LGPD

Lei Geral de Proteção de Dados

MELHORES PRÁTICAS

FAST MEDIC

• EXCELÊNCIA NA GESTÃO DE SAÚDE •

15 ANOS

LGPD

Lei Geral de Proteção de Dados

MELHORES PRÁTICAS

“Proteger dados pessoais, é garantir nossa própria identidade.”

Diz respeito a nossa identidade, como somos vistos, como somos julgados.

FAST MEDIC

• EXCELÊNCIA NA GESTÃO DE SAÚDE •

15 ANOS

LGPD

Lei Geral de Proteção de Dados

MELHORES PRÁTICAS

Um resumo rápido sobre a Lei Geral de Proteção de Dados

Introdução

O que a LGPD representa para as empresas?

Capítulo 1

As empresas devem respeitar princípios para tratar dados pessoais

Capítulo 2

Motivos para se adequar

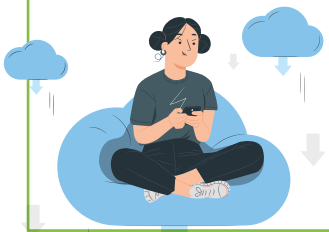
Capítulo 3

Os titulares de dados têm direitos claros

Capítulo 4

Para implementar a LGPD, as empresas devem estar aptas à diversas regras

Capítulo 5



Mas como seria na prática?

Capítulo 6

O que nós, da Fast Medic fazemos?

Capítulo 7

Como a Fast Medic protege suas informações?

Capítulo 8

FAST MEDIC

EXCELÊNCIA NA GESTÃO DE SAÚDE

15 ANOS

LGPD
Lei Geral de Proteção de Dados
MELHORES PRÁTICAS

Um resumo rápido sobre a Lei Geral de Proteção de Dados

A nova **Lei de Geral de Proteção de Dados**, sancionada em 2020 e já está em vigor!

Ela vem para estabelecer regras claras de práticas mais transparentes e seguras sobre como as empresas lidam com dados pessoais. O objetivo é devolver à mão dos titulares de dados, o poder sobre os próprios dados pessoais e dados sensíveis.

Compartilhamos dados pessoais todos os dias. Nomes e e-mails das pessoas são coletados para fazer cadastros, validações, conferências, etc. No trabalho voluntário, as pessoas preenchem formulários com os seus dados pessoais, em livrarias ou feiras de livros, também podem ser coletados dados financeiros! E quando há atendimento médicos em hospitais, não é feita uma ficha médica? E todos esses dados não são armazenados ou cuidados pela equipe da instituição?

A **LGPD** atua regulamentando o tratamento de dados do início ao fim, ou seja, desde a coleta dos dados até o cuidado final de quem se presta a mantê-los ou transmiti-los para outrem. Então, quem está coletando e tratando os dados de uma pessoa ou empresa deve garantir um certo grau de segurança para o titular dos dados.

Mas o que são Dados Pessoais e Dados Sensíveis?

Dados Pessoais são todas as informações que podem ser usadas para identificar uma única pessoa, como por exemplo CPF, RG, PIS, CNH, Endereços, entre outros. Isoladas ou não, se for possível unir um conjunto de dados e como resultado, identificar uma pessoa, já podemos considerar como dados pessoais.

Dados Sensíveis são dados mais especiais, relacionados à aspectos muito íntimos do titular e podem gerar prejuízos e constrangimento somente por sua exposição pública. Como a sua divulgação pode gerar prejuízo ou constrangimento em algumas circunstâncias, há algumas regras específicas para o seu recolhimento.

FAST MEDIC
• EXCELÊNCIA NA GESTÃO DE SAÚDE •
15 ANOS

LGPD
Lei Geral de Proteção de Dados
MELHORES PRÁTICAS

CAPÍTULO 1

O que a LGPD representa para as empresas?

Obrigatoriedade de proteger Dados Pessoais

Isso quer dizer implementar controles mais rígidos sobre como gerenciam e protegem dados pessoais, sejam de colaboradores, associados ou qualquer indivíduo, incluindo crianças, que tem tratamento diferenciado.

Processos deverão ser implementados e os existentes adaptados, incluindo sistemas de software (quando aplicável).

Ferramentas e sistemas devem ser adequados para implementar e atender requisitos, além de adaptação de atividades.

As empresas devem monitorar seu risco e garantir conformidade com a Lei de forma contínua

A **LGPD** é desafiadora, complexa e abrange controles rígidos de segurança para todas as áreas. É necessário monitoramento constante e uso de tecnologias para automatizar atividades.

FAST MEDIC
EXCELÊNCIA NA GESTÃO DE SAÚDE
15 ANOS

LGPD
Lei Geral de Proteção de Dados
MELHORES PRÁTICAS

CAPÍTULO 2

As empresas devem respeitar princípios para tratar dados pessoais

1. Princípio da Adequação

Está previsto no inciso II, do artigo 6.º da **LGPD**, 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.

CAPÍTULO 2

... continuação

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.

LGPD
Lei Geral de Proteção de Dados
MELHORES PRÁTICAS

CAPÍTULO 3

Motivos para se adequar

1

Evitar sanções

A Lei prevê **multa de até 2%** do faturamento da empresa, além também da possibilidade de ter que indenizar os titulares de dados.

2

Impacto na reputação da Empresa

A publicização da infração e do infrator gera quebra de confiança da sociedade, dos clientes e dos usuários

3

Bloqueio das atividades

A Lei prevê a possibilidade de bloqueio, suspensão da atividade de tratamento dos dados e até mesmo a eliminação dos dados pessoais que foram utilizados indevidamente.

4

Riscos Comerciais

A inadequação pode gerar empecilhos na realização de parcerias e contratos, tendo em vista a adoção de boas práticas tem sido um critério importante tanto para o consumidor quanto para os fornecedores e prestadores de serviço.

FAST MEDIC
• EXCELÊNCIA NA GESTÃO DE SAÚDE •
15 ANOS

LGPD
Lei Geral de Proteção de Dados
MELHORES PRÁTICAS

CAPÍTULO 4

Os titulares de dados têm direitos claros

Os titulares dos dados pessoais podem buscar junto ao Controlador:

- Os titulares podem solicitar às empresas a confirmação da existência do tratamento de seus dados;
- Eles podem solicitar acesso a seus dados pessoais;
- Eles podem solicitar a correção de dados incompletos, inexatos ou desatualizados, além da anonimização das informações.
- Eles podem solicitar o bloqueio ou eliminação de dados pessoais desnecessários, excessivos ou tratados em desconformidade com a **LGPD**;
- Eles podem solicitar a portabilidade de seus dados pessoais a outro fornecedor de produto ou serviço;
- Eles podem solicitar a eliminação de dados tratados com o seu consentimento; e a revogação de seu consentimento.

FAST MEDIC
EXCELÊNCIA NA GESTÃO DE SAÚDE
15 ANOS

LGPD
Lei Geral de Proteção de Dados
MELHORES PRÁTICAS

CAPÍTULO 5

Para implementar a LGPD, as empresas devem estar aptas à:

1. Fornecer meios para os titulares de dados com a opção de autorizar ou não o uso de seus dados;

2. Mostrar quais dados estão sendo coletados e justificar onde e como serão utilizados;

3. Respeitar a solicitação de exclusão de informações pessoais arquivadas;

4. Ser transparentes e claros em suas políticas de privacidade;

5. Ser capazes de notificar rapidamente as autoridades e os titulares, em caso de incidentes de vazamento de dados;

6. Manter registros organizados de todas as atividades de processamento de dados;

7. Transferir dados apenas para países que garantam os mesmos níveis de proteção de dados.

8. Eleger com um responsável para gerir os processos de tratamento de dados, o chamado DPO (Data Protection Officer)

9. Ter a comprovação de autorização para uso de dados pessoais dos titulares.

10. Facilitar a disponibilização de cópias das informações sobre os usuários, quando solicitado.

FAST MEDIC
• EXCELÊNCIA NA GESTÃO DE SAÚDE •
15 ANOS

LGPD
Lei Geral de Proteção de Dados
MELHORES PRÁTICAS

CAPÍTULO 6

Mas como seria na prática?

1. Verifique os sistemas de terceiros. Este cuidado é necessário pois você poderá estar violando a Lei indiretamente.

2. Implemente uma política e processos para gerenciar solicitações de titulares.

3. Mantenha um registro dos consentimentos para aqueles que já optaram por participar e aqueles que ainda estão optando por fazê-lo.

4. Crie uma agenda de retenção para dados. Quando os dados chegaram ao final do seu período de retenção, destrua-os de acordo com uma política de destruição de dados.

5. Treine sua equipe para que **TODOS** entendam o que constitui dados pessoais, de início explique e exemplifique os papeis do controlador, processador, DPO, também é de extrema importância ficar claro o que significa cada um dos 10 princípios da LGPD.

6. Treine anualmente todos os colaboradores para identificar violação de dados e mantenha um registro destes eventos.

7. Implemente uma política de Resposta à Incidentes alinhada ao seu Relatório de Impacto à Proteção de Dados - RIPD.

FAST MEDIC
EXCELÊNCIA NA GESTÃO DE SAÚDE
15 ANOS

LGPD
Lei Geral de Proteção de Dados
MELHORES PRÁTICAS

CAPÍTULO 6

... continuação

8. Defina regras de segurança física dos dados (HDs, USB, sistemas de arquivamento de papel, picadors de papéis, armário com cadastros impressos, etc.)

9. Bloqueie com segurança todos os dados pessoais (use processos e tecnologia)

10. Considere quais indivíduos devem ter acesso aos dados em cada dispositivo

11. Elabore/Atualize a política de privacidade (para incluir a identidade do responsável pelo processamento e a base legal, o interesse legítimo, qualquer destinatário ou categorias de destinatários dos dados pessoais, o direito de retirar o consentimento a qualquer momento e o período de retenção de dados).

12. Realize auditorias internas para verificar a conformidade com a **LGPD** e também quanto a norma de segurança adotada (Exemplo: ISO27001).

13. Realize periodicamente testes de intrusão (Pentest ou Penetration Tests), tenha fornecedores especializados.

14. Use os relatórios de Pentest para identificar as vulnerabilidades e potenciais invasões a fim de corrigir e aumentar a segurança, como também para passar confiança aos associados, demonstrando que existe preocupação e responsabilidade com a segurança e privacidade dos dados.

FAST MEDIC
EXCELÊNCIA NA GESTÃO DE SAÚDE
15 ANOS

LGPD
Lei Geral de Proteção de Dados
MELHORES PRÁTICAS

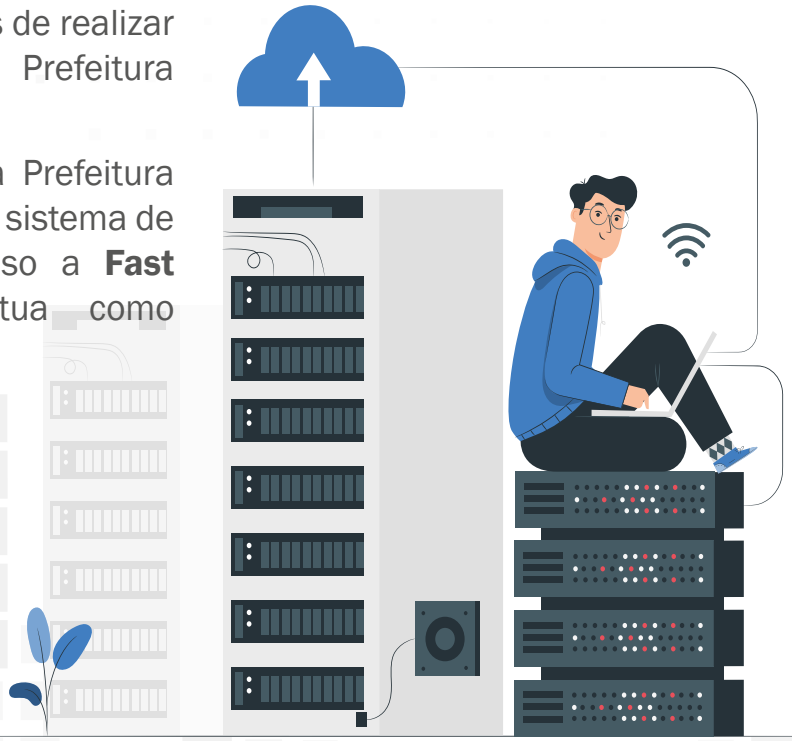
CAPÍTULO 7

O que nós, da Fast Medic fazemos?

Somos Operadores de Dados, uma empresa que realiza o tratamento de dados pessoais em nome dos Controladores (nossos clientes), fornecendo dados precisos e atualizados para qualquer outro órgão do Governo que solicite acesso à estas informações.

Segue um exemplo para que você entenda melhor esses papéis:

- Um paciente fornece uma série de dados pessoais a um Posto de Saúde antes de realizar um determinado procedimento. A Prefeitura nesse caso é o controlador.
- Para trabalhar com estes dados, a Prefeitura precisa processá-los por meio de um sistema de um fornecedor contratado, no caso a **Fast Medic**, que neste exemplo atua como Operadora de Dados.



FAST MEDIC
• EXCELÊNCIA NA GESTÃO DE SAÚDE •
15 ANOS

LGPD
Lei Geral de Proteção de Dados
MELHORES PRÁTICAS

CAPÍTULO 8

Como a Fast Medic protege suas informações?

Com a preocupação de estar alinhado a elevados padrões de integridade, legalidade e transparência, a **Fast Medic** criou em 2018 a área de Compliance, que tem como objetivo certificar a conformidade dos negócios em relação às regulamentações das suas áreas de atuação.

A **Fast Medic** também possui um **Programa de Governança em Privacidade e Segurança da Informação** que - através dos nossos profissionais qualificados e dedicados - assume o papel exclusivo de garantir a integridade e disponibilidade dos sistemas e serviços que garantem acesso aos dados dos titulares que armazenamos.

Nossa área de Segurança e Compliance zela pelo cumprimento dos controles internos da empresa.

Mas para que isso aconteça, é importante que todos estejam alinhados e atuem de acordo com os termos da legislação brasileira e com as diretrizes contidas no **Código de Conduta, Anticorrupção e Ética**.

Visite nosso site

www.fastmedic.com.br

FAST MEDIC
• EXCELÊNCIA NA GESTÃO DE SAÚDE •
15 ANOS