

Cartilha - LGPD (Lei Geral de Proteção de Dados)

# ORIENTAÇÕES SOBRE PROTEÇÃO DOS DADOS PESSOAIS/ FORNECEDORES

2022



**Cuidar da**  
privacidade de  
dados pessoais  
é cuidar **de você.**

**Unimed Grande Florianópolis**

## 1. Conhecendo a Lei Geral de Proteção de Dados Pessoais

A Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709, de 14 agosto de 2018) é uma lei de caráter geral, que tem por objetivo a regulamentação da utilização de dados pessoais no Brasil.

A LGPD tem forte inspiração no General Data Protection Regulation – GDPR<sup>1</sup>, que é a legislação de proteção de dados pessoais vigente na União Europeia e nos países do Espaço Econômico Europeu, e tem grande influência global, devido aos padrões e exigências por ela fixados, para que organizações do mundo todo possam oferecer seus serviços e vender seus produtos no espaço territorial abrangido pela legislação.

No Brasil, a LGPD não é a primeira norma jurídica a tratar de proteção de dados pessoais, pois antes dela podemos destacar as abordagens feitas pelo Código de Defesa do Consumidor e Marco Civil da Internet, ainda que em caráter setorial e, portanto, não tão aprofundado quanto a LGPD, que tem uma abrangência maior.

Além da LGPD e de outras normas jurídicas que se aplicam às atividades de tratamento de dados pessoais em alguns setores, como é o caso da área da saúde, existem normas administrativas setoriais, editadas por órgãos como a Agência Nacional de Saúde Suplementar – ANS, os Conselhos Estaduais e Federal de Medicina, entre outros, que também são aplicáveis e devem ser observadas para que as operações de tratamento de dados pessoais sejam realizadas em total conformidade com a legislação vigente.



<sup>1</sup> <https://gdpr-info.eu/>

## 2. Dados Pessoais

Dado pessoal é toda e qualquer informação relacionada à pessoa natural identificada ou identificável. São informações que, além de serem tidas como dados, representam parte da história daquele indivíduo.

Para que tenhamos uma melhor compreensão do assunto, é necessário dividirmos os dados pessoais em duas categorias, para que possamos entender as diferenças existentes entre os dados pertencentes a cada uma delas.

### 2.1 Dados Pessoais Triviais

Nesta categoria de dados pessoais, estão inclusos aqueles dados que são utilizados e compartilhados por nós frequentemente em nosso cotidiano como, por exemplo:



É importante esclarecer que, quando falamos de dados pessoais triviais, não existe uma limitação legal quanto aquilo que pode ser considerado como dado pessoal, tendo em vista que, além daqueles dados que nos acompanham ao longo da vida – como os números de identificação de nossos documentos pessoais – existem outros que podem ser produzidos, como os dados de geolocalização, score de crédito, entre outros.

### 2.2 Dados Pessoais Sensíveis

A diferenciação entre os dados pessoais triviais e os de natureza sensível é feita pela LGPD no intuito de conferir maior proteção a estes dados, tendo em vista que por serem relacionados à intimidade ou à questões que podem gerar algum tipo de exposição pessoal, os dados pessoais sensíveis, quando não tratados em conformidade com a Lei, podem ocasionar transtornos, sofrimento ou aviltamento aos seus titulares como discriminação, segregação e seletividade.

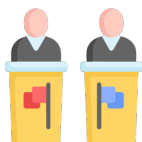
Diferente do que acontece com os dados pessoais triviais, os sensíveis são enumerados taxativamente pela LGPD, ou seja, para ser considerado com um dado pessoal sensível, é necessário que ele esteja elencado entre aqueles que a Lei cita. São eles:



Dados pessoais 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.

Assim sendo, os dados pessoais sensíveis demandam cuidados adicionais dos agentes de tratamento, pois uma operação de tratamento realizada em desconformidade com a Lei, pode causar graves prejuízos ao titular de dados.

## 2.3 Dados Pessoais Sensíveis na Área da Saúde

Qualquer dado pessoal sensível tem uma grande importância, para os seus titulares, para a LGPD e para os agentes que promovem o seu tratamento. O tratamento de dados pessoais sensíveis direcionados para a área da saúde ocorre de forma mais constante e corriqueira do que em outras áreas.

Exemplos de dados pessoais sensíveis, tratados na área da saúde:



Resultado de exame de DNA (dado genético);



Informações do prontuário médico (dados de saúde);



Informações sobre a vida sexual do paciente (para fins estatísticos e de execução de políticas públicas).

Além da LGPD e de outras normas jurídicas que se aplicam às atividades de tratamento de dados pessoais em alguns setores, como é o caso da área da saúde, existem normas administrativas setoriais, editadas por órgãos como a Agência Nacional de Saúde Suplementar – ANS, os Conselhos Estaduais e Federal de Medicina, entre outros, que também são aplicáveis e devem ser observadas para que as operações de tratamento de dados pessoais sejam realizadas em total conformidade com a legislação vigente.

### 3. Aplicação da LGPD

Como já citado anteriormente, a LGPD possui um caráter de aplicação geral, o que é exposto em sua própria nomenclatura. E isso significa que a norma é aplicável tanto a pessoas jurídicas, quanto a pessoas físicas, que realizam operações de tratamento de dados pessoais com finalidade de cunho econômico e profissional, exceto aquelas exclusivamente realizadas no âmbito das relações pessoais (para fins particulares e não econômicos).

#### Exemplos:

- **Administração Pública:**
  - Federal;
  - Estadual;
  - Municipal.
- **Empresas Privadas:**
  - Nacionais;
  - Transnacionais.
- **Cooperativas;**
- **Profissionais Liberais.**



A LGPD tem um alcance muito amplo, abrangendo diversas áreas, e com a área da saúde, não seria diferente. Quando falamos no dever de observância à LGPD, cabe dizer que, independentemente de atuar como pessoa física ou jurídica, médicos, dentistas, psicólogos, fisioterapeutas, entre outros, precisam se adequar aos requisitos legais, sendo que o mesmo é aplicável à empresas que atuem prestando serviços na área da saúde como, por exemplo, laboratórios, clínicas e consultórios.

#### 3.1 Aplicação Territorial da LGPD

Mesmo sendo uma norma de abrangência nacional, a LGPD pode se aplicar a agentes de tratamento que, porventura, não estejam em território nacional. Para tanto, alguns requisitos de aplicação são estabelecidos:

- A operação de tratamento de dados pessoais é realizada no Brasil;
- Os dados pessoais tratados tenham foram coletados território nacional;
- Dados pessoais foram tratados, visando a disponibilização de produtos e/ou serviços em território Brasileiro.

## 3.2 Exceções à Aplicação da LGPD

A LGPD também possui algumas exceções quanto à sua aplicação, o que se faz necessário para que atividades pessoais e cotidianas não sejam proibidas ou passíveis de sanções punitivas.

Isso ocorre quando:

- Os dados pessoais são utilizados por pessoa natural para fins exclusivamente particulares e não econômicos, como listas de convidados, grupos de WhatsApp, desde que não tenham cunho comercial e envio de correspondências pessoais;
- Os dados pessoais são utilizados para fins exclusivamente jornalísticos, artísticos e acadêmicos, como para a veiculação de informações através de reportagens e para o embasamento de produções científicas;
- Os dados pessoais são utilizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, como ocorre no caso de investigações e atividades de repressão policial a crimes;
- Os dados pessoais, apesar de tratados em território nacional, são originários de países que possuam legislações de proteção de dados pessoais a nível equivalente ou superior à LGPD sem que ocorra o compartilhamento destes dados com outros agentes, com exceção do controlador.

## 4. Operações de Tratamento de Dados Pessoais

São tidas como sendo operações de dados pessoais toda e qualquer atividade que, nos termos da LGPD, inclua, de alguma forma, a utilização destes dados.

A Lei enumera algumas destas situações:



Coleta;



Produção;



Recepção;



Classificação;



Utilização;



Acesso;



Reprodução;



Transmissão;



Distribuição;



Processamento;



Arquivamento;



Armazenamento;



Eliminação;



Avaliação ou Controle da Informação;



Modificação;



Comunicação;



Transferência;



Difusão ou extração.

Apesar de extensa, a enumeração de operações de tratamento de dados trazida pela LGPD não é exaustiva, ou seja, é possível que existam ou venham a existir outras operações de tratamento de dados pessoais, que não estejam entre as elencadas pela Lei.

Na área da saúde, visualizamos procedimentos que desencadeiam operações de tratamento de dados pessoais como, por exemplo, o cadastro de um paciente, faturamento de contas médicas, a realização de exames, que além de envolver diretamente dados pessoais sensíveis também pode produzi-los. É importante ressaltar que, ainda que um determinado dado de saúde seja produzido através do emprego de alguma técnica ou procedimento, também será considerado como dado pessoal sensível.

## 5. A Lei Geral de Proteção de Dados Pessoais e seus Princípios

Em seu artigo 6º, a LGPD enumerou 10 princípios, que servem como orientadores e como premissas de demonstração da boa-fé dos agentes de tratamento na realização de suas atividades. São eles:

- **Finalidade:** de acordo com este princípio, as operações de tratamento de dados pessoais somente podem ser realizadas se possuírem finalidade legítima, específica, explícita e informada ao titular de dados.

O que se entende por finalidade para o cumprimento deste princípio, é não tratar os dados pessoais com outro objetivo que não seja aquele informado no momento da coleta. Também é importante não realizar operações de tratamento de dados, que contrariem as expectativas do titular. Por exemplo, caso o paciente vá até a clínica realizar um exame de rotina, a clínica não pode compartilhar seus dados cadastrais com uma rede de farmácias, pois a finalidade não é essa.

- **Adequação:** o princípio da adequação vincula e limita o tratamento de dados pessoais às hipóteses informadas ao titular, auxiliando na concretização e dando continuidade às premissas do princípio da finalidade.

Na prática, esse princípio significa que a utilização de um dado pessoal deve ser exatamente aquela que foi informada ao titular quando o dado foi coletado. É importante que as finalidades informadas não sejam extrapoladas e que os dados não sejam compartilhados com terceiros não autorizados, como o exemplo da clínica no item anterior.

- **Necessidade:** determina que o tratamento de dados pessoais deverá ser o menos intrusivo possível, limitando-se ao mínimo necessário para o atingimento de suas finalidades, sem que ocorra o tratamento de forma indiscriminada e excessiva.

Tendo em vista que informações pessoais são fragmentos da história do titular, limitar a coleta de dados ao mínimo necessário para alcançar determinado objetivo e não promover operações de tratamento intrusivas, além de ser uma determinação legal, também representa uma medida de humanização do atendimento e preocupação com o paciente/cliente.

- **Livre acesso:** o titular de dados pessoais tem o direito de acesso aos seus dados, à forma como são tratados e ao tempo de duração do tratamento. Além disso, para que este princípio seja cumprido na íntegra, os dados pessoais devem ser armazenados de maneira com que o acesso a eles se dê de forma facilitada.

O acesso a qualquer dado pessoal deve ser franqueado e facilitado ao seu titular de dados. E isso é ainda mais importante quando falamos de dados de saúde, tendo em vista a relevância deste para os seus titulares.

- **Qualidade dos dados pessoais:** os dados pessoais precisam ser mantidos com o maior nível de exatidão possível, para que as operações de tratamento realizadas a partir deles se deem da forma mais assertiva. Para tanto, é direito do titular corrigir e complementar seus dados pessoais, o que não deve ser impedido e nem burocratizado pelos agentes de tratamento.

A necessidade de ter informações exatas a respeito do titular de dados é comum a todas as áreas, mas quando falamos da saúde, essa necessidade é ainda maior, tendo em vista que informações inexatas podem ocasionar graves impactos, como no caso de prontuários médicos ou de exames trocados.





- **Transparência:** o tratamento de dados pessoais precisa ser realizado de forma clara e transparente para que o titular de dados consiga, de maneira facilitada, saber quais dados estão sendo tratados, quais operações de tratamento estão sendo realizadas e por quais agentes.

Demonstrar a transparência com que o estabelecimento ou o profissional liberal realizam suas atividades, além de ser um princípio da LGPD, pode aumentar significativamente os níveis de confiança de seus pacientes ou clientes.

● **Segurança:** tal princípio estabelece que os agentes de tratamento são obrigados a adotar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

A preocupação com a segurança dos ativos informacionais vem crescendo constantemente ao longo dos últimos anos. Isso ocorre devido ao protagonismo que estes ativos têm assumido, sendo que, para algumas organizações, chegam a ser até mais valiosos do que seus ativos físicos. Nesse sentido, quando falamos em dados pessoais na área da saúde, a importância de garantir a segurança é ainda maior, pois o acesso não autorizado, a perda ou a destruição de dados de saúde, pode implicar em consequências gravíssimas.



● **Prevenção:** os danos decorrentes do tratamento de dados pessoais devem ser prevenidos adequadamente, através da adoção de medidas aptas para tanto.

Para efeito de atendimento a este comando da LGPD, deve-se agir proativamente, antecipando a ocorrência de riscos e ameaças, prevenindo seus efeitos.

**Não discriminação:** é vedada a realização de toda e qualquer operação de tratamento de dados pessoais para fins discriminatórios. Sendo que, a discriminação pode se dar não somente por fatores como raça e cor, mas também por outros como, por exemplo, renda, idade e gênero que pode levar à seletividade na concessão de crédito, à desigualdade salarial, entre várias práticas ilegais.

Dados pessoais não podem ser utilizados para promover ações discriminatórias, o que fica ainda mais evidente quando falamos de dados relacionados à saúde do titular de dados.

**Responsabilização e prestação de contas:** este princípio estabelece a obrigação que os agentes de tratamento têm de demonstrar a adoção de medidas eficazes e capazes de comprovar que estão cumprindo e atendendo às disposições da LGPD de forma adequada. Portanto, além de cumprir a Lei, é necessário demonstrar o atendimento a este princípio.

Para estar adequado à LGPD, além de adotar as medidas necessárias, é preciso comprovar a sua adoção. A documentação de normas internas e políticas são parte deste processo, mas existem outras, como o controle de acesso a documentos como resultados de exames, receituários e cópias de prontuários, que também são considerados como provas positivas do atendimento a este princípio.

## 6. Tratamento de Dados Pessoais Sensíveis

Dados pessoais sensíveis devem ser tratados de acordo com as hipóteses adequadas de fundamentação para o seu tratamento. Isso ocorre justamente por conta da sua sensibilidade, ou seja, o conteúdo de determinadas informações pode gerar discriminação, constrangimento e até eventuais prejuízos ao seu titular. Por isso, as hipóteses que autorizam o seu tratamento são limitadas a:

- Consentimento do titular.
- Cumprimento de obrigação legal ou regulatória pelo controlador.
- Para a execução de políticas públicas (privativo da Administração Pública).
- Realização de estudos por órgãos de pesquisa.
- Exercício regular de direito em contratos e processos judiciais, administrativos ou arbitrais.
- Proteção da vida ou incolumidade física do titular ou terceiro.
- Tutela da saúde, em procedimento realizado por profissionais da área de saúde, serviços de saúde ou autoridades sanitárias.
- Prevenção à fraude e garantia de segurança do titular.



A diferenciação que a LGPD faz entre as hipóteses que autorizam o tratamento de dados pessoais triviais e sensíveis deixa ainda mais evidente a importância que o tratamento destes dados, nos quais incluem-se os dados de saúde, seja realizado em conformidade com a Lei.

## 7. Direitos dos Titulares de Dados Pessoais

A LGPD cuidou de estabelecer direitos para os titulares de dados pessoais, sendo que, o atendimento à eventuais requisições destes é uma das maiores obrigações dos agentes de tratamento, sendo ainda um grande ponto de atenção, uma vez que o não atendimento a tais requisições é tido como conduta em desconformidade com a Lei e passível de aplicação de sanções punitivas, dentre elas, a multa pecuniária.

### 7.1 Saiba quais são os Direitos dos Titulares de Dados Pessoais

- Confirmação da existência de tratamento.
- Acesso aos dados.
- Correção de dados incompletos, inexatos ou desatualizados.
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei.
- Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante Requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador.
- Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da Lei.
- Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados.
- Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.
- Revogação do consentimento, nos termos do § 5o do art. 8o da Lei.

A garantia do exercício dos direitos do titular de dados é, sem dúvida, uma das maiores responsabilidades dos agentes de tratamento no atendimento às disposições da LGPD. Na área da saúde, o exercício destes direitos deve ser igualmente garantido, contudo observando-se questões importantes como normas regulatórias, códigos de ética profissional e, em alguns casos, o período de guarda de determinados documentos.

## 8. Sanções Punitivas Aplicáveis em caso de Descumprimento da LGPD

O processo de adequação à LGPD, assim como ocorre com outras leis de compliance (conformidade), é algo muito estrutural, que demanda, entre várias outras coisas, uma mudança de mentalidade e comportamentos. Após o início do processo de adequação, isso costuma trazer grandes benefícios e oportunidades de melhoria para as organizações. Portanto, o medo das sanções punitivas não deve ser o principal fator que impulsiona uma organização a se adequar à LGPD.

Ainda que as sanções punitivas não devam representar a principal motivação que leva uma organização a se adequar à LGPD, não podemos ignorá-las, tampouco, negligenciar os severos impactos negativos, que vão muito além das multas pecuniárias.

A fim de ilustrar os impactos negativos que uma organização em desconformidade com a LGPD pode sofrer, convém analisarmos algumas outras situações que, a depender do caso concreto, podem ser muito mais onerosas para a organização do que as multas:

- **Danos Reputacionais:** a forma como uma organização é vista, reflete diretamente em fatores importantíssimos como a sua imagem perante seus clientes, a forma como ela é vista pela sociedade e a sua capacidade de atrair bons colaboradores. Esses fatores podem ser afetados pela ocorrência de vazamentos e tratamento indevido de dados, que gerem algum tipo de exposição ou experiência negativa para seus titulares, entre várias outras situações decorrentes de não conformidades com a LGPD. Ao longo das últimas décadas, os danos reputacionais ganharam um grande enfoque, pois, ao contrário do que se pensava, um dos maiores ativos de uma organização é o que ela representa para o seu público e para a sociedade. E isso ficou cada vez mais evidente, quando os danos à imagem de algumas organizações, começaram a se traduzir em prejuízos financeiros, muitas vezes ocasionados pela perda de clientes e, conseqüentemente, de receita, por conta da má reputação adquirida em razão da prática de atividades ilícitas e da desconformidade com determinadas leis. Ainda, cabe dizer que o setor da saúde pode ser ainda mais suscetível a esse tipo de dano, levando em consideração a natureza de suas atividades e a importância que as informações sobre o estado de saúde dos pacientes têm para este setor.



● **Danos que Podem ser Causados Pelo Bloqueio e Eliminação de Dados Pessoais Envolvidos em Infrações:** a depender do modelo de negócio da organização, os dados pessoais e o seu tratamento são vitais para a maioria e, em alguns casos, para todos os seus processos de negócio. O bloqueio e a eliminação de dados pessoais em algumas situações é uma das medidas punitivas mais gravosas impostas pela LGPD, podendo paralisar operações e até organizações inteiras, o que resultaria em vertiginosos prejuízos. No setor da saúde, seria extremamente difícil operar sem ter acesso aos dados pessoais dos pacientes, uma vez que isso comprometeria o acesso dos profissionais ao histórico, prontuários e resultados de exames

## 8.1 Conheça Todas as Sanções Punitivas da LGPD

- Advertência com indicação de prazo para adoção de medidas corretivas;
- Multa simples de até 2% limitada a R\$ 50 Milhões (cinquenta milhões de reais) do faturamento da pessoa jurídica de direito privado por infração;
- Multa diária;
- Publicização da infração;
- Bloqueio dos dados pessoais a que se refere a infração até sua regularização;
- Eliminação dos dados pessoais a que se refere a infração;
- Suspensão do tratamento dos dados pessoais a que se refere a infração;
- Proibição parcial ou total de exercer atividades de tratamento de dados.

## 9. Personagens da LGPD



A LGPD caracteriza e elenca alguns personagens, figuras às quais ela faz menção explícita. Esta caracterização é muito importante, pois, ao contrário de outras normas que somente trazem consigo comandos positivos ou negativos – o que fazer ou o que não fazer, a LGPD, ao estabelecer seus personagens, atribui a eles direitos, deveres e obrigações, sendo necessária a diferenciação de cada um deles em relação aos demais, principalmente, quando se fala em agentes de tratamento de dados, para efeitos de responsabilização e dosimetria desta.

Estas são as pessoas elencadas pela LGPD:

- **Titular de Dados:** o titular de dados é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Na área da saúde, os principais exemplos de titulares de dados são os pacientes, beneficiários de planos de saúde e clientes do estabelecimento, os colaboradores e profissionais liberais que prestam serviços.



- **Controladores:** de acordo com a LGPD, o controlador pode ser qualquer pessoa física ou jurídica, de direito público ou privado, que promova operações de tratamento de dados pessoais, decidindo ativamente sobre as premissas a serem aplicadas ao tratamento. Por ser extremamente amplo, o conceito de controlador divide-se em:

**Controlador Singular** – é aquele a quem, privativamente, competem todas as decisões acerca das operações de tratamento de dados pessoais por ele realizadas. Nessa hipótese se encaixam as organizações e profissionais que promovam individualmente o tratamento de dados pessoais para atingir suas finalidades, como clínicas e hospitais, que realizam todo o tratamento de seus pacientes internamente, ou que contam com o auxílio de que prestadores de serviço, tidos como operadores.

**Controlador Conjunto** – como o próprio título sugere, diferentemente do controlador singular, o controlador conjunto atua juntamente com outro ou com outros controladores, dividindo, assim, as tomadas de decisão e, conseqüentemente, a responsabilidade. Contudo, vale frisar que, controladoria conjunta não é sinônimo de divisão equitativa de responsabilidades em caso de infrações à lei. Nesse caso, cada controlador conjunto responde na medida em que contribuiu ou decidiu ativamente com relação ao evento danoso. Podemos exemplificar o conceito de controlador conjunto, através da atuação de clínicas e hospitais que realizam determinados procedimentos em conjunto e, para isso, precisam ter acessos aos dados pessoais do paciente. Sendo que, cada um deles é responsável pelas operações de tratamento que desempenham.



● **Operador:** o operador é qualquer pessoa física ou jurídica, de direito público ou privado, que realiza operações de tratamento de dados em nome do controlador, seguindo as premissas de tratamento de dados por ele estabelecidas. A caracterização da figura do operador na área da saúde pode ser visualizada através da prestação de serviços na realização de exames laboratoriais para um hospital, na qual o laboratório realiza exames a pedido do hospital, de acordo com seus requisitos e entrega os resultados, não tendo poder decisório nas operações de tratamento de dados.

**Atenção!** – Colaboradores não são considerados operadores de dados.



● **Encarregado pelo Tratamento de Dados Pessoais ou Data Protection Officer (DPO):** o encarregado ou DPO é pessoa física ou jurídica, indicada pelo controlador para atuar como ponto focal na organização, fazendo a comunicação entre o controlador, a Agência Nacional de Proteção de Dados e os titulares de dados pessoais. Além disso, o encarregado ou DPO tem um papel importantíssimo no atingimento e na manutenção de níveis de conformidade aceitáveis, pois, pode atuar, de forma concomitante, desde o início do processo de adequação da organização à LGPD, e posteriormente a ele, no Programa de Governança em Privacidade e Proteção de Dados Pessoais.



- **Encarregado pelo Tratamento de Dados Pessoais ou Data Protection Officer (DPO):** Autoridade Nacional de Proteção de Dados (ANPD): a ANPD é uma autarquia especial<sup>2</sup>, que tem por objetivo fiscalização e a aplicação de sanções concernentes à proteção de dados pessoais no país, e também, a interpretação e normatização de determinados pontos da LGPD. Portanto, além de exercer o papel regulatório, a ANPD também fornecerá parâmetros para a aplicação da LGPD.

## 10. Cuidados a Serem Tomados Pelos Fornecedores

A Unimed Grande Florianópolis está comprometida a cumprir com as obrigações impostas pela LGPD e pelas demais normas de caráter jurídico e administrativo que regulam a proteção de dados pessoais no país.

Para alcançarmos e mantermos níveis adequados de privacidade e proteção de dados pessoais em nossa Organização, é necessário que nossos fornecedores compartilhem do mesmo comprometimento, adequando-se à LGPD e tratando dados pessoais em conformidade com a Lei.

Pensando nisso, elaboramos algumas orientações que podem ser muito úteis, tanto na prestação de serviços dos fornecedores à Cooperativa quanto na execução de suas próprias ações internas de adequação à LGPD.

<sup>2</sup> Medida Provisória 1.124, de 13 de julho de 2022: Altera a Lei no 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais, transforma a Autoridade Nacional de Proteção de Dados em autarquia de natureza especial e transforma cargos em comissão.

- Iniciar, dar continuidade ou concluir um projeto de adequação à LGPD.
- Designar um time de privacidade, para apoiar as atividades do processo de adequação.
- Nomear um Encarregado pelo Tratamento de Dados Pessoais (DPO). Uma das obrigações impostas pela LGPD, é a divulgação da Identidade do DPO, conforme estabelecido no art. 41, §1o, que estabelece que a identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador. No caso da Unimed Grande Florianópolis, o nosso DPO, é a GEP Soluções em Compliance.
- Definir formas de atendimento às requisições de direitos dos titulares.
- Estabelecer políticas essenciais. Minimamente, a organização deve possuir políticas de privacidade e de segurança da informação.
- Realizar treinamentos periódicos para os colaboradores, sobre privacidade e proteção de dados pessoais e segurança da informação.
- Observar as finalidades para as quais os dados pessoais foram coletados, e não permitir que ocorram desvios.
- Adotar boas práticas de segurança da informação, como a elaboração de procedimentos de backup, gestão de senhas e uma estrutura de T.I adequada ao ramo de atividade e ao volume da operação do fornecedor.
- Observar o período de retenção dos dados pessoais.
- Estabelecer procedimentos documentados para a eliminação de dados, em meio físico e digital.
- Coletar apenas os dados pessoais estritamente necessários para a execução de suas atividades.
- Não tratar dados pessoais em desconformidade com a LGPD.



- Obedecer às disposições contratuais estabelecidas com a Unimed Grande Florianópolis.
- Acatar as orientações que poderão ser passadas pela Cooperativa durante a execução do contrato.
- Estabelecer regras de controle de acesso e privilégios para ambientes físicos e virtuais.
- Configurar o bloqueio automático de tela por inatividade.
- Não compartilhar dados com terceiros não autorizados.

Estes são apenas alguns exemplos dos cuidados que devem ser tomados pelos fornecedores para garantir a privacidade e a observância das disposições da LGPD. Vale lembrar, que as recomendações contidas nesta cartilha são essenciais para os fornecedores que possuem contratos firmados ou desejem contratar com a Unimed Grande Florianópolis.

A responsabilidade em manter os dados pessoais de nossos beneficiários, colaboradores e parceiros, é de todos nós. Por isso, entendemos que é necessário o comprometimento de todos os nossos fornecedores, para que possamos proporcionar mais segurança a todos os envolvidos em nossos processos de negócio, e disseminar a cultura da privacidade na sociedade.



## Referências Bibliográficas

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020].

*Documento elaborado em 30/8/2022. Versão 1.0*

*Divisão Jurídica e Consultivo*





HOSPITAL  
UNIMED

Exames de Imagem

Unimed  
Grande  
Florianópolis

Unimed

Unimed



Grande  
Florianópolis

ANS - N° 36044-9