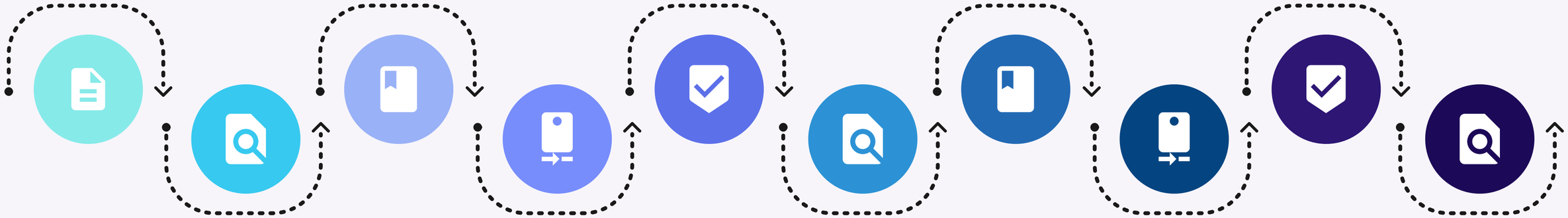
Guia de adequação à LGPD

8 Passos

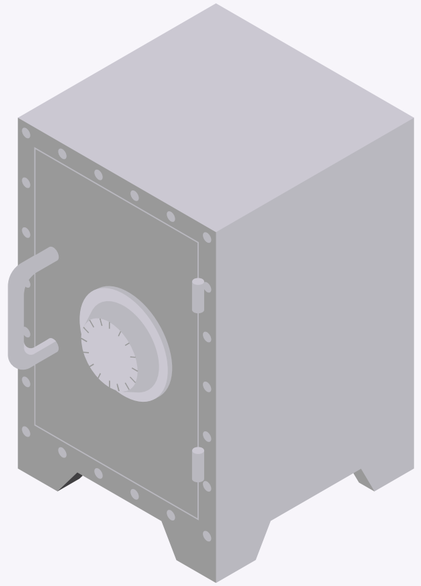
Para desenvolver uma cultura de proteção de dados

EJUR
SOLUÇÕES JURÍDICAS

SUMÁRIO



O que é a Lei Geral de Proteção de Dados?



A **Lei nº 13.709** surgiu a fim de **padronizar** normas e práticas adotadas que visam oferecer uma **segurança jurídica** e uma **proteção aos dados pessoais** coletados no Brasil. Os impactos são essenciais, tanto para os portadores dos dados, quanto para as empresas, para que se evite futuros problemas com vazamento de dados.

A LGPD assegura direitos tanto para **dados virtuais**, quanto para **dados físicos**. Entre as ações proibidas pela nova lei estão a coleta, o uso e o armazenamento de dados **sem o consentimento do portador**.

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular;

A linha do tempo da Lei Geral de Proteção de Dados

Foi **sancionada** no Brasil em **14 de agosto de 2018**, pelo então presidente Michel Temer

2018

2020

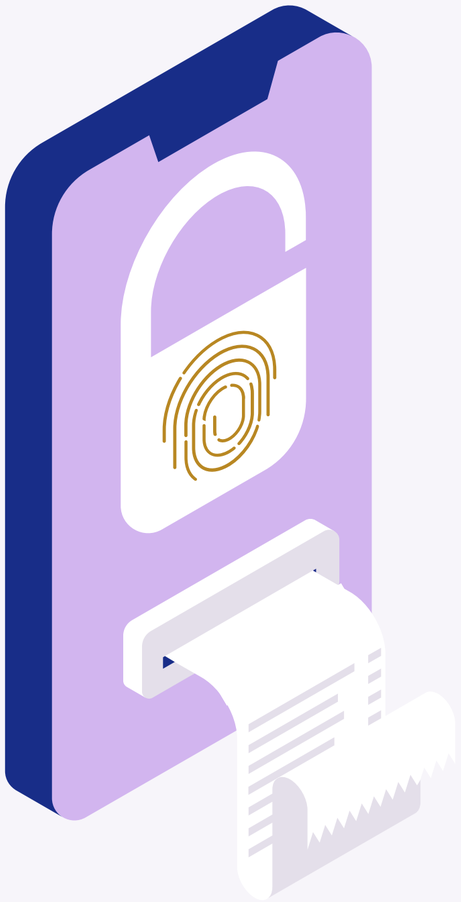
A lei **entrou em vigor** dia **18 de setembro de 2020**

As **sanções** previstas na LGPD são aplicáveis a fatos ocorridos **após 1º de agosto de 2021**

2021

A quem a lei se aplica?

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.



A LGPD se aplica a todos os cidadãos brasileiros ou estrangeiros independente de sexo ou idade, como também empresas de todas as naturezas.

Protege **todas as pessoas (físicas e jurídicas)** que possuem informações particulares atreladas a um tratamento de dados **realizado em território nacional**.

Quais são os dados que a lei contempla?

Dados Pessoais

Toda informação relacionada à pessoa natural (física) identificada ou identificável

Nome completo, e-mail, telefone, RG, CPF, endereço, e dados indiretos como endereços de IP e geolocalização

Dados Sensíveis

Esses dados exigem um consentimento específico dos titulares

Origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato, organização de caráter religioso, filosófico ou político, vida sexual, dado genético ou biométrico

Dados Anonimizados

Dado relativo a titular que não permite ser identificado; perdem a possibilidade de associação, direta ou indireta, a um indivíduo

Estatísticas sobre a idade de pessoas que acessaram o site da empresa

Dados Pseudo-Anonimizados

Semelhante aos dados que perdem a associação; entretanto, é incentivado pelo próprio regulamento como forma de reduzir os riscos

Dados pessoais salvos em uma nuvem

Direito dos Titulares

CORREÇÃO DOS DADOS

O titular pode solicitar à empresa a correção de dados pessoais incompletos, inexatos ou desatualizados. Como por exemplo, atualizações de endereços, número de telefones ou estado civil

ANONIMIZAÇÃO, BLOQUEIO OU ELIMINAÇÃO DE DADOS

O titular pode solicitar a anonimização dos dados, não havendo a possibilidade de vinculá-lo ao indivíduo. Também é possível solicitar o bloqueio ou a eliminação de dados quando forem desnecessários ou tratados em desconformidade com a lei

CONFIRMAÇÃO DE ACESSO

O titular pode solicitar a confirmação da existência de tratamento e acesso aos seus dados pessoais através de informações claras sobre a origem dos dados e existência de registro

Direito dos Titulares

PORTABILIDADEDE

A Lei ainda prevê que o titular de dados pode solicitar a portabilidade de seus dados, dessa forma, solicitando a transferência de seus dados pessoais

COMPARTILHAMENTO

Caso queira, o titular pode solicitar informações sobre as entidades com as quais seus dados são compartilhados

REVOGAÇÃO DE CONSENTIMENTO

Ainda, o titular tem direito, caso queira, revogar o consentimento dado para o tratamento de dados pessoais, mediante solicitação

DIREITO À INFORMAÇÃO

É direito do titular saber exatamente como o controlador utiliza seus dados e como ele o compartilha, devendo ser expressamente nomeado

O que acontece se a minha empresa não se adequar à LGPD?

As sanções previstas pela LGPD, dispostas nos artigos 52 a 54 da lei, começaram a sua vigência no dia **1º de agosto de 2021**. Os agentes de tratamento de dados que cometerem infrações previstas serão sujeitos à aplicação das seguintes sanções pela autoridade nacional:

Advertência com indicação de prazo para adoção de medidas corretivas;

Multa simples de até 2% do faturamento da empresa no seu último exercício, excluídos os tributos, e limitada no total de R$50.000.000,00 por infração;

Multa diária observado o limite previsto no item acima;

publicização da infração cometida;

Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

Eliminação dos dados pessoais aos quais se refere a infração.

Agora que você já conhece a LGPD, siga os 8 passos para adequar a sua empresa!

Passo 01

Identifique os momentos de Coleta de Dados da sua empresa

A coleta de dados é um mecanismo de pesquisa para a **elaboração do planejamento para desenvolvimento do negócio** e da sua atuação no mercado. Por meio da análise a ser elaborada, em face das informações recolhidas, é possível **estudar e reconhecer os indicadores-chave de desempenho**, os **KPI's** (*Key Performance Indicator*) – fundamentais para compreender a condução das atividades.

Como, por exemplo:

Taxa de Conversão

Ou apenas "win rate", define os leads convertidos em vendas finais.

Custo de aquisição de clientes

Calcula a relação entre o gasto publicitário e seu retorno em clientes.

Churn Rate

Mede a proporção de evasão de clientes.

Net Promoter Score (NPS)

Indica a probabilidade de indicação de sua marca a outras pessoas.

Essa coleta pode acontecer de diferentes maneiras. Sendo sua periodicidade maleável à *necessidade*, podendo acontecer de maneira contínua, alternada ou ocasional, suas metodologias variam entre fatores de qualidade e tempo. Em metodologias primárias, a procura é por **informações atuais contabilizados para usos específicos**. É nesse cenário que a coleta de dados de terceiros realiza sua performance:

PESQUISAS ONLINE

SONDAGEM

ENTREVISTAS

QUESTIONÁRIOS

Além de mecanismos como o requerimento de nome e e-mail por **LANDING PAGE**, o uso de **COOKIES**, a inscrição para recebimento de **NEWSLETTER**, os disparos de **MAILING** para prospecção de clientes.

Para as metodologias secundárias, que reaproveitam **dados antigos para estudo**, fontes internas como **conteúdos contratuais e resumos executivos** podem ser apontados como coletas de dados.

A importância de que essas ferramentas sejam identificadas na conduta da empresa está no **mapeamento de possíveis infrações** ao reconhecimento do **consentimento do usuário** que possui seus dados apurados. Ao prezar pelo direito à privacidade, a **LGPD** faz com que essas estratégias precisem passar pelo **filtro da autorização prévia** e, nesse sentido, avaliar como a abordagem do *marketing digital*, por exemplo, pode conflitar esses elementos é essencial para a garantia da segurança jurídica do negócio!

Passo 02

Avalie os riscos e previna um possível vazamento de dados

A máxima “riscos são inerentes aos negócios”, não é mais novidade para os que pretendem empreender!

No entanto, os riscos relacionados ao **vazamento de dados** é uma realidade recente para os **médios e pequenos negócios**. O motivo desses riscos constituírem uma nova preocupação para os empreendedores que não lidam apenas com multinacionais, é que os dados pessoais, atualmente, são os **ativos comerciais mais valiosos** de um empreendimento.

Desta forma, as empresas não devem encarar a estruturação de um sistema de proteção de dados como meros gastos, mas como **investimentos que podem resguardar o negócio de sanções administrativas** estabelecidas em Leis e da perda de credibilidade no mercado.

A principal estratégia utilizada pelas empresas no **contingenciamento de riscos** de ameaças e ataques cibernéticos é a **Estrutura de Segurança Cibernética do NIST**, sendo este o sistema de gerenciamento utilizado pelas empresas privadas dos Estados Unidos, Japão e Israel. O funcionamento do NIST consiste em **cinco funções primárias**.

Todas estas funções, que visam a gestão de riscos da informação coletada e armazenada pela empresa, são estruturadas de forma personalizada para se considerar a realidade do empreendimento em questão.

A partir da **Estrutura de Segurança Cibernética do NIST**, quando houver um vazamento de dados ou situação similar que coloque em *risco* a segurança de dados financeiros, clientes, fornecedores ou até mesmo segredos de negócios, é de suma importância que o empreendimento conte com um **Plano de Respostas a Incidentes**. Este documento, elaborado com **antecedência** e pensado conforme a gestão corporativa de cada negócio, é responsável por **nortear a administração** a responder a falha na segurança de **forma mais rápida possível**, com objetivo de minimizar as informações perdidas.

Passo 03

Atente-se aos Controladores de Segurança

Evitar ao máximo qualquer vazamento de informações é a meta que não se deve deixar de lado, prevenindo, assim, todas as sanções agora aplicáveis pela lei, as quais podem ir muito além do financeiro. Para isso, é necessário se ter em mente a importância dos **controladores de segurança**, tais como o **firewall**, o **antivírus**, o **antispam** e o **backup**. Todos eles, em conjunto, auxiliarão na *prevenção de incidentes de dados e de crimes cibernéticos*.

1. **Firewall**
é a primeira linha de defesa que um sistema pode possuir.

2. **Antivírus**
detecta e remove programas maliciosos.

3. **Antispam**
impede a chegada de mensagens indesejadas.

4. **Backup**
faz a prevenção contra a perda dos dados importantes.

1

Firewall

Através de um hardware ou um software, o **firewall** trabalha para **conter o alastramento dos vírus** e evitar que esses cheguem a outros dispositivos. Agindo como um verdadeiro **filtro**, o firewall estabelece *quais informações podem entrar ou sair* da rede privada a partir das **instruções e regras de acesso** determinadas pela empresa ou administrador, liberando ou bloqueando sites e monitorando o comportamento do funcionário dentro do sistema, por exemplo.

Assim, torna-se uma ferramenta aliada à segurança de dados, tendo em vista que grande parte das **rotinas de trabalho** das empresas precisam da internet - um ambiente de grande risco - e se interessam pela **otimização do trabalho**, o que também pode ser alcançado, uma vez que o controlador distribui o **acesso aos colaboradores** de modo **estratégico**.

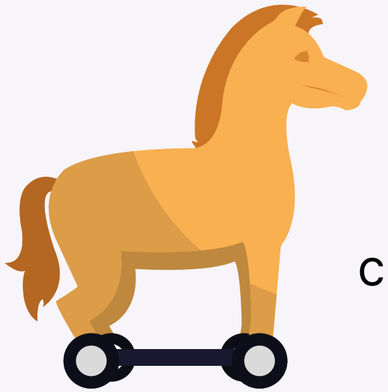
2

Antivírus

O **antivírus** é aquele o software **protege os aparelhos de códigos e vírus** cuja finalidade é interferir no funcionamento dos dispositivos para, não apenas **corromper**, mas **destruir** os dados ou transferir informações para outros locais. Como os vírus podem adentrar o dispositivo através de muitos meios - desde sites a pen drives - essa ferramenta é imprescindível para a **proteção das informações**, dado que possui agilidade na **detecção** e contenção de ameaças virtuais, podendo fazer essa varre-dura através do **escaneamento de vírus** já conhecidos (*cujas informações já foram estabelecidas no software do antivírus*), de um **sensoriamento heurístico** (*o qual busca instruções não executáveis nos programas usuais do dispositivo*), de uma **busca algorítmica** ou de uma **checagem de integridade** (*registrando os dígitos verificadores e funcionando, futuramente, como um "anticorpo"*).

Vista a **relevância** desse controlador, é proveitoso que a empresa estude a **possibilidade do antivírus corporativo,** uma alternativa interessante para aquelas que trabalham com **grande volume de dados** e dispositivos. Diferentemente dos antivírus comuns, os corporativos agem de **forma centralizada**, não protegendo apenas o computador, mas **toda a rede**. Dessa forma, além de facilitar a gestão do TI, livram de ameaças todos os aparelhos conectados a ela e criam uma **barreira de segurança** de todos os ângulos, proporcionando uma prevenção mais completa.

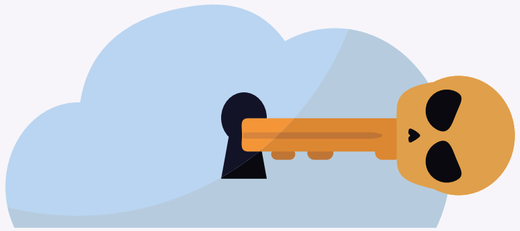
3



Antispam

O **antispam** bloqueia **mensagens indesejadas**, provindas de comportamentos na internet para a propagação de notícias falsas até de e-mails cheios de publicidade - também conhecidos como *junk mails* - que, além de prejudicar a produtividade - uma vez que os e-mails importantes se perdem em meio à massa de propaganda - podem ser utilizados para práticas ilegais, como **golpes e fraudes**. Esse tipo de ataque é conhecido com *phising* e, nele, ao enviar o texto, o golpista tem como objetivo fazer com que a vítima clique em um link, baixe um arquivo, faça um pagamento ou envie informações solicitadas a fim de **obter informações pessoais ou confidenciais**. Com esses dados em mãos, muitos também cobram por resgate, mas mesmo após a entrega do valor, **não devolvem as informações**, gerando um **grave** incidente na proteção de dados e na segurança interna.

4



Backup

Por fim, tem-se o **backup**, o ato de copiar arquivos e **armazená-los** em sistemas secundários, **prevenindo a perda dos dados** em qualquer problema que houver. Ele é estritamente importante, pois fornece a oportunidade de se ter **cópias de segurança** em mais de um dispositivo fora do sistema principal, dando a possibilidade de **recuperação** dos dados em caso de desastre. Além de também poder ser feito por meio de um *hardware* ou *software*, atualmente existe o serviço de manter seus dados numa **nuvem**, opção automática e regular. No entanto, fornecer todos os dados que sua empresa possui para terceiros pode ser uma ideia desagradável para muitos; assim, optam por adquirir seus próprios ***datacenters***, o que pode ser um custo relativamente alto. Logo, os métodos devem ser estudados a fim de se encontrar a melhor opção, **mas sem nunca deixar de fazê-lo**.

Passo 04

Possua uma Política de Privacidade

A **política de privacidade** pode ser entendida, basicamente, como um **contrato de adesão** na qual são assumidos **direitos e deveres** unilateralmente e insuscetíveis de serem negociados, uma vez que a aceitação ou recusa depende da contraparte, mas que fica impossibilitada de influenciar na elaboração do contrato. No caso da política de privacidade, o contrato estabelece as regras de proteção à privacidade e os **procedimentos que serão adotados pela empresa para o tratamento das informações pessoais** de seus usuários mediante o acesso em um **site, aplicativo ou sistema**, esclarecendo-os como e para qual finalidade essas informações estão sendo coletadas, expondo sobre o **modo de obtenção, utilização, armazenamento, proteção dos dados** e inclusive sobre com quem serão compartilhados.

Esse documento promove a **segurança dos usuários** ao evitar o vazamento de informações pessoais nesse contexto digital, preocupação que já era aparente no **Código de Defesa do Consumidor** e foi reforçada com o **Marco Civil da Internet**, em 2014, que garante ao usuário o **direito à publicidade** e a **clareza em políticas de uso** de organizações que fornecem serviços através de plataformas na internet.

Além disso, é **imprescindível** para promover, na relação da empresa com os seus clientes:

- **Confiança;**
- **Credibilidade;**
- **Transparência.**

Com a edição da **Lei Geral de Proteção de Dados** (**LGPD**), a importância da política de privacidade ganhou cada vez mais repercussão, uma vez que prevê uma série de *obrigações* quanto ao procedimento de **coleta**, **armazenamento**, **tratamento** e **compartilhamento** de dados pessoais, através da manutenção do **princípio da transparência e da segurança** de modo a fornecer informações claras, precisas e facilmente acessíveis, além do documento ter que refletir a realidade do negócio conforme dispõe o **princípio da responsabilização** e prestação de contas como demonstração da adoção de medidas eficientes para o cumprimento das **normas** e boas práticas de proteção de dados pessoais.

Ademais, com a nova lei em vigor a **política de privacidade** deve indicar as **hipóteses legitimadoras da coleta e do tratamento** das informações do usuário, indicadas no *artigo 7º*, como por exemplo o **consentimento**, fornecendo também, o contato do encarregado – ou *data protection officer* – para responder as solicitações dos usuários quanto a proteção de dados.

Passo 05

Possua um Termo de Uso

Em regra, os **termos de uso** instituem as circunstâncias da contratação, as **obrigações** e os **limites de responsabilidade** da empresa e dos usuários sobre os serviços prestados ou produtos ofertados. Ou seja, esse documento se figura como um tipo de **contrato digital** e por isso deve atender as especificidades de cada negócio. Tais condições devem estar dispostas de forma evidente e pré-estabelecida, garantindo **privacidade, segurança** e **proteção** para ambas as partes. Vale lembrar que essas regras de uso devem sempre estar subordinadas à LGPD.

As empresas que já possuírem a maturidade na gestão de segurança dos dados coletados têm menos desafios para se adequarem a **LGPD**. Entretanto, aquelas que ainda não investiram para implementar tais condutas e documentos podem sofrer **sanções administrativas** e punições por ressarcimento a possíveis danos causados. Assim, é evidente que a utilização de termos de uso é um dos requisitos necessários para se trilhar um caminho de **confiança entre o usuário e empresa**. Além disso, cria-se uma gestão de segurança da informação para a própria organização interna, possibilitando alcançar credibilidade no mercado.

Você aceita nossos Termos de Uso e Política de Privacidade?

Passo 06

Tenha uma cultura de proteção de dados na sua empresa

A adoção de bons sistemas e aparatos de segurança da informação são imprescindíveis para adequação a **LGPD**, porém nada adianta investir nestes e esquecer-se das equipes que os administram. Importante lembrar que estes sistemas dependem diretamente da avaliação e **subjetividade humana**, e, portanto, não cumprirão corretamente sua função caso o time empresarial não os compreenda. Diariamente, o funcionário lida com espécies de informação essenciais para o funcionamento da instituição, como estratégias de gestão, segredos de produção e principalmente, **dados pessoais** dos clientes, que caso sejam expostos indevidamente, podem inviabilizar investimentos, gerar custas judiciais e prejudicar as relações de confiança entre organização e consumidores.

Desta forma, visando o bem-estar legal e competitivo da empresa, é interessante que todos os funcionários tenham conhecimento básico da **LGPD** e a seriedade implicada pelo **tratamento de dados pessoais**, bem como as consequências de um possível vazamento de dados e respectivas sanções legais.

Assim, a implementação de um **treinamento** sobre a Lei Geral de Proteção de Dados aos funcionários atuará em dois principais objetivos: **redução de riscos** nos processos internos e externos e **aumento da produtividade**. Isso porque uma equipe com maior acesso à informação e capacitação profissional, apresenta maiores índices de motivação e menores níveis de erro, criando uma verdadeira **vantagem competitiva** dentro do setor.

Passo 07

Possua um Código de Ética e de Conduta

O Código de Ética e de Conduta é um documento que reúne os **princípios éticos** da empresa, normalmente baseados nos valores e no propósito da organização.

Seu objetivo é orientar a todos que atuam em nome da empresa sobre como agir de forma correta, superando dilemas e tomando sempre as **melhores decisões** de forma ética e responsável.

Ter um **Código de Ética e de Conduta** é importante pois previne desvios de comportamentos compatíveis com a **segurança da informação** durante o período em que o colaborador está na organização e também quando este se desliga da empresa. Isso porque muitas pessoas carregam consigo os dados relacionados à empresa quando dela se desligam e até mesmo utilizam essas informações posteriormente.

Passo 08

Divida funções e responsáveis pelo tratamento de dados

Como todo vínculo social e jurídico, a LGPD se compõe de pessoas e da relação presente entre elas, as quais pressupõe direitos, obrigações e responsabilidades. É notório que a principal pessoa desse relacionamento se configura no Titular, ou seja, o proprietário do dado, porém não devemos esquecer daqueles responsáveis pelo tratamento da informação, uma vez que dependem deles toda a dinâmica regularizada pela Lei.

Agentes de Tratamento

Controlador

Responsável pelas decisões de tratamento das informações.

Operador

Responsável por realizar o tratamento dos dados pessoais.

Encarregado

Responsável pela comunicação entre controladores, os titulares dos dados pessoais e ANPAD.

O tratamento consiste em todo em qualquer processo que envolva **informações** de pessoas naturais ou jurídicas, em qualquer circunstância, seja ela nos ambientes privados ou públicos, além de todos meios, como os físicos ou digitais. Dessa maneira, os dados são tratados na:

1) CAPTAÇÃO
2) MANIPULAÇÃO
3) ARMAZENAMENTO
4) EXCLUSÃO

Com isso, percebe-se que os **Agentes de Tratamento** estarão atuantes desde a gênese do relacionamento com o Titular, podendo persistir até o seu fim ou até mesmo na pós-relação, em determinados casos expressos por Lei.

Agentes de Tratamento

Obrigatórios pela LGPD

Controlador

O Controlador deve em garantir os preceitos da Lei e associá-los com a dinâmica de funcionamento de informações da empresa. Para isso, parte de sua responsabilidade consiste em certificar o consentimento do Titular, dispor e adequar sobre condições de tratamento, elaborar relatórios de impactos, além de zelar pelos direitos do Titular.

Operador

O Operador terá como papel a realização das demandas passadas pelo Controlador, as quais se configuraram no processamento dos dados, nos procedimentos de segurança e na observância das práticas da Lei. Além disso, deve possuir muito cuidado em seu trabalho, visto que caso seja responsável por dano, surge a obrigação de reparação.

Encarregado

O Encarregado, apesar de **não ser obrigatório por Lei**, atua ao intermediar a comunicação entre o Titular, os Agentes de Tratamento e a **Autoridade Nacional de Proteção de Dados (ANPD)**. Assim, será o Encarregado que receberá reclamações, dará esclarecimentos, fará a orientação e executará as providências necessárias para a melhor atuação do tratamento. Mesmo não sendo uma exigência da LGPD, nas legislações europeias, o Encarregado, ou melhor, o ***Data Protection Officer*** (DPO), possui um papel indispensável e poderá a exigir em determinadas situações sua presença.

Fique atento à ANPD!

A Lei Geral de Proteção de Dados, por ainda ser uma Lei recente e em constante evolução, é indispensável, para um efetivo serviço como Agente de Tratamento, acompanhar as disposições da ANPD. Nessas orientações, estarão diversas publicações explicitando cada função e responsabilidade das pessoas envolvidas na relação de dados, circunstâncias primordiais para o verdadeiro e protetivo funcionamento do tratamento. Destaca-se, nessa composição, o **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado**, lançado no mês de maio de 2021, documento fundamento para adequação às normas da Lei.

Conclusão

A LGPD tem como principal objetivo garantir ao titular de informações maior autonomia e segurança. Para isso, desenvolveu-se estratégias de responsabilização visando incentivar empresas a tratarem dados pessoais com maior atenção e sigilo. Desse modo, as organizações devem ser claras e diretas quanto ao recolhimento de informações privadas, restringindo-se a captação de apenas dados essenciais.

O referencial teórico desse e-book foi retirado da obra:

Segurança Digital - Proteção de Dados nas Empresas

de Patrícia Peck

SOBRE A EJUR

A **EJUR Soluções Jurídicas**, Empresa Júnior da Universidade Estadual Paulista (**UNESP**), foi fundada em 1994, desempenhando nestes anos um importante papel na regulamentação de startups, pequenas e microempresas do Interior Paulista.

Somos apaixonados por **empreendedorismo** e nossa missão é auxiliar os empreendedores a concretizarem seus sonhos, oferecendo **suporte jurídico** de qualidade e de baixo custo.

EDIÇÃO E REVISÃO

Beatriz Adas
Coordenadora de Marketing

Giovanna Spineli
Assessora de Marketing

Júlia Bensi
Assessora de Marketing

AUTORES

Ana Carolina Campos
Consultora Jurídica

Beatriz Adas
Coordenadora de Marketing

Giovanna Martins
Consultora Jurídica

Giovanna Spineli
Assessora de Marketing

Júlia Bensi
Assessora de Marketing

Lorena Galavotti
Coordenadora de Execução

Maria Clara Okasaki
Assessora de Marketing

Marina Colafemea
Assessora de Projetos

Pedro Américo
Consultor Jurídico

Pedro Bachur
Diretor de Mercado

Sabrina Macedo
Presidente da EJUR


EJUR
SOLUÇÕES JURÍDICAS