoais como condição para o fornecimento de produto ou de serviço ou para o exercício de direito, caso aplicável;

• Dos demais direitos do titular, nos termos da LGPD.

Tais informações deverão ser disponibilizadas de forma clara, adequada e ostensiva.

SAIBA MAIS

Crianças:

No caso de tratamento de dados pessoais de crianças, as informações devem ser fornecidas de maneira simples, clara e acessível, considerando as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do público-alvo. As empresas poderão empregar recursos audiovisuais ou afins para passar as informações pertinentes. Dessa forma, além do fornecimento de informações aos pais ou ao responsável legal, que deverá consentir com o tratamento, será possível proporcionar um adequado entendimento à criança.

Confirmação e acesso aos dados pessoais:

A qualquer momento, o titular dos dados pessoais tem o direito de obter confirmação da existência de tratamento e acesso aos seus dados pessoais. Isso poderá se dar de duas formas:

• Em formato simplificado, caso a confirmação ou o acesso seja providenciado imediatamente;
• Por meio de declaração clara e completa, com indicação da origem dos dados, inexistência de registro, critérios utilizados e finalidade do tratamento, conforme o caso, no prazo de quinze dias a contar da data do requerimento do titular dos dados.

As informações deverão ser fornecidas por meio eletrônico ou de forma impressa, de acordo com a solicitação do titular.

Adicionalmente, quando o tratamento de dados tiver fundamento no consentimento ou em contrato, o titular poderá solicitar cópia eletrônica integral dos seus dados pessoais.

Correção, anonimização, pseudonimização, bloqueio ou eliminação de dados pessoais:

O titular dos dados poderá requerer a correção de dados que considere incompletos, inexatos ou desatualizados, bem como solicitar a anonimização, bloqueio ou eliminação de dados pessoais considerados como desnecessários, excessivos ou tratados em desconformidade com a LGPD.

Para fins da LGPD, “anonimização” é um procedimento por meio do qual um dado perde a possibilidade de identificar um titular, enquanto “bloqueio” significa suspensão temporária de qualquer operação de tratamento de dados pessoais.

Ademais, no caso de dados tratados com fundamento no consentimento, o titular dos dados poderá solicitar a eliminação de quaisquer dados coletados, ressalvadas as hipóteses de guarda permitidas pela LGPD, o que inclui a guarda de dado especialmente para cumprimento de obrigação legal pelo controlador ou para uso exclusivo do controlador, sendo que, neste último caso, os dados deverão ser anonimizados.

Caso a empresa tenha realizado uso compartilhado de dados cuja correção, anonimização, bloqueio ou eliminação fora requisitado pelo titular dos dados, a empresa deverá informar de maneira imediata tal providência aos demais agentes de tratamento de modo que repitam o procedimento.

SAIBA MAIS

Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

Para fins de atendimento dessa regra, "pseudonimização" é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

Portabilidade dos dados pessoais:

A LGPD instituiu o direito de portabilidade, pelo qual o titular dos dados poderá, mediante requisição expressa, solicitar a transferência de seus dados pessoais a outro fornecedor de serviço ou produto.

Revisão de decisão automatizada:

O titular dos dados poderá requisitar a revisão, por pessoa natural, de decisões tomadas unicamente com base em tratamento automatizado, inclusive decisões destinadas à formação de perfis. O titular dos dados ainda poderá solicitar a disponibilização de informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para formação da decisão automatizada.

E em caso de impossibilidade de cumprimento imediato?

Caso não possa cumprir de imediato a providência requerida pelo titular dos dados, o controlador deverá enviar ao titular uma justificativa com as razões que impediram o cumprimento imediato do direito exercido ou uma comunicação para indicar que não é o agente de tratamento dos dados e, caso tenha conhecimento, apontar quem é o agente de fato.

OBRIGAÇÕES

Quais obrigações o titular dos dados pode exigir do controlador?

O QUE VOCÊ PRECISA SABER

Dentre as obrigações previstas na LGPD, o controlador deve:

OBRIGAÇÕES

- 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 autoridade nacional de proteção de dados, elaborar relatório de impacto à proteção de dados;
- Informar o titular caso haja alguma alteração na finalidade para a coleta de dados;
- Responder solidariamente, em conjunto com o operador, se causar a terceiros danos por violação da LGPD.

ONDE POSSO ENCONTRAR ESTE TEMA NA LGPD? Artigos 5º, 7º §5, 8º §2º, 9 a 11, 14, 16, 18, 20, 33, 37 a 42, 48, 50 e 52

QUE PROVIDÊNCIAS VOCÊ DEVE TOMAR?

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.

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.

SAIBA MAIS

Cabe ao controlador tomar as decisões acerca do tratamento de dados pessoais, bem como zelar por sua conservação e atender aos requisitos e exigências formulados pelas autoridades. Nesse sentido, a LGPD impõe ao controlador as seguintes responsabilidades:

• Provar que o consentimento foi obtido em conformidade com a Lei.

• Confirmar a existência ou providenciar o acesso a dados pessoais, mediante requisição do titular, em formato simplificado, imediatamente, ou por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, fornecida no prazo de até 15 (quinze) dias.

• Manter registro das operações de tratamento de dados pessoais que realize, podendo a autoridade nacional determinar que seja elaborado relatório de impacto à proteção de dados (pessoais ou sensíveis) referente às suas operações.

• Caso a autoridade faça essa requisição, o controlador não pode esquecer de inserir no relatório, no mínimo, as seguintes informações:
- Descrição dos tipos de dados coletados;
- Metodologia utilizada para a coleta de dados;
- Metodologia utilizada para garantir a segurança das informações;
- Análise do controlador com relação a essas medidas, salvaguardas e mecanismos de mitigação de riscos adotados.

O controlador também é responsável por indicar quem é o encarregado pelo tratamento dos dados pessoais, divulgando publicamente, de forma clara e objetiva, preferencialmente no seu sítio eletrônico, a identidade da pessoa e suas informações de contato. Em linhas gerais, as atividades do encarregado consistem em:

• Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

• Receber comunicações da autoridade nacional e adotar providências;

• Orientar os funcionários e os contratados da organização a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;

• Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares emitidas pela autoridade nacional de proteção
de dados.

SAIBA MAIS

Nas hipóteses em que o consentimento for exigido, o controlador deverá informar o titular caso haja alguma alteração na finalidade para a coleta de dados. Nesse momento, o titular poderá optar por renovar o consentimento ou revoga-lo.

Caso não haja consentimento do titular, o controlador somente poderá fundamentar o tratamento de dados pessoais atestando que há finalidade legítima para tanto. Com relação a essa exigência, somente dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados e devem ser adotadas medidas que garantam sua transparência.

O controlador que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para tanto, exceto em caso de o titular dos dados tê-los tornado manifestamente públicos.

O controlador responde solidariamente com o operador se, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à LGPD.

É facultado ao controlador formular regras de boas práticas e de governança que estipulem condições de organização, procedimentos, normas de segurança, padrões técnicos, obrigações específicas, mecanismos internos de supervisão e mitigação de riscos, bem como outros aspectos relacionados ao tratamento de dados pessoais, desde que respeitadas suas competências.

É permitida a conservação de dados pelo controlador quando encerrado o período de tratamento para que seja possível cumprir com as obrigações legais e regulatórias.

O controlador também pode fazer uso exclusivo desses dados, desde que anonimizados, sendo seu acesso por terceiros expressamente vedado na Lei.

TRANSFERÊNCIA INTERNACIONAL DE DADOS

E se os dados forem tratados fora do Brasil?

O QUE VOCÊ PRECISA SABER

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.

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

ONDE POSSO ENCONTRAR ESTE TEMA NA LGPD?
Artigos 3º, 33, 34 a 36

QUE PROVIDÊNCIAS VOCÊ DEVE TOMAR?

Adotar cautela no envio de dados a organizações no exterior e ter a segurança de que elas cumprem 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 autoridade nacional caso haja alteração nas garantias que tenham sido entendidas como suficientes para a realização de transferência internacional de dados.

SAIBA MAIS

A LGPD se aplica a qualquer operação de tratamento de dados, independentemente do país de sua sede ou do país em que estejam localizados os dados, conforme o item Abrangência deste guia.

A LGPD determina expressamente as hipóteses em que é permitida a transferência internacional de dados, quais sejam:

• Para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto na lei;

• Quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na Lei, através de cláusulas contratuais específicas para determinada transferência, cláusulas-padrão contratuais, normas corporativas globais ou selos, certificados e códigos de conduta regularmente emitidos;

• Quando a transferência for necessária para cooperação jurídica internacional entre órgãos públicos de inteligência, investigação e persecução, observados os instrumentos de direito internacional, ou quando for resultado de compromisso assumido em acordo de cooperação internacional;

• Quando autorizada a transferência pela autoridade nacional de proteção de dados;

• Quando a transferência for necessária para executar políticas públicas ou atribuições legais do serviço público;

• Quando o titular fornecer seu consentimento específico e em destaque para a transferência, tendo sido fornecida informação prévia e distinta de outras finalidades sobre o caráter internacional da operação;

• Quando necessário para cumprimento de obrigação legal ou regulatória pelo controlador;

• Para execução de contrato ou procedimentos relacionados ao contrato do qual seja parte o titular, desde que requerido pelo próprio titular;

• Para exercício regular de direitos em processo judicial, administrativo ou arbitral.

Não obstante, o nível de proteção dos dados do país estrangeiro ou do organismo internacional será avaliado pela autoridade nacional de proteção de dados que observará, dentre outras hipóteses, a adoção de medidas de segurança, a natureza dos dados e as normas gerais vigentes no país de destino ou no organismo internacional.

SEGURANÇA E NOTIFICAÇÕES

E se ocorrer algum incidente que resulte em vazamento de dados?

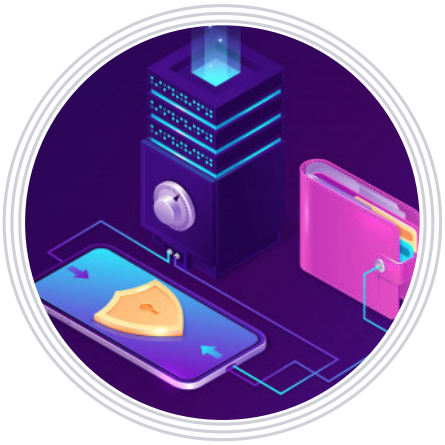
O QUE VOCÊ PRECISA SABER

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 prazo razoável, à autoridade nacional de proteção de dados e ao titular dos dados.

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

Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas, der causa ao dano. A responsabilidade será subjetiva e solidária.



ONDE POSSO ENCONTRAR ESTE TEMA NA LGPD?
Art. 44, parágrafo único e 46 ao 51

QUE PROVIDÊNCIAS VOCÊ DEVE TOMAR?

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.

SAIBA MAIS

Os agentes de tratamento deverão proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito dos dados pessoais. Para tanto, deverão adotar uma série de medidas de segurança, técnicas e administrativas.

Caberá à autoridade nacional determinar os padrões técnicos mínimos de segurança de proteção de dados pessoais, principalmente sobre dados sensíveis. Tais requisitos podem ser também estabelecidos por autoridades setoriais, como para o setor de saúde, financeiro, entre outros.

Apesar de qualquer pessoa que intervenha no tratamento de dados ter a obrigação de garantir a segurança, os agentes de tratamento que derem causa ao dano respondem pelos danos decorrentes da inobservância das medidas de segurança.

É recomendável que os agentes também adotem medidas técnicas que tornem os dados pessoais afetados ininteligíveis para que terceiros não autorizados não possam acessá-los. A adoção de tais medidas técnicas será levada em conta para analisar a gravidade do incidente.

Casos de incidente de segurança que possam acarretar risco ou dano relevantes aos titulares deverão ser comunicados à: (i) autoridade nacional e ao (ii) titular dos dados, em prazo razoável (a ser definido pela autoridade), e (iii) órgãos reguladores setoriais.

Essa comunicação deverá conter no mínimo as seguintes informações:
• descrição da natureza dos dados pessoais afetados;
• os titulares envolvidos;
• as medidas técnicas e de segurança utilizadas para a proteção dos dados;
• os riscos relacionados ao incidente;
• os motivos da demora, no caso de a comunicação não ter sido imediata;
• as medidas adotadas para reverter ou mitigar os efeitos do prejuízo causado pelo incidente.

A depender da gravidade do incidente, a autoridade nacional poderá determinar a adoção de determinadas providências, como: ampla divulgação do fato em meios de comunicação e medidas para reverter ou mitigar os efeitos do incidente.

Os agentes de tratamento de dados poderão, individualmente ou por meio de associações, formular regras de boas práticas e de governança sobre o tratamento de dados pessoais, que estabeleçam:
• as condições de organização, funcionamento e procedimentos aplicáveis ao tratamento dos dados pessoais (incluindo reclamações e petições de titulares);
• as normas de segurança e padrões técnicos;
• obrigações específicas para os diversos envolvidos no tratamento;
• as ações educativas;
• os mecanismos internos de supervisão e de mitigação de riscos;
• outros aspectos relacionados ao tratamento de dados pessoais.

O controlador, aplicando os princípios de segurança e prevenção, poderá implementar programa de governança em privacidade e demonstrar a efetividade de seu programa de governança em privacidade quando apropriado.

SANÇÕES

E se houver descumprimento da LGPD?

O QUE VOCÊ PRECISA SABER

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

As sanções administrativas aplicáveis pela autoridade nacional, em razão das infrações às normas da LGPD, vão desde advertência 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.

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

ONDE POSSO ENCONTRAR ESTE TEMA NA LGPD?
Art. 52 ao 54

QUE PROVIDÊNCIAS VOCÊ DEVE TOMAR?

Executar uma análise de conformidade dos procedimentos de tratamento de dados com a LGPD para identificar o cumprimento completo da norma.

Em caso de descumprimento, buscar sempre cooperar e minimizar o dano prontamente.

Ter à sua disposição uma equipe interna e externa que possa atender prontamente às solicitações da autoridade nacional de proteção de dados, visando a diminuir o risco de aplicação de sanções em seus maiores níveis.

SAIBA MAIS

Em razão das infrações às normas da LGPD, os agentes de tratamento de dados estão sujeitos às seguintes penalidades:
• advertência, com indicação de prazo para adoção de medidas corretivas;
• multa de até 2% do faturamento da empresa ou do grupo limitada, no total, a R$ 50 milhões por infração;
• publicização 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;

Todas as sanções serão precedidas de um procedimento administrativo que garanta a ampla defesa do infrator. As sanções serão aplicadas considerando as particularidades de cada caso e os seguintes parâmetros e critérios:
• gravidade e a 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 reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano;
• adoção de política de boas práticas e governança;
• pronta adoção de medidas corretivas;
• proporcionalidade entre a gravidade da falta e a intensidade da sanção.

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

Na aplicação da sanção de multa diária, a autoridade nacional 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 transnacionais, as multas aplicadas em uma jurisdição não serão compensadas ou abatidas com as aplicadas em outra na qual também verificados os efeitos do evento.

CEUMA
GRUPO EDUCACIONAL

GUIA PARA A **LEI GERAL** DE **PROTEÇÃO DE DADOS**