

Manual de Orientação

Manual de Orientação Lei Geral de Proteção de Dados -MAN 004 INST

LEI 13.709/2018

Lei Geral de Proteção de Dados



abramge • sinamge • sinog



Apresentação

O Sistema Abramge/Sinamge/Sinog apresenta mais uma edição da série “Manual de Orientação”, publicação periódica que objetiva auxiliar as operadoras de planos de saúde associadas, na implantação e ou implementação de processos internos que atendam às normas e regras do setor de saúde suplementar.

A demanda por materiais orientativos que alcancem a todas as operadoras associadas foi identificada a partir de dúvidas e solicitações enviadas pelas operadoras, bem como a necessidade de uniformizar entendimentos. A partir daí, o Sistema Abramge/Sinamge/Sinog resolveu consolidar todo o material referente a novas normas e transpor regras para um material orientativo.

Esperamos que a publicação auxilie os representantes das operadoras de planos de saúde associadas na alteração e adequação de processos internos, contribuindo tecnicamente para o planejamento e tomada de decisão dos gestores, promovendo a melhoria contínua e desenvolvimento das atividades das operadoras de planos de saúde.

“A vigência da Lei Geral de Proteção de Dados foi adiada pelo Governo Federal para maio de 2021.

No dia 29 de abril de 2020, o governo Federal incluiu no Texto da Medida Provisória 959, que trata do auxílio emergencial para manutenção do emprego, o adiamento da vigência da Lei Geral de Proteção de Dados (LGPD).

Tal medida prevê a prorrogação da entrada em vigor da LGPD de agosto de 2020 para 3 de maio de 2021.

Recomendamos, de qualquer forma, que as operadoras prossigam em seus projetos de adequação à LGPD.”

Comitê Executivo Abramge/Sinamge/Sinog

Reinaldo Camargo Scheibe – Presidente da Abramge

Cadri Massuda – Presidente do Sinamge

Geraldo Almeida Lima – Presidente do Sinog

Carlito Marques – Secretário Geral da Abramge

Expediente Editores Responsáveis

Superintendente Executivo: Marcos Novais

Projeto Gráfico: Roney Dionizio

Revisão: Camila Castioni



1. Sumário

| | |
|--|----|
| 1. Sumário | 3 |
| 2. Introdução | 6 |
| 3. Abrangência | 6 |
| 4. Objetivos | 7 |
| 5. Referências Normativas | 7 |
| 6. Operacionalização | 8 |
| 6.1 Visão Geral da Lei | 9 |
| 6.1.1 Lei Geral de Proteção de Dados - Trajetória Histórica e Conceitual | 10 |
| 6.2 A Lei Geral de Proteção de Dados em Planos | 11 |
| 6.3 Bases Legais para o Tratamento de Dados Pessoais | 14 |
| 6.4 Abrangência. | 16 |
| 6.4.1 Aplicabilidade da LGPD | 16 |
| 6.4.2 Não Aplicabilidade da LGPD. | 16 |
| 6.4.3 Certificação ISO/IEC 27.001 2013 x LGPD | 17 |
| 6.5 Princípios Gerais da LGPD | 18 |
| 6.6 Boas Práticas de Adequação à LGPD no Dia a Dia das Operadoras | 21 |
| 6.7 Situações Específicas para o Setor da Saúde | 23 |
| 6.7.1 Proibição da Prática de Seleção de Risco. | 23 |
| 6.7.2 <i>Health Analytics</i> | 23 |



1. Sumário

| | |
|--|----|
| 6.8 Direito dos Titulares de Dados Pessoais | 24 |
| 6.9 Os agentes de Tratamento de Dados Pessoais | 28 |
| 6.9.1 Controlador | 28 |
| 6.9.2 Operador | 29 |
| 6.9.3 Encarregado | 30 |
| 6.9.4 Fluxo do Relacionamento dos Agentes da Informação | 31 |
| 6.10 Regras Consentimento | 32 |
| 6.10.1 Tratamento de Dados Sem o Consentimento do Titular | 33 |
| 6.11 Legítimo Interesse | 34 |
| 6.12 Dados de Crianças e Adolescentes | 35 |
| 6.13 Término do Tratamento de Dados Pessoais | 36 |
| 6.14 Governança em LGPD | 37 |
| 6.15 Segurança em LGPD | 39 |
| 6.16 Violações e Sanções | 42 |
| 6.17 Principais Pontos de Atenção para Implantação da LGPD | 45 |
| 6.17.1 Dados que Exigem Mais Proteção | 45 |
| 6.17.2 Reaproveitamento de Bases | 46 |
| 6.17.3 Utilização de Dados Públicos | 46 |
| 6.17.4 Dados Anônimos | 47 |
| 6.17.5 Incidentes | 47 |
| 6.17.6 Cuidados na criação de Perfis | 48 |
| 6.17.7 Atos de Terceiros | 48 |



1. Sumário

| | | |
|--------|--|----|
| 6.18 | Check List para Implantação da LGPD | 49 |
| 6.19 | Framework de Processos LGPD | 50 |
| 6.19.1 | Detalhamento do Framework por Processos LGPD | 51 |
| 6.19.2 | Avaliação de Requisitos por Área de Negócio | 53 |
| 6.20 | Quadro de Resumos | 55 |
| 6.20.1 | Resumo da LGPD | 55 |
| 6.20.2 | Resumo Direito dos Titulares | 56 |
| 6.21 | Publicação da Lei Geral de Proteção de Dados | 57 |
| 7. | Documentos Associados | 59 |
| 8. | Glossário / Siglas e Definições | 61 |
| 8.1 | Siglas | 62 |
| 8.2 | Definições | 62 |
| 9. | Revisões e Atualizações | 64 |
| 10. | Anexos | 65 |
| 10.1 | Referências Legais | 66 |



2. Introdução

A Lei Geral de Proteção de Dados (LGPD) tem suma importância na construção e consolidação do mercado digital, devendo cada operadora encontrar a melhor maneira de promover sua implantação, assegurando a todas as pessoas a proteção dos seus dados sejam elas colaboradores, beneficiários OU fornecedores.

No cenário atual, inovações tecnológicas surgem a todo momento e impactam diretamente a sociedade, influenciando na maneira como se relacionam e consomem produtos e serviços. Certamente, este novo cenário significa progresso e acesso à informação, mas ao mesmo tempo, nos deparamos com um mundo totalmente sem fronteiras, e é justamente esse o desafio nesse momento: dar segurança jurídica e maior proteção aos direitos dos titulares dos dados, apoiando e orientando sobre a implantação da LGPD, de forma harmoniosa.

3. Abrangência

Este manual se destina às operadoras e suas áreas operacionais diretamente impactadas pela Lei 13.709 (Lei Geral de Proteção de Dados).



4. Objetivos

O objetivo deste Manual Orientativo é contribuir para a implementação da LGPD, trazendo conceitos, regras e detalhando os impactos operacionais nas operadoras de planos de saúde.

5. Referências Normativas

| |
|--|
| Medida Provisória 869 |
| RN 195 ANS |
| ISO 27001 |
| Lei 12.527 Acesso à Informação |
| Lei 12.737 Carolina Dieckman |
| Lei 12.965 Marco Civil |
| Lei 13.709 Proteção de Dados |
| Medida Provisória 959 |
| Lei 13.853/2019 Criação da ANPD |
| Lei 14.010/2020 Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus |
| Lei 14.058/2020 Auxílio Emergencial |
| PORTARIA Nº 1, DE 8 DE MARÇO DE 2021 que estabelece o Regimento Interno da Autoridade Nacional de Proteção de Dados - ANPD. |

6

Operacionalização



6.1 Visão Geral da Lei

A aprovação da Lei Geral de Proteção de Dados (LGPD), em agosto de 2018, estabeleceu as bases para a consolidação de um marco regulatório para a proteção de dados pessoais no Brasil, até então garantidos na Constituição, no Código Civil, no Marco Civil da Internet e nas normas de proteção ao consumidor.

Seu objetivo é regulamentar o tratamento de dados pessoais de clientes e usuários por parte de empresas públicas e privadas.

O longo período entre a data de publicação da LGPD (agosto/2018) e o início da sua vigência (setembro/2020) deriva da complexidade das ações que precisam ser tomadas pelas empresas para adaptação aos novos parâmetros legais.

Com isso a partir de setembro de 2020, todas as operadoras de planos de saúde deverão seguir os procedimentos previstos na nova lei. As operadoras que não cumprirem com as novas exigências estarão sujeitas a uma multa que pode chegar até R\$ 50 milhões.

No final do ano de 2018 foi aprovada a lei que cria a Autoridade Nacional de Proteção de Dados (ANPD), por meio da Medida Provisória nº 869/2018, convertida na Lei 13.853/2019.

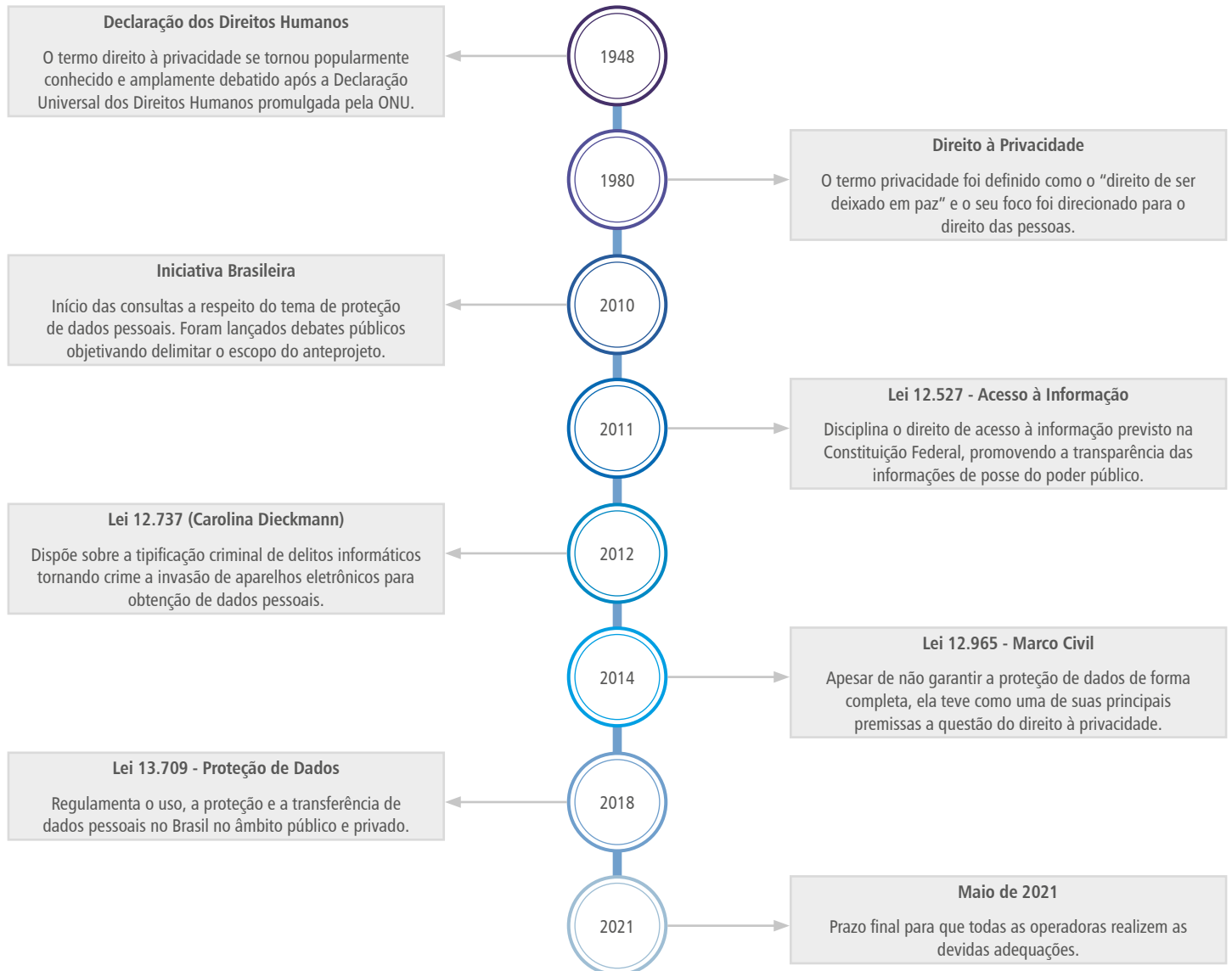
A ANPD terá um papel tríplice de:

1. **fiscalização** - poderá editar normas e procedimentos, deliberar sobre a interpretação da LGPD e requisitar informações relacionadas ao tratamento de dados pessoais;
2. **sanção** - terá poderes para instaurar processo administrativo quando houver descumprimento à LGPD e terá competência exclusiva para aplicar as sanções previstas na LGPD; e
3. **educação** - irá difundir o conhecimento sobre a LGPD e medidas de segurança, apresentando diretrizes para interpretação da lei, estimulando padrões para serviços e produtos que facilitem o controle de titulares sobre seus dados pessoais e elaborando estudos sobre melhores práticas nacionais e internacionais de proteção de dados pessoais, entre outros.





6.1.1 Lei Geral de Proteção de Dados - Trajetória Histórica e Conceitual





6.2 A Lei Geral de Proteção de Dados em Planos

A LGPD tem gerado muitas dúvidas e questionamentos em todos os setores, especialmente em saúde, já que a maioria dos dados são considerados sensíveis. A área da saúde deve ter atenção com a proteção de dados de pacientes e médicos.

Operadoras, hospitais, clínicas médicas, clínicas odontológicas e laboratórios estão envoltas com cadastros, amostras, fichas e prontuários, laudos de exames e diagnósticos.

Nesse cenário é preciso ter cuidados como não deixar computadores desbloqueados, incluir a necessidade de login e senha de acesso, não possuir sistemas desatualizados sem antivírus, redes wi-fi abertas, servidores de e-mail desprotegidos e até mesmo equipes que compartilham informações de pacientes e médicos livremente, sem qualquer tipo de criptografia. Também não é incomum profissionais que já foram desligados da instituição continuarem como usuários ativos dos sistemas, com acesso a informações sensíveis.

O fato é que nos dias de hoje há notícias de diversos incidentes envolvendo áreas da saúde, tais como sequestro de dados, manipulação de resultado de exames, vazamento de prontuários, compartilhamento indevido de dados de saúde para fins comerciais etc.

A proteção dos dados ganha contornos ainda mais importantes em saúde, já que é dever das instituições o sigilo de dados pessoais e o Conselho Federal de Medicina possui regras rígidas sobre manuseio e armazenamento de prontuário de paciente.

“A Lei Geral de Proteção de Dados vem ao encontro do dever de sigilo já presente na área da saúde, de forma a preservar os dados pessoais dos pacientes armazenados nos bancos de dados das diversas instituições do sistema de saúde.”

Neste contexto, as operadoras de saúde deverão se adequar afim de se prevenirem em relação às sanções por vazamentos de dados de pacientes, ataques hackers e falha humana decorrente da atuação de seus colaboradores que tiverem acesso aos dados de beneficiários.





Alguns pontos importantes a serem observados pelo setor de saúde, como:

Fazer uma identificação de todos os dados coletados e armazenados pela instituição;

Revisar as regras de privacidade para que fique muito bem definido quem poderá acessar, controlar, processar e transferir os dados;

Levantamento de pacientes (novos e antigos), colaboradores, prestadores de serviços, parceiros, sócios. É necessário que essas informações sejam categorizadas;

Revisar os termos de consentimento assinados pelo paciente e informá-lo quando e por quem os seus dados serão utilizados, bem como a possibilidade de solicitar a exclusão desses dados;



Investir em proteção física e virtual – as informações necessitam ser armazenadas em ambientes comprovadamente seguros e controlados;

.....

Implantar soluções de proteção e segurança, com redes criptografadas e softwares de monitoramento;

.....

Ter atenção com a hospedagem desses dados em servidores estrangeiros, em países que não possuam qualquer regulamentação sobre a segurança da informação;

.....

Antes de utilizar recursos de inteligência artificial é necessário explicar ao paciente o que exatamente será feito com seus dados.



6.3 Bases Legais para o Tratamento de Dados Pessoais

Este tema se encontra na LGPD nos artigos 5º, inciso XII; do 7º ao 16; com conclusão no 37.

O tratamento de dados pessoais é possível na medida em que essa atividade tenha uma base jurídica. Com efeito, a LGPD estabelece dez bases legais:





O tratamento de dados pode ser entendido como qualquer procedimento que envolva a utilização de dados pessoais, tais como coleta, classificação, utilização, processamento, armazenamento, compartilhamento, transferência, eliminação, entre outras ações.

Todo esse processo exige a presença de três figuras centrais: o controlador, o operador e o encarregado.



Que providências tomar:

Avaliar cuidadosamente qual base legal para tratamento de dados pode ser utilizada no caso concreto;

Quando o tratamento de dados pessoais for baseado no consentimento, o controlador deve manter documentação comprobatória da sua obtenção em conformidade com a legislação;

Quando o tratamento de dados pessoais for baseado no interesse legítimo, o controlador deve adotar medidas para garantir a transparência de tal tratamento, que poderá sempre ser revisto pela autoridade nacional de proteção de dados à luz do caso concreto;

Manter registro e fundamentação das operações de tratamento de dados pessoais, especialmente quando baseado no interesse legítimo.



6.4 Abrangência

Este tema da LGPD se encontra nos artigos: 1º, 3º e 4º.

6.4.1 Aplicabilidade da LGPD

A LGPD se aplica em qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, incluindo, portanto, as operadoras de planos de saúde, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

1. A operação de tratamento seja realizada no território nacional;
2. A atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; e
3. Os dados pessoais objeto do tratamento tenham sido coletados no território nacional, isto é, quando o titular dos dados aqui se encontre no momento da coleta.

Assim, através de princípios e regras, a LGPD traça novos limites para o relacionamento daquele que controla as informações (controladores), quem as manipula (operadores) e o proprietário dos dados pessoais (titulares).

6.4.2 Não Aplicabilidade da LGPD

A LGPD não se aplicará ao tratamento de dados pessoais quando:

1. Realizado por pessoa natural para fins particulares;
2. Realizado para fins jornalísticos ou artísticos ou acadêmicos;
3. Realizado para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (que será objeto de lei específica); ou
4. Provenientes de fora do território nacional e que não seja objeto de comunicação, uso compartilhado com agentes de tratamento brasileiros ou objeto de transferência de dados com outro país que não o de proveniência, desde que este país de proveniência proporcione grau de proteção adequado aos da lei brasileira.

Que providências tomar:

Organizações que realizam o tratamento de dados pessoais no território brasileiro ou oferecem produtos ou serviços a indivíduos localizados no Brasil devem entender o impacto da LGPD em suas atividades e como se adequar às suas regras. A contratação de consultoria técnica e jurídica especializada para realizar o diagnóstico é uma medida aconselhável.



6.4.3 Certificação ISO/IEC 27.001 2013 x LGPD



A norma ISO/IEC 27.001:2013 teve sua origem em novembro de 2005 quando da adaptação do padrão BS 7799 Parte 2 (*British Standards*) pela ISO (*Internacional Organization for Standardization*) e pelo IEC (*International Electrotechnical Commission*), e foi integralizada nacionalmente pela ABNT - Associação Brasileira de Normas Técnicas - que traduziu a norma em 2006.

Tal norma trata especificamente dos requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação (SGSI) dentro da empresa, buscando garantir a confidencialidade, integridade e disponibilidade de um sistema de segurança.

Já a Lei Geral de Proteção de Dados – lei federal 13.709, sancionada em agosto de 2018, vai além, dispendo sobre a proteção de dados pessoais no Brasil e tratando acerca da coleta e tratamento de dados pessoais.

É importante esclarecer que a LGPD busca regular a forma adequada de tratamento dos dados pessoais, levando em consideração a transparência nas relações, principalmente com o titular dos dados, criando a obrigação àqueles que tratam os dados pessoais, de garantir os direitos dos titulares sobre tais informações.

Apesar da ISO/IEC 27.001:2013 cobrir diversos aspectos indispensáveis ao processo de adequação com a LGPD, como padrões mínimos de segurança e gestão de incidente, não garante o cumprimento total da Lei, visto que há exigências que extrapolam a gestão da segurança da informação.

Outro ponto a se destacar é que possuir a certificação é entendido pela LGPD como boa prática, ou seja, existiu boa fé na tentativa de prevenção ao incidente de dados, e quando comprovada perante a Autoridade Nacional de Proteção de Dados, pode resultar em atenuante de multa.

Portanto a certificação ISO/IEC 27.001:2013 ainda não é suficiente para a adequação à LGPD. Além disso, a natureza complementar dessas normas se destaca também pela análise de seus princípios norteadores. A LGPD é regida por 10 (dez) princípios, sendo que somente 2 (dois) deles são abarcados pela norma ISO/IEC 27.001:2013 a segurança e a prevenção.



6.5 Princípios Gerais da LGPD

Este tema se encontra na LGPD no artigo 6º.

A LGPD estabelece alguns princípios que se aplicam a todas as atividades de tratamento de dados. São valores gerais que orientam a compreensão, interpretação e aplicação das regras estabelecidas pela LGPD e que devem sempre ser considerados quando uma atividade envolver tratamento de dados pessoais.

São eles:

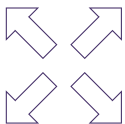


1. Finalidade:

A partir da implantação da LGPD não será mais possível tratar dados pessoais com finalidades genéricas ou indeterminadas. O tratamento de cada informação pessoal deve ser feito com fins específicos, legítimos, explícitos e informados. Ou seja, as operadoras devem explicar para que usarão cada um dos dados pessoais.

Essas finalidades também devem estar dentro dos limites da lei e devem vir expressamente acompanhadas de todas as informações relevantes para o titular.

Além disso, a operadora não está autorizada a modificar a finalidade durante o tratamento.



2. Adequação:

Os dados pessoais tratados devem ser compatíveis com a finalidade informada pela operadora. Ou seja, sua justificativa deve fazer sentido com o caráter da informação que você pede.



3. Necessidade:

As operadoras em geral devem utilizar apenas os dados estritamente necessários para alcançar as suas finalidades. Procure fazer uma ponderação entre o que é realmente essencial para o seu negócio e o que é apenas conveniente. Lembre-se que quanto mais dados você tratar, maior será a sua **responsabilidade**, inclusive em casos de vazamentos e incidentes de segurança.



4. Livre acesso:

A pessoa física titular dos dados tem o direito de consultar, de forma simples e gratuita, todos os dados que a empresa detenha a seu respeito.

Além disso, devem ser especificadas questões como: o que a empresa faz com as suas informações, de que forma o tratamento é realizado e por quanto tempo é utilizado e guardado.



5. Qualidade dos dados:

Deve ser garantido aos titulares que as informações que a operadora tenha sobre eles sejam verdadeiras e atualizadas. É necessário ter atenção à exatidão, clareza e relevância dos dados, de acordo com a necessidade e com a finalidade de seu tratamento.



6. Transparência:

Todas as informações passadas pela operadora, em todos os seus meios de comunicação, devem ser claras, precisas e verdadeiras.

Além disso, a operadora não pode compartilhar dados pessoais com outras pessoas de forma oculta. Se você repassa dados pessoais para terceiros, inclusive para operadores que sejam essenciais para a execução do serviço, o titular precisa saber.



7. Segurança:

Todas as informações passadas pela operadora, em todos os seus meios de comunicação, devem ser claras, precisas e verdadeiras.

Além disso, a operadora não pode compartilhar dados pessoais com outras pessoas de forma oculta. Se você repassa dados pessoais para terceiros, inclusive para operadores que sejam essenciais para a execução do serviço, o titular precisa saber.



8. Prevenção:

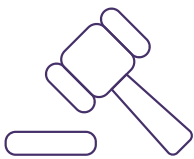
O princípio da prevenção objetiva que as operadoras adotem medidas prévias para evitar a ocorrência de danos em virtude do tratamento de dados pessoais. Ou seja, as operadoras devem agir antes dos problemas e não somente depois.



9. Não Discriminação:

Os dados pessoais jamais podem ser usados para discriminar ou promover abusos contra os seus titulares.

A própria LGPD já criou regras específicas para o tratamento de dados que frequentemente são utilizados para discriminação, 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.



10. Responsabilização e Prestação de Contas:

Além de se preocuparem em cumprir integralmente a Lei, **as operadoras devem ter provas** e evidências de todas as medidas adotadas, para demonstrarem a sua boa-fé e a sua diligência.

Alguns bons exemplos estão na comprovação que fizeram treinamentos de equipe, a contratação de **consultorias especializadas**, a utilização de protocolos e sistemas que garantam a segurança dos dados e o acesso facilitado do titular a empresa sempre que preciso.

Que providências tomar:

Revisar e adequar as políticas (internas e em relação a terceiros), contratos, procedimentos e demais atividades que envolvam tratamento de dados pessoais (tanto de clientes quanto de empregados) aos princípios estabelecidos na LGPD.

Manter registros, preferencialmente por escrito, que demonstrem a adoção de medidas para adequação das operações de tratamento aos princípios estabelecidos na LGPD, independentemente do tamanho da base de dados existente.



6.6 Boas Práticas de Adequação à LGPD no Dia a Dia das Operadoras



1. Revise as políticas de segurança de informação da operadora

É preciso separar um tempo para rever todas as medidas que já são adotadas pela operadora para detectar e corrigir possíveis problemas quanto à proteção dos dados pessoais. Na prática, considere criar um programa de **governança corporativa**, com normas e políticas claras e detalhadas para que todos tenham ciência de como os dados devem ser coletados, utilizados, monitorados e protegidos na sua empresa.

2. Adote soluções de cloud computing

A computação em nuvem tem ajudado diversas empresas a estarem mais seguras, já que essas soluções cumprem vários requisitos de segurança, ajudando no armazenamento seguro dos dados e nos backups periódicos.

3. Fique atento aos dispositivos que os colaboradores trazem de casa

Mesmo que isso seja muito comum, permitir que os colaboradores utilizem dispositivos particulares para o trabalho (como smartphones, tablets, notebooks e pen drives) precisa ser analisado com cautela.

Nesse caso, é importante que todos conheçam as políticas de segurança de dados da empresa, e, claro, será preciso reforçar a segurança dos softwares utilizados nesses dispositivos, evitando vazamentos e invasões (intencionais ou não).

Todos precisam estar cientes de suas responsabilidades no manuseio dos dados que circulam na empresa.

4. Defina um encarregado para a segurança dos dados

O artigo 41 da LGPD (Lei nº 13.709/2018) esclarece que a empresa precisa nomear um **encarregado pelo tratamento de dados pessoais**, o Data Protection Officer (DPO), cuja identidade e contato deverão ser divulgadas publicamente, de preferência, no site da empresa.



5. Adotar formas de consentimento para a coleta e o tratamento de dados

Todos os dados pessoais que forem coletados, utilizados e armazenados pela operadora precisam ter o consentimento dos titulares – seja por escrito ou por meio virtual. Lembre-se que o titular precisa saber **exatamente** a finalidade dessa coleta e como seus dados serão utilizados pela empresa – então, nada de pedir o consentimento de forma “genérica”.

6. Monitore o ambiente de TI em tempo real

Os dados da operadora são ativos muito importantes e precisam de monitoramento e proteção em tempo real, evitando situações graves, como vazamentos e sequestro de dados.

7. Reavalie os dados pessoais que a operadora já possui

Caso os titulares não tenham consentido a coleta e o uso de seus dados pessoais, será necessário entrar em contato novamente para solicitar.

Uma dica para isso é enviar e-mail explicando sobre as mudanças por conta da LGPD, afirmando que a operadora se preocupa em estar em dia com a lei e com a segurança dos dados. Por fim, solicite que os usuários leiam os novos termos de uso e política de privacidade, fornecendo um novo consentimento, caso estejam de acordo.

8. Revise os contratos com os fornecedores

Aproveite esse tempo de adequação à LGPD para rever também os contratos com todos os fornecedores que possuem, de forma direta ou indireta, acesso aos dados da empresa.

Se for preciso, é aconselhável que se estabeleça um novo contrato prevendo a conformidade legal no tratamento dos dados pessoais, sob a pena de responsabilização solidária.

9. Treine os colaboradores para conhecerem a LGPD

Promova um ciclo de palestras e debates com os colaboradores para que eles tenham conhecimento sobre a LGPD e como essa lei impactará a rotina da operadora. É preciso que todos entendam a importância do cuidado com os dados pessoais. Lembre-se que os dados pessoais de seus colaboradores também se enquadram na LGPD.

10. Fique de olho em possíveis mudanças na lei

A criação da Autoridade Nacional, por exemplo, havia sido vetada no final de 2018, mas voltou ao texto original da lei, sendo recentemente aprovado pelo Congresso Nacional por meio de Medida Provisória (MP 869).

Por isso, fique sempre de olho em novas alterações, medidas provisórias e novos requisitos de adequação à Lei sobre os dados pessoais. Se for preciso, invista em uma consultoria jurídica para esclarecer dúvidas eventuais.



6.7 Situações Específicas para o Setor da Saúde

6.7.1 Proibição da Prática de Seleção de Risco

No § 5º do art. 11, a LGPD veda às operadoras de planos privados o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários.

Vale dizer, portanto, que cumpridas as regras de elegibilidade para ingresso em plano coletivo, não é lícito instituir nenhum outro critério.

O setor de saúde suplementar, em sua já consolidada regulação, possui regras que disciplinam todo o processo de contratação de planos privados, o que, mais uma vez, confirma a importância de um diálogo consistente entre a LGPD e a legislação setorial.

Não significa uma vedação completa, permanecendo lícito que as operadoras realizem estudos populacionais, avaliando o comportamento de carteiras para o fim de aplicar uma precificação justa e adequada para cada grupo.



6.7.2 Health Analytics

De tempos em tempos, tem-se notícia de algum gigante da tecnologia que fez uso irresponsável e com propósitos puramente comerciais de dados de saúde de indivíduos. Contudo, a ciência de dados sempre foi um poderoso aliado dos profissionais da saúde.

Se a expressão “*data analytics*” corresponde à prática de se obter *insights* e informações relevantes a partir de uma massa de dados agregados, no contexto da saúde, a expressão “*health analytics*” tem enorme utilidade na identificação de possíveis doenças crônicas, das tendências de determinada população e na melhoria do sistema de saúde, por meio do uso racional e eficiente de recursos.

E iniciativas semelhantes não precisam ocorrer ao arpejo da privacidade.

Está claro que a LGPD não deve ser capturada por uma orientação que caminha na contramão da inovação tecnológica e do desenvolvimento científico e econômico – e nem deveria, tendo em vista o previsto por seu art. 2º, inciso V.

Para sustentar projetos inovadores para a área da saúde, que levem em consideração a ciência de dados e a privacidade desde sua concepção, é preciso que a organização realize um mapeamento de dados bem planejado, capaz de apontar suas fragilidades atuais e planos de remediação necessários, mas também de utilizar a tecnologia de modo sustentável, que assegure os direitos do titular e use a tecnologia em favor do desenvolvimento e melhoria da saúde.

6.8 Direito dos Titulares de Dados Pessoais

Este tema da LGPD se encontra nos artigos 8º, § 5º; 9º, caput/ e § 3º; 14, § 6º; e do 17 ao 22

A LGPD estabelece categoricamente que “toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei”. Ou seja, dados pessoais são de titularidade da pessoa natural a quem dizem respeito, e, portanto, não pertencem aos agentes de tratamento. Essa mesma lei estabelece diversos direitos que o titular possui e pode exercer em relação aos agentes de tratamento, a qualquer momento e mediante requerimento expresso, que deve ser atendido sem custos para o titular, em prazos e termos a serem futuramente definidos em regulamento, a saber:



Direito de confirmação do tratamento: O titular tem direito à confirmação da existência de tratamento, ou seja, direito de saber se seus dados pessoais são ou não objeto de tratamento por um determinado controlador. Esse direito deriva do princípio da transparência previsto no artigo 6º, inciso VI, da LGPD, pelo qual garante-se aos titulares “informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial”.

Direito de acesso: O titular de dados pessoais tem assegurado o acesso aos seus dados pessoais tratados pelo controlador. Ou seja, o titular pode exigir do controlador cópia dos dados pessoais de sua titularidade que são objeto de tratamento por esse controlador. Esse direito deriva do princípio do livre acesso, previsto no artigo 6º inciso IV, da LGPD, pelo qual garante-se aos titulares a “consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais”.



Correção de dados incompletos, inexatos ou

desatualizados: Um dos principais direitos do titular de dados pessoais é o direito à correção, ou retificação, das informações a seu respeito. Esse direito é derivado do princípio da qualidade dos dados, previsto no artigo 6º inciso V, da LGPD, pelo qual garante-se aos titulares “exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento”.

Anonimização, bloqueio ou eliminação de dados: O titular pode exigir que dados pessoais tidos como desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD sejam anonimizados, bloqueados ou eliminados. Esse direito deriva do princípio da necessidade, previsto no artigo 6º, inciso III, da LGPD, pelo qual garante-se a “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”.

Portabilidade dos dados a outro fornecedor de serviço

ou produto: O titular poderá (i) receber os dados pessoais que forneceram a um controlador de modo estruturado, normalmente em formato interoperável ou de uso corriqueiro e que possa ser lido automaticamente por computadores (machine-readable), para que possam ser utilizados por outro fornecedor de serviço ou produto; e/ou (ii) exigir a transferência direta desses dados pessoais a outro fornecedor de serviço ou produto, igualmente em formato que possibilite a utilização dos dados pessoais pelo novo fornecedor. Note-se que nem sempre essa segunda hipótese será tecnicamente possível, dada a potencial incompatibilidade de sistemas ou mesmo de estruturas de bancos de dados, situação em que os dados pessoais devem ser fornecidos diretamente ao titular.

Uso compartilhado de dados: A LGPD assegura ao titular o direito de saber com quais entidades públicas e privadas o controlador realizou uso compartilhado de dados. O setor privado deve estar preparado para responder a essas requisições por meio da manutenção de registros de tratamento de dados pessoais (record of processing activities), tal como exigido pelo artigo 37 da LGPD. Um dos elementos mais complexos do uso compartilhado de dados está na obrigação imposta pelo § 6º do artigo 18, pelo qual “o responsável deverá informar de maneira imediata aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados, a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento”.



Possibilidade de não fornecer consentimento: A LGPD impõe aos controladores que utilizam o consentimento como base legal de tratamento de dados pessoais que informem aos titulares (i) a possibilidade de não fornecer consentimento, quando factível, e (ii) as consequências da negativa, que em boa parte das vezes significará a impossibilidade de usufruir de determinado produto ou serviço.

Revogação do consentimento: Os controladores devem informar aos titulares que eles têm o direito de revogar seu consentimento a qualquer tempo e como podem exercer esse direito, preferencialmente por meio de um procedimento rápido e simplificado e sem serem prejudicados.

Eliminação dos dados pessoais tratados com o consentimento do titular: O titular pode exigir, mediante requerimento expresso, a eliminação dos dados pessoais tratados com o seu consentimento, exceto nas hipóteses previstas no artigo 16 da LGPD (cumprimento de obrigação legal ou regulatória pelo controlador; estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados).

Direito de petição: A LGPD estabelece que “o titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional” (art. 18, § 1º), de forma a deixar claro que o órgão responsável por receber eventuais queixas ou denúncias formuladas pelos titulares de dados pessoais é a Autoridade Nacional. É importante observar que o § 8º do mesmo artigo diz que “o direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor”. Daí não decorre, porém, que organismos de defesa do consumidor possam exercer o mesmo papel da Autoridade Nacional. Isso apenas significa que, em nome da facilitação de seus direitos, o titular pode peticionar a esses organismos, cuja função nesse contexto é limitada a receber a petição com a queixa ou a denúncia e encaminhá-la à Autoridade Nacional.



Direito de oposição: O § 2º do artigo 18 da LGPD estipula que “o titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei”. Em outras palavras, toda vez que a base legal de tratamento de dados não for o consentimento e houver descumprimento da LGPD, o titular pode se opor ao tratamento de seus dados pessoais, independentemente da adoção de medidas corretivas ou imposição de penalidades, exigindo a imediata interrupção de qualquer atividade de tratamento.

Que providências tomar:

Adotar medidas técnicas que garantam o tratamento de dados de forma segura. Desenvolver processos internos e criar políticas que permitam realizar a criação e manutenção de registros das operações de tratamento de dados;

Conservar os dados visando atender a finalidade pela qual foram coletados e para cumprir com obrigações legais e regulatórias;

Nomear o encarregado pelo tratamento dos dados pessoais.



6.9 Os agentes de Tratamento de Dados Pessoais

Este tema está na LGPD artigos 5º, 7º §5, 8º §2º, 9º ao 11, 14, 16, 18, 20, 33, 37 ao 42, 48, 50 e 52

A LGPD define os papéis dos agentes de tratamento, definidos pela lei como “Controlador”, “Operador” e “Encarregado”.

6.9.1 Controlador

O controlador é quem exerce controle geral sobre as finalidades para as quais e as maneiras pelas quais os dados pessoais são e serão tratados. Em outras palavras, será o controlador que decidirá o “porquê” e o “como” da atividade de tratamento de dados, sendo o agente responsável por todo o ciclo de vida dos dados – da sua coleta à sua exclusão.

Como consequência da posição como principal tomador de decisões e do maior poder de controle sobre os procedimentos e as finalidades envolvendo o uso dos dados pessoais, o controlador também terá maiores responsabilidades sobre tais dados e, eventualmente, sobre quaisquer violações decorrentes do processo de tratamento dos mesmos.

O controlador não apenas representa a figura central na proteção dos direitos dos titulares – devendo observar a legislação e garantir que as atividades de processamento exercidas por todos os agentes envolvidos estejam em conformidade com a lei – mas também exerce funções relevantes para a cadeia de tratamento de dados. Dois dos principais deveres do controlador são, por exemplo, a elaboração de relatório de impacto à proteção de dados pessoais e a nomeação de um encarregado pelo tratamento de dados pessoais para atuar como canal de comunicação entre o controlador e a Autoridade Nacional de Proteção de Dados e o controlador e os titulares.

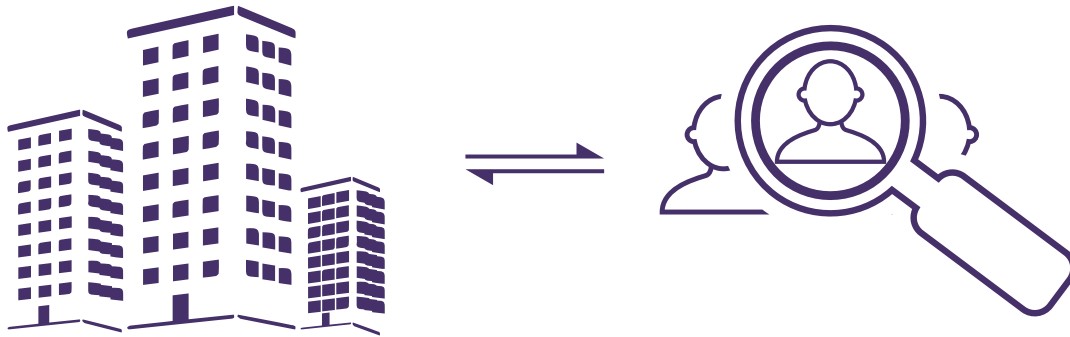


O controlador ainda é responsável pelos seguintes processos:

1. obtenção de consentimento específico do titular, quando necessário;
2. informação e prestação de contas e pela garantia de portabilidade dos dados;
3. garantia de transparência no tratamento de dados baseado em legítimo interesse;
4. manutenção de registro das operações de tratamento de dados pessoais, especialmente quando baseado no legítimo interesse;
5. reparação de danos patrimoniais, morais, individuais ou coletivos causados por violação à legislação de proteção de dados pessoais, e
6. comunicação à autoridade nacional e ao titular quando da ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.



6.9.2 Operador



O operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. O operador não controla os dados e não pode alterar a finalidade ou o uso do conjunto particular de dados relacionados a determinado tratamento, devendo tratar tais dados de acordo com as instruções e dentro das finalidades definidas e impostas pelo controlador.

Apesar de o operador atuar em nome do controlador e obedecendo as suas decisões, é comum que o controlador de dados conceda ao agente operador um certo grau de discricionariedade e liberdade sobre o processo de tratamento dos dados, permitindo que exerça controle sobre o modo com que os dados serão tratados. Nesse sentido, o operador poderá exercer certo controle principalmente sobre os aspectos técnicos relativos a como um serviço específico será prestado.

Isso quer dizer que o operador tem a liberdade de utilizar a sua experiência na operação de tratamento de dados e seus conhecimentos técnicos para decidir como conduzir certas atividades em nome do controlador. No entanto o operador não poderá tomar decisões relevantes, como: quais dados serão usados e qual a finalidade, e nem quais conteúdos utilizar. Tais decisões podem ser tomadas tão somente pelo controlador, pois é esse quem possui poder decisório.

6.9.3 Encarregado

O encarregado é a 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 (ANPD).



A ANPD poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.



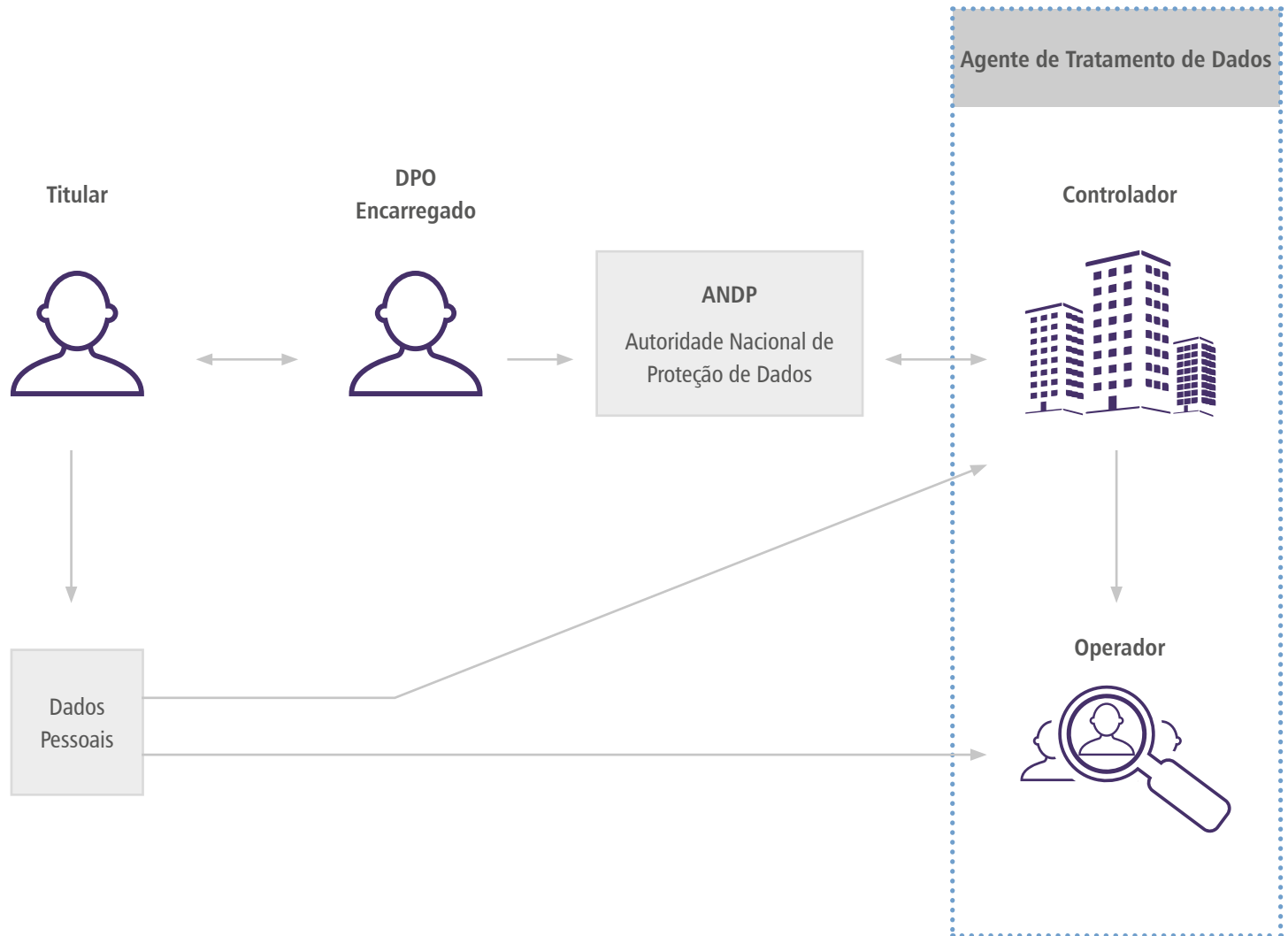
Entre as principais funções do encarregado, estão:

1. Recepcionar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
2. Receber comunicações da autoridade nacional e adotar providências;
3. Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
4. Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Deverá ser divulgada publicamente, de forma clara e objetiva, preferencialmente no website do controlador, a identidade e as informações de contato do encarregado.



6.9.4 Fluxo do Relacionamento dos Agentes da Informação









6.10 Regras Consentimento

O tratamento dos dados pessoais só pode ser realizado em dez hipóteses estabelecidas pela LGPD, conhecidas como as bases legais de Tratamento.

Uma das bases legais de tratamento é o consentimento do titular, ou seja, a concordância com o tratamento de seus dados pessoais para uma finalidade determinada.

O consentimento, no entanto, precisa respeitar alguns requisitos para que seja considerado válido:

-  **Livre:** o consentimento deve refletir uma manifestação livre da vontade do titular. Ou seja, o titular dos dados não pode ser compelido a consentir com o tratamento.
-  **Informado:** o titular deve ter recebido informações claras, objetivas e suficientes para decidir de maneira consciente se concorda com o tratamento de seus dados pessoais para as finalidades mencionadas.
-  **Inequívoco:** o consentimento deve ser demonstrado de maneira inequívoca. Isso pode ser feito por escrito ou por outros meios que demonstrem a vontade do titular, desde que não deixem dúvidas (por exemplo, gravação de uma ligação telefônica). Consentimentos implícitos, que não tenham sido registrados, ou que deixem por algum motivo dúvidas sobre a vontade do titular, poderão ser desconsiderados.
-  **Relacionado a uma finalidade determinada:** o titular de dados deverá autorizar o tratamento de dados para uma finalidade específica. Autorizações genéricas ou vagas podem ser consideradas nulas







Além de se atentar aos pontos acima, é muito importante que as operadoras de planos de saúde se atendem ao fato de que o consentimento é revogável a qualquer tempo pelo titular de dados pessoais.



6.10.1 Tratamento de Dados Sem o Consentimento do Titular

A LGPD traz nove hipóteses em que é possível tratar dados pessoais sem obter o consentimento do titular. Entre elas, as que possuem maior relevância para as operadoras de plano de saúde são:

-  **Cumprimento de obrigação legal ou regulatória:** se uma lei ou uma regulamentação setorial exige determinada atividade de tratamento de dados, não é preciso solicitar a autorização do titular de dados. É o caso, por exemplo, de registros de acesso a aplicações online para cumprir com as obrigações de retenção previstas no Marco Civil da Internet, legislação que exige que os últimos seis meses de atividade do usuário sejam registrados pelas empresas que oferecem funcionalidades online.
-  **Para executar um contrato ou procedimentos preliminares relacionados a um contrato celebrado com o titular de dados pessoais.** Por exemplo, para entregar um produto ou um serviço adquirido após a conclusão da compra, naturalmente é preciso conhecer o nome completo, o endereço e outras informações de contato do consumidor. O tratamento desses dados pessoais é feito justamente para cumprir o contrato celebrado.
-  **Para o exercício regular de direitos em processo judicial, administrativo ou arbitral.** Ou seja, o armazenamento ou outra forma de tratamento de dados pessoais para utilização em eventual processo judicial é possível, independente de autorização do titular. Por exemplo, pode ser necessário guardar o histórico de compras e dados de contato de consumidores em casos de litígios pós-venda.
-  **Para atender aos interesses legítimos da empresa responsável pelo tratamento ou aos interesses legítimos de terceiros, desde que o tratamento de dados não ofereça um risco importante aos direitos e liberdades fundamentais dos titulares de dados.** Esses pontos são detalhados na seção seguinte, que trata especificamente do legítimo interesse, mas é importante compreender que a LGPD exige a análise do impacto à privacidade do titular de dados e a documentação dessa análise quando se utiliza o legítimo interesse.

As outras hipóteses previstas na LGPD envolvem tratamentos de dados para a proteção da vida ou da incolumidade física do titular dos dados ou de terceiros, para a proteção do crédito, para a tutela da saúde, ou situações específicas de tratamento de dados pela administração pública ou por órgão de pesquisa.

Nessas hipóteses é recomendável avaliar se o tratamento de dados sensíveis realmente compensa a necessidade de cumprir com as exigências adicionais previstas na LGPD.



6.11 Legítimo Interesse

O tratamento de dados pessoais com base no legítimo interesse é, certamente, a hipótese mais abrangente e flexível prevista na LGPD. A lei não estabelece em quais situações existe ou não um legítimo interesse para tratar dados pessoais, e indica que essa análise deverá ser realizada a partir de situações concretas.

É mais provável que exista um legítimo interesse em situações em que o tratamento a ser realizado esteja dentro das expectativas razoáveis dos titulares de dados e tenham um pequeno impacto à sua privacidade, ou se houver uma justificativa relevante para o tratamento.

Existem três elementos que devem ser considerados:

1. Identificar para quais finalidades o tratamento será realizado, e se essas finalidades são legítimas e consideradas a partir de situações concretas;
2. Verificar se é realmente necessário realizar o tratamento de dados para atingir aquela finalidade; e
3. Balancear o interesse legítimo identificado com os direitos e as liberdades fundamentais dos titulares de dados que sejam impactados por esse tratamento.

A LGPD não apresenta uma lista pré-estabelecida do que constitui ou não legítimo interesse, justamente por esta determinação acontecer de acordo com cada caso concreto específico. A LGPD cita como exemplos o apoio e a promoção de atividades do responsável pelo tratamento dos dados pessoais.

Isso significa que, em tese, o tratamento de dados pessoais para finalidades atreladas a atividades de marketing poderia ser realizado com fundamento no legítimo interesse, desde que observados os requisitos e os elementos indicados acima. Na prática, sempre será necessária uma análise detalhada de cada atividade de marketing e das maneiras e finalidades do tratamento para confirmar se é possível ou não utilizar o legítimo interesse como base legal.

Uma vez verificada a possibilidade de tratar dados pessoais com base no legítimo interesse, é necessário elaborar um relatório de impacto à proteção de dados pessoais (conhecido em inglês como Data Protection Impact Assessment – DPIA). Esse relatório deve descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades e aos direitos dos titulares de dados, bem como medidas, salvaguardas e mecanismos de mitigação de risco adotados. A Autoridade Nacional de Proteção de Dados poderá solicitar a apresentação desse relatório.

6.12 Dados de Crianças e Adolescentes

O tratamento de dados pessoais de crianças (menores de 12 anos) só pode ser realizado com o consentimento específico e destacado de um dos pais ou do responsável legal.

O consentimento legal e o consentimento da LGPD não se confundem. De tal modo, não é possível afirmar que a única base legal aplicável é o consentimento. Além disso, há na própria lei uma exceção ao consentimento específico mencionado:

Art.14

§ 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.

Em qualquer hipótese de tratamento de dados pessoais de crianças ou adolescentes, as informações sobre o tratamento devem ser fornecidas de maneira simples, clara e acessível, consideradas suas características físicas, perceptivas, sensoriais, intelectuais e mentais, com uso de recursos audiovisuais quando adequado.





6.13 Término do Tratamento de Dados Pessoais

A LGPD estipula a obrigatoriedade de eliminação dos dados pessoais ao término do tratamento. Isso ocorre nas seguintes hipóteses:

1. verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica;
2. fim do período de tratamento;
3. comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento, resguardado o interesse público; ou
4. determinação da autoridade nacional, quando houver violação da lei.

Contudo, a LGPD estipula que a conservação dos dados pessoais será autorizada em alguns casos: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; c) transferência à terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na lei; ou d) uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Note-se que certas atividades de tratamento (tais como operações de saúde) justificam o tratamento contínuo dos dados pessoais envolvidos, não existindo nessas hipóteses um dever geral de eliminação dos dados pessoais (por exemplo, a própria existência de modelos de continuidade de tratamento para o beneficiário requer o contínuo tratamento e análise de dados).



6.14 Governança em LGPD



No contexto de adequação à LGPD e para garantir o efetivo cumprimento das suas disposições, é altamente recomendável que as instituições adotem programas de governança em privacidade, especialmente tendo em vista as obrigações de controles internos, prevenção à lavagem de dinheiro e política de segurança cibernética previstas na Regulamentação Setorial.

Esses programas devem estabelecer, por exemplo, condições, regimes e procedimentos internos para o tratamento de dados pessoais, normas de segurança da informação, padrões técnicos, alocação de responsabilidades e obrigações aos diversos colaboradores envolvidos nas atividades de tratamento, ações educativas, mecanismos internos de supervisão e mitigação de riscos, procedimentos de resposta a incidentes de segurança, entre outros.

É também muito importante que todos os processos, decisões, esforços e ações relacionados à governança de dados pessoais na empresa sejam documentados e mantidos em arquivo para apresentação à ANPD, se necessário.

A adoção de políticas de boas práticas e governança não apenas auxilia a instituição a cumprir com as obrigações estabelecidas pela LGPD, como evidencia os esforços nesse sentido e será considerada (como um atenuante) na aplicação de penalidades em caso de descumprimento da LGPD.

Do ponto de vista prático, um programa de governança em privacidade deve:



demonstrar o comprometimento da instituição em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

ser aplicável a todo o conjunto de dados pessoais que estejam sob o controle da empresa, independentemente do modo como se realizou sua coleta;

ser adaptado à estrutura, à escala e ao volume das operações da instituição, bem como à sensibilidade dos dados tratados;

estabelecer políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

ter o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

estar integrado a sua estrutura geral de governança e estabelecer e aplicar mecanismos de supervisão internos e externos;

contar com planos de resposta a incidentes e remediação; e

ser atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.



6.15 Segurança em LGPD

Este tema da LGPD se encontra no Art. 44, parágrafo único e do Art. 46 ao Art. 51

Deverão ser adotadas medidas de segurança com a finalidade de garantir a proteção dos dados pessoais contra acessos não autorizados e situações acidentais ou até mesmo ilícitas. O primeiro passo é identificar a natureza dos dados objeto do incidente. Se forem dados criptografados ou anonimizados, por exemplo, os riscos serão menores.

Casos de incidente de segurança deverão ser comunicados, em prazo razoável, à Autoridade Nacional de Proteção de Dados e ao titular dos dados.

Dependendo da gravidade do incidente, a autoridade poderá determinar a adoção de determinadas providências e eventual comunicação a outros órgãos reguladores, como CVM (Comissão de Valores Mobiliários), BACEN (Banco Central) e ANS (Agência Nacional de Saúde Suplementar).

Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas, motivar o dano.

Que providências tomar?

Desenvolver sistemas de identificação e combate de incidentes de segurança, bem como treinar uma equipe de TI para garantir a execução destes procedimentos;

Revisar os acordos de seguros para garantir cobertura em caso de incidentes de segurança;

Criar políticas e procedimentos internos, bem como parcerias com prestadores de serviços técnicos e de assessoria jurídica, para que a resposta a ser dada a incidentes seja feita de modo a atender os requisitos previstos na LGPD.



Os agentes de tratamento deverão proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito dos dados pessoais. Para tanto deverão adotar uma série de medidas de segurança técnicas e administrativas.



Caberá à autoridade nacional determinar os padrões técnicos mínimos de segurança de proteção de dados pessoais, principalmente sobre dados sensíveis. Tais requisitos podem ser também estabelecidos por autoridades setoriais, como para o setor de saúde, financeiro, entre outros.

Apesar de qualquer pessoa que intervenha no tratamento de dados ter a obrigação de garantir a segurança, os agentes de tratamento responsáveis respondem pelos danos decorrentes da inobservância das medidas de segurança.

É recomendável que os agentes também adotem medidas técnicas que tornem os dados pessoais afetados ininteligíveis para que terceiros não autorizados não possam acessá-los. A adoção de tais medidas técnicas será levada em conta na determinação da gravidade do incidente.



Casos de incidente de segurança que possam acarretar risco ou dano relevantes aos titulares deverão ser comunicados à autoridade nacional e ao titular dos dados, em prazo razoável (a ser definido pela autoridade), e órgãos reguladores setoriais.

Essa comunicação deverá conter no mínimo as seguintes informações:

- descrição da natureza dos dados pessoais afetados;
 - os titulares envolvidos;
- as medidas técnicas e de segurança utilizadas para a proteção dos dados;
 - os riscos relacionados ao incidente;
- os motivos da demora, no caso da comunicação não ter sido imediata.

A depender da gravidade do incidente, a autoridade nacional poderá determinar a adoção de determinadas providências, como a ampla divulgação do fato em meios de comunicação ou medidas para reverter ou mitigar os efeitos do incidente.

Portanto, é recomendável que os agentes de tratamento tenham um plano de ação de relações públicas bem desenhado, em compliance com as políticas internas e ações estratégicas de todas as áreas da Cia.

Os agentes de tratamento de dados poderão, individualmente ou por meio de associações, formular regras de boas práticas e de governança sobre o tratamento de dados pessoais, que estabeleçam:

- as condições de organização, funcionamento e procedimentos aplicáveis ao tratamento dos dados pessoais (incluindo reclamações e petições de titulares);
- as normas de segurança e padrões técnicos;
- obrigações específicas para os diversos envolvidos no tratamento;
- as ações educativas;
- os mecanismos internos de supervisão e de mitigação de riscos;
- outros aspectos relacionados ao tratamento de dados pessoais.





6.16 Violações e Sanções

Este tema da LGPD se encontra entre os artigos 52 e 54



Além da possibilidade de aplicação de sanções civis definidas na Lei nº 8.078, de 11 de setembro de 1990, e em legislação específica, a LGPD prevê sanções de caráter administrativo na hipótese de seu descumprimento.

As sanções administrativas aplicáveis pela autoridade nacional, em razão das infrações às normas da LGPD, vão desde advertência até a imposição de sanções de natureza pecuniária, que podem chegar a *2% do faturamento do grupo no Brasil, limitada a R\$ 50 milhões por infração.

As sanções podem ser aplicadas cumulativamente, por dia e por quantidade de infração, mas sempre com base na gravidade e extensão da violação.

Em razão das infrações às normas da LGPD, os agentes de tratamento de dados estão sujeitos às seguintes penalidades:

- advertência, com indicação de prazo para adoção de medidas corretivas;
- multa de até 2% do faturamento da empresa ou do grupo limitada, no total, a R\$ 50 milhões por infração;
- publicização da infração após devidamente apurada e confirmada a sua ocorrência;

* No seu último exercício, excluídos os tributos



- bloqueio dos dados pessoais correspondentes à infração até a sua regularização;
- suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
- suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
- proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados;
- eliminação dos dados pessoais correspondentes à infração.

Todas as sanções serão precedidas de um procedimento administrativo que garanta a ampla defesa do infrator. As sanções serão aplicadas considerando as particularidades de cada caso e os seguintes parâmetros e critérios:

- gravidade e a natureza das infrações e dos direitos pessoais afetados;
- boa-fé do infrator;
- vantagem auferida ou pretendida pelo infrator;
- condição econômica do infrator;
- reincidência;
- grau do dano;
- cooperação do infrator;
- adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano;
- adoção de política de boas práticas e governança;
- pronta adoção de medidas corretivas;
- proporcionalidade entre a gravidade e a intensidade da sanção.



No cálculo do valor da multa a autoridade nacional poderá considerar o faturamento total da empresa ou do grupo de empresas nos termos do art. 52, § 2º, da Lei.

Na aplicação da sanção de multa diária, a autoridade nacional deverá fundamentar a aplicação da sanção observando a gravidade e a extensão do dano ou prejuízo causado.

Em casos de incidentes transnacionais, as multas aplicadas em uma jurisdição não serão compensadas ou abatidas com as aplicadas em outra.



Que providências tomar?

Analisar continuamente a conformidade dos procedimentos de tratamento de dados em relação à LGPD, averiguando o cumprimento completo da norma. Caso identificado o descumprimento, cooperar e trabalhar em processos para minimizar o dano. Ter à sua disposição uma equipe multidisciplinar que possa atender prontamente às solicitações da autoridade nacional de proteção de dados, visando diminuir o risco de aplicação de sanções.




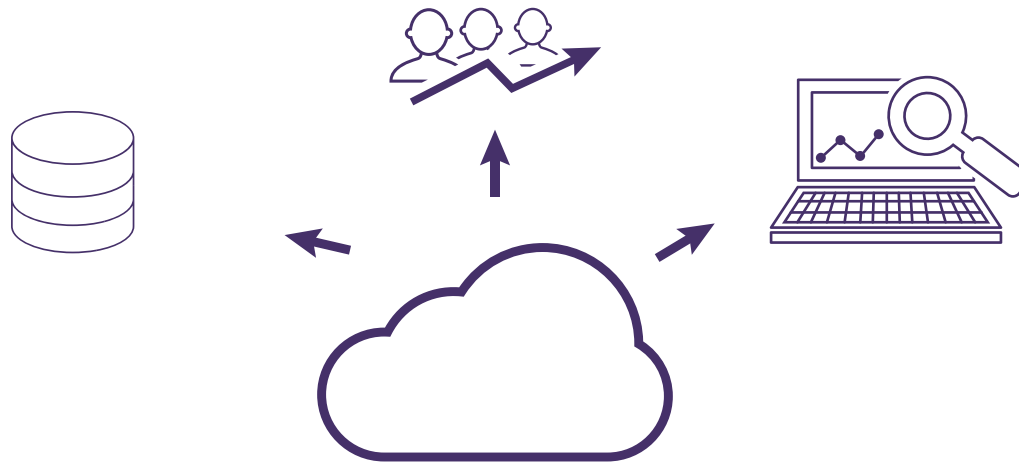
6.17 Principais Pontos de Atenção para Implantação da LGPD

6.17.1 Dados que Exigem Mais Proteção

O tratamento de algumas categorias de dados pessoais oferece maiores riscos de danos aos respectivos titulares e por isso são tratados pela LGPD como “dados sensíveis”.

São considerados dados sensíveis pela LGPD: 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. É importante observar que a fotografia do rosto de uma pessoa pode ser considerada dado biométrico.

| Dados Pessoais | | Dados Pessoais Sensíveis |
|--|---|--|
| <ul style="list-style-type: none">• Nome• Endereço• Número de identificação• Dados de localização• Identificadores eletrônicos (e-mail, endereço de IP)• Geolocalização• Número de telefone e dados de conexão |  | <ul style="list-style-type: none">• Origem racial ou étnica• Opiniões políticas• Convicções religiosas ou filosóficas• Filiação sindical• Dados genéticos• Dados biométricos tratados simplesmente para identificar um ser humano• Dados relacionados com a saúde• Dados relativos à vida sexual ou orientação sexual |



6.17.2 Reaproveitamento de Bases

Se os dados foram coletados para um uso específico e a base legal atribuída não contemplava o desenvolvimento desses novos produtos ou serviços, provavelmente será necessário obter um novo consentimento dos titulares de dados pessoais.

Alternativamente é necessário verificar se o tratamento de dados pessoais realizado para o desenvolvimento desses novos produtos ou serviços poderia ser enquadrado em uma das outras nove hipóteses em que é permitido tratar dados pessoais sem consentimento, e se atende aos princípios estabelecidos na LGPD, destacadamente aos da transparência, finalidade, adequação e necessidade.

6.17.3 Utilização de Dados Públicos

Não deixam de ser dados pessoais aqueles que estão publicamente disponíveis – seja porque foram tornados públicos pelo titular, seja porque encontram-se em bases de acesso público. Nesses casos, a LGPD permite que dados pessoais sejam utilizados sem necessidade de obtenção de consentimento do titular, mas continua sendo necessário enquadrar esse tratamento em uma das outras bases legais disponíveis e observar todos os direitos dos titulares de dados e os princípios estabelecidos pela LGPD.

Ou seja, é necessário dar transparência tanto ao tratamento do dado quanto à finalidade, enquadrando em uma base legal e franqueando ao titular acesso às informações.



6.17.4 Dados Anônimos

Dados anonimizados não são considerados dados pessoais, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. É importante, no entanto, confirmar se os dados podem realmente ser considerados anônimos. Em muitas ocasiões, dados aparentemente anônimos podem ser facilmente identificados.

Por exemplo: há situações em que os dados pessoais passam por procedimentos que removem identificadores pessoais (como nome e CPF), os quais são substituídos por números, códigos ou hashes, criando-se uma nova base de dados. Porém, se o detentor dessa base de dados também tiver acesso à base original identificada ou puder cruzar informações de outras bases de dados às quais tem acesso para identificar os titulares, essa base de dados supostamente anonimizada será, em verdade, considerada apenas pseudonimizada, aplicando-se normalmente a LGPD.

6.17.5 Incidentes

Incidentes de segurança que possam acarretar risco ou dano aos titulares de dados devem ser comunicados à Autoridade Nacional de Proteção de Dados e aos respectivos titulares de dados. A LGPD estabelece o conteúdo mínimo que deve constar da notificação.

Além disso, a autoridade nacional, ao verificar a gravidade do incidente, poderá determinar providências adicionais, tais como a ampla divulgação do fato em meios de comunicação e medidas para reverter ou mitigar os efeitos do incidente.

Toda empresa deve criar e manter um plano de resposta a incidentes, definindo como agir interna e externamente nessas situações.



6.17.6 Cuidados na criação de Perfis

O titular dos dados pessoais tem sempre o direito de solicitar a revisão de seus perfis (de comportamento, de consumo, dentre outros) formados de maneira automatizada com algoritmos, por exemplo.

Outro ponto de atenção envolvendo a formação de perfis é a dificuldade em torná-los anônimos. Perfis compostos por um grande volume de informações, ainda que não estejam atribuídas a um identificador pessoal como nome, CPF ou RG, por vezes possibilitam a identificação da pessoa a quem se referem por meio de inferências. Isso porque quanto maior o volume e mais específicas as informações acerca de uma pessoa (ainda que não identificada), menor o universo de indivíduos a quem aqueles dados podem ser atribuídos.

6.17.7 Atos de Terceiros

Todos os profissionais ou empresas que tomarem decisões e estiverem diretamente envolvidos nas atividades de tratamento de dados pessoais realizadas em violação à lei serão solidariamente responsáveis pelo ressarcimento dos danos causados aos titulares, salvo se puderem provar que (i) não realizaram o tratamento de dados pessoais que lhes é atribuído, ou (ii) embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados, ou (iii) o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros.

Por esses motivos, é bastante importante trabalhar com parceiros comerciais que estejam buscando se adequar à LGPD, já que eventual desconformidade alheia pode conforme as circunstâncias do caso, acarretar responsabilidade solidária.



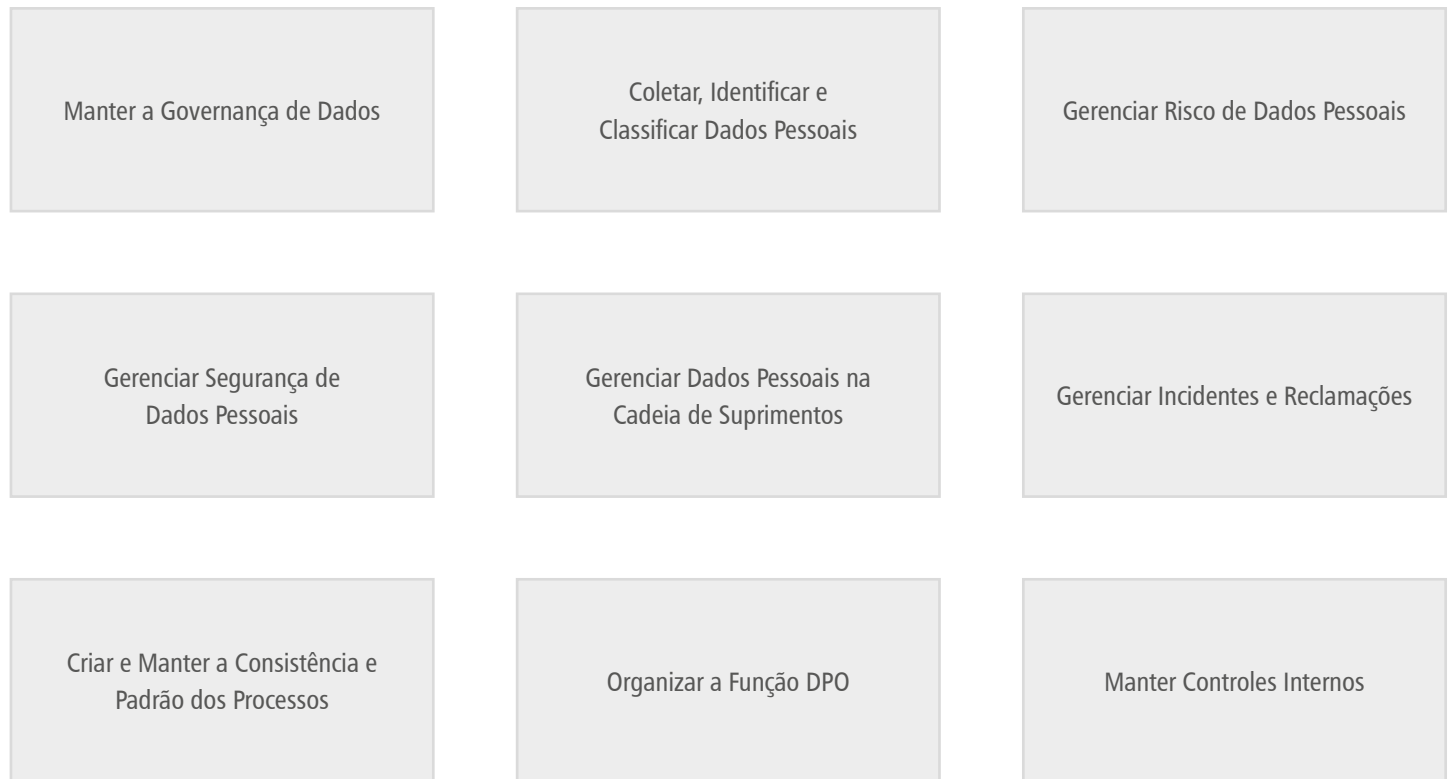
6.18 *Check List* para Implantação da LGPD

- ✓ Fazer um mapeamento geral de todas as atividades que envolvem tratamentos de dados pessoais, incluindo processos de coleta, armazenamento e compartilhamento, verificando também se há tratamento de dados pessoais sensíveis.
- ✓ Definir as bases legais mais apropriadas para o tratamento de dados, conforme a finalidade específica (consentimento, legítimo interesse, execução de contrato, cumprimento de obrigação legal ou regulatória, proteção ao crédito, etc).
- ✓ Analisar se há discrepâncias entre as obrigações legais e as atividades da empresa e definir quais estratégias adotar para adequação.
- ✓ Alocar responsabilidades internas para execução das ações necessárias.
- ✓ Implementar ferramentas que permitam aos titulares de dados pessoais exercerem seus direitos garantidos pela LGPD.
- ✓ Elaborar, revisar, adaptar e aditar contratos que envolvam tratamento e/ou compartilhamento de dados pessoais, tanto nas relações com usuários e consumidores, quanto nas relações com fornecedores e parceiros comerciais.
- ✓ Elaborar relatórios de impacto à proteção de dados pessoais nos casos de tratamento baseado em legítimo interesse e em outras situações em que isso seja recomendável.
- ✓ Elaborar e revisar políticas internas, planos de resposta a incidentes e outros documentos sobre privacidade e proteção de dados pessoais.
- ✓ Revisar e implementar técnicas e procedimentos de segurança da informação e programas de privacidade (privacy by design/by default).
- ✓ Estabelecer um programa de governança em proteção de dados pessoais.
- ✓ Engajar as várias áreas da empresa no projeto, em especial aquelas que são afetadas pelo LGPD, por utilizarem dados de clientes ou dos colaboradores em suas atividades.
- ✓ Treinar seus funcionários e educá-los sobre a importância e os impactos da LGPD.
- ✓ Em seguida a essa mobilização inicial, deve-se então realizar uma avaliação do estado atual da empresa em relação ao requerido pela LGPD. Com isso tem-se uma visão mais clara das não conformidades existentes, bem como a prontidão da organização para assumir essa jornada.
- ✓ O passo seguinte é a definição de um plano de ação (*roadmap*) para atingir seu objetivo, conforme a priorização feita pela organização em relação aos principais pontos encontrados.
- ✓ Verificar se os terceiros também estão em conformidade com a LGPD.



6.19 *Framework* de Processos LGPD

O modelo de processos agrupa as atividades em torno de nove processos centrais. Para cada processo central, existem vários subprocessos que cobrem aspectos detalhados de dados pessoais. Entenda:



Este framework cobre todos os requisitos e artigos da LGPD e é baseado em boas práticas de governança e segurança da informação, como ITIL, COBIT, ISO 27.000, ISO 20.000, ISO 29.100. Para implantação, os profissionais devem aproveitar as práticas de governança e segurança já existentes e utilizados na organização.



6.19.1 Detalhamento do *Framework* por Processos LGPD

1. Manter a Governança LGPD

Estabelecer framework LGPD

Manter logs de tratamento de dados

Manter normas corporativas obrigatórias

Manter normas de consentimento

Manter normas de solicitações

Manter normas para gestão de reclamações

2. Coletar, Identificar e Classificar Dados Pessoais

Gerenciar o ciclo de vida dos dados

Conduzir a identificação de dados pessoais

Manter a classificação de dados pessoais

Manter o registro de dados pessoais

Gerenciar a exclusão e alteração de dados

3. Gerenciar Riscos

Realizar avaliação de risco

Conduzir a avaliação de impacto

Gerenciar o tratamento de risco

Realizar validação de risco

4. Gerenciar Segurança de Dados Pessoais

Gerenciar níveis de proteção

Gerenciar anonimato

Gerenciar criptografia

Gerenciar acessos

Gerenciar testes e *assessment*



5. Gerenciar a Cadeia de Suprimentos

Gerenciar terceiros de acordo com a LGPD

Manter acordos SLAs, termos e contratos

Gerenciar o impacto da cadeia de suprimentos

Obter controles de terceiros (testes, evidências, auditoria)

6. Criar e Manter a Consciência

Manter a conscientização

Gerenciar habilidades e educação

Gerenciar treinamentos

7. Organização as Funções

Controlador | Operador | Encarregado

Gerenciar orçamento e recursos

Gerenciar interfaces organizacionais

Gerar e gerenciar relatórios internos e externos

Gerenciar serviços externos

8. Manter Controles Internos

Manter controles de dados de terceiros

Manter processos de manutenção

Manter controles de armazenamento

Manter controles de exclusão

Manter controles de monitoramento e realizar revisão independente da garantia da qualidade em LGPD



6.19.2 Avaliação de Requisitos por Área de Negócio

| Área de Tecnologia da Informação |
|---|
| Existe política de segurança da informação? |
| Existe área de proteção da informação - <i>security officer</i> ? |
| Existe levantamento dos sistemas que processam e armazenam dados pessoais? |
| Todos os sistemas permitem atender pedidos dos titulares de dados (acesso, alteração e eliminação)? |
| Todos os sistemas atendem a política de segurança da informação? |
| Existe plano de resposta a incidentes? |
| São realizadas análise de vulnerabilidade dos sistemas? |
| São realizadas auditorias nos sistemas? |

| Área de Recursos Humanos |
|--|
| Quais os controles de segurança sobre os CVs armazenados? |
| Existe cláusula nos contratos sobre consentimento formal para armazenamento e tratamento das informações pessoais, inclusive em servidores de terceiros? |
| Existe aceite para a política de segurança da informação? |
| São realizados treinamentos sobre segurança da informação? |
| Foram feitas revisões nos contratos dos prestadores de serviços sobre proteção de dados? |
| O armazenamento de informações sobre plano de saúde folha de pagamento e treinamento atendem a LGPD? |



Área Comercial

Foram revistos os procedimentos de envio de newsletters e outras comunicações a clientes e prospects?

Foram feitas revisões nos formulários?

Área Jurídica/Riscos/Compliance

Os contratos vigentes dispõem de cláusulas adequadas à LGPD?

Foram revistos os termos de uso e política de privacidade dos serviços na web?

Existem contratos internacionais que devem ser revistos?

Área Administrativa

Existe a área responsável pelo tratamento de dados pessoais?

Existe seguro com cobertura para incidentes de segurança?

Existe consentimento formal dos candidatos para armazenamento e tratamento dos dados pessoais?



6.20 Quadro de Resumos

6.20.1 Resumo da LGPD

| | | | | |
|--|---|---|---|--|
| Tratar dados pessoais (Art. 1º) | Avaliar o alcance territorial da Lei e transferência internacional de dados (Arts. 3º e 4º) | Reportar-se à Autoridade Nacional de Proteção de Dados (ANPD) (Art. 5º) | Adequar-se a pelo menos uma das 10 bases legais de tratamento (Art. 7º) | Definir o tratamento de dados sensíveis (Art. 11º) |
| Manter o registro do processamento de dados (Art. 37º) | Gerenciar o direito dos titulares (acesso, oposição, portabilidade, etc) (Caput e § 3º) | Nomear um DPO – encarregado pela proteção de dados (Art. 4º) | Reportar as violações de Dados (Art. 48º) | Gerenciar eventuais infrações diante de sanções de até R\$50 milhões por infração (Art. 52º) |



6.20.2 Resumo Direito dos Titulares



Confirmação de que existem um ou mais tratamentos de dados sendo realizados



Acesso aos dados pessoais conservados que lhe digam respeito



Correção de dados pessoais incompletos, inexatos ou desatualizados



Eliminação de dados pessoais desnecessários, excessivos ou caso o seu tratamento seja ilícito



Portabilidade de dados a outro fornecedor de serviço ou produto, observados os segredos comercial e industrial



Eliminação de dados (exceto quando o tratamento é legal, mesmo que sem o consentimento do titular)



Informação sobre compartilhamento de seus dados com entes públicos e privados, caso isso exista



Informação sobre o não consentimento, ou seja, sobre a opção de não autorizar o tratamento e as consequências da negativa



Revogação do consentimento, nos termos da lei



Reclamação contra o controlador dos dados junto à autoridade nacional



Oposição, caso discorde de um tratamento feito sem seu consentimento e o considere irregular



6.21 Histórico da Lei Geral de Proteção de Dados



A Lei Geral de Proteção de Dados (LGPD) entrou em vigor em 18.09.2020, e tem como objetivo garantir mais segurança e transparência às informações pessoais coletadas por empresas públicas e privadas.

Dados que devam ser protegidos são informações geradas por pessoas, seja on-line ou não. São os rastros deixados ao visitar sites, o cadastro feito, entre outras situações.

Com a publicação da Lei 13.709/2018, alterada pela Lei 13.853/19, foram várias as tentativas de adiamento da norma.

Em abril 2020, o Presidente da República editou a Medida Provisória nº 959/2020 cuja pauta abordou o Auxílio Emergencial. A citada MP previa também o adiamento do início das regras de proteção de dados para maio de 2021, porém o art. 4 onde era estabelecido foi revogado pelo Senado por meio do Projeto de Lei de Conversão (PLV) 34/2020, prevendo a entrada em vigor conforme os termos da Lei, após o prazo para sanção presidencial de 15 dias úteis.

A Lei 14.058/2020 publicada no DOU, no dia 18 de setembro, sancionou o texto vindo do Senado, sem conter o conteúdo que previa



o adiamento da Lei Geral de Proteção de Dados. Sendo assim, passou a vigorar a LGPD no Brasil. A Lei trouxe regulamentou também o benefício emergencial para preservação de emprego e renda, outro assunto tratado na mesma medida provisória (959/2020).

A LGPD é uma lei que visa garantir direitos para cidadãos e consumidores sobre como ocorrerá o tratamento de dados pessoais; esta é uma legislação de interesse para todos os setores da economia pois padroniza o cuidado dessas informações.

Antes haviam regras que se aplicavam somente a algumas áreas, agora existe uma lei geral que reconhece que os dados pessoais devem ser protegidos.

Com a vigência da Lei 13.709/2018, alterada pela Lei 13.853/2019, é previsto que as empresas devem armazenar e processar os dados pessoais, além de tratar e proteger qualquer informação que possa identificar as pessoas.

A regulamentação exata vai depender da ANPD (Autoridade Nacional de Proteção de Dados), que deve orientar as empresas sobre as medidas técnicas de proteção, fiscalizar e editar normas previstas na LGPD sobre o tratamento de dados pessoais por pessoas físicas e jurídicas.

O Decreto 10.474/2020, de 26 de agosto, que aprovou a estrutura da Autoridade Nacional de Proteção de Dados, previu a sua entrada em vigor apenas na data de publicação da nomeação do Diretor-Presidente da ANPD, cuja autarquia é subordinada à Presidência da República.

Quando a empresa reconhecer que aconteceu algum problema, precisará solucioná-lo, entender sua dimensão e notificar a ANPD e as pessoas envolvidas, cabendo à autoridade nacional decidir se a empresa agiu corretamente após detectado o incidente de segurança.

Se a ANPD considerar que serão necessárias sanções, a lei estabelece alguns critérios e limites. A multa poderá alcançar até 2% do faturamento da empresa ou no máximo R\$ 50 milhões.

A LGPD está vigente, sendo que a aplicação das multas previstas pelo art. 52 iniciam apenas em 1º de agosto 2021, conforme estabelecido em alteração da Lei 14.010/20.

O dinheiro das multas será destinado ao Fundo de Defesa de Direitos Difusos (FDD), que financia projetos quem tenham como objetivo reparação de danos ao consumidor, meio ambiente, patrimônio e outros.

7

Documentos Asociados



Não aplicável

8

Glossário / Siglas e Definições



8.1 Siglas

ABRAMGE: Associação Brasileira de Planos de Saúde

ANPD: Autoridade Nacional de Proteção de Dados

IA: Inteligência Artificial

LGPD: Lei Geral de Proteção de Dados

8.2 Definições

Dado pessoal: informação relacionada à pessoa natural identificada ou identificável. Essa informação representa todo e qualquer dado que possa tornar uma pessoa identificável, seja ela diretamente relacionada ao seu titular (como um nome ou número de documento) ou mesmo indiretamente relacionada, mas com potencial de identificação (como endereço, idade, informações sobre hábitos de compra, etc).

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.

Dado anonimizado: dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais.

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

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.



Agentes de tratamento: o controlador e o operador.

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

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.

Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional de 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.

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 civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

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.

Autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta lei.

9

Revisões e Atualizações



Revisões e Atualizações

| Data | Atualização /Revisão | Elaborado por: |
|---------------|----------------------|--|
| Junho de 2020 | Elaboração Manual | Equipe Técnica Sistema Abramge/Sinamge/Sinog |
| Outubro 2020 | Atualização Manual | Equipe Técnica Sistema Abramge/Sinamge/Sinog |
| Abril 2021 | Atualização Manual | Equipe Técnica Sistema Abramge/Sinamge/Sinog |

10

Anexos



10.1 Referências Legais

Medida Provisória 869

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Mpv/mpv869.htm

RN 195 ANS

<https://www.ans.gov.br/component/legislacao/?view=legislacao&task=TextoLei&format=raw&id=MTQ1OA==>

Lei 12.527 Acesso à Informação

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm

Lei 12.737 Carolina Dieckman

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

Lei 12.965 Marco Civil

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

Lei 13.709 Proteção de Dados

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

Medida Provisória 959

http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Mpv/mpv959.htm



Lei 13.853/2019

http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13853.htm

Lei 14.010/2020

http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14010.htm

Lei 14.058/2020

<https://www2.camara.leg.br/legin/fed/lei/2020/lei-14058-17-setembro-2020-790639-norma-pl.html#:~:text=EMENTA%3A%20Estabelece%20a%20operacionaliza%C3%A7%C3%A3o%20do,6%20de%20julho%20de%202020>

Este manual é um documento dinâmico e objetiva a colaboração de todos os nossos associados.
As contribuições poderão ser enviadas para economia@abramge.com.br para análise e atualização.



abramge • sinamge • sinog

ABRAMGE - Associação Brasileira de Planos de Saúde

SINAMGE - Sindicato Nacional das Empresas de Medicina de Grupo

SINOG - Associação Brasileira de Planos Odontológicos

Rua Treze de Maio, 1540 - Bela Vista . São Paulo - SP

CEP: 01327-002 - TEL: 11 3289-7511 - imprensa@abramge.com.br

www.abramge.com.br | www.sinamge.com.br | www.sinog.com.br