1. **O que é LGPD?**

**Princípios:**

**1. Princípio da Adequação**

Está previsto no inciso II, do artigo 6.º da LGPD e prevê a “compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento”.

Os dados devem ser tratados de acordo com a sua destinação. A coleta de dados deverá ser compatível com a atividade fim do tratamento.

**2. Princípio da Necessidade**

A coleta de dados deve ocorrer de forma restritiva, cuidando para que o tratamento dos dados pessoais esteja restrito à finalidade pretendida.

**3. Princípio da Transparência**

Visa garantir aos titulares, informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento dos dados.

**4. Princípio do Livre Acesso**

Possibilitar que o titular dos dados consulte livremente, de forma facilitada e gratuita, a forma e a duração do tratamento dos dados, bem como sobre a integralidade deles.

**5. Princípio da Qualidade dos Dados**

Este princípio busca garantir aos titulares dos dados a exatidão, a clareza, a relevância e a atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

**6. Princípio da Segurança**

Compreende medidas técnicas e administrativas para proteger os dados de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

**7. Princípio da Prevenção**

É um dos pilares da Segurança da Informação, buscando a antecipação de eventualidades, com a adoção de medidas para prevenir a ocorrência de danos em razão do tratamento de dados pessoais.

**8. Princípio da Responsabilização e Prestação de Contas**

Neste princípio espera-se que o controlador ou o operador demonstrem todas as medidas eficazes e capazes de comprovar o cumprimento da lei e a eficácia das medidas aplicadas.

**9. Princípio da Não Discriminação**

O tratamento dos dados não pode ser realizado para fins discriminatórios, ilícitos ou abusivos, ou seja, não se pode excluir de titulares de dados pessoais, no momento de seu tratamento, informações determinadas por características, sejam elas de origem racial ou étnica, opinião política, religião ou convicções, geolocalização, filiação sindical, estado genético ou de saúde ou orientação sexual.

**10. Princípio da Finalidade**

Previsto no inciso I do art. 6.º da LGPD, emprega-se como a “realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades”, ou seja, o dado deverá, na coleta, ter a indicação clara e completa que a justifique.

**Base Legal:**

As 10 bases legais da LGPD são:

* Consentimento do titular;
* Legítimo interesse;
* Cumprimento de obrigação legal ou regulatória;
* Tratamento pela administração pública;
* Realização de estudos e de pesquisa;
* Execução ou preparação contratual;
* Exercício regular de direitos;
* Proteção da vida e da incolumidade física;
* Tutela de saúde do titular;
* Proteção de crédito.

**Obrigações e Boas Práticas:**

**1. Revise todas as políticas de segurança da informação**

O primeiro passo para aplicar conceitos da LGPD é a revisão de todas as políticas de segurança de informação da companhia. É a partir de uma análise mais aprofundada do que foi realizado que se torna possível identificar os erros e estabelecer novos padrões de proteção.

Também é importante garantir que toda a companhia esteja envolvida nesse processo. Ou seja, as políticas de segurança precisam ser revisadas e todos os profissionais devem ser informados sobre as novas regras e práticas que devem ser adotadas.

**2. Conscientize a empresa sobre a LGPD**

Com a empresa engajada nessa proposta, fica mais fácil apresentar e conscientizar todos os colaboradores sobre a importância da LGPD. Mas não se trata de uma explicação simples ou conceitual sobre o que é a legislação. É fundamental que eles entendam como a mudança impacta o dia a dia de trabalho, as práticas que devem ser adotadas e aquelas que precisam ser evitadas.

Afinal, trata-se de uma mudança cultural, e é necessário que toda a organização esteja na mesma página. Por mais que os líderes e gestores saibam e coloquem a LGPD na prática, os resultados só vão ser efetivos com uma transformação geral. O processo começa por cima, mas é necessário que todos tenham a consciência de como é uma questão necessária para o sucesso da companhia.

**3. Aposte em uma cultura de Governança e Conformidade**

Mais importante do que qualquer outra etapa é a criação de uma cultura que valorize a Governança e a Conformidade. De nada vai adiantar adotar algumas práticas se a empresa como um todo não estiver disposta a se adaptar e a entender a importância da LGPD. Essa é uma mudança que precisa começar nos cargos mais altos da hierarquia.

A partir do comportamento dos líderes da organização, torna-se mais fácil estimular todos os profissionais a adotarem práticas que contribuam para a maior transparência e sigam todas as regras estipuladas pela LGPD. Quando essa cultura é implementada, a tendência é que a adaptação seja ainda mais fácil e os resultados, mais significativos e duradouros.

**4. Defina um comitê de implementação**

Além de estabelecer políticas claras de Governança e Conformidade, é preciso delegar profissionais responsáveis por cuidar da segurança de todos os dados armazenados pela sua empresa. É importante destacar o papel do Data Protection Officer (DPO), um especialista responsável por estabelecer e gerenciar tudo o que se refere à LGPD.

O DPO precisa conhecer a legislação a fundo e garantir que todas as regras sejam colocadas em prática pela companhia. Ele vai ser o responsável por gerenciar toda a organização em torno de uma maior transparência, assegurando que os dados e informações estejam sempre protegidos.

**5. Conheça o fluxo de informações da empresa**

Para que a colocar a LGPD em prática, também é preciso ter uma visão mais clara sobre o fluxo de informações da empresa. A ideia é entender exatamente como os processos funcionam. Quando um dado é coletado, onde fica armazenado? Quais são os padrões de segurança? Quem tem acesso? O que está sendo feito de forma certa e o que precisa melhorar?

A partir dessa definição, fica mais fácil encontrar os erros e as correções que precisam ser feitas em cada etapa da jornada, não deixando que nenhuma falha passe despercebida.

**6. Tenha clareza sobre o tempo de uso dos dados**

Uma das questões mais importantes da LGPD é em relação ao tempo que as informações coletadas por uma empresa podem ser utilizadas. Portanto, ao pedir pelo consentimento do usuário sobre os seus dados, a transparência é fundamental. É preciso explicar por quanto tempo aquelas informações vão ficar armazenadas e assegurar a exclusão das mesmas após o tempo estipulado.

**7. Reveja os documentos e cláusulas contratuais**

Já pensou se um dos seus principais fornecedores não estiver adequado à LGPD? Isso significa que as ações dele se tornam responsabilidade da sua empresa, o que pode acarretar uma série de problemas. Para se manter em conformidade com a lei, portanto, é fundamental rever todos os contratos e garantir que os parceiros também estejam seguindo a legislação.

O ideal é fazer uma revisão sobre todos os documentos e cláusulas contratuais em vigor que envolvam as operações do seu negócio. Apesar de trabalhosa, essa é uma tarefa essencial para evitar problemas futuros por conta de uma assinatura passada.

**8. Organize os documentos sobre proteção de dados**

A organização dos documentos e informações também precisa ser realizada de acordo com as orientações da LGPD. Isso garante que nenhum entrave surja de maneira inesperada para a sua empresa.

**9. Crie um canal de comunicação com os usuários**

A transparência, muito presente quando se fala em LGPD, também deve ser colocada em prática externamente. Ou seja, os gestores devem criar um canal para que os usuários possam se comunicar com a empresa de forma simples e prática.

Seja para tirar dúvidas pontuais, seja para fazer um pedido de exclusão dos seus dados, essa comunicação pode ser muito benéfica para a companhia.

**10. Tome as medidas cabíveis quando houver vazamento**

Com um comitê definido e a LGPD implementada, as chances de que algum problema aconteça são muito menores. Isso não significa que elas não existam.

Por isso, é necessário ter uma equipe sempre preparada para atuar de forma eficaz em caso de situações mais graves, como vazamento de dados. Desde a comunicação e o contato aos usuários prejudicados até as ações técnicas para minimizar os impactos.

**11. Invista no treinamento da equipe**

Para que o LGPD funcione na prática, os profissionais precisam estar em constante aperfeiçoamento. Por isso, cabe aos líderes e gestores investirem em ações de treinamento das suas equipes para que a legislação seja cumprida. Por mais que o conceito tenha sido explicado no início do projeto, existem mudanças e orientações que precisam ser reforçadas de tempos em tempos.

**12. Mantenha a empresa atualizada**

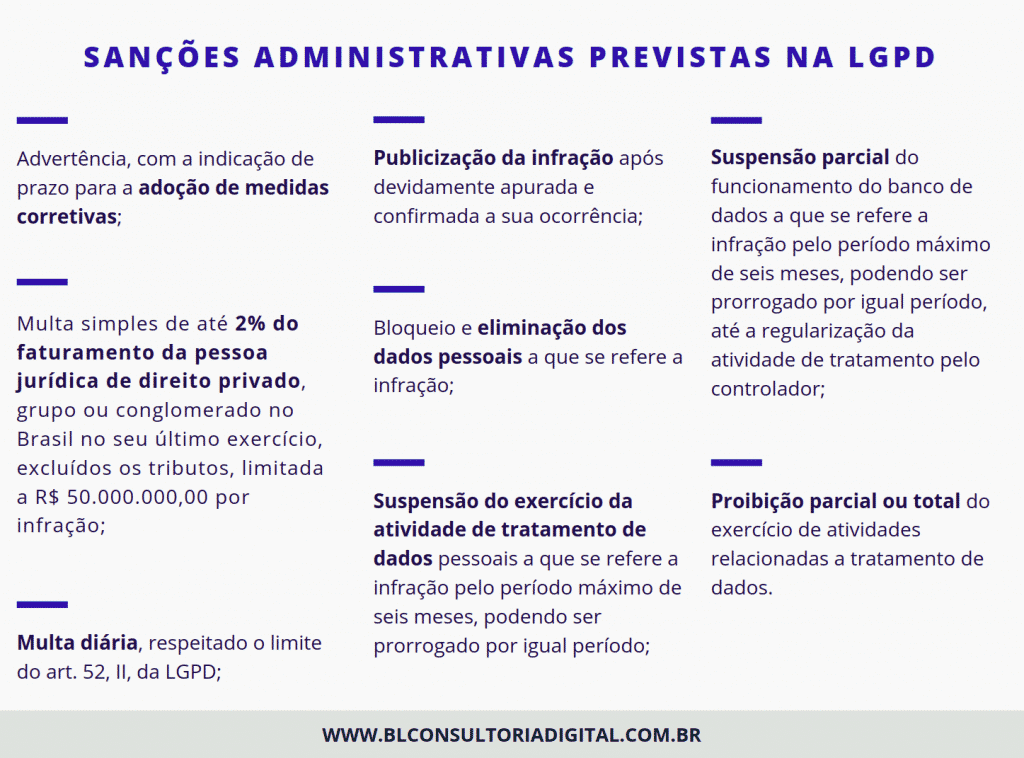
Apesar de a LGPD ser um marco em relação à regulamentação de práticas e regras nos ambientes digital e físico, isso não significa que ela não passe por alterações em um futuro não tão distante. Com tantas mudanças no mercado e na sociedade em geral, é possível que a legislação também precise de atualizações futuras, e a sua empresa precisa se preparar.

Uma nova tendência, uma falha global, uma pandemia, enfim, as alterações podem surgir por conta dos mais variados motivos. O mais importante é garantir que o seu negócio esteja atento às possíveis mudanças e preparado para se adaptar e realizar os ajustes necessários. Afinal, adequar-se à LGPD é um trabalho que precisa sempre ser monitorado.

Colocar a LGPD em prática é muito importante para a realidade de qualquer empresa. Tanto para aprimorar ações de Marketing Digital quanto para que os processos e a experiência oferecida aos seus clientes sejam cada vez melhores. Em um momento em que a fidelização é essencial para as organizações, fazer com que o seu público confie na sua companhia é um diferencial competitivo.

Mas quando se fala em gestão de informações dentro de uma organização, a LGPD é apenas uma parte das mudanças que precisam ser realizadas. Por isso, é importante que você se aprofunde em outras questões, também. O que acha de conhecer a diferença entre dados primários e dados secundários de marketing nas empresas?

**Sanções e Penalidades**



**O que é GDPR?**

GDPR é um projeto para proteção de dados e identidade dos cidadãos da União Europeia que começou a ser idealizado em 2012 e foi aprovado em 2016. Embora a região já tivesse leis relacionadas à privacidade, elas datavam de 1995 e, mesmo com algumas atualizações, não correspondiam ao cenário tecnológico atual. A decisão de criar o regulamento vem daí.

**Quais os principais passos para implementação da LGPD em uma determinada empresa?**

1. Conheça tudo sobre a lei

Este tópico parece óbvio, mas não é. Antes de começar efetivamente a aplicar a LGPD, conheça absolutamente tudo sobre ela. Leia o arquivo na íntegra, disponibilizado no site do governo federal, e tenha atenção a cada um dos tópicos. Caso tenha dúvidas, procure um especialista na área e tenha a certeza de que você entendeu tudo o que o documento determina.

2. Faça um mapeamento de todos os dados disponíveis na sua empresa e estude os riscos de vazamento ou de tratamento inadequado

Depois de conhecer detalhes da LGPD, é o momento de reunir todas as fontes de dados que a sua empresa tem. Lembre-se de se cercar por todos os lados: veja quais são os dados de clientes, dos colaboradores e dos fornecedores. A partir disso, avalie qual o ciclo de vida de cada um deles, as falhas no processo de tratamento e os riscos de vazamento. Em equipe, trace estratégias a fim de que as informações sejam acessadas apenas por pessoas autorizadas e para as finalidades permitidas na LGPD.

3.Revise os seus documentos (internos e externos)

Os documentos oficiais que estabelecem normas e diretrizes para a sua empresa devem ser revisados (pelo departamento Jurídico ou por uma consultoria especializada, de preferência), garantindo que todos os tópicos estejam em conformidade com a nova lei. Não se esqueça de incluir nessa lista também os documentos digitais.

4.Garanta a transparência do seu negócio

As práticas adotadas pela sua empresa para assegurar que todos os processos estejam de acordo com a LGPD devem ser conhecidas por todos. Por isso, a palavra-chave é transparência: reúna tudo em um material, descrevendo o que deverá ser seguido por todo o time posteriormente à vigência. Avalie a possibilidade de criar um documento de perguntas frequentes, visando garantir o conhecimento por parte de toda a empresa e o esclarecimento de eventuais dúvidas.

Transparência com o cliente ou usuário do seu serviço também é fundamental. Caso algum processo sofra modificações consideráveis, avise-os, por meio de uma comunicação clara e eficaz.

5.Tenha um comitê interno responsável pela LGPD

Reúna os profissionais diretamente envolvidos com dados (Jurídico, TI, Comercial, Vendas, Financeiro etc.) e recomende que eles façam parte de um Comitê de Compliance. A sugestão é definir pontos focais, de cada área, que ficarão responsáveis pelo assunto. A atuação do comitê será, em linhas gerais, possibilitar que todos os processos da empresa estejam sendo realizados de acordo com a LGPD.

Se possível, contrate (ou eleja) um Data Protection Officer (DPO), o profissional com conhecimento técnico (jurídico e regulatório) que poderá conduzir todas as definições. Ele será o intermediador entre os titulares dos dados, a fiscalização e as empresas.

6.Valide as bases legais para os dados pessoais tratáveis

As fontes de dados que a sua empresa tem precisam ser validadas. Em outras palavras, esse é o momento de justificar para o governo o motivo de o seu negócio ter aqueles dados e com qual finalidade eles serão utilizados. Antes de entender essa tarefa como concluída, confira quais são os procedimentos corretos de validação para cada caso.

7. Defina uma forma de gerenciar pedidos de titulares e de órgãos reguladores

Isso servirá para estabelecer qual será o procedimento padrão para as solicitações dos seus clientes ou quando houver a fiscalização dos órgãos reguladores. Aqui, é importante registrar um documento com cada passo desse processo, que poderá ser consultado a qualquer hora pelos profissionais envolvidos.

8. Ofereça treinamento para a equipe que lida diretamente com os dados

É imprescindível que todas as pessoas que trabalham em sua empresa conheçam integralmente as novas regras estabelecidas na LGPD – especialmente quem lida diretamente com dados pessoais, internos ou externos. Esse alinhamento vai garantir que todos estão a par das mudanças e evitar que possíveis desvios se deem.

Verifique até mesmo a possibilidade de gravar pílulas de conteúdo em vídeo com as recomendações principais acerca da LGPD. O material pode ser disponibilizado para os colaboradores que tratam diretamente com dados como um jeito fácil de acesso às orientações imprescindíveis.

9. Faça um Plano de Segurança da Informação

Quanto mais se aproxima a data de início de vigência da LGPD, mais se fala em segurança da informação. Por isso, sugerimos que haja um Plano de Segurança da Informação, voltado para a proteção de dados pessoais. Isso pode ser mais uma tarefa do comitê criado para trabalhar com as questões da LGPD.

10. Olhe para a frente e estude novos produtos ou serviços

Depois de ter seguido os passos mais importantes e necessários, comece a olhar para o futuro próximo. Pense como sua empresa pode oferecer produtos levando em conta a privacidade dos dados. Essa prática, aliás, deve integrar a cultura organizacional da empresa: é fundamental que todo o time se habitue a considerar as novas regras no desenvolvimento de novos processos ou produtos.

Agora que você conheceu os passos para garantir que a LGPD seja implementada com segurança em sua empresa, descubra também as possibilidades do marketing de dados e explore as possibilidades em seu negócio.

**Cite um exemplo de vazamento de dados**

Credenciais de usuários do Uber Eats foram encontradas na deep web pela Cyble, uma empresa de cibersegurança que monitora o ambiente não indexado pelos mecanismos de busca padrão.

De acordo com a Cyble, nove arquivos TXT – ou seja, arquivos de texto sem formatação – com informações valiosas sobre os entregadores e clientes do Uber Eats foram vazados na dark web por um cibercriminoso.

publicidade

Entre as informações disponibilizadas estavam credenciais de 579 clientes, bem como dados confidenciais de 100 motoristas, incluindo nome completo, número de contato e detalhes do cartão bancário.

Os dados disponibilizados dá a possibilidade de acessar as informações pessoais juntamente com os detalhes do cartão – uma combinação perigosa em mãos erradas.