

Data da publicação
01 de Novembro de 2020

**QUAL O IMPACTO
NA MINHA EMPRESA?**

CARTILHA LEI GERAL DE PROTEÇÃO DE DADOS

2020
NOVEMBRO



Não tire cópia desse documento. Faça o download aqui.





APRESENTAÇÃO

A **Associação Brasileira das Administradoras de Imóveis (ABADI)** e o **Secovi Rio** se uniram mais uma vez para elaborar e entregar uma cartilha de orientação ao associado.

Este material tem o objetivo de abordar a temática da Lei Geral de Proteção de Dados (LGPD) e orientar sobre a utilização dos dados pessoais, observando os direitos e garantias dos titulares, o impacto da Lei nas administradoras de imóveis e a necessidade de criação de políticas internas.

Com essa cartilha, as duas instituições que trabalham em prol de um mercado imobiliário mais saudável e ético dedicam-se a entregar um conteúdo que sirva como referência para auxiliar o desempenho da sua administradora no que tange à Lei Geral de Proteção de Dados, em vigor desde setembro de 2020.

Rafael Thomé – Presidente da ABADI

Pedro Wähmann – Presidente do Secovi Rio



AUTOR

Leonardo Perseu é advogado, pós-graduado em Direito Empresarial Privado, Legal Law Master, Direito Societário e Mercado de Capitais.

Perseu também é consultor na área adequação e implementação de conformidade com a LGDP e membro da Associação Nacional dos Profissionais de Privacidade de Dados (ANPPD).



LEONARDO PERSEU




ÍNDICE

1.	O que é LGPD – Lei Geral de Proteção de Dados (Lei Federal 13.709/2018)	7
2.	Abrangência – Qual impacto da Lei na minha empresa	7
3.	Principais objetivos da Lei.	7
4.	A quem se aplica a Lei	8
5.	Espécies de Dados Pessoais	8
6.	Agentes de Tratamento de Dados Pessoais	9
7.	O que é e quais as funções do Encarregado de Dados (DPO)	10
8.	Direitos dos titulares de dados pessoais	11
9.	As Bases Legais do Tratamento – Destaque para a(s) base(s) legal(ais) de tratamento para Administradoras de Imóveis	12
10.	Princípios a serem seguidos na adequação e conformidade com a Lei	14
11.	Os documentos que devem ser elaborados na adequação de conformidade e suas funções	15
12.	O que fazer em caso de um incidente de segurança	16
13.	ANPD e as sanções previstas na Lei	16
14.	Benefícios da conformidade com a Lei	18
15.	O passo a passo de uma implementação de conformidade	18
16.	Conclusão	19



ANEXO I

MODELO DE POLÍTICA DE PRIVACIDADE EM CONFORMIDADE COM A LGPD

TIMBRE EMPRESA

Política de Privacidade
Atualizada em XXX de OUTUBRO de 2020

Nós da **(nome da empresa)**, somos comprometidos com o assunto privacidade e proteção de dados pessoais, considerando o tema como um de nossos valores mais importantes.

Por essa razão, disponibilizamos a seguir nossa Política de Privacidade, como forma de dar transparência sobre a maneira através da qual coletamos, utilizamos, processamos, armazenamos, compartilhamos e protegemos os dados pessoais empregados na viabilização do nosso modelo de negócio.

Quem somos?

A **(nome da empresa)** uma administradora de imóveis que **(descrever todas as atividades ligadas)**. Em resumo, nós prestamos serviços profissionais e trabalhando junto com nossos clientes e parceiros comerciais procuramos, de forma segura, atingir as finalidades específicas detalhadas acima.

A presente política aplica-se às seguintes organizações e suas filiais:
(descrição completa das empresas do mesmo grupo econômico)

Como você pode nos contatar para tratar sobre assuntos relacionados a privacidade de dados?

Direcione as suas dúvidas e solicitações para o "Encarregado pelo tratamento de dados pessoais da **(nome da empresa)** **(nome do DPO)** por meio de um dos contatos abaixo: **(e-mail exclusivo)** ou Rua XXXXXXXXXXXXXXXXXXXX – CEP XXXXXXX **(meio físico)**.

Como coletamos dados pessoais?

Para viabilizarmos nossas atividades enquanto empresa, é necessário que realizemos coleta e tratamento de algumas informações que são consideradas pela legislação brasileira como dados pessoais, isto é,

Clique no botão ou na imagem para acessar o documento



Download



ANEXO II

CHECKLIST DE SEGURANÇA DE DADOS

Checklist de Segurança para defender a sua Empresa

PRS CONSULTORIA JURIDICA

Preencha o **checklist** e **priorize** as defesas tecnológicas e das informações da sua empresa:

<input type="checkbox"/> Fazer inventário e controle de ativos de hardware	<input type="checkbox"/> Fazer inventário e controle de ativos de software
<input type="checkbox"/> Gerenciar vulnerabilidades	<input type="checkbox"/> Controlar o uso de contas com privilégios administrativos.
<input type="checkbox"/> Configurar e manter softwares e aplicativos de dispositivos móveis ou computadores sempre atualizados com as últimas correções de segurança dos fabricantes	<input type="checkbox"/> Realizar monitoramento e análise de logs de auditoria dos sistemas de informação
<input type="checkbox"/> Proteger e-mails e navegadores da Web	<input type="checkbox"/> Implantar e gerenciar defesas contra malware
<input type="checkbox"/> Restringir e controlar portas IP, protocolos e serviços	<input type="checkbox"/> Gerenciar recursos de recuperação de dados (Backup)
<input type="checkbox"/> Configurar adequadamente firewalls, roteadores e switches de rede	<input type="checkbox"/> Gerenciar defesas de perímetro e servidores na zona desmilitarizada (DMZ)
<input type="checkbox"/> Implantar e gerenciar políticas de proteção de dados	<input type="checkbox"/> Definir e implantar controle de acessos físico e lógicos rigorosos a dados
<input type="checkbox"/> Implantar e gerenciar controle de acesso Wireless	<input type="checkbox"/> Controlar e monitorar acesso a contas de sistemas
<input type="checkbox"/> Implantar programa de conscientização em segurança de dados	<input type="checkbox"/> Gerenciar e auditar segurança de sistemas usados pela empresa (internos ou externos)
<input type="checkbox"/> Implantar e gerenciar processos de resposta a incidentes de segurança ou privacidade de dados	<input type="checkbox"/> Realizar testes de intrusão nas redes de dados

Clique no botão ou na imagem para acessar o documento



Download



1 O QUE É LGPD – LEI GERAL DE PROTEÇÃO DE DADOS (LEI FEDERAL 13.709/2018)

A Lei Geral de Proteção de Dados Pessoais é a legislação brasileira que regula as atividades de tratamento de dados pessoais, que alterou os artigos 7º e 16 do Marco Civil da Internet e iniciou a sua vigência em 18/09/2020.

A **LGPD** estabelece regras sobre o tratamento de dados pessoais, com objetivo de proteger os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural, impondo mais proteção aos dados pessoais e penalidades pelo seu descumprimento.

2 ABRANGÊNCIA – QUAL IMPACTO DA LEI NA MINHA EMPRESA

A **LGPD** veio para mudar de forma significativa a cultura no tratamento de dados pessoais e, conseqüentemente, como as empresas coletam, armazenam e compartilham dados pessoais de seus clientes e colaboradores.

Com a entrada em vigor da **LGPD**, os titulares de dados pessoais passaram a ter uma série de direitos e garantias, alçadas a categoria de fundamentais, veremos isso detalhadamente mais adiante.

Para a **LGPD** tratamento de dados é toda e qualquer operação realizada por pessoa natural ou jurídica de direito público ou privado tais como: **coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle de informação, modificação, comunicação, transferência, difusão ou extração.**

3 PRINCIPAIS OBJETIVOS DA LEI

- *Respeito à privacidade;*
- *Inviolabilidade da intimidade, honra e imagem;*
- *Liberdade de expressão, informação, comunicação e opinião;*
- *Defesa do titular de dados, livre iniciativa e livre concorrência;*



- *Desenvolvimento econômico, tecnológico e inovação;*

- *Direitos humanos, livre desenvolvimento da personalidade, dignidade e exercício da cidadania;*

- *Liberdade de expressão, informação, comunicação e opinião;*

4 A QUEM SE APLICA A LEI

Conforme previsto no Art. 3º a **LGPD** se aplica a qualquer operação de tratamento de dados realizada por pessoa natural, pessoa jurídica de direito público ou de direito privado, **independente do meio, do país de sua sede ou do país onde estejam localizados os dados**, desde que:

- A operação seja realizada no **território nacional**;

- A atividade de tratamento tenha por **objetivo a oferta ou o fornecimento de bens e serviços ou o tratamento de dados de indivíduos localizados no território nacional**;

- Os dados pessoais tenham sido **coletados em território nacional**;

5 ESPÉCIES DE DADOS PESSOAIS

Dado Pessoal é toda e qualquer informação que possa levar a identificação, direta ou indireta, de uma pessoa; qualquer dado que possa ser associado a um indivíduo, fazendo com que a aplicação da norma se concentre sobre o poder que este indivíduo tem sobre seus dados.

A definição de dado pessoal pode influenciar no equilíbrio de poder entre o cidadão e aquele que coleta e utiliza os dados, sendo subdivididos nas seguintes categorias:

- **Dados Pessoais Comuns: Diretos**, ou seja, informações de pessoas físicas identificadas ou identificáveis: nome completo, e-mail, telefone, registro geral (RG), cadastro pessoa física (CPF) e endereço; **Indiretos**: endereços de IP, geolocalização e identificadores eletrônicos;

- **Dados Sensíveis**: são dados que merecem **especial atenção** e cujo tratamento pode ensejar a discriminação de seu titular, ou seja, origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organizações religiosas, filosóficas e políticas, dados sobre saúde, vida sexual, dados genéticos e biométricos.



OBS.: Os dados sensíveis, pelo potencial discriminatório que apresentam, devem ser protegidos de forma mais rígida pela empresa, cabendo aqui uma dica em relação ao tratamento desse tipo de dados pessoal “**o menos é mais**”, portanto, estes **só devem ser coletados quando, e somente só, forem extremamente necessários e indispensáveis, o que pode vir a prevenir riscos desnecessários.**

• **Dados Anônimos:** são dados que se referem a pessoas que não podem ser identificadas – como dados estatísticos, por exemplo. Um dado anônimo, ainda que seja referente a uma pessoa (ou grupos de pessoas), **não permite a identificação do titular, são os denominados dados anonimizados.**

6 AGENTES DE TRATAMENTO DE DADOS PESSOAIS

De acordo com a LGPD os agentes de tratamento são o **CONTROLADOR** e **OPERADOR** (Art. 5º, inciso VI e VII) e **suas responsabilidades** estão previstas nos Art. 37 a 40 da lei.

• **Controlador:** qualquer pessoa natural ou jurídica, de direito público ou privado, a quem **COMPETE TOMAR AS DECISÕES REFERENTES AO TRATAMENTO DE DADOS PESSOAIS;**

• **Operador:** qualquer pessoa natural ou jurídica, de direito público ou privado, que **REALIZA O TRATAMENTO DE DADOS PESSOAIS EM NOME DO CONTROLADOR.**

OBS.1.: Uma empresa pode agregar as duas funções, como é o caso das Administradoras de Imóveis, pois além de tomar as decisões sobre o tratamento de dados, vai realizar efetivamente o tratamento.

OBS.2.: Tanto o controlador quanto o operador têm a **obrigação legal de manter o registro das operações de tratamento de dados de forma segura**, sendo certo que a ANPD (Autoridade Nacional de Tratamento de Dados) e outros órgãos de controle (MP, PROCON, etc.) poderão **exigir os documentos obrigatórios para verificação de conformidade**, como por exemplo, Relatório de Impacto de Proteção de Dados (**RIPD**), Relatório de Legítimo Interesse (**RLI**), Política de Privacidade (**atualizada**), Termos de Uso e Consentimento, etc.



OBS.3.: Ambos agentes são responsáveis – **SOLIDÁRIOS** - em caso de incidente de dados pessoais que causem dano patrimonial, moral ou coletivo, mas o **risco dessa solidariedade pode ser minimizado com a realização de uma boa implementação de conformidade na fase de revisão dos contratos com terceiros, parceiros e colaboradores.**

7 O QUE É E QUAIS AS FUNÇÕES DO ENCARREGADO DE DADOS (DPO)

Uma figura exigida pela **LGPD** em qualquer situação é o D.P.O (*Data Protection Officer*) ou Encarregado de Dados Pessoais, que é o profissional indicado pelo controlador e será o responsável de cuidar de todas as questões referentes à proteção dos dados dentro da empresa.

É possível que o encarregado seja um empregado da corporação (pessoa natural) ou um terceiro prestador de serviços (pessoa física ou jurídica). Além disso, apesar da **LGPD** não trazer exigências específicas quanto à qualificação desse

profissional, orientamos que este agregue profundos conhecimento de TI e bases sólidas de direito regulatório.

Sua identidade e as informações de contato devem ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador e obrigatoriamente na política de privacidade.

Suas funções estão devidamente delineadas na **LGPD** (Art. 41, parágrafo 2º, incisos I a IV), ou seja:

- *Aceitar reclamações e comunicações dos titulares de dados, prestar esclarecimentos e adotar providências;*
- *Receber as comunicações da ANPD e adotar providências; (aqui cabe uma observação de que ele também deverá responder aos demais órgãos de fiscalização)*
- *Orientar os funcionários e os contratados da entidade 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.*



8 DIREITOS DOS TITULARES DE DADOS PESSOAIS

Os direitos dos titulares de dados estão previstos nos Artigos 8º, 9º e 18 da LGPD e são os seguintes:

- *Confirmação da existência de tratamento;*
- *Acesso aos dados;*
- *Correção de dados incompletos, inexatos ou desatualizados;*
- *Anonimização, bloqueio ou eliminação de dados;*
- *Revisão das decisões tomadas exclusivamente com base em dados pessoais;*
- *Portabilidade dos dados a outro fornecedor de serviço ou produto;*
- *Informação das entidades com as quais o controlador realizou uso compartilhado;*
- *Informação sobre a possibilidade de não fornecer consentimento;*
- *Reclamação à autoridade nacional de dados;*
- *Oposição ao tratamento;*

Algumas observações devem ser feitas a respeito dos direitos e garantias dos titulares de dados pessoais, em especial sobre anonimização, bloqueio e eliminação de dados; como também sobre portabilidade, possibilidade de não fornecer consentimento e o direito a oposição ao tratamento de dados.

Muito se tem falado sobre consentimento, mas o consentimento é uma das bases legais para o tratamento de dados, sendo certo que, **no caso específico das administradoras de imóveis temos pelo menos, em princípio, outras três bases legais para o tratamento, ou seja, cumprimento de obrigação legal, exercício regular de direito e o legítimo interesse do controlador.**

Tais bases legais devem ser utilizadas quando da interseção entre o objeto social da administradora e a confecção da nova política de privacidade e do relatório de impacto de proteção de dados.

Portanto, não será em qualquer situação que o titular, indiscriminadamente, poderá exigir, por exemplo, a exclusão dos seus dados da base de dados da administradora, muito menos se opor ao tratamento, uma vez que existe um vínculo contratual que une a administradora a um condomínio ou a um proprietário de imóvel locado, por exemplo.

Mas em determinadas situações específicas, como por exemplo, a **transferência de dados para celebração de contrato de seguro**, o titular deverá ser **comunicado previamente** sobre esse compartilhamento de dados com uma corretora ou uma seguradora e ele poderá se opor a esse tratamento.



Portanto, é de suma importância quando da implementação de conformidade com a **LGPD** que a administradora adote medidas (por vezes simples) para minimizar riscos e problemas que possam vir a surgir quando do tratamento nessas situações, uma boa consultoria irá direcionar a empresa nesse sentido, como também elaborar documentos que previnam riscos e produzam provas para o caso de incidentes no tratamento de dados pessoais.

Quanto a portabilidade, ainda não há uma definição específica sobre como e de que forma esse direito poderá ser exercido, cabendo ao Conselho Diretor da ANPD regulamentar a matéria (Art. 18, inciso V, Art. 40 da LGPD c/c Art. 4º, inciso II, letra “c” do Decreto n. 10.474 26/08/2020).

9 AS BASES LEGAIS DO TRATAMENTO

A **LGPD** em seu Art. 7º prevê dez bases legais para o tratamento de dados pessoais, destacando ainda que **somente essas bases legais viabilizam o tratamento de dados**.

Como a presente cartilha se destina especificamente ao mercado imobiliário, em especial as administradoras de imóveis, nos limitaremos a tratar das bases legais aplicáveis a esse segmento.

Para fundamentar e documentar todo processo de implementação de conformidade com a **LGPD**, as administradoras poderão utilizar as seguintes bases legais: **cumprimento de obrigação legal, execução de contrato ou diligências pré-contratuais, exercício regular de direito, legítimo interesse do controlador e consentimento**.

No **cumprimento de obrigação legal**, os controladores (administradoras) deverão observar os princípios pertinentes, especialmente no tocante: **(i)** a adstrição do tratamento à finalidade específica de cumprimento da determinação legal, **(ii)** a adoção dos meios adequados e necessários para tal, bem como **(iii)** a preocupação com todos os direitos do titular, dentre os quais se destaca o direito de ser informado do tratamento de dados (§ 1º, do art. 7º, da LGPD) e o direito de ter os dados disponibilizados nos exatos termos do que for especificado pela autoridade nacional (§ 2º, do art. 7º, da LGPD), por exemplo, o necessário cadastro e guarda de documentos de colaboradores internos, no mínimo, pelo prazo exigido pela legislação trabalhista.

Quanto a **execução de contrato ou diligências pré-contratuais** as administradoras utilizarão muito essa base legal, pois é da essência do segmento a celebração de várias espécies de contrato, como por exemplo: administração condominial, locação e compra e venda; **mas vale destacar que a guarda desses**



documentos, e, conseqüentemente, dados pessoais, não podem ficar armazenados por tempo indeterminado ou indefinidamente, na consultoria são definidos os prazos e orientada a forma de anonimização desses dados.

A base legal do **exercício regular de direito** em processo administrativo, judicial ou arbitral, ressalva o uso de dados pessoais para o necessário direito que as partes têm de produzir provas umas contra as outras, ainda que estas se refiram a dados pessoais da parte adversa.

O **legítimo interesse** do controlador é uma base legal que se destaca das demais por ser mais elástica em sua aceção e por não ter balizas taxativas, viabilizando atividades de tratamento de dados que estariam inviabilizadas, seja por um engessamento atinente à obtenção do consentimento ou por qualquer falta de fundamento das bases anteriores.

O Art. 10 da LGPD atribuiu o uso do **legítimo interesse** somente em situações concretas, resguardando a utilização de dados estritamente necessários para atendimento de determinada finalidade e pela transparência sobre atividade a atividade de tratamento; sempre sujeito a eventual pedido da ANPD para apresentação de relatório de impacto à proteção de dados (RIPD) sobre o referido tratamento, sendo de suma importância a elaboração de um RIPD criterioso.

A existência de um interesse legítimo requer uma avaliação cuidadosa e criteriosa para saber se o titular dos dados pode razoavelmente prever, no momento e no contexto em que os dados pessoais são colhidos, que esses poderão vir a ser tratados com as finalidades específicas.

Por fim, o **consentimento** é a base legal mais comentada do momento, mas, como vimos anteriormente, nem tudo se resume a consentimento no tratamento de dados. As administradoras devem se preocupar em solicitar consentimento prévio em determinadas situações específicas, como por exemplo, no caso de oferecimento de “produtos ou serviços” diversos aos locatários, condomínio ou condôminos - seguros (prestamista, conteúdo etc.); como também dos parentes do colaboradores internos que possuem direito/interesse nos benefícios legais (plano de saúde, auxílio creche, etc).



10 PRINCÍPIOS A SEREM SEGUIDOS NA ADEQUAÇÃO E CONFORMIDADE COM A LGPD

Foram introduzidos 10 princípios de proteção de dados e todos partindo da boa-fé, asseguram os direitos e garantias dos titulares, são eles:

- **Finalidade:** Dever de informar previamente ao titular, de forma clara, os propósitos legítimos e específicos do tratamento dos dados;
- **Adequação:** Dever de informar ao titular as finalidades do tratamento de seus dados;
- **Necessidade:** Somente devem ser tratados os dados necessários para a realização do objetivo informado;
- **Livre Acesso:** O titular dos dados deve ter acesso a consulta fácil e gratuita sobre o tratamento dos seus dados;
- **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;
- **Transparência:** Garantia ao titular de informações claras e precisas sobre seus dados;
- **Segurança:** Adoção de medidas técnicas e administrativas para proteger e garantir a integridade dos dados;
- **Prevenção:** Adoção de medidas preventivas contra a ocorrência de incidentes sobre os dados do titular;
- **Não Discriminação:** É vedado o tratamento de dados com fins discriminatórios;
- **Responsabilização e Prestação de Contas:** Os agentes de tratamento devem adotar e informar as medidas que comprovem o cumprimento das normas de proteção de dados e sua eficiência.

OBS.: Quando da elaboração dos documentos para implementação de conformidade (relatórios e políticas), os princípios devem ser observados e correlacionados com as bases legais.



11 OS DOCUMENTOS QUE DEVEM SER ELABORADOS NA ADEQUAÇÃO DE CONFORMIDADE E SUAS FUNÇÕES

- **Relatório de Impacto à Proteção de Dados Pessoais (RIPD):** documento obrigatório realizado tomando por base as diretrizes do negócio do controlador, contendo a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco; esse documento poderá ser exigido pela ANPD e órgãos de fiscalização;

- **Relatório de Legitimação de Interesse (RLI):** documento que faz a correlação entre a(s) base(s) legal(ais) ao interesse do controlador, esse documento pode, ou não estar incluído no RIPD;

- **Relatório de Violação de Dados Pessoais (Plano de Resposta):** em caso de incidente com dados, o DPO deve se reportar a ANPD para comunicar o incidente e para isso é necessária a confecção de um relatório específico e detalhado;

- **Política de Segurança de Dados Pessoais:** forme um comitê interno de Segurança de Informação (SI) que normalmente composto pelo DPO, Jurídico e TI. Esse será o time responsável por definir e escrever em conjunto com o consultor a política de proteção de dados. O documento é um manual completo de como a empresa cuida e manipula dados pessoais de clientes e colaboradores, informando as técnicas utilizadas para SI.

- **Política de Privacidade, Cookies e Termo de Uso:** a empresa deve criar uma Política de Privacidade em conformidade com LGPD, sopesando os princípios, indicando claramente quais são as ferramentas e processos aplicados para garantir a privacidade dos dados recolhidos.

- **Aviso de Privacidade para funcionários e/ou Código de Conduta:** documento que concentra todas as diretrizes para a gestão dos dados pessoais dos colaboradores. Incluindo aqueles que possam causar danos como discriminação ou situações de constrangimento.

- **Definir a política de retenção de dados:** a LGPD prevê que os dados só sejam guardados enquanto tiverem um propósito. Com isso, é necessário indicar o período que os dados serão arquivados. Por exemplo, se a empresa concede o auxílio creche para crianças de até cinco anos, não será permitido ter os registros dos filhos dos colaboradores arquivados por seis anos, desde que não seja necessário para cumprimento de obrigação legal.



- **Cronograma de retenção de dados:** a empresa deverá definir um cronograma para verificação dos dados coletados. Isto é, de tempos em tempos, checar o que deve ou não ser mantido, eliminando o tratamento assim que a finalidade for alcançada ou os dados não forem mais necessários.
- **Programa de Treinamento de Pessoal:** elaborar um programa de treinamento de pessoal seve para, eventualmente, comprovar para os entes fiscalizadores que a empresa se preocupa em disseminar a nova cultura em relação ao tratamento de dados pessoais, estando seus colaboradores engajados e preparados em preservar a privacidade dos clientes.

12 O QUE FAZER EM CASO DE UM INCIDENTE DE SEGURANÇA

Boas práticas de governança visam disseminar e promover a multiplicação do conhecimento entre controladores e envolvidos com o objetivo de mitigar os riscos e ter clareza nas informações dadas aos titulares.

Um alto nível de documentação, torna mais fácil a prestação de informações para ANPD e Órgãos Fiscalizadores.

Em casos de incidente com risco ou dano relevante aos titulares, a empresa deve:

- Acionar o encarregado de dados (DPO) e o Comitê de Segurança;
- Detalhar a natureza dos dados afetados;
- O que está sendo feito para reverter ou amenizar os efeitos;
- Informar os riscos relacionados;
- Informar sobre os titulares envolvidos;
- Indicar as medidas técnicas e de segurança utilizadas na proteção dos dados;
- Após todo o levantamento, documentar tudo no relatório de incidente de dados, e, se for necessário, reportar a ANPD e aos titulares de dados envolvidos no incidente.

13 ANPD E AS SANÇÕES PREVISTAS NA LGPD

A ANPD (Autoridade Nacional de Proteção de Dados) é um órgão da administração pública federal, dotada de autonomia técnica e decisória, com jurisdição no território nacional e com sede e foro no Distrito Federal, tem o objetivo de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural.



Com funções de natureza normativo-interpretativa, fiscalizatória e integrativa. Além de editar as normas e procedimentos para a proteção dos dados, a ANPD é responsável por solicitar informações sobre o tratamento de dados, fiscalizar e punir casos de descumprimento da lei e ainda promover a cooperação com autoridades de mesma natureza de outros países.

Cabe ainda a Autoridade facilitar a adequação da LGPD para micro e pequenas empresas com normas e procedimentos específicos.

Por oportuno, vale destacar que somente em agosto de 2021 a ANPD poderá aplicar as sanções previstas no Art. 52, **mas não se pode esquecer que outros órgãos poderão fiscalizar e tomar medidas administrativas e/ou judiciais cabíveis em caso de descumprimento da LGPD.**

As sanções previstas na LGPD são as seguintes:

- **Advertência**, com indicação de prazo para adoção de medidas corretivas;
- **Multa simples** de até 2% (dois por cento) 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\$ 50.000.000,00 por infração;

- **Multa diária**, observado o limite total de R\$ 50.000.000,00;
- **Publicização da infração** após devidamente apurada e confirmada a sua ocorrência;
- **Bloqueio** dos dados pessoais a que se refere a infração até a sua regularização;
- **Eliminação** dos dados pessoais a que se refere a infração;
- **Suspensão parcial do funcionamento do banco de dados** a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
- **Suspensão do exercício da atividade de tratamento dos dados pessoais** a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
- **Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.**



14

BENEFÍCIOS DA CONFORMIDADE COM A LEI

- *Proteção, organização e maior gerenciamento dos dados pessoais;*

Mais segurança para seus clientes, funcionários e colaboradores;

- *Marketing coerente com os interesses de sua empresa;*
- *Armazenamento de dados relevantes para o seu negócio (otimização);*

15

O PASSO A PASSO DE UMA IMPLEMENTAÇÃO DE CONFORMIDADE

- *Definir o encarregado de dados (DPO) e Comitê Multidisciplinar;*
- *Elaborar o mapeamento detalhado de entrada e tratamento dos dados (data mapping), sumarizar, segmentar e fragmentar todo caminho dos dados por categoria e acessos;*

- *Identificar riscos (gap's) no tratamento de dados pessoais;*
- *Definir e implantar processos para gestão de incidentes, gestão da comunicação com os titulares dos dados, gestão da comunicação com a ANPD e gestão da Segurança da Informação;*
- *Elaborar os relatórios e documentos previstos em lei;*
- *Elaborar o termo de consentimento específico para obter autorização tratamento de dados pessoais considerados sensíveis pela lei;*
- *Elaborar e definir as políticas de privacidade e uso nos sistemas e aplicativos que efetuam a coleta de dados pessoais para atender a lei;*
- *Treinar as equipes, colaboradores e terceirizados envolvidos quanto às normas e políticas da empresa referentes à proteção e privacidade dos dados;*
- *Analisar contratos de colaboradores internos e externos, incluindo as cláusulas necessárias (internos) e exigir que os fornecedores estejam em conformidade com a LGPD.*



16 CONCLUSÃO

O objetivo desta cartilha é justamente orientar e compartilhar nossa visão e metodologia, de forma condensada, bem como o caminho que entendemos mais eficiente rumo a essa tão alardeada e relevante conformidade com a LGPD, nos inspiramos nas melhores práticas já utilizadas, visando aplicar uma abordagem simples e condizente com a realidade das organizações na busca pela adequação.

Esperamos que tenham gostado e que tomem a decisão mais assertiva para iniciarem o plano de adequação e conformidade com a **LGPD**.



 **Facebook** facebook.com/abadiassoc

 **Instagram** [@abadioficial](https://instagram.com/abadioficial)

 **Facebook** facebook.com/secovi.rio

 **Instagram** [@secovirio](https://instagram.com/secovirio)



**QUAL O
IMPACTO
NA MINHA
EMPRESA?**

CARTILHA LEI GERAL DE PROTEÇÃO DE DADOS

