BOAS PRÁTICAS

CARTILHA SOBRE A

# LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

PRÓ-SAÚDE
ASSOCIAÇÃO BENEFICENTE DE ASSISTÊNCIA SOCIAL E HOSPITALAR

# APRESENTAÇÃO

Com o intuito de esclarecer os principais aspectos da nova legislação voltada à proteção de dados no Brasil, este material foi desenvolvido pela Pró-Saúde como forma de difundir conhecimento e demonstrar a necessidade de envolvimento de todos os seus colaboradores nas adequações necessárias a garantia de privacidade e a confidencialidade dos dados pessoais dos membros da entidade e de seus stakeholders (pacientes, seus familiares, fornecedores, prestadores de serviços).

# O QUE É A LEI GERAL DE PROTEÇÃO DE DADOS?

Em uma sociedade cada vez mais movida e orientada por dados pessoais e empresariais nas redes, crescem movimentos para proteção do lado mais frágil da cadeia – o titular do dado. Um novo pacto social, fundamentado na transparência, no respeito nas relações comerciais e nas questões de políticas públicas, mostrava-se cada vez mais necessário.

A *General Data Protection Regulation* (GDPR), em vigor desde maio de 2018 na Europa, formalizou as regras para coleta e uso de dados pessoais em 28 países, prevendo duras punições para entidades públicas ou privadas que não cumprirem suas diretrizes em todo continente europeu. A GDPR englobou também as organizações que fazem negócios com seus cidadãos em qualquer parte do mundo e, somada aos escândalos de vazamentos de dados de grandes empresas, despertou a urgência de uma adequação internacional.

Inspirada na GDPR, o Brasil editou a Lei Geral de Proteção de Dados (LGPD) que por sua vez entrou em vigor dia 17 de setembro de 2020 e regulamenta o uso e a proteção de dados pessoais em território nacional.

Com base na legislação europeia, a Lei nº 13.709/2018 consolida, atualiza e aprimora as regras de coleta e uso de dados pessoais que estavam de alguma forma previstas no Marco Civil da Internet, no Código de Defesa do Consumidor e na própria Constituição Federal.

A LGPD prevê requisitos para que o tratamento de dados seja legítimo, cria as figuras do "titular dos dados", "controlador" e "operador", dispõe sobre as medidas necessárias à sua observância, como a implementação de medidas técnicas e administrativas visando a proteção de dados, bem como as sanções em caso de descumprimento.

As obrigações são aplicáveis para operações de tratamento de dados realizadas por pessoa física ou jurídica, de direito público ou entidades privadas que coletem, tratem, armazenem ou lidem, de alguma forma, com informações pessoais.

Esta nova legislação visa, portanto, o equilíbrio entre o Direito à Privacidade, o incentivo à inovação e não veda a utilização dos dados pessoais. Entretanto, as adequações nos processos internos e contratos para que os direitos dos titulares sejam respeitados é fundamental como medida de prevenção das pesadas sanções previstas na lei. A multa poderá chegar a 2% do faturamento, com teto de R$50 milhões (por infração), e as denúncias poderão ser realizadas pelo próprio titular do dado que se sentir lesado.

## OBJETIVOS DA LGPD

A LGPD tem como objetivo formal *"proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural"*. Em resumo, esta legislação possui três compromissos bem claros quanto à gestão de dados pessoais:

- a exigência de **um propósito ou finalidade** para o tratamento dos dados;
- a **exigência do consentimento informado do titular** para o tratamento;
- transparência na gestão do tratamento dos dados.

Como ponto de partida, é importante definir que um dado pessoal é qualquer informação referente a um indivíduo. Pode ser uma informação profissional (local de trabalho, salário), de identificação (nome, documento), física (altura, sexo, idade, doenças), geográfica (endereço, localização), relacionada a hábitos (leitura, compras), etc.

## COMO A LGPD IMPACTA O DIA A DIA DA PRÓ-SAÚDE?

A Pró-Saúde lida constantemente com dados de seus clientes (pacientes-clientes), fornecedores, prestadores de serviços, colaboradores, enfim, os stakeholders envolvidos em suas operações e atividades diárias e está firmemente comprometida com o propósito de manter a confidencialidade das informações sob sua responsabilidade, de acordo com os mais elevados padrões legais e éticos.

Para tanto, é de suma importância que os nossos colaboradores, prestadores e fornecedores de serviços adotem às políticas e procedimentos da Entidade, em especial aqueles que visem a confidencialidade e privacidade de dados.

Considerando que cabe a cada um de nós o dever de proteger e salvaguardar os dados pessoais de seus respectivos titulares, é importante que esse cuidado esteja presente em todas as formas de acesso, como papel, qualquer meio eletrônico, verbal, telefônico, entre outros.

Os dados pessoais sensíveis, ou seja, aqueles que envolvem 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 e dado genético ou biométrico, devem ser acessados apenas quando for necessário em razão de motivos relacionados ao trabalho, como tratamento médico, por exemplo.

Alguns exemplos de situações nas quais podemos trazer riscos a privacidade de pacientes e colaboradores, em hospitais, são:

- Utilização de celulares para produção de imagens no interior de estabelecimentos de saúde (vedado de acordo com a Política de Comunicação);
- Fornecimento de informações de pacientes por telefone ou aplicativo de mensagens;
- Falta de controle de acesso ao prontuário do paciente e do colaborador;
- Compartilhamento de senhas de acesso ao prontuário eletrônico e a sistemas de uso interno;
- Liberação do resultado de exames sem a devida confirmação do usuário.

É importante ressaltar que, informações dos titulares de dados (assim entendidos colaboradores, pacientes, clientes, prestadores e fornecedores de serviços, etc.) não devem ser discutidas ou expostas em nenhuma área pública, incluindo elevadores, corredores e refeitórios, especialmente junto com terceiros estranhos aos fluxos de trabalho.

## PRINCÍPIOS

Para facilitar o reconhecimento de boas condutas e também das práticas que são inadequadas no dia a dia de uma instituição, destacam-se os **10 princípios** que norteiam a LGPD e que devem ser respeitados:

**Finalidade:** o tratamento dos dados pessoais deve ser feito de acordo com propósitos legítimos, específicos, explícitos e informados ao titular. Ou seja, a entidade deve explicar para que usará cada um dos dados pessoais.

**Adequação:** Os dados pessoais tratados devem ser compatíveis com a finalidade informada pela entidade. Ou seja, a justificativa deve fazer sentido com o caráter da informação solicitada.

**Necessidade:** aqui vale a regra do mínimo possível, ou seja, somente os dados que são realmente necessários àquela utilização devem ser utilizados aos titulares.

**Livre acesso:** a pessoa física titular dos dados tem o direito de consultar, de forma simples e gratuita, todos os dados que a entidade detenha a seu respeito. Além disso, devem ser especificadas questões sobre o que a empresa faz com as suas informações, de que forma o tratamento é realizado e por quanto tempo, por exemplo.

**Qualidade dos dados**: deve ser garantido aos titulares que as informações que a empresa tenha sobre eles sejam verdadeiras e atualizadas.

**Transparência**: todas as informações passadas pela empresa, em todos os seus meios de comunicação, devem ser claras, precisas e verdadeiras. Além disso, a entidade não pode compartilhar dados pessoais com outras pessoas de forma oculta.

**Segurança**: uso de medidas técnicas e administrativas que protejam os dados pessoais de acessos não autorizados, situações acidentais ou ilícitas, de destruição, perda, alteração, comunicação ou difusão.

Prevenção: medidas utilizadas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

**Não Discriminação**: os dados pessoais jamais podem ser usados para discriminar ou promover abusos contra os seus titulares. São os chamados “dados pessoais sensíveis”, como os que tratam sobre 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 e dado genético ou biométrico.

**Responsabilização e Prestação de Contas**: além do cumprimento integral da lei, os agentes de tratamento devem comprovar que realizam todas as medidas necessárias, para demonstrarem a sua boa-fé e a sua diligência.

Alguns bons exemplos da aplicação destas disposições é a realização de treinamentos de equipe, a utilização de protocolos e sistemas que garantam a segurança dos dados e o acesso facilitado do titular dos dados, se preciso.

## SENDO ASSIM, A LEI GARANTE DIREITOS COMO

- **Confirmação e acesso**: o titular pode solicitar a confirmação da existência de tratamento, bem como solicitar o acesso aos dados pessoais coletados e obter informações claras sobre a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento.
- **Correção**: o titular pode solicitar alterações em seus dados (correções, atualizações e exclusões).
- **Eliminação**: o titular dos dados pode solicitar a exclusão de seus dados dentro de determinado sistema.
- **Portabilidade**: deve ser possível que o titular consiga exportar seus dados pessoais de um sistema para outro.
- **Direito a explicação**: o titular pode solicitar informações sobre todos os algoritmos que interagem com seus dados para entender, por exemplo, porque um empréstimo do banco foi negado.

## OBRIGAÇÕES DOS CONTROLADORES E OPERADORES

Por definição legal, **Controlador** é toda pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dado pessoal.

Já o **Operador** é toda pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento dos dados pessoais em nome do controlador. As obrigações de ambos são extensas e próximas. Destacam-se:

- Observância dos princípios gerais e garantia dos direitos dos titulares dos dados;
- Adoção de medidas de segurança, técnicas e administrativas;
- Registrar as operações de tratamento de dados pessoais, mesmo após o seu término;
- Garantir a segurança da informação em relação aos dados pessoais que forem tratados;
- Reparação de danos aos titulares caso ocorra tratamento indevido dos dados pessoais;
- Formulação de regras de boas práticas e de governança;
- Sujeição às sanções administrativas aplicadas.

## RESPONSABILIDADE LEGAL

A partir do início da vigência da Lei, toda empresa deve ter um responsável certificado para gestão dos dados pessoais, o chamado *Data Protection Officer* (DPO).

A Autoridade Nacional de Proteção de Dados Pessoais (ANPD), quando da sua estruturação, será a entidade responsável por orientar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados (LGPD) e poderá, a partir de 3 de maio de 2021, segundo Medida Provisória 959/20, a autuar empresas públicas e privadas, de todos os portes, que não estiverem em conformidade, cobrando do *Data Protection Officer* (DPO) explicações no âmbito legal.

# CONCLUSÃO

A LGPD vem justamente para aprimorar a forma como as instituições tratam os dados pessoais dos titulares, razão pela qual a adequação a esta nova legislação será um processo que envolverá todos os departamentos da Entidade, trazendo uma transformação cultural na maneira de lidar com os dados que circulam dentro da organização, assumindo a responsabilidade de manter o sigilo, proteger e garantir a privacidade de todos.

É importante lembrar que a Pró-Saúde já possui políticas e procedimentos relacionados à privacidade e confidencialidade das informações nas relações formalizadas com seus colaboradores em sua missão humanitária de assistência à saúde e à educação.

PRÓ-SAÚDE

ASSOCIAÇÃO BENEFICENTE DE
ASSISTÊNCIA SOCIAL E HOSPITALAR