LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

IRMANDADE DA SANTA CASA DE MISERICÓRDIA CURITIBA 1852

SANTA CASA de Curitiba

Hospital Maternidade ALTO MARACANÃ

UNICA Unidade Integrada de Crise e Apoio à Vida

APRESENTAÇÃO

Com o intuito de esclarecer os principais aspectos desta nova legislação voltada à proteção de dados no Brasil, este material foi desenvolvido pela Irmandade da Santa Casa de Misericórdia de Curitiba 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 e seus familiares, fornecedores, prestadores de serviços).

INTRODUÇÃO – 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 a 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, vinha se mostrando 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), vigente desde 18 de setembro de 2020, que regulamenta o uso e a proteção de dados pessoais em todo o território nacional.

Com base na legislação europeia, a Lei nº 13.709/2018 consolida, atualiza e torna mais robustas 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 as 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 do 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 são fundamentais 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: (i) a exigência de **um propósito ou finalidade** para o tratamento dos dados; (ii) a **exigência do consentimento informado do titular** para o tratamento do dado; e (iii) **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:

- de identificação (nome, RG, CPF);
- profissional (salário, local de trabalho);
- física (altura, sexo, idade);
- geográfica (localização, endereço);
- relacionada a hábitos (compras, leitura, pesquisas), etc.

COMO A LGPD IMPACTA O DIA A DIA DA IRMANDADE DA SANTA CASA DE MISERICÓRDIA DE CURITIBA?

A ISCMC lida constantemente com dados de seus clientes (pacientes), 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 a sua responsabilidade, de acordo com os mais elevados padrões legais e éticos.

Para tanto, é de suma importância que nossos colaboradores, prestadores e fornecedores de serviços adiram 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 e seus respectivos titulares, é importante que esse cuidado esteja presente em todas as formas de acesso, seja eletrônico, físico, verbal, telefônico, etc.

O acesso aos dados pessoais sensíveis, ou seja, aqueles que envolvem origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual e dado genético ou biométrico, sejam realizados apenas quando for necessário, por exemplo, em razão de motivos relacionados ao trabalho (tratamento médico) ou por obrigação legal (processos judiciais).

São exemplos de situações que podem haver riscos à privacidade de pacientes e colaboradores em Hospitais:

- Utilização de celulares para produção de imagens no interior de estabelecimentos de saúde (vedado de acordo com a Política Interna da Instituição);
- Fornecimento de informações de pacientes por telefone ou aplicativo de mensagens;
- Falta de controle de acesso ao prontuário do paciente ou 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 e/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 de 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 solicitados 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 como: o que a empresa faz com suas informações; de que forma o tratamento é realizado; por quanto tempo, etc.

Qualidade dos dados: deve ser garantido ao titular dos dados que as informações que a empresa tenha sobre ele 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 (físicas ou jurídicas) de forma oculta.

Segurança: uso de medidas técnicas e administrativas que protejam os dados pessoais de acessos não autorizados, de 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 a 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 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 dos dados pode solicitar a confirmação da existência de tratamento, bem como solicitar 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 dos dados pode solicitar alterações em seus dados (correções, atualizações).
- Eliminação: o titular dos dados pode solicitar a exclusão de seus dados

dentro de determinado sistema (banco de dados).

- Portabilidade: deve ser possível que o titular consiga exportar seus dados de um sistema para outro (envio do prontuário médico de um Hospital para outro, por exemplo).
- Direito à explicação: o titular dos dados 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 competem as decisões referentes ao tratamento de dados pessoais.

Já o *Operador*, é toda pessoa natural 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 pela gestão dos dados pessoais, o chamado DPO - *Data Protection Officer* ou Encarregado.

A Autoridade Nacional de Proteção de Dados (ANPD), quando da sua estruturação, será o órgão responsável por orientar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados (LGPD) e poderá, a partir de 01 de agosto de 2021, segundo a Medida Provisória 959/2020, a autuar empresas públicas e privadas, de todos os portes, bem como pessoas físicas, que não estiverem em conformidade, cobrando do DPO - *Data Protection Officer* explicações no âmbito legal.

CONCLUSÃO

A LGPD vem justamente para aprimorar a forma como o tratamento dos dados pessoais dos titulares é realizado, 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, com a assunção conjunta da responsabilidade de manter o sigilo, proteger e garantir a privacidade de todos.

Por oportuno, é importante lembrar que a ISCMC 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.

LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

IRMANDADE DA SANTA CASA DE MISERICÓRDIA CURITIBA 1852

SANTA CASA de Curitiba
Complexo Hospitalar e Ambulatorial
Hospital de Ensino e Pesquisa

Hospital Maternidade ALTO MARACANÃ

UNICA
Unidade Integrada de Crise e Apoio à Vida