ANS - Nº3293339

Cartilha LGPD

Lei Geral de Proteção de Dados

Unimed Criciúma

Diretoria Executiva

Dr. Leandro Avany Nunes
Presidente

Dra. Clarissa Inês Almeida
Vice-Presidente

Dr. Rodrigo Benedet Scheidt
Superintendente

Dr. Gustavo Machado Viana
Diretor Administrativo Hospitalar

Dr. Fábio José Fabrício de Barros Souza
Diretor Técnico Hospitalar

Comissão de Formatação
do Comitê de Segurança da Informação

Dra. Clarissa Inês Almeida
Vice-Presidente

Dr. Rodrigo Benedet Scheidt
Superintendente

Sintia Michels Steiner
Gestora de Integração e Estratégia

Marcos Roberto de Faveri Souza
Gestor Jurídico e DPO

Kleber Folchini
Gestor de Tecnologia da Informação

Luiz Antonio Ferraro Dal Pont
Coordenador de Segurança da Informação

Leonardo da Silva Serafim
Analista de Segurança da Informação

Gabriel Corrêa Zilli
Analista de Compliance e Integridade

Histórico de Revisões

OPS-GOV-MAN-001

Emissão Inicial
Revisão 00 – 25/03/2021
Revisão 01 – 28/03/2024

Sumário

1. Introdução

A **Lei Geral de Proteção de Dados** regula a atividade sobre o uso de dados pessoais, de colaboradores e de terceiros, por todos os tipos de organizações que operam em território brasileiro, estabelecendo rigorosas sanções, em caso de descumprimento de suas determinações.

A elaboração da LGPD foi pautada no General Data Protection Regulation (GDPR), Regulamento de Proteção de Dados da União Europeia. No Brasil, a proteção de dados possui natureza jurídica de direito e garantia fundamental, com base no inciso XII-A do art. 5º e o inciso XXX do art. 22 da Constituição Federal, acrescentados pela Emenda Constitucional nº 17.

Sua aplicação se estende a qualquer pessoa, física ou jurídica, de direito público ou privado, que realize o tratamento de dados pessoais, online e/ou offline. Promove-se assim ações de conscientização no sentido de inserir o respeito a privacidade e sigilo dos dados dessas pessoas físicas em atividades profissionais cotidianas.

Os dados deverão ser utilizados apenas para as finalidades específicas para as quais foram coletados e devidamente informadas aos titulares (Princípio da Finalidade). Somente devem ser colhidos os dados mínimos necessários para que se possa atingir a finalidade (Princípio da Minimização da coleta). Após alcançada a finalidade pela qual eles foram coletados, deve ser feita a imediata exclusão dos dados (Princípio da Retenção Mínima).

Assim, a importância da referida Lei se reflete em maior segurança jurídica e proteção aos direitos dos titulares de dados.

1.1 Apresentação

A Lei nº 13.709 – Lei Geral de Proteção de Dados foi aprovada em agosto de 2018 e terá vigência a partir de agosto de 2020. O assunto é de suma importância, pois visa a segurança jurídica, padronizando normas e práticas, promovendo a proteção de dados pessoais de todos os cidadãos, em âmbito nacional.

Abrange dados pessoais obtidos em qualquer tipo de suporte seja físico, como papel, até som, imagem ou virtual. Ocorrendo o vazamento dessas informações coletadas, serão analisados por um Comitê e os envolvidos deverão reparar os danos, seja patrimonial, moral, individual ou coletivo.

1.2 Objetivo da Lei

O objetivo da lei é garantir a proteção aos dados pessoais obtidos (inclusive por meios digitais), respeitados os direitos fundamentais de liberdade, integridade e de privacidade, que possam ser eventualmente violados pela má utilização dessas informações, permitindo maior confiança em relação à coleta e uso de dados, maior segurança jurídica e, em consequência, o fomento ao desenvolvimento econômico e tecnológico da sociedade, à medida que estabelece regras claras sobre proteção de dados pessoais.

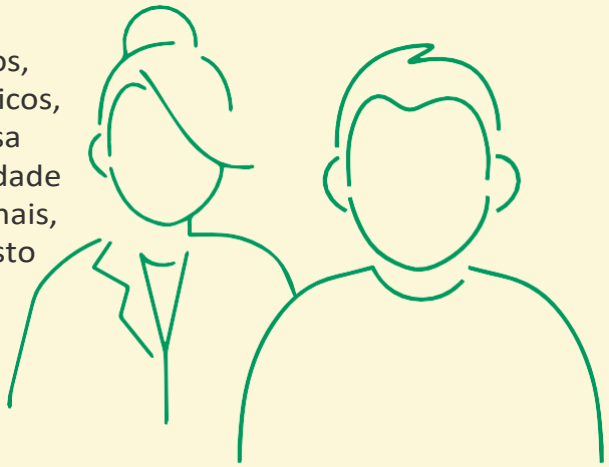
1.3 Fundamentos da Proteção de Dados

- O respeito à privacidade.
- A autodeterminação informativa.
- A liberdade de expressão, de informação, de comunicação e de opinião.
- A inviolabilidade da intimidade, da honra e da imagem.
- O desenvolvimento econômico e tecnológico e a inovação.
- A livre iniciativa, a livre concorrência e a defesa do consumidor.
- Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

2. A Quem se Aplica

Esta lei é aplicada não só para pessoas naturais (físicas), mas também para pessoas jurídicas de direito público e privado no qual realizam o tratamento dos dados coletados, seja por meio físico ou digital.

Cabe destacar que a lei não se aplica ao tratamento de dados realizado para fins exclusivamente particulares e não econômicos, para fins exclusivamente jornalísticos, artísticos, acadêmicos, de segurança pública, de defesa nacional, de segurança do Estado ou de atividade de investigação ou repressão de infrações penais, entre outras, conforme expressamente disposto em seu artigo 4º.



3. Direito dos Titulares dos Dados

Para estar em conformidade com a Lei Geral de Proteção de Dados, as empresas precisam atender às necessidades dos titulares dos dados, tais como:

- Conhecimento do processo de tratamento de dados pessoais.
- Acesso total aos seus dados sob custódia da empresa.
- Correção ou atualização de seus dados.
- Anonimização.
- Possibilidade de solicitação de portabilidade dos dados para outras empresas.
- Exclusão dos dados a qualquer tempo.
- Informação sobre compartilhamento de dados.
- Revogação do consentimento.

4. Pontos Importantes

A Lei Geral de Proteção de Dados (LGPD) apresenta pontos importantes em toda sua extensão.

Os dados deverão ser utilizados apenas para as finalidades para as quais foram coletados e as finalidades devem ser devidamente informadas aos titulares. Somente devem ser colhidos os dados mínimos necessários para que se possa atingir a finalidade. Após alcançada a finalidade pela qual eles foram coletados deve ser feita a imediata exclusão dos dados.

Com o intuito de facilitar a aplicação da referida legislação, relacionamos os pontos a seguir:

- Abrangência: Quaisquer dados pessoais obtidos em qualquer tipo de suporte (papel, eletrônico, em ambiente virtual, som, imagem, etc.).
- Regra para todos: Criação de um panorama de segurança jurídica para todo o país.
- Fiscalização centralizada: Ficará a critério da Autoridade Nacional de Proteção de Dados Pessoais (ANPD).
- Transparência: Ocorrendo vazamento de dados, a ANPD e os indivíduos afetados devem ser comunicados.
- Finalidade e necessidade: Os quesitos de tratamento devem ser previamente informados ao cidadão.
- Contratos de adesão: Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou serviço, o titular deverá ser claramente informado.
- Responsabilidade civil: O responsável que, em razão do exercício de atividade de tratamento de dados, causar dano patrimonial, moral, individual ou coletivo, será obrigado a repará-lo.

5. Conceitos Específicos

A interpretação do texto legal requer a observância de conceitos específicos relacionados na LGPD, conforme segue:

- Agentes de tratamento: o controlador e o operador;
- Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
- Autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta lei;
- Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
- Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;
- Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
- Controlador: pessoa física ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais;
- Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
- Encarregado (DPO): pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados;
- Operador: pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
- Órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no país, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico;
- Relatório de Impacto à Proteção de Dados Pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;
- Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
- Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;
- Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados

pessoais por entidades e órgãos públicos no cumprimento de suas competências legais, ou entre entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

5.1 Dado Pessoal

É qualquer informação que possa levar a identificação de uma pessoa natural, de forma direta ou indireta, por referência a um nome, a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica, cultural ou social. Podemos tomar como exemplo Nome, Endereço, E-mail, Endereço de IP, CPF, etc.

5.2 Dado Pessoal Sensível

Dado pessoal 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, dado genético ou biométrico, quando vinculado a uma pessoa natural.

5.3 Tratamento

Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

6. Princípios

As condutas conceituadas como “tratamento da informação” deverão observar:

- Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
- Finalidade: realização do tratamento para os propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
- Livre acesso: garantia aos titulares de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
- Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios, ilícitos ou abusivos;
- Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
- Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
- Qualidade dos dados: garantia aos titulares de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
- Responsabilização e prestação de contas: demonstração pelo agente da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e inclusive, da eficácia dessas medidas;
- Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão das informações sob custódia;
- Transparência: garantia aos titulares de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

7. Privacidade dos Dados Pessoais

Privacidade de dados significa o consentimento do controle da exposição e disponibilidade de informações sobre terceiros, disseminados e compartilhados no meio digital ou não.

Segurança de dados e privacidade têm abordagens bastante diferentes para alcançar o objetivo principal. A segurança de dados está principalmente focada em proteger a informação de ataques cibernéticos e violações, enquanto a privacidade trabalha a maneira como essa informação é coletada, compartilhada e utilizada.

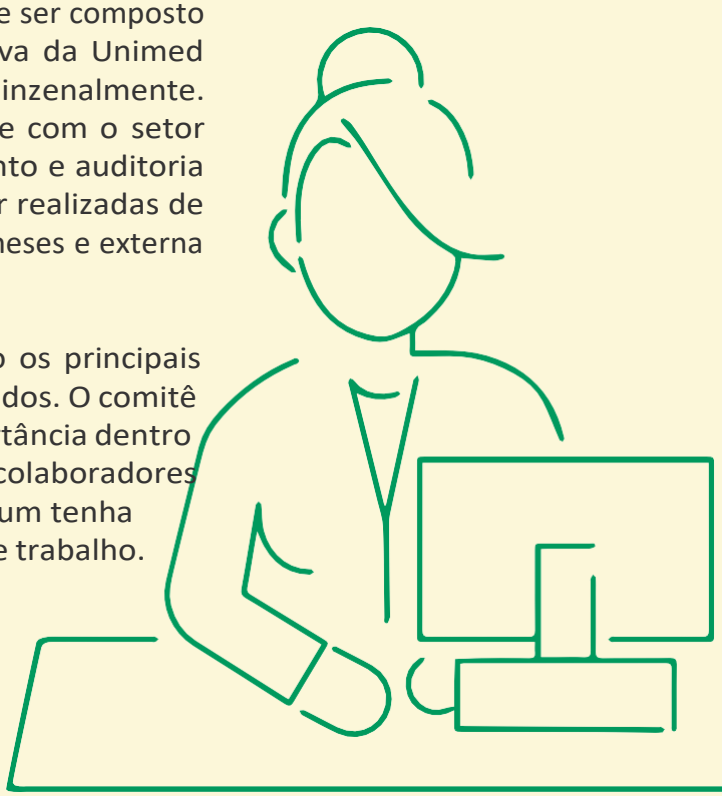
Na atualidade, a informação tornou-se um dos bens mais valiosos. Diariamente usamos, absorvemos, produzimos e transmitimos informações o tempo todo. Desta forma, podemos afirmar que um dos grandes desafios contemporâneos é assegurar a proteção e a privacidade para estes dados.

Esta garantia se aplica independentemente do meio ou forma de tratamento dos dados coletados ou recebidos, incorrendo que todo aquele que faz uso do dado deve observar as regras legais.

Desta forma, para que haja o cumprimento das obrigações e procedimentos previstos na lei, o conceito de privacidade dos dados pessoais deverá nortear qualquer tratamento de dados realizado pelos controladores.

8. Comitê e seus Membros

O comitê de Segurança da Informação deve ser composto por membros indicados pela Diretoria Executiva da Unimed Criciúma, o qual deverá reunir-se semanal ou quinzenalmente. Este comitê também é responsável juntamente com o setor de Tecnologia da Informação pelo gerenciamento e auditoria de Segurança da Informação no qual devem ser realizadas de forma interna em períodos não superiores a 06 meses e externa a cada 18 meses.



Os membros que compõe o comitê são os principais atores no tratamento dos dados pessoais coletados. O comitê de segurança da informação é de extrema importância dentro da empresa, porém, é necessário que todos os colaboradores façam a sua parte. Por isso, é preciso que cada um tenha consciência ao realizar as atividades na rotina de trabalho.

9. Critérios para Uso de Dados

O consentimento é a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada, exceto nas seguintes situações:

- Para a proteção do crédito, nos termos do Código de Defesa do Consumidor.
- Para o cumprimento de obrigação legal ou regulatória pelo responsável pelo tratamento.
- Para a realização de estudos por órgão de pesquisa, sem a individualização da pessoa.
- Para o exercício regular de direitos em processos judiciais, administrativo ou arbitral.
- Para execução de contrato ou procedimentos preliminares relacionados a um contrato.
- Pela administração pública, para o uso compartilhado de dados necessários à execução de políticas públicas.
- Para a tutela de saúde, com procedimento realizado por profissionais da área ou por entidades sanitárias.

10. Proteção do Denunciante

A Lei Geral de Proteção de Dados (LGPD), em seu art. 1º da lei deixa claro o objetivo da nova norma: “proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, seja por meios digitais ou não”. No art. 5º são expostos importantes conceitos para a correta compreensão e aplicação da lei.

O Comitê de Segurança da Informação deve aprovar as medidas de proteção à identidade das pessoas que procuram os canais de denúncia como ouvidoria, SAC, direção, coordenadores, comissões, registro de ocorrência e urnas para registrar suas manifestações, quanto à prestação de serviços e à conduta dos Colaboradores.

Existem alguns conceitos que auxiliam na aplicação adequada das cautelas aos processos de proteção de dados pessoais sensíveis, que são:

- Denúncia: ato que indica a prática de ilícito ou irregularidade cuja solução dependa da atuação dos órgãos apuratórios competentes da Empresa.
- Denunciante: toda pessoa física ou jurídica que denuncia qualquer ilícito ou irregularidade.
- Elemento de identificação: qualquer dado ou informação que permita a associação direta ou indireta do denunciante à denúncia por ele realizada.
- Regras de proteção à identidade: conjunto de medidas ou procedimentos adotados com a finalidade de proteger a identidade do denunciante e garantir o tratamento adequado aos elementos de identificação da denúncia, implementado por meio do sistema de tecnologia utilizado pelos canais de denúncia.

11. Responsabilidades, Segurança e Sanções

O operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador.

Os controladores que estiverem diretamente envolvidos no tratamento de dados e que porventura, causarem danos ao titular, respondem solidariamente.

A Autoridade Nacional de Proteção de Dados (ANPD), criada pela Lei nº 13.853/2019, atuará como uma agência reguladora. Dentre suas inúmeras atribuições, está a obrigação de fiscalizar e aplicar sanções em caso de descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso.

A Autoridade Nacional de Proteção de Dados verifica o incidente e poderá determinar aos agentes de tratamento (controlador e operador) as providências necessárias para eliminar irregularidades, incertezas jurídicas ou situações contenciosas no âmbito de processos administrativos.

Os agentes de tratamento de dados ficam sujeitos às seguintes sanções:

- Advertência, com indicação de prazo para adoção de medidas corretivas.
- Multa de até 2% (dois por cento) do faturamento da empresa, limitada ao total de R$ 50.000.000,00 (cinquenta milhões de reais) por infração.
- Multa diária, observado o valor total acima.
- Publicização da infração após apuração e confirmação da ocorrência.
- Bloqueio do tratamento dos dados pessoais a que se refere a infração.
- Eliminação dos dados pessoais a que se refere a infração.

Nesse contexto, é importante esclarecer que o Comitê de Segurança da Informação sempre possibilita que o denunciante se mantenha anônimo. Trata-se de uma questão essencial, pois os fatos relatados pelos denunciantes são bastante sensíveis. O anonimato, portanto, visa garantir ao usuário a tranquilidade e a segurança necessárias para o reporte das informações.

As sanções seguirão critérios como gravidade da infração, boa fé do infrator, possíveis vantagens econômicas auferidas pelo infrator, reincidência, cooperação para esclarecimento do caso, demonstração de evidências de mecanismos e procedimentos e adoção de boas práticas de segurança para minimizar possíveis danos causado aos titulares.

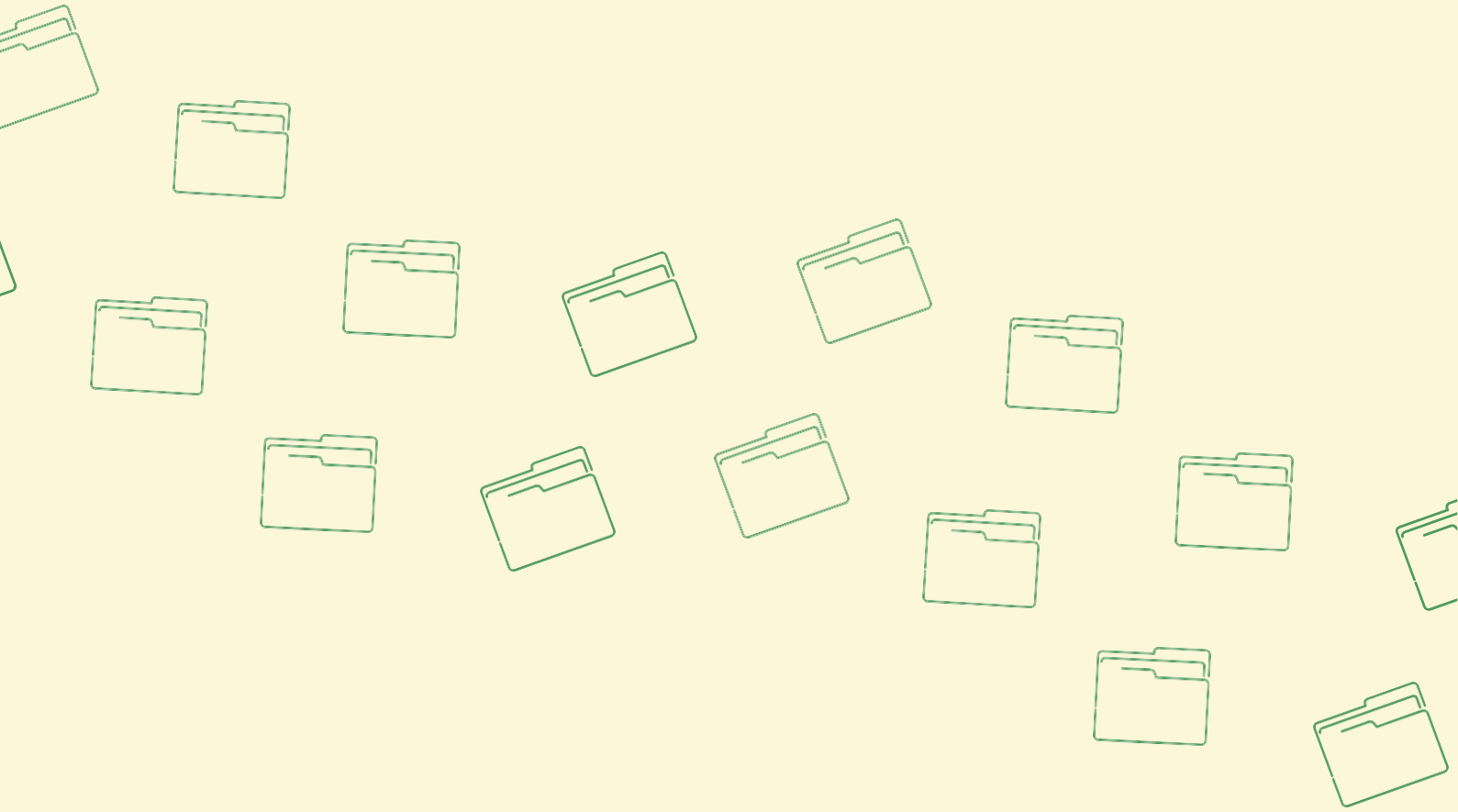
12. Tratamento dos Dados Alinhado a um Processo de Governança

É importante entender como a Operadora de Saúde Unimed Criciúma e Recursos Próprios funcionam em todas as suas esferas e identificar as áreas com maior acesso a dados pessoais em suas operações.

Para isso, vale realizar um trabalho em conjunto com as áreas de gerenciamento de riscos, visando a identificação com controle interno que possa facilitar o cumprimento de alguns princípios estabelecidos na Lei Geral de Proteção de Dados. A partir de seus resultados, possa identificar quais são os objetivos e finalidades da Operadora, a fim de analisar os dados que efetivamente são necessários para atingir tais objetivos.

Vale ter sempre em mente que se o titular solicitar a eliminação dos dados ou quaisquer informações concernentes ao seu tratamento, bem como na eventualidade de uma visita da fiscalização, o Comitê de Segurança da Informação deverá estar preparado para fornecê-las de forma clara.

Logo, todo o processo de mapeamento deve considerar também o pressuposto de que ambas as hipóteses podem acontecer a qualquer momento. Demonstramos no fluxo a seguir a sequência e a importância de manter um processo de governança preocupado com a segurança e o gerenciamento das informações dentro da Operadora.



UMA REGRA PARA TODOS:
Cria um cenário de segurança jurídica válido para todo o país.

MAIS PARA O CIDADÃO:
O consentimento é a base para que os dados possam ser tratados.

DEFINIÇÃO DO CONCEITO:
Estabelece, de maneira clara, o que são dados pessoais.

AS EXCEÇÕES:
Sem consentimento, apenas se for indispensável para cumprir critérios legais.

ABRANGÊNCIA TERRITORIAL:
Não importa se a organização ou centro de dados estão dentro ou fora do Brasil.

TRANSFERÊNCIA INTERNACIONAL:
Permite o compartilhamento com outros países que também protejam dados.

FISCAL CENTRALIZADO:
Ficará a cargo da Autoridade Nacional de Proteção de Dados Pessoais (ANPD).

RESPONSABILIDADE:
Define os agentes de tratamento de dados e suas funções.

GESTÃO DE RISCO E FALHAS:
Quem gere base de dados pessoais terá que fazer essa gestão.

TRANSPARÊNCIA:
Se ocorrer vazamento de dados, ANPD e indivíduos afetados devem ser avisados.

PENALIDADES RÍGIDAS:
Falhas de segurança podem gerar multas pesadas.

FINALIDADE E NECESSIDADE:
São quesitos do tratamento que devem ser previamente informados ao cidadão.

Em relação aos dados pessoais armazenados no banco de dados da Unimed Criciúma, é imprescindível identificar o interesse ou o consentimento do titular para qualquer tratamento de dados que resulte em compartilhamento das informações. Para o atendimento a esse conjunto de leis, é importante a criação de uma cláusula geral de concordância para divulgação de dados, em documentos e contratos. Também para garantir o cumprimento da legislação, o armazenamento de dados sensíveis deverá ser seguro e com acesso controlado devendo ter como fundamento as bases legais que a Lei nos impõe, partindo do principal objetivo que seria o consentimento do titular.

12.1 Consentimento do Titular

- Cumprimento de Obrigação Legal.
- Políticas Públicas.
- Estudos por órgãos de pesquisas.
- Execução Contratual.
- Processo Judicial.
- Proteção da Vida.
- Tutela da Saúde.
- Interesse Legítimo.
- Proteção do Crédito.

13. Considerações finais

A Lei Geral de Proteção de Dados pretende criar uma cultura de respeito e integridade à privacidade dos dados pessoais, no intuito de garantir segurança e tranquilidade aos clientes, parceiros e consumidores, prevenindo eventuais fraudes ou uso indevido que possa afetar a intimidade, a honra e a imagem do titular de tais dados, ou até a tentativa de obter alguma vantagem ilícita com a Cooperativa. Ela visa que o titular dos dados tenha direito sobre o controle ou, ao menos, sobre a transparência do tratamento de seus dados pessoais, para que tenham ciência dos fins a que seus dados estejam sendo utilizados.

A Lei Geral de Proteção de Dados faz parte do conjunto de normas, formado também pela Lei de Acesso à Informação (Lei nº 12.527/2011) e pela Lei da Transparência (LC nº 101/2009), que exige clareza na divulgação de atos e ações, ao mesmo tempo em que estabelece restrições quanto a divulgação dos dados pessoais.

Diante da análise da legislação, verifica-se que a adequação às novas determinações legais é complexa e não será imediata. Portanto, é fundamental que a empresa seja célere em se preparar para o atendimento à Lei Geral de Proteção de Dados.

14. Referências bibliográficas

ASSOCIAÇÃO NACIONAL DE HOSPITAIS PRIVADOS (ANAHP). Lei geral de proteção de dados: Recomendações aos Hospitais. 1. Ed. 2018. Disponível em: <https://conteudo.anahp.com.br/cartilha-lgpd-anahp>. Acesso em: 09 set. 2020.

CONFEDERAÇÃO DAS SANTAS CASAS E HOSPITAIS FILANTRÓPICOS (CMB). Lei geral de proteção de dados: Cartilha orientativa. 1. Ed. 2018. edição - Disponível em: <https://www.cmb.org.br/cmb/documentos/GuiaLGPD-2020.pdf>. Acesso em: 09 set. 2020.

CONFEDERAÇÃO NACIONAL DO COMÉRCIO DE BENS, SERVIÇOS E TURISMOS. Cartilha: Lei geral de proteção de dados. 2019. Disponível em: <http://www.cnc.org.br/editorias/diario-legislativo/livros/cartilha-lei-geral-de-protecao-de-dados>. Acesso em: 10 set. 2020.

VILHENA, Pedro. Lei geral de proteção de dados. 2019. Tribunal de Justiça - Rio Grande do Sul. Disponível em: <https://www.tjrs.jus.br/export/poder_judiciario/tribunal_de_justica/centro_de_estudos/horizontes/2019-04-25_-_LGDP_TJRS.pdf>. Acesso em: 09 set. 2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 24 jul. 2020

ANS - Nº329339

Unimed
Criciúma