CARTILHA DA POLÍTICA MULTIDISCIPLINAR DA LGPD

V. 0421.1

ANS - nº 41652-5

1. INTRODUÇÃO

Em um mercado cada vez mais global que exige transparência em todos os setores da economia.
Com uma sociedade cada vez mais movida e orientada por dados pessoais e empresariais nas redes, o Brasil ingressou nesse pacto social mundial de proteção ao titular do dado.
A General Data Protection Regulation (GDPR), formalizou as regras para coleta e uso de dados pessoais em 28 países, prevendo duras punições em todo continente europeu e também com as organizações em todo o mundo.
Assim, inspirada na GDPR, foi criada no Brasil a Lei Geral de Proteção de Dados (LGPD) em maio de 2018, que entrou em vigor em Setembro/2020, passando a ser infrativa em Agosto de 2021.
O objetivo formal da LGPD é “proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”.
A LGPD está impulsionando e qualificando a regra de negócios no Brasil, elevando o nível de privacidade e proteção de dados, com adequações para transações comerciais, processos e fluxos internos, garantindo um ambiente operacional seguro, por meio da transparência.
Precisamos envolver todos os departamentos e colaboradores, pois será uma transformação na maneira de lidar com os dados que circulam dentro da operadora.
Nosso plano de ação engloba funções multidisciplinares para mudança comportamental, com o envolvimento de pessoal, em todas as áreas, com gestão de risco e compliance, adequando e integrando as rotinas da operadora, com posturas proativas, em busca de transparência e confiabilidade, evitando brechas.
Os números relacionados ao vazamento de dados são superlativos, por isso mitigar os riscos é pauta do nosso dia a dia, mesmo com todos os esforços temos exemplos de casos de grande repercussão, como: C&A, YAHOO, SEBRAE entre outros; por isso, todos os esforços estão sendo utilizados para reduzir drasticamente a exposição ao risco e minimizar possíveis sanções.
A implementação dessas ações irá trazer um impacto positivo não somente nos processos “obrigatórios”, mas também em aspectos menos tangíveis como a transformação cultural de rotinas operacionais pautadas na prevenção, que fortalece a reputação da marca da operadora perante o mercado.
Por isso, proteger a integridade do titular do dado e o direito de saber o que é feito com as informações pessoais, é a demonstração da operadora em se comprometer com o ativo mais importante da atualidade, o DADO.

2. PRINCIPAIS DIREITOS DO TITULAR DO DADO

2.1 Privacidade dos dados pessoais;

2.2 Solicitar a confirmação se existe e como o dado está sendo tratado;

2.3 Ter acesso aos dados pessoais coletados e obter informações claras sobre a origem da coleta dos dados;

2.4 O titular pode solicitar alterações em seus dados (correções, atualizações e exclusões);

2.5 Eliminação do cadastro do banco de dados, solicitando a inexistência de registro, devendo ser observado contudo, se o dado poderá ser mantido por tempo determinado para atender as obrigações legais da operadora;

2.6 Portabilidade: deve ser possível que o titular consiga exportar seus dados pessoais de um sistema para outro;

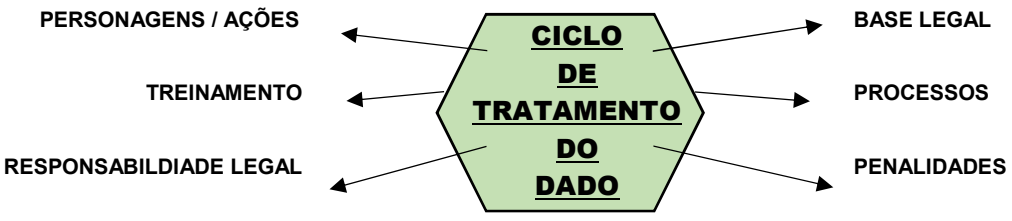
2.7 Direito a explicação: o titular pode solicitar informações sobre todos os algoritmos que interagem com seus dados para entender, por exemplo, porque um empréstimo do banco foi negado;

2.8 Responsabilidade da operadora sobre o uso de dados pessoais assim classificados:

2.8.1 DADOS QUE IDENTIFICAM (ex: nome, RG ou CPF);

2.8.2 DADOS IDENTIFICÁVEIS (ex: endereço IP, geolocalização do beneficiário, orientação política ou religiosa, entre outros).

3. CICLO DE TRATAMENTO DE DADOS



4. PERSONAGENS / AÇÕES

São as pessoas envolvidas no processo para o cumprimento à LGPD, sendo eles:

4.1 **Titular do dado** é a “pessoa natural a quem se referem os dados pessoais que são objeto de tratamento”.

4.2 **Agente de Governança**, pessoa que define quem decide o quê, como e quando as ações serão executadas;

4.3 **Agente de Risco** dedica-se a analisar possíveis ameaças à realização dos trabalhos a serem realizados;

4.4 **Agente de Compliance** (Conformidade), refere-se a pessoa que dita as rotinas de constante vigilância interna a fim de assegurar o objetivo principal de zelar pela conformidade dos processos e operações, em acordo com leis e regulamentações locais bem como em relação às políticas, normas, manuais e procedimentos internos, proporcionando confiança;

4.5 **Benchmarking interno** (avaliação comparativa interna), pessoa que analisa as rotinas dentro da própria empresa, buscando melhorar as boas práticas, desenvolvendo metodologia de segurança, visando adequação aos modelos de negócio, considerando a proteção dos dados pessoais

4.6 **Agentes de tratamento**, são classificados como:
4.6.1 **Controlador** é quem, precisa tomar as decisões de como o dado será tratado
4.6.2 **Operador** é quem vai executar as ordens do controlador

4.7 **Encarregado** é o responsável pelo canal de comunicação entre o titular do dado e os agentes de tratamento

4.8 **DPO** (Data Protection Officer / Proteção de Dados e Privacidade), responsável por reportar o cumprimento da lei para a ANPD

4.9 **ANPD** (Autoridade Nacional de Proteção de Dados)

4.10 **Comitê Multidisciplinar** formado pelo corpo administrativo, financeiro, comercial, técnico e jurídico da operadora, que ficará a cargo de criar a "CARTILHA DA POLÍTICA MULTIDICIPLINAR DA LGPD".
4.10.1 Este comitê atua em caráter consultivo e colaborativo, associado as suas respectivas atribuições, destacam-se por promover práticas e princípios de conduta, com padrão de comportamento, oferecendo suporte necessário para sua efetiva implantação. Supervisionando a inclusão de estruturas adequadas de governança, gestão de riscos, controles internos com o mapeamento de dados.

4.11 **Gestão de Riscos** é o Processo de Avaliação de Riscos com o objetivo de promover o aprimoramento institucional por meio de instrumentos que contribuem com a melhoria de sua Governança e propiciam maior eficácia organizacional.

4.12 **TRATAMENTO DE DADOS PESSOAIS** Significa toda operação realizada com dados pessoais, tais como:
4.12.1 Coleta
4.12.2 Produção
4.12.3 Recepção
4.12.4 Classificação
4.12.5 Utilização
4.12.6 Acesso
4.12.7 Reprodução
4.12.8 Transmissão
4.12.9 Distribuição
4.13.10 Processamento

4.13.10 Arquivamento
4.13.11 Armazenamento
4.13.12 Eliminação
4.13.13 Avaliação
4.13.10 Controle
4.13.11 Modificação
4.13.12 Comunicação
4.13.13 Transferência
4.13.14 Extração

5. TREINAMENTO

Conscientizar e capacitar continuamente os parceiros e colaboradores sobre a abrangência e impactos da Lei, com o objetivo de eliminar brechas decorrentes de pequenas ações particulares em uma atividade regular dentro da operadora, com orientações gerais como:
5.1 **Transparência:** Informações prestadas aos titulares dos dados de forma clara, resumida porém precisa, onde demonstra o conceito usando poucos recursos;

5.2 **Responsabilidade e prestação de contas:** Medidas e rotinas eficazes para o fiel cumprimento da lei;

5.3 **Adequação:** das rotinas para atender a finalidade da coleta do dado.

5.4 **Necessidade:** Identificar a real necessidade de coleta e utilização do dado, restringindo apenas aos necessários para o tratamento.

5.4 **Finalidade:** Propósito legítimo, específico, explícito pelo qual o dado foi coletado.

5.3 **Prevenção:** Medidas para evitar o vazamento de dados e riscos ao titular do dado.

5.4 **Segurança:** Medidas técnicas, administrativas e jurídicas para a proteção dos dados pessoais.

5.5 **Quantidade dos Dados:** O estritamente necessário, dados exatos, claros, relevantes para a prestação de serviço.

5.6 Não discriminação: Não utilização para fins discriminatórios e ilícitos.

5.7 **Livre acesso:** dar ao titular do dado o acesso à coleta e tratamento do mesmo, “CICLO DE VIDA DOS DADOS” (onde, como, quando, porque, para quem o dado é transitado).

6. RESPONSABILIDADE LEGAL

TEXTO EM DESENVOLVIMENTO (hierarquia dos personagens ...)

7. BASES LEGAIS - AS BASES LEGAIS DA LGPD, OU SEJA, OS REQUISITOS DE TRATAMENTO DE DADOS ESTABELECIDOS NO ART. 7 DA LEI

7.1. As 10 Bases Legais:

7.1.1 Consentimento do titular art. 7, I, LGPD
7.1.2 Legítimo Interesse art. 7, IX, LGPD
7.1.3 Cumprimento de obrigação legal ou regulatória art. 7, II, LGPD
7.1.4 Tratamento pela administração pública art. 7, III, LGPD
7.1.5 Realização de estudos e de pesquisas art. 7, IV, LGPD
7.1.6 Execução ou preparação contratual art. 7, V, LGPD
7.1.7 Exercício regular de direitos art. 7, VI, LGPD
7.1.8 Proteção da vida e da incolumidade física art. 7, VII, LGPD
7.1.9 Tutela de saúde do titular art. 7, VIII, LGPD
7.1.10 Proteção de crédito art. 7, X, LGPD

7.2. As 04 Bases Legais mais utilizadas no segmento de saúde suplementar, em particular pela PrimaVida Dental são:

7.2.1 Consentimento do titular, art. 7, I, LGPD
7.2.2 Legítimo Interesse, art. 7, IX, LGPD
7.2.3 Cumprimento de obrigação legal ou regulatória, art. 7, II, LGPD
7.2.4 Execução ou preparação contratual, art. 7, V, LGPD

7.2.1 Essas bases legais são assim classificadas:

7.2.1 Consentimento do titular, art. 7, I, LGPD

O consentimento fornecido pelo titular é a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (art. 5, XII, LGPD).

7.2.1.1 Nesse sentido, o consentimento do beneficiário é a máxima para executar as operações com seus dados pessoais.
Obter o consentimento deve ser o objetivo principal, por isso seguimos as seguintes condições:
a) **Validade** do consentimento é a condição de existência do ato, mas, para que se torne válida, devemos seguir alguns requisitos entre eles:
b) **Manifestação de vontade** deve ser livre, consciente e voluntária, formada mediante o conhecimento do titular dos dados de todas as informações necessárias para tal, o que inclui a finalidade do tratamento de dados e eventual compartilhamento;
c) As condições de validade do consentimento se confundem com o cumprimento dos direitos do beneficiários e dos princípios previstos na LGPD, por isso, para harmonizar esses três pontos é preciso chancelar os seguintes direitos:
c.1) Acesso às informações sobre seus dados;
c.2) Permitir que o titular controle seus dados.
c.3) Explicar cada um deles e seus desdobramentos.
d) Existência do consentimento é necessária que sejam seguidos alguns critérios, para que se obtenha consentimento espontâneo e voluntário, sendo:

d.1) **Clareza das informações** sobre o uso de dados, como os dados serão coletados, a finalidade de seu uso (art. 6, V, LGPD);
d.2) **Confirmação da existência** de tratamento (art. 18, III, LGPD);
d.3) **Atualização das informações e do consentimento**, conforme a alteração no tratamento de dados (art. 9, § 2º, LGPD);
d.4) **Direito a revisão e controle** pelo titular dos dados de decisões tomadas, apenas em tratamento de dados pessoais que afetem seus interesses (art. 20, LGPD), significando que o titular do dado pode realizar alterações ainda que isso possa resultar na revogação do consentimento, devendo ser observado as regras gerias que estabelecem a legislação:
d.4.1) **Correção** de dados incompletos, inexatos ou desatualizados (art.18, III, LGPD);
d.4.2) **Armazenamento** dos dados deve ser feito em formato que favoreça o exercício do direito de acesso (art. 18, § 1º, LGPD);
d.4.3) **Portabilidade** dos dados (art. 18, V, LGPD);
d.4.4) **Eliminação** dos dados, salvo as exceções previstas no art. 16, a exemplo do Cumprimento de obrigação legal ou regulatória, devendo para esses casos emitir declaração justificando os motivos que o impediram de fazer o procedimento (art. 18, § 4º, I e II, LGPD);
d.4.4.1) O titular do dado tem a liberdade para autorizar, negar ou revogar (reconsiderar) autorização anteriormente concedida para tratamento de seus dados pessoais com procedimento gratuito e facilitado (art. 8, § 5º, LGPD);
d.5) **Eficácia do consentimento**, é a forma como foi realizada, através de cláusulas contratuais com finalidade determinada, ou instrumento jurídico complementar, tais como aditivo e apenso.

7.2.2 Legitimo interesse

7.2.2.1 Está ligado diretamente a atividade comercial, sendo no caso concreto a Prestação de Serviços na Odontologia de Grupo no segmento de Mercado Saúde Suplementar, fundamentada em uma das 10 bases legais.
7.2.2.2 De acordo com o art. 7, IX e o art. 10 da LGPD, o legítimo interesse poderá basear o tratamento para finalidades legítimas da atividade, podendo o primeiro englobar diversas hipóteses para o tratamento de dados, desde que observado:
a) **Apoio e promoção** da atividade;
b) **Proteção regular** dos direitos e expectativas da qualidade na prestação de serviços devendo atentar para as seguintes condições:
b.1) Coletar somente os dados pessoais estritamente necessários para a finalidade pretendida (art. 10, § 1º,LGPD);
b.2) Garantir a transparência do tratamento de dados (art. 10, § 2º, LGPD);
b.3) As legítimas expectativas do titular devem ser respeitadas (art. 10, II, LGPD);
b.4) Os princípios da LGPD e os direitos do titular devem ser assegurados (art. 10, II, LGPD);
b.5) Adequar os demais critérios de tratamento de dados de acordo com o tipo, como dados sensíveis de crianças e adolescentes.
c) **Legítima expectativa** do titular são as expectativas de que o uso do dado será tratado com uma finalidade especifica, diante do instante que foi coletado.
d) **Medidas de segurança** do legitimo interesse:
d.1) Produção de relatório de impacto à proteção de dados pessoais (art. 10, § 3º, LGPD), devendo ser observado o disposto no art. 37, parágrafo único da mesma lei; e Registro das operações de tratamento de dados pessoais que realizado (art. 37, LGPD);
d.2) Teste de Ponderação, inspirado na GDPR, sem obrigação legal de fazer na LGPD, tem como objetivo avaliar a utilização do legítimo interesse conforme o caso concreto.

7.2.3 Cumprimento de obrigação legal ou regulatória

O tratamento de dados para cumprimento de obrigação legal ou regulatória é uma regra de legalidade ampla que busca preservar o interesse da segurança jurídica por força de lei, mesmo após o encerramento do vínculo negocial que originou o tratamento, é permitido armazenar dados pessoais em função do cumprimento de obrigações do ordenamento jurídico como um todo, devendo ser nesses casos observado os prazos para o armazenamento dos dados nas normas específicas.

7.2.4 Execução de contratos

O consentimento do titular pode ser realizado como expressão de vontade no momento da formalização do contrato, portanto, o ato de assinar o contrato é o consentimento tácito para os usos dos dados em função da preparação e execução contratual.

8. PROCESSOS

8.1 Todo o ciclo de vida dos dados pessoais dentro da empresa deve ser levantado e analisado pelo comitê multidisciplinar que garantirá sua total adequação à LGPD, seguindo quatro passos:

8.1.1 TECNOLOGIA
8.1.2 SEGURANÇA DA INFORMAÇÃO
8.1.3 AUDITORIA E CONTROLE
8.1.4 DATA MAPPING (MAPEAMENTO DE DADOS)
8.1.5 PRINCÍPIO DA BOA FÉ
8.1.6 REVISÃO JURIDICA

8.1.1 TECNOLOGIA

A tecnologia que tem por objetivo a oferta de estrutura e flexibilidade para atender as necessidades da operadora nos diversos estágios de adequação à LGPD de forma a minimizar o risco, envolvendo no trabalho em conjunto, a segurança da informação com o comitê multidisciplinar que estabelece políticas de governança para a gestão e exclusão dos dados pessoais, passando por todas as etapas do ciclo de vida do dado, que precisam ser devidamente documentadas para que haja respaldo jurídico em caso de acionamento judicial.

8.1.2 SEGURANÇA DA INFORMAÇÃO

- Varredura de servidores locais e em nuvem, além de estações de trabalho;
- Checagem da configuração das ferramentas em uso;
- Criptografia de dados;

• Adoção de ferramenta de DLP (Data Loss Prevention);
• Segregação de permissões de acessos;
• Implementação de alarmes para identificar invasões ou tentativas de acesso indevidas;
• Política de backup;
• Monitoramento da ação de terceiros com dados compartilhados;

8.1.3) AUDITORIA E CONTROLE

• Operação contínua de monitoramento e gestão do ambiente de rede;
• Testes de penetração e vulnerabilidade da rede;
• Comprovação da origem e do direito de uso dos dados;
• Garantia de que os dados possam ser exportados de forma segura;
• Garantir que o titular do dado consiga ter acesso de forma clara e segura;
• Rastreabilidade dos dados;
• Gerenciar os controles internos;
• Examinar cuidadosamente os riscos operacionais;
• Analisar e prevenir fraudes;
• Desenvolver programas de melhoria contínua;
• Estabelecer normas técnicas;
• Realizar auditorias periódicas;

8.1.4 DATA MAPPING

É o mapeamento de dados, documento essencial no processo de adequação às normas da LGPD em suma com 6 passos:

- Adequar as rotinas operacionais da operadora;
- Identificar e nomear os personagens responsáveis por cada área;
- Mapear os dados pessoais e sensíveis através de fluxograma de atividades;
- Avaliar o mapeamento de dados identificando os possíveis pontos de riscos;
- Criar uma política de segurança e privacidade;
- Monitorar periodicamente a polícia criada de forma a corrigir e/ou aprimorar.

8.1.5 PRINCÍPIO DA BOA FÉ

Assumindo o princípio da boa fé, demonstrar na Política de Segurança e Privacidade que em caso de algum problema com o trato dos dados pessoais, temos todos os nossos processos operacionais documentados para demonstrar nosso empenho e preocupação em estar adequado, com investimentos em segurança da informação e compliance, para prevenir e tratar situações de vazamentos de dados pessoais, de forma a mitigar possíveis sanções administrativas e também proteger a reputação da operadora.

8.1.6 REVISÃO JURIDICA

Conta com o objetivo de cobrir as lacunas legais que possam ser encontradas pelo comitê multidisciplinar em qualquer etapa do fluxo do mapeamento de dados, ressaltando a importância de documentar todo o processo como forma de provar o empenho da operadora em se adequar à LGPD para mitigar possíveis demandas jurídicas, mostrando o comprometimento com a aplicação da Lei em toda nossa operação, a exemplo de ações como:
Revisão de todos os formulários e contratos da operadora de forma a conter cláusulas claras sobre consentimento, coleta, armazenamento e finalidade de uso.
Desenvolver planos de ação para mitigar a exposição do dado.

9. PENALIDADES / MULTA

No Brasil a multa poderá chegar a 2% do faturamento, com teto de R$50 milhões (por infração), além de outras medidas educativas e sanções aplicadas pelo poder judiciário e as denúncias poderão ser realizadas pelo próprio titular do dado que se sentir lesado.

10. FONTE

- LGPD
- MP JÁ ESTÁ ATUANDO COM SANÇÕES
- CDC
- CP
- Código de Defesa do Consumidor
- Constituição Federal
- Blog Fausto Macedo / O ESTADÃO DE SÃO PAULO
- ANS
- Vexia
- Lei de Acesso à Informação (Lei nº 12.527/2011 – LAI)
- Marco Civil da Internet (Lei nº 12.965/2014)
- Fernanda Cortes Lopes Mainieri, head do departamento jurídico da Vexia
  "É como se nós fossemos os olhos da Lei em cada pedacinho da operação, para não deixar passar nada, protegendo a companhia e, principalmente, o titular do dado."
- Maurício Santos, líder de Segurança da Informação da Vexia:
  "Não basta ter controle sobre os dados pessoais dentro da empresa, mas ainda é preciso ter como provar que esses controles existem e mantê-los vivos em um processo de monitoramento contínuo visando adequação à LGPD ao longo do tempo."