



LGPD:

um desafio para as empresas

Da proteção de dados pessoais
à privacidade



Índice

3

Introdução

4

1. Enfim, sem mais tardar, nasce a LGPD

8

2. Aplicação da LGPD nas empresas

11

3. Processos, ferramentas e multas

15

Conclusão

Introdução

Pensar em segurança digital, proteção de dados e privacidade passou a ser uma necessidade e uma tarefa diária, principalmente para as organizações.

Durante os últimos anos, vimos como o processo de tratamento de dados pessoais de usuários, tanto em serviços como em redes sociais, passou a ganhar importância no mundo virtual, principalmente após o escândalo de uso político de dados envolvendo o Facebook e a Cambridge Analytica. Alguns especialistas em segurança afirmam que os dados pessoais passaram a ser o “novo petróleo” em nossa sociedade digital.

Diante desse cenário, em todo o mundo, empresas tiveram que adotar medidas que pudessem abordar o processo de tratamento de dados pessoais de seus usuários. A Europa é um exemplo bastante claro disso, já que as empresas que fazem parte dos países da União Europeia passaram a ser acompanhadas pelo Regulamento Geral sobre a Proteção de Dados (GDPR, sigla em inglês). No Brasil não foi diferente, em setembro de 2020 entrou em vigor a Lei Geral de Proteção de Dados (LGPD) que estabelece regras para uso, proteção e transparência de informações pessoais no país.

As ameaças à informação, brechas de segurança e vazamentos de dados são incidentes que ocorrem diariamente com empresas de todos os portes, podendo comprometer os dados pessoais de usuários. Além disso, caso isso se torne público, pode ainda impactar de forma negativa a reputação de uma companhia, tornando-a menos confiável e mostrando que aquela empresa não trata as informações sensíveis de clientes com o devido cuidado.

A LGPD, como toda lei, traz consigo sanções e multas, apesar disso muitos negócios estão sendo notificados por órgãos responsáveis pelo direito do consumidor, o que mostra que ainda há muito trabalho a ser feito. Um estudo realizado em junho e julho de 2020, aponta que [64% das empresas brasileiras não estão em conformidade com a Lei Geral de Proteção de Dados](#), o que representa uma grande parcela de companhias que precisam de ajuda e um melhor entendimento sobre a lei para poderem adequar seus processos e forma de negócio.

Neste guia, temos o objetivo de auxiliar empresas e organizações para que conheçam o cenário no qual a LGPD foi inserida, como se adequar a nova lei e quais são os desafios para o seguimento corporativo em relação a essa nova realidade.

1 Enfim, sem mais tardar, nasce a LGPD

Contextualização e vigência

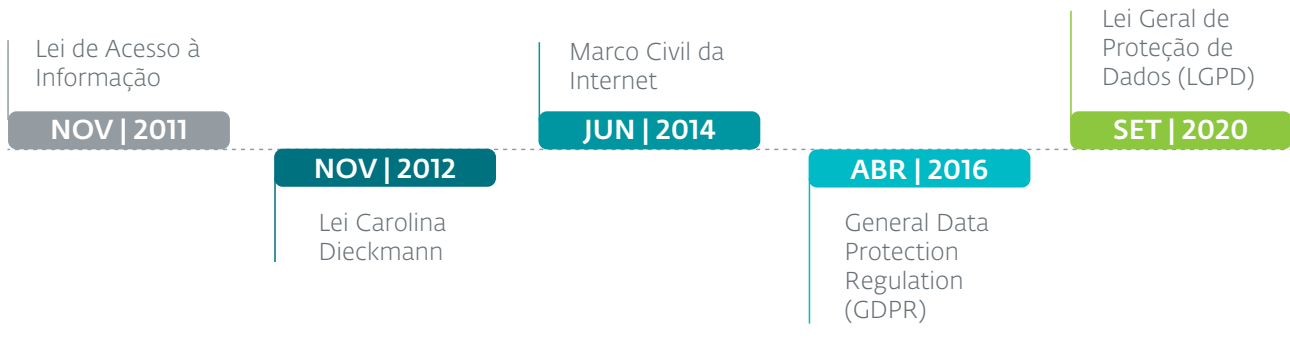
O cenário de regulamentação para a proteção de dados ganhou destaque em 2016 com a GDPR. Naquela época, o mundo encontrava-se em meio aos escândalos de privacidade que envolviam o Facebook e a Cambridge Analytica, o que trouxe bastante visibilidade e discussão sobre o assunto.

Em meio a um clima de repercussão de incidentes à nível mundial envolvendo a proteção e a privacidade de dados pessoais, o assunto também acabou entrando na pauta da política brasileira, já que o país, até aquele momento, não contava com uma legislação específica que pudesse garantir a segurança de dados de usuários e estabelecer responsáveis pelo tratamento desse tipo de informação. Anteriormente, o Brasil chegou a contar com outras legislações que garantiam o direito à privacidade, como a Lei de Acesso à Informação (2011), Lei Carolina Dieckman (2012) e o Marco Civil da Internet (2014), mas nada tão específico.

Inicialmente, a LGPD chegou para alterar o Marco Civil da Internet, que regulava essas transações até então. Em agosto de 2018, a lei nacional de proteção de dados foi divulgada pelo Diário Oficial da União. No entanto, apesar de ter sido sancionada, houve o veto à criação da Autoridade Nacional de Proteção de Dados (ANPD) e, além disso, a regulamentação só entraria em vigor em fevereiro de 2020, ou seja, apenas 8 meses após a data oficial de sanção.

Ainda em 2018, o então presidente Michel Temer promulgou uma medida provisória e autorizou a criação da ANPD, estendendo também o prazo de vigência da nova lei para agosto de 2020.

Depois de diversas reviravoltas na data de vigência da LGPD, em setembro de 2020, principalmente em decorrência da pandemia de Covid-19, o Projeto de Lei (PL) 1179/2020 foi sancionado e convertido na Lei nº 14.010/2020, mantendo a vigência da LGPD para agosto de 2020 (data retroativa), mas com a condição de que as multas e sanções apenas começassem a valer a partir de agosto de 2021.



O que é a LGPD e quais princípios norteiam a nova lei?

A Lei Geral de Proteção de Dados estabelece regras sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais, impondo mais proteção nos processos e aplicando penalidades para os casos de não cumprimento. A nova lei se aplica a qualquer pessoa, física ou jurídica (pública ou privada) que faça o tratamento de dados pessoais, destacando-se como um dos grandes marcos sobre a proteção e privacidade de dados no Brasil.

Para entender a LGPD, também é fundamental compreender a interpretação da lei em relação a dados pessoais:



Dados pessoais: são os dados que permitem a identificação direta ou indireta de uma pessoa, como RG, CPF, passaporte, carteira de habilitação, endereço, telefone, e-mail, IP e até mesmo cookies.



Dados pessoais sensíveis: o artigo quinto da LGPD prevê que sejam considerados dados sensíveis todos aqueles que façam referência a "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".

A LGPD usa de direitos fundamentais de liberdade e de privacidade como parâmetro para as regras a respeito da coleta e armazenamento de dados pessoais, incluindo também o compartilhamento desse tipo de informação. Nesse contexto, existem 10 princípios que norteiam o processo estabelecido para o tratamento de dados pessoais, de acordo com a LGPD. Cada organização ou empresa deve respeitar esses princípios para estar em conformidade com a lei, considerando o cuidado na forma de coleta e tratamento de dados pessoais de seus clientes.

1

Finalidade

Só é possível trabalhar com dados de clientes para propósitos legítimos, específicos, explícitos e informados ao titular dos dados, sem possibilidade de tratamento posterior que seja incompatível com suas finalidades.

2

Adequação

O uso dos dados deve ser compatível com as finalidades informadas ao titular, de acordo com o contexto do negócio. A justificativa de coleta e tratamento dos dados deve fazer sentido com o caráter das informações solicitadas pela empresa.

3

Necessidade

As empresas apenas devem solicitar dados de clientes que sejam estritamente necessários para alcançar as suas finalidades. É preciso fazer uma ponderação entre o que é realmente essencial para o negócio. Resumindo, os dados armazenados devem atender ao princípio da necessidade.

4

Livre acesso

O cliente ou titular dos dados tem o direito de consultar, de forma simples e gratuita, todos os dados que a empresa detenha a seu respeito. Os dados devem poder ser acessados pelo usuário a qualquer momento. Além disso, o titular deve saber o que a empresa faz com os seus dados e de que forma o tratamento é realizado e por qual período.

5

Qualidade dos dados

É uma espécie de complemento do princípio anterior. Neste caso, o cliente deve poder atualizar, completar ou excluir dados que estejam incorretos ou sejam incompatíveis, garantindo a qualidade de seus dados. É fundamental ter atenção, exatidão, clareza e relevância dos dados nesse processo, tendo em conta a necessidade e a finalidade de seu tratamento.

6

Transparência

Trata-se do direito do cliente de ser informado e entender de forma clara e transparente como os dados serão tratados e quais os responsáveis pelo processo. Esse princípio também inclui a transparência em casos de incidentes de segurança sofridos pela empresa, como casos de vazamentos de dados. Além disso, a empresa não pode compartilhar dados pessoais com outras pessoas ou empresas sem que o titular seja informado.

7

Segurança

Os dados pessoais devem ser tratados de uma forma que garanta a devida segurança e confidencialidade, incluindo evitar o acesso a dados pessoais ou equipamentos usados para o seu tratamento ou o uso dos mesmos por pessoas não autorizadas. Essa etapa deve evitar qualquer tipo de incidente de segurança como vazamento de dados, roubo ou mesmo a distribuição das informações. O papel das empresas é buscar procedimentos, meios e tecnologias que garantam a proteção e segurança dos dados pessoais.

8

Prevenção

Além de toda a tecnologia e da inversão em sistemas que sejam adequados, as equipes que compõem as empresas devem ser treinadas para que o tratamento de dados ocorra de forma eficaz. Por exemplo, o ideal é realizar a restrição de dados dentro das áreas para que nem todos os departamentos tenham acesso aos dados de clientes. O objetivo é evitar a ocorrência de danos em virtude do tratamento de dados pessoais durante o processo interno. Resumindo, as empresas devem tomar medidas antes que ocorra qualquer tipo de incidente que possa comprometer os dados pessoais de seus clientes.

9

Não discriminação

Um pouco fora da estrutura de sistemas, esse princípio faz referência a forma como os dados são utilizados. Ou seja, as empresas não podem utilizar esse tipo de dado como forma de discriminação ou promover qualquer tipo de abuso contra os seus titulares. A LGPD criou regras específicas para o tratamento de dados pessoais sensíveis, como os que tratam sobre origem racial ou étnica, religião, opinião política, saúde, entre outros.

10 Responsabilização e prestação de contas

Trata-se da prestação de contas tanto aos clientes como também as autoridades sobre o que acontece na empresa em relação ao cumprimento da LGPD. É necessário demonstrar à Autoridade Nacional de Dados que os objetivos propostos foram cumpridos. Neste caso, as empresas devem ter provas e evidências de todas as medidas implementadas.

LGPD (brasileira) x GDPR (europeia)

Como já mencionamos, a LGPD é baseada na lei de regulamentação europeia, a GDPR, uma das maiores referências de uma lei de proteção de dados no mundo. Apesar disso, as duas regulamentações contam com diferenças, principalmente se tivermos em conta os cenários nos quais são aplicadas.

Veja algumas comparações entre a LGPD e a GDPR:

		
 Tratamento de dados de menores	Todas as crianças menores de 18 anos devem contar com o consentimento dado pelos pais ou responsáveis.	Aceita o consentimento dado por crianças, desde que tenham pelo menos 16 anos. Para o caso de menores de 16 anos, o consentimento deve ser dado pelos pais.
 Abrangência	Nacional.	Internacional.
 Transferência internacional de dados	A lei estabelece apenas diretrizes genéricas que devem ser acompanhadas pelas autoridades nacionais.	A transferência internacional de dados pessoais pode ser realizada independente de autorização específica no caso de que a comissão europeia reconheça que o país terceiro garante um nível de proteção devidamente adequado.
 Multas	Até 2% do faturamento com limite de R\$ 50 milhões.	De € 10 milhões, ou o máximo de 2% do faturamento anual, podendo chegar a € 20 milhões, com o máximo de 4% do faturamento anual.

2 Aplicação da LGPD nas empresas

Para entender o processo de adaptação e aplicação da LGPD nas empresas, é necessário ter em conta alguns aspectos: atores envolvidos, ciclo de vida e a forma de tratamento de dados pessoais. Por isso, é fundamental que as empresas possam implementar ações para a melhoria e segurança dos processos destacados pela nova lei.

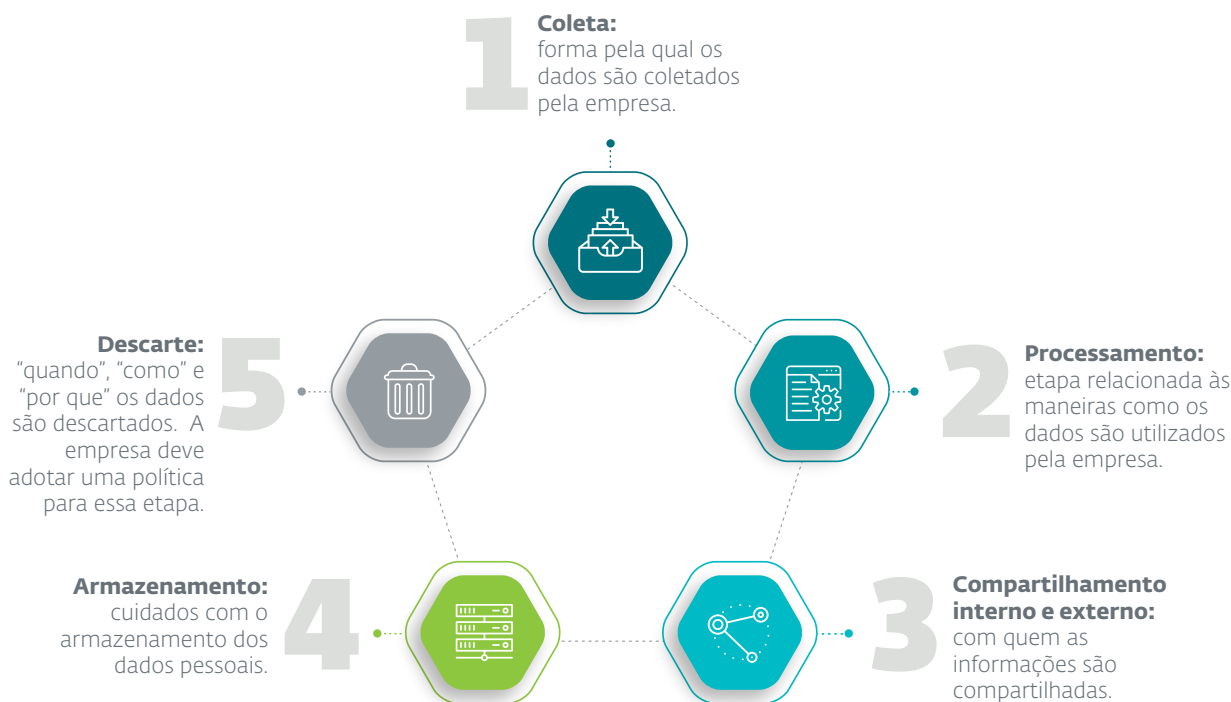
Quem são os atores envolvidos na LGPD?



Ciclo de vida de dados pessoais previstos na LGPD

O ciclo de vida de dados pessoais é algo abordado na LGPD. Esse processo envolve todas as informações pessoais que transitam (desde a coleta até o descarte) por uma empresa ou organização, ou seja, todo o período em que os dados pessoais do titular são armazenados na empresa.

Ao total, existem 5 ações que podem resumir esse processo:



Com a LGPD, como as empresas podem tratar dados pessoais?

O primeiro ponto a ser levado em consideração sobre a manipulação dos dados pessoais é que, para que possam ser coletados, é necessário o consentimento expresso do titular. O consentimento se aplica sempre a uma finalidade, impossibilitando o uso de uma aprovação genérica. Caso seja necessário usar os dados do titular para outros fins é necessário que haja uma nova aprovação do titular.

A grande maioria das bases já possuem dados de diversos titulares. Os dados previamente existentes também deverão receber autorização dos titulares para serem mantidos, tratados e processados.

Para assegurar que os dados sejam tratados adequadamente será necessário que cada empresa conte com o auxílio de um *Data Protection Officer* (DPO) ou encarregado. Esse profissional deve estipular quais serão as formas mais adequadas para o tratamento dos dados desde o momento em que são recebidos até seu armazenamento ou eventual descarte. Ele também deve ter autonomia para exercer mudanças, caso necessárias, e intermediará o contato da autoridade responsável por fiscalizar a proteção dos dados pessoais e a empresa.

Os dados também poderão ser tratados para os seguintes fins:

-  Cumprimento de obrigação legal ou regulatória do controlador.
-  Execução de políticas públicas pela administração pública.
-  Realização de estudos por órgãos de pesquisa.

-  Quando necessário para execução de contrato ou procedimentos preliminares a um contrato do qual seja parte o titular, a pedido do titular.
-  O exercício regular de direitos em processos judiciais, administrativos ou arbitrais.
Proteção da vida ou da incolumidade física do titular ou de terceiros.
-  Tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias.
-  Quando necessário para atender aos interesses legítimos do controlador ou de terceiros, salvo quando prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção de seus dados pessoais.
-  Para proteção do crédito.

3 Processos, ferramentas e multas

Para se adequar à LGPD, primeiro temos que ter em mente qual é o ramo ou segmento no qual determinada empresa atua, pois cada um deles possui riscos e necessidades de processos específicos. Apesar da lei ser para todos, a forma como organizações entrarão em conformidade com a regulamentação pode ser totalmente distinta. Não existe uma receita para se adequar à lei e sim processos e etapas que são essenciais independentemente do tipo de empresa que estamos lidando.

Confira alguns desses processos:

1 Conscientização e capacitação

Mostrar aos funcionários, desde cargos mais baixos à alta diretoria, a importância da LGPD. Isso pode ser feito através de treinamentos para cada setor, workshops e ações dentro da empresa, de acordo com o porte da companhia.

2 Mapeamento de dados

Nessa etapa, é necessário saber quais funcionários manipulam em seu dia a dia dados de terceiros e entender o fluxo dessas informações. Algumas perguntas devem ser feitas aqui: Quando esses dados entraram na empresa? Quem obteve acesso a eles? São compartilhados ou não? Possuem alguma segurança para seu uso? Onde estão armazenados? São dados úteis ou já podem ser descartados? Todas elas são questões primordiais para compreender o volume e o uso de dados pessoais de clientes.

3 Análise de brechas

Após a conclusão da segunda fase, é preciso analisar quais situações podem vir a ser um problema para a organização e entender como resolver cada uma delas.

4 Plano de ação

Definir prioridades, analisar maiores riscos e começar a agir segundo os casos mais urgentes

5 Implementação

É hora de colocar a mão na massa. Após todos da empresa entenderem a importância do tratamento de dados, mapeamento de informações, análise de possíveis vulnerabilidades e riscos, estabelecimento de um plano de ação, chega o momento de começar a implementar tecnologias, ferramentas e mudança de processos para que a adequação seja realizada com sucesso.

6 Monitoramento

Essa fase não conta com uma “conclusão definitiva”, ou seja, precisa estar em constante mudança e controle para que todos os passos realizados tenham valido a pena. O encarregado de administrar os dados, também conhecido como *Data Protection Officer* (DPO), deve estar atento a quais novos dados entram na empresa, qual a política de privacidade para eles, quem tem acesso a essas informações, se há necessidade de alterar algum dos pontos acima, enfim, é realmente preciso monitorar o tratamento dos dados e seus processos de maneira frequente.

Ferramentas

As ferramentas que podem ser utilizadas para a adequação à LGPD, da mesma forma que os processos, variam de acordo com a forma de trabalho e o porte da empresa. Algumas organizações podem contar com as tecnologias de proteção citadas abaixo e outras podem não ter noção nenhuma sobre como ou o porquê utilizar essas ferramentas, por isso, é importante citar e explicar algumas delas.



Firewall

Uma das soluções mais básicas de segurança e que deveria fazer parte de todo e qualquer ambiente. As versões mais tradicionais de firewall baseiam suas regras em IPs e portas, e têm papel essencial na proteção do entorno de rede. O firewall permite proteger as informações através do monitoramento e da restrição de IPs maliciosos que estejam tentando se comunicar com a rede ou impedindo que usuários internos tenham acesso a endereços maliciosos na Internet.



Soluções de proteção de endpoint

Boa parte dos ataques mais comuns são interrompidos quando se tem esse tipo de solução nos equipamentos; se a solução por si só já interrompe boa parte dos ataques, consequentemente também impedirá que o criminoso tenha acesso a informação que está sendo protegida.



WAF/DBF

As siglas representam *Web Application Firewall* e *Database Firewall*, que em tradução livre significam Firewall de aplicação Web e Firewall de Banco de Dados, respectivamente. Essas são ferramentas mais avançadas de detecção e conseguem impedir, por exemplo, consultas em larga escala em partes do site onde não deveria haver esse comportamento, tentativa de enumeração de banco de dados, inserção de caracteres em excesso em formulários e diversos outros recursos úteis que podem impedir que suas aplicações se comportem de forma anormal a ponto de um criminoso conseguir extrair dados dela.



Proteção física e Criptografia

A proteção física pode ter muitas abordagens, desde uma porta que impeça que curiosos acessem os computadores principais ou servidores, até proteção perimetral envolvendo câmeras de segurança, catracas, controle biométrico e uma série de outros dispositivos. Todos os recursos empregados têm somente um destino, garantir acesso aos meios físicos somente a pessoas autorizadas.

Como nenhuma das soluções de segurança é a prova de falhas, a proteção física não é uma exceção. Caso um criminoso consiga ter acesso às mídias físicas que contêm os dados sigilosos, elas também devem estar adequadamente protegidas por meio de criptografia, para que mesmo que os criminosos tentem o acesso lógico aos dados, eles sejam impedidos pela necessidade de senha exigida para descriptografá-los.



Múltiplo fator de autenticação (senhas)

Uma das formas para barrar acessos indevidos é adicionar um fator à autenticação, como, por exemplo, uma senha temporária gerada em um app que o usuário tenha. Dessa forma, além da senha do usuário em si, o criminoso precisaria desse token para realmente acessar o ambiente, tornando-o bem mais seguro mesmo em casos de vazamentos de senhas. Também é possível adotar uma política de uso de senhas complexas e impor uma adequação a todos os usuários, sem exceção.



Gestão/Distribuição de patch e atualizações

Apesar de atuarem de forma indireta, as soluções de gestão e aplicação de patches são pontos importantes para a saúde de um ambiente e auxiliam na prevenção de acessos ilegítimos. Muitos softwares em suas versões antigas possuem falhas que, se exploradas adequadamente, podem conceder acesso indevidos aos criminosos.



DLP

Os *Data Loss Prevention*, que em tradução livre significa Prevenção contra Vazamento de Dados, como o nome sugere, impedem que os dados mais importantes para a empresa não sejam trafegados sem o devido consentimento. Eles podem impedir que, por exemplo, determinados arquivos sejam enviados para um pen-drive ou HD externo, que informações sejam coladas em e-mails, ou que determinados tipos de dados sejam carregados em formulários na Internet. As aplicações desse tipo de ferramenta diminuem drasticamente a chance de exposição de dados sigilosos de forma intencional ou acidental.



Desenvolvimento seguro e revisão de código

Esse ponto não é exatamente uma tecnologia de segurança, apesar de ser possível contratar revisões de código focadas em segurança, mas é parte importante de um ambiente para empresas que desenvolvem suas próprias aplicações ou compram/contratam aplicações personalizadas para seu ambiente. Aplicar segurança desde o desenvolvimento diminui consideravelmente as chances de problemas com pontos vulneráveis, seja para o armazenamento/tratamento dos dados recebidos, ou para evitar que partes da aplicação sofram com ataques ao buffer.

Multas e sanções

A entrada em vigor da LGPD estabeleceu um importante marco para a história da proteção de dados no Brasil, principalmente tendo em conta os diversos casos de incidentes de segurança envolvendo informações pessoais e sensíveis de clientes. O não cumprimento da LGPD pode caracterizar sérios problemas para uma empresa.

Em primeiro lugar, desde os pontos de vista jurídico e financeiro. Para entender melhor em números, as empresas que não se preocuparem com a privacidade e segurança dos dados podem chegar a pagar até 2% do faturamento do último exercício fiscal – valor limitado a R\$ 50 milhões.

Quem aplica essas multas é a ANPD que notifica os agentes de tratamento (controlador e operador) caso a LGPD não seja cumprida. Existe uma série de sanções que vão desde advertências com o objetivo de indicar um prazo para adoção de medidas corretivas e multas simples – citada acima – incluindo multas diárias com limite de R\$ 50.000.000,00 até a suspensão parcial ou total e ainda proibição do tratamento de dados por parte da empresa.

Além do pagamento de multas, o não cumprimento da LGPD pode acabar afetando a reputação de uma companhia e, mais ainda, a confiança que os clientes têm quanto a segurança de seus dados pessoais e privacidade, causando danos irreversíveis para a marca.

Conclusão

A LGPD representa um divisor de águas quando nos referimos a segurança de dados pessoais no Brasil.

Nunca se discutiu tanto a importância da **proteção de dados** e os cuidados com a **privacidade**, dois fatores que ao longo dos últimos anos se tornaram fundamentais para os processos corporativos em todo o mundo. O intuito deste documento foi apresentar a LGPD de forma simples e objetiva, destacando aspectos básicos como seus princípios, atores, estruturas, impactos e, principalmente, como as empresas podem **compreender este novo processo** e **direcionar ações de conformidade** com as novas determinações.

O processo de adequação das empresas não é responsabilidade apenas das equipes de Tecnologia da Informação (TI), mas também deve ser visto e tratado com todas as áreas que compõem uma organização. Cada colaborador, independentemente de sua área, pode ter um papel fundamental nesse processo que se tornou **necessário e urgente**. A adequação exige maturidade por parte de todos os envolvidos a fim de evitar possíveis incidentes de segurança e consequências legais e de reputação.

É necessário que as empresas estejam preparadas e com seus processos voltados para a criação de canais, mecanismos e serviços seguros. Os consumidores estão cada vez mais cientes da responsabilidade que as empresas devem ter com a proteção de seus dados.

SOBRE A ESET

+ 110 milhões
de usuários em todo o mundo

13
centros de pesquisa e
desenvolvimento no mundo

+ 400 mil
clientes corporativos

200
países e territórios

Para mais informações sobre a ESET, visite: www.eset.com/br