



LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Guia completo com tudo o que você precisa
saber para sua empresa se adequar à LGPD.



SUMÁRIO

Introdução.....	03
O que é a Lei Geral de Proteção de Dados.....	04
Os princípios da LGPD.....	07
As bases legais da LGPD.....	09
Sobre os direitos dos titulares dos dados e as sanções previstas.....	11
Passos iniciais para adequar a empresa à LGPD.....	13
Monte uma equipe multidisciplinar para cuidar das adequações.....	14
Conheça os dados da sua empresa.....	14
Defina uma estratégia.....	15
Implemente as medidas necessárias.....	15
Avalie e mantenha a estratégia.....	15
Clientes AWS têm facilidade para se adequar à LGPD.....	16
Função da AWS segundo a LGPD.....	17
A AWS como um controlador de dados.....	17
A AWS como um processador de dados.....	18
Responsabilidade compartilhada de segurança.....	18
Conclusão.....	20
Sobre a FLEXA.....	21



INTRODUÇÃO

Com a aprovação presidencial, em agosto de 2018, as empresas teriam até 18 meses para se adaptarem às novas regras trazidas pela **Lei Geral de Proteção de Dados Pessoais** — portanto, a nova legislação entraria em vigor em 2020. Com a pandemia do coronavírus (COVID-19), esse prazo foi estendido para 2021 — há, neste momento, projetos de novos adiamentos tramitando no Congresso Nacional; é importante acompanhar.

De qualquer forma, é muito importante que os gestores já se movimentem para realizar as adequações em processos, tecnologias, operações etc. Os impactos e os desafios são grandes; logo, é preciso buscar conhecimento e até ajuda especializada em alguns casos.

O que muitas empresas não consideram é o tempo necessário para se adequar à LGPD. Se sua empresa começar agora, ela levará vários meses para implementar tudo o que essa nova Lei exige. Em alguns casos, esse tempo pode até ultrapassar 1 ano.

Neste e-book, buscamos reunir as informações mais importantes para as empresas. Nos capítulos que seguem, você vai ver o que é a LGPD, quais são suas bases legais, que sanções ela prevê para as empresas que não cumprem... Também vai ver o que é recomendável fazer em termos tecnológicos, e muito mais!

Boa leitura!





O que é a Lei Geral de Proteção de Dados Pessoais



Inspirada no Regulamento Geral de Proteção de Dados (GDPR), o regulamento europeu, a Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece regras para a coleta, manipulação, armazenamento e compartilhamento de dados pessoais gerenciados pelas organizações brasileiras e que atuam no território nacional.

Entre as ações restringidas pela LGPD estão a coleta e o uso de dados pessoais sem consentimento, tanto pelo setor privado quanto pelas autoridades públicas, bem como o uso de informações pessoais para praticar a discriminação ilegal ou injusta.

Trata-se, portanto, de uma legislação que faz parte do contexto brasileiro de adaptação progressiva às melhores práticas globais de gerenciamento de dados e abrange todas as empresas que oferecem serviços ou têm operações envolvendo manipulação de dados no Brasil.

A seguir estão os benefícios que a LGPD oferece aos cidadãos brasileiros:



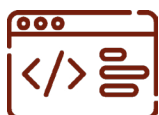
DIREITO À PRIVACIDADE

Proteção de dados pessoais, garantindo aos usuários maior controle sobre suas informações; incentivo de práticas de transparência e segurança baseados nos direitos e nas liberdades fundamentais dos cidadãos.



NORMAS CLARAS PARA AS EMPRESAS

Com a LGPD, a coleta, o armazenamento, o tratamento e o compartilhamento de dados pessoais seguem normatizações jurídicas bastante rígidas. Isso significa que empresas públicas e privadas precisam entrar em acordo com os usuários sobre o que vão fazer com suas informações pessoais.



PROMOÇÃO DE DESENVOLVIMENTO TECNOLÓGICO

A legislação também visa pavimentar o caminho para o desenvolvimento tecnológico e econômico da sociedade brasileira. Ela gera bases legais para que o país avance em direção à transformação digital, uma vez que ele está cada vez mais orientado a dados.



GARANTIA DOS DIREITOS DOS CONSUMIDORES

A Lei Geral de Proteção de Dados também está ancorada na garantia de livre-iniciativa, livre concorrência e defesa dos direitos dos consumidores/usuários. Em um país onde cada vez mais surgem negócios virtuais e o comércio eletrônico/digital não para de expandir, a LGPD dá aos consumidores mais garantia de proteção.



FORTALECIMENTO DA CONFIANÇA

Com a LGPD, a letra da lei vai ao encontro dos esforços de aumento de confiança da sociedade na coleta, no armazenamento e no uso de dados dos cidadãos. Ela cria limites e direitos, por exemplo, para o comércio online (e-commerce), que vem crescendo ano a ano no país. Um outro ponto dentro do fator “fortalecimento da confiança” é a segurança jurídica, que evita que as empresas cometam erros ou sejam julgadas unicamente com base em jurisprudência — a LGPD estabelece regras para que o Poder Judiciário as aplique nos casos que enfrentar.



Os princípios da LGPD



Entre os princípios que regem a LGPD, apontados no Artigo 6º da lei, destacam-se:

Finalidade

empresas públicas e privadas devem tratar os dados pessoais com propósitos legítimos, específicos, explícitos e informados

Transparência

as informações prestadas pela empresa aos titulares dos dados devem ser claras e precisas

Adequação e necessidade

o tratamento dos dados deve ser compatível com a finalidade e utilização apenas dos dados estritamente necessários

Segurança

as empresas devem utilizar medidas técnicas e administrativas para proteger os dados

Livre acesso

as empresas devem dar acesso integral ao titular dos dados sempre que ele requisitar

Prevenção

as empresas devem utilizar medidas para evitar danos aos titulares dos dados

Qualidade dos dados

as empresas devem garantir que os dados são claros, exatos, relevantes e atualizados

Não discriminação

e não devem utilizar os dados para fins discriminatórios e abusivos



As bases legais da LGPD



Já no artigo 7º da Lei Geral de Proteção de Dados Pessoais estão discriminadas 10 bases legais para o tratamento dos dados. Elas são relativas a:

- **Consentimento:** somente dados autorizados pelo titular podem ser tratados/processados;
- **Cumprimento de obrigação legal:** só utilizar e manter dados para cumprir uma lei/regulamento, nunca para além disso (visa não chocar a LGPD com outras regulamentações em vigor);
- **Execução de contrato:** o consentimento do titular dos dados é mantido durante toda a vigência de um contrato ou até que ele o revogue;
- **Legítimo interesse:** as empresas públicas e privadas não precisam solicitar consentimento dos titulares dos dados quando é comprovado o legítimo interesse, mas sempre dando a eles a opção de revogação da autorização a qualquer momento;
- **Processo judicial:** os dados pessoais podem ser utilizados como provas em um processo judicial ou administrativos, independente do consentimento do titular;
- **Crédito:** os dados podem ser usados para fins de análise e concessão ou não de crédito (no Cadastro Positivo aprovado recentemente, por exemplo);
- **Proteção à vida:** podem ser coletadas informações pessoais para proteger uma pessoa que, por exemplo, está correndo risco de vida e não tem condições de consentir;
- **Tutela da saúde:** dados pessoais podem ser utilizados por órgãos de saúde (hospitais, por exemplo), sem necessidade de consentimento;
- **Pesquisa:** organizações sem fins lucrativos podem processar dados pessoais para pesquisas (universidades, entre outras entidades de investigação científica);
- **Política pública:** órgãos públicos podem processar dados pessoais para desenhar e aplicar políticas públicas.



Sobre os direitos dos titulares dos dados e as sanções previstas



A LGPD prevê uma série de direitos aos titulares dos dados. Na prática, os donos dos dados podem obter:

- Confirmação da existência de tratamento dos dados;
- Acesso facilitado aos seus dados;
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados ilicitamente;
- Eliminação dos dados;
- Portabilidade;
- Informação das entidades que receberam seus dados;
- Informação sobre a possibilidade de não fornecer o consentimento;
- Revogação do consentimento;
- Reclamação à autoridade relativa ao uso indevido de seus dados
- Oposição ao tratamento de seus dados.

E as empresas que violarem a LGPD estarão sujeitas à aplicação de avisos, multas, embargos, suspensões e proibições parciais ou totais ao desempenho de suas atividades. As multas podem atingir até 2% da receita da organização, com um limite de 50 milhões de reais por violação.



Passos iniciais para adequar a empresa à LGPD



Confira, a seguir, os passos iniciais que devem ser dados para preparar o seu negócio para a LGPD!

Monte uma equipe multidisciplinar para cuidar das adequações

É interessante unir profissionais do direito, de TI e das áreas administrativas da empresa para uma força tarefa relativa à LGPD. Na maioria dos casos, também é interessante buscar ajuda de uma consultoria especializada. A primeira medida deve ser se informar sobre o tema e montar um planejamento de como começar a encaixar o negócio nas letras da lei.



Conheça os dados da sua empresa

Em seguida, deve-se fazer um levantamento dos dados da empresa, com foco nos dados pessoais processados (de funcionários, clientes, parceiros de negócios etc.). Assim, fica mais fácil identificar e avaliar a conformidade do fluxo de dados levantados com relação ao que normatiza a LGPD.



Defina uma estratégia

Muito provavelmente, vai ser preciso redesenhar processos e reformular práticas de processamento/tratamento de dados pessoais na empresa. Essa é a terceira fase de adequação à LGPD. Ela deve ser focada em fechar gaps, alocar recursos, definir que ferramentas e práticas devem ser implementadas etc.



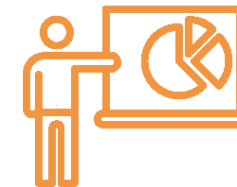
Implemente as medidas necessárias

Depois de tudo identificado e da estratégia bem definida (com prazos, metas etc.), é hora de implementar novos processos (técnicos, de segurança, de governança etc.), fazer testes, conscientizar e treinar funcionários.



Avalie e mantenha a estratégia

Por fim, chegamos à última fase, que será praticamente contínua: criar uma estrutura de prova de conformidade, definir mecanismos de monitorização para conseguir avaliar se a empresa está cumprindo ou não com as diretrizes da LGPD.





**Clientes AWS têm
facilidade para se
adequar à LGPD**



Os especialistas em conformidade, proteção de dados e segurança da AWS têm trabalhado com clientes em todo o mundo para responder dúvidas e ajudá-los a se preparar para a execução de cargas de trabalho na nuvem após a LGPD entrar em vigor.

Essas equipes também estão revisando as operações e as responsabilidades da AWS em relação aos requisitos da LGPD a fim de garantir que os serviços da AWS possam ser usados em conformidade com a LGPD assim que a lei entrar em vigor.

Função da AWS segundo a LGPD

De acordo com a LGPD, a AWS pode atuar tanto como um controlador de dados quanto como um processador de dados. Na LGPD, um controlador de dados é definido como a pessoa física ou jurídica, pública ou privada, que é responsável por decisões relacionadas ao processamento de dados pessoais. Na LGPD, um processador de dados é definido como a pessoa física ou jurídica, pública ou privada, que executa o processamento de dados pessoais em nome do controlador.

A AWS como um controlador de dados

Quando a AWS coleta dados pessoais e determina os fins e os meios de processamento desses dados pessoais (por exemplo, quando a AWS coleta



e armazena informações de seus clientes diretos para registro de contas, administração, acesso a serviços, atributos de serviço ou informações de contato para a conta da AWS com o objetivo de fornecer auxílio por meio de atividades de suporte ao cliente), ela atua como um controlador de dados.

A AWS como um processador de dados

Quando clientes e provedores de soluções da AWS usam os serviços da AWS para processar dados no conteúdo de seus respectivos clientes, a AWS atua como um processador de dados.

Clientes e provedores de soluções da AWS podem usar os controles disponíveis nos serviços da AWS, inclusive controles de configuração de segurança, para processar e armazenar dados pessoais. Nessas circunstâncias, o próprio cliente ou parceiro do APN pode atuar como um controlador de dados ou processador de dados, e a AWS atua como um processador de dados.

Responsabilidade compartilhada de segurança

Segurança e conformidade são responsabilidades compartilhadas entre a AWS e o cliente. Quando o cliente transfere seus dados e sistemas de computação para a nuvem, as responsabilidades de privacidade e



segurança são compartilhadas entre o cliente e o provedor de serviços de nuvem.

Quando os clientes migram para a Nuvem AWS, a AWS é responsável pela proteção da infraestrutura subjacente que oferece suporte à nuvem, e os clientes são responsáveis por tudo aquilo que colocam na nuvem ou conectam à nuvem.

Normalmente essa diferenciação da responsabilidade é mencionada como segurança da nuvem vs. segurança na nuvem.

Esse modelo compartilhado pode ajudar a reduzir a carga operacional do cliente e oferecer a flexibilidade e o controle necessários para implantar a infraestrutura dele na Nuvem AWS.

A AWS opera, gerencia e controla os componentes de infraestrutura, desde o sistema operacional de hospedagem e a camada de virtualização até a implementação de serviços com abstração e a segurança física das instalações nas quais os serviços operam.

Os clientes assumem a responsabilidade e o gerenciamento pelo sistema operacional convidado (inclusive por atualizações e patches de segurança), por outros aplicativos de software associados e pela configuração do firewall do grupo de segurança fornecido pela AWS.





CONCLUSÃO

Conte com a Flexa para adequar sua empresa à LGPD

Como você viu, os impactos da Lei Geral de Proteção de Dados Pessoais (LGPD) já são grandes. Mesmo aquelas que ainda não começaram a fazer as adequações necessárias, sabem que esse é um desafio.

A boa notícia é que não é preciso se desesperar. Aqui na Flexa Cloud, nós estamos preparados para ajudar nossos clientes a se adequar por meio das soluções e dos serviços da AWS.

Nós sabemos que a LGPD não diz respeito unicamente à tecnologia. Há outras frentes que precisam ser modificadas para que a empresa esteja em conformidade com a nova legislação.

Com objetivo de abranger a maior área de conhecimento possível dentro da LGPD, na parte jurídica, a Flexa trabalha com um renovado escritório de advocacia, bem como firmamos parceria com a GS Segurança da Informação e Computação Forense, tudo com o objetivo de apresentar um serviço de qualidade, pois entendemos que trabalhar com a implantação da LGPD demanda uma multidisciplinaridade de conhecimentos.

Então, você já sabe: se precisar de ajuda, conte conosco!

SOBRE A FLEXA

Há 11 anos no mercado, a Flexa é referência em Cloud (Migração para nuvem). Todo esse êxito é compreensível quando se olha sua trajetória, marcada por parcerias de grande sucesso. A primeira delas, com a New Relic, empresa dos Estados Unidos que atua na área de monitoramento de performance de aplicativos, teve início em 2012.

De lá pra cá, as parcerias expandiram cada vez mais e, com elas, o portfólio de produtos da Flexa. Logo depois da New Relic a AWS Amazon, líder mundial em computação em nuvem, entrou no time de parceiros da empresa. Isso aconteceu em 2013. Um ano depois chegou a vez da Zadara, empresa estadunidense que oferece soluções de armazenamento. Assim como as outras duas parceiras.

Em 2017 outra empresa norte americana firma parceria com a Flexa: a Zerto, que oferece soluções em Disaster Recovery. Em 2018 a israelense Spotinst chega para auxiliar os clientes da Flexa a reduzir custos de gastos nas nuven. Por fim, em 2019, a Sumo Logic, solução de SIEM, incorporou as fileiras da Flexa, ampliando sua oferta ao mercado.

Com uma equipe técnica de alta qualidade, parceiros reconhecidos nacional e internacionalmente, a Flexa tem como uma das principais marcas de sua história a busca pela excelência nos serviços prestados.

**FALE CONOSCO
AGORA!**

