

GUIA LGPD

Lei Geral de Proteção de Dados

Versão 1.0 - Outubro de 2021

SENAC BAHIA
www.ba.senac.br

Moralidade

Relacionamentos



Confiança



Responsabilidade



Princípios

SENAC - Serviço Nacional de Aprendizagem Comercial

ADMINISTRAÇÃO REGIONAL DA BAHIA

Presidente do Conselho Regional

Carlos de Souza Andrade

Diretora Regional do Senac Bahia - Marina Vianna Alves de Almeida

Dados Internacionais de Catalogação na Publicação (CIP)

G943 Guia da lei geral de proteção de dados (LGPD) [recurso eletrônico] /
Salvador, 2021.

32 p.: il.

Acesso em: <https://intranet.ba.senac.br/Login.pdf>

1. Direito à privacidade. 2. Guia. 3. Proteção de dados. 4. Segurança da Informação. I. SENAC. II. Título .

CDD 342.810858

Elaborada pela Bibliotecária Verônica Oliveira CRB-5/1864

Serviço Nacional de Aprendizagem Comercial

SENAC

Sumário

A Lei Geral de Proteção de Dados Pessoais (LGPD).....	3
O que é a LGPD?	4
Dados Pessoais	5
Papéis Envolvidos	6
Tratamento	7
Consentimento	9
Princípios da LGPD	14
Quando é aplicável?	16
Fases para adequação	17
Adequação à LGPD	18
Direito dos titulares dos dados	24
Bases legais.....	25
Quem fiscaliza.....	27
Sanções	28
Capítulos da Lei.....	29
Considerações finais	30
Referências.....	31

A Lei Geral de Proteção de Dados Pessoais (LGPD)

A **Lei Geral de Proteção de Dados Pessoais (LGPD)** representa um importante avanço para o Brasil pois estabelece diretrizes importantes e obrigatórias de como devem ser tratados os dados dos brasileiros no processo de coletas, armazenamentos, alterações, descartes e proteção, prevendo punições para descumprimento em casos de vazamentos ou outras irregularidades.

A LGPD foi inspirada na **General Data Protection Regulation (GDPR)**, que entrou em vigência em 2018 na União Europeia, fortalecendo a necessidade de leis equivalentes que protegessem dados pessoais no Brasil.

Em 14 de agosto de 2018, a **Lei Geral de Proteção de Dados do Brasil (LGPD)** - Lei 13.709/2018 - foi sancionada, mas entrou em vigor em setembro de 2020, traçada em princípios éticos como a transparência, a prestação de contas e a boa-fé. A Lei visa preservar o direito constitucional à liberdade e à privacidade que todos os indivíduos brasileiros têm, assim como protegê-los de danos causados por rupturas desses direitos.

O **SENAC BAHIA** vem adotando medidas para se adequar à lei, visando garantir a privacidade de dados dos indivíduos e mitigando os riscos do uso indevido de informações pessoais contidas em suas bases digitais ou físicas.

Este e-book tem como objetivo orientar o planejamento das ações de adequação no Senac para além do cumprimento da lei, conscientizando os colaboradores em relação aos cuidados com informações que circulam na Instituição.

DÚVIDAS SOBRE A LEI?

Site: www.senac.ba.br
(Aba – Compliance)



ONDE REGISTRAR?

- lgpd.ti@ba.senac.br
(público interno)
- dpo@ba.senac.br (público externo)



COMO ACESSAR MINHAS INFORMAÇÕES?

No site do Senac, por meio
do CPF e ou CNPJ.



O que é a LGPD?

LGPD segundo definição da lei

“Tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.”

www.planalto.gov.br



Dados Pessoais

Artigo 5º

Dado pessoal

Qualquer informação que possa levar à identificação de uma pessoa física (nome completo, número de CPF, endereço, filiação...).

Dado pessoal sensível

Assim considerado por haver a real possibilidade de mau uso para fins discriminatórios e prejudiciais ao indivíduo, como informações relativas à raça/etnia, religião, opinião política, sexualidade e dados genéticos ou biométricos (como a biometria facial ou o DNA de um indivíduo).



Dado anonimizado

Um dado pessoal ou dado pessoal sensível passa a ser um dado anonimizado quando deixa de ser diretamente relacionado a uma pessoa. Isso acontece, por exemplo, quando um conjunto de dados sensíveis (como a autodeclaração de raça dos colaboradores de uma empresa) torna-se estatística (a porcentagem de colaboradores que se identificam com cada raça).

Banco de dados

Seja digital, seja físico, um banco de dados é qualquer conjunto de dados pessoais.

Papéis Envolvidos

Artigo 5º

Titular

Indivíduo a quem os dados pessoais sendo tratados se referem. É o soberano de qualquer assunto relacionado ao tratamento dessas informações e tem capacidade de consentir, ou não, com o tratamento.

Controlador

Responsável pelas decisões relacionadas ao tratamento dos dados pessoais. Entre outros pontos, é o controlador quem decide que dados serão tratados, de que forma e com que fim. Ele também é o principal responsável em caso de quaisquer incidentes que envolvam dados pessoais.

Operador

Quem trata os dados em nome de outra entidade, ou seja, em nome do controlador. O operador deve sempre seguir estritamente as ordens do controlador em relação ao tratamento dos dados.

Encarregado

A LGPD prevê que operadores e controladores tenham um encarregado, pessoa responsável por intermediar a comunicação entre os titulares, o controlador e a Autoridade Nacional de Proteção de Dados.



Tratamento

Artigo 5º

Tratamento

Toda e qualquer ação realizada com os dados pessoais de um titular, desde a coleta e armazenamento até o compartilhamento e uso. O ciclo completo de um dado pessoal, portanto, começa na coleta e termina na exclusão ou anonimização.

Agentes de tratamento

Tanto o operador quanto o controlador são agentes de tratamento; a responsabilidade final é sempre do controlador, mas o operador também tem obrigações a cumprir e pode ser responsabilizado em alguns casos, como quando não seguir as instruções do controlador.

Bloqueio

Suspensão do tratamento de dados, que não isenta o operador e o controlador de precisarem proteger os dados pessoais e o banco de dados em que se encontram.

Órgão de pesquisa

Especificados no texto da LGPD porque tais órgãos têm regras diferenciadas para o tratamento de dados e pedido de consentimento.

Eliminação

Exclusão de dados pessoais.

Transferência internacional de dados

Quando os dados pessoais são transferidos para fora do Brasil. É preciso assegurar que os dados terão proteção de nível equivalente ao proporcionado pela LGPD.

Uso compartilhado de dados

Quando os dados pessoais não ficam limitados a um único ente (privado ou público). Órgãos públicos podem compartilhar dados na prática de suas obrigações legais, enquanto entes privados podem fazê-lo mediante devido consentimento do titular.

Relatório de impacto à proteção de dados pessoais

Se houver qualquer risco de que determinado tratamento de dados possa vir a causar danos ao titular, é dever do controlador manter esse relatório. Dessa forma, em caso de incidentes, é possível entender os perigos da situação e trabalhar para mitigá-los mais rapidamente. A manutenção do relatório também visa comprovar que o tratamento que gera esses riscos recebe os devidos cuidados para evitá-los.



Consentimento

Artigo 5º

O QUE É

De acordo com o Art. 5º, Inciso XII, da LGPD, **consentimento** é a “manifestação **livre, informada e inequívoca** pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”. É a permissão dada pelo titular para que determinado dado ou dados pessoais sejam tratados. Deve ser pedido de forma explícita, clara e transparente pelo operador ou controlador, e se referir a uso específico e limitado.

Livre

O titular não pode ser obrigado a dar o seu consentimento e este também não pode ser obtido de forma automática, como em caixas de textos já pré-selecionadas ou em casos em que a própria navegação na plataforma já pressupõe o aceite de todas as condições.

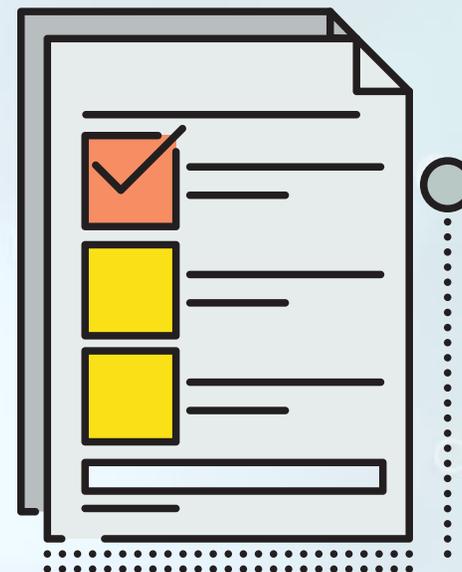
Informada

O titular deve compreender exatamente o que ele está consentindo, conhecer motivo e finalidade do termo antes de tomar qualquer decisão. Além disso, a informação deve ser passada de forma completa, transparente e simples.

Inequívoca

Não pode haver dúvidas sobre a verdadeira aceitação daquelas condições pelo titular e o “atendimento” deve se esforçar ao máximo para garantir a compreensão.

O ônus da prova de que o consentimento foi obtido em conformidade com a Lei é da Instituição e não do Titular.



O termo de consentimento para o uso dos dados pessoais nas bases sistêmicas da Instituição, assim como a sua solicitação, atenderá aos princípios de transparência, de forma clara e acessível, seguindo as diretrizes:

- **A finalidade** – para que a coleta dos dados será solicitada?
- **A utilização** – como serão manipulados os dados solicitados?
- **O tratamento** – como serão armazenados e descartados os dados coletados?

Com os esclarecimentos sobre o uso das informações pessoais, o **Titular** estará apto a aceitar o termo de consentimento e fornecer seus dados. Concederá permissão para que seus **DADOS (informações)** sejam utilizados pelo requisitante, autorizando seu uso para os fins especificados.

AGENTES ENVOLVIDOS NO CONSENTIMENTO

Titular

É a pessoa natural a quem se referem os dados que serão tratados (Art. 5º, Inciso V);

Controlador

É a “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais” (Art. 5º, Inciso VI);

Operador

É a “pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador” (Art. 5º, Inciso VII);

Atendente

É a “pessoa natural ou jurídica, de direito público ou privado, que realiza a coleta de dados pessoais em nome do controlador” (Art. 5º, Inciso VIII);

COMPREENSÃO QUANTO O USO DOS DADOS PESSOAIS SEGUNDO A LEI 13.709/2018.

Com a adequação à LGPD a Instituição terá que compreender a importância e o significado de consentimento e como ele pode impactar no fluxo dos procedimentos e processos que manipulam os dados pessoais de

Clientes, Alunos, Docentes, Colaboradores, Pais, Responsáveis e Fornecedores. As informações no termo de consentimento devem ser claras e apresentar os responsáveis por fornecê-las.

Para que os dados de uma pessoa possam ser tratados pela Instituição, é necessária a solicitação de consentimento para o Titular, observando o Art. 7º da LGPD - (Lei Geral de Proteção de Dados).

CONSENTIMENTO EM CASOS ESPECIAIS

A **Lei Geral de Proteção de Dados (LGPD)** exige que o consentimento seja obtido de forma específica e destacada. São eles:

- Dados pessoais sensíveis: o tratamento de dados pessoais sensíveis somente poderá ocorrer quando o titular ou seu responsável legal autorizar, de forma específica e destacada, para finalidades determinadas.
- Dados pessoais de crianças e de adolescentes: o consentimento deve ser específico e em destaque, fornecido por pelo menos um dos pais ou pelo responsável legal.
- Transferência internacional de dados pessoais: o consentimento, deve ser específico e em destaque, com informação prévia sobre o caráter internacional da operação, distinguindo claramente de outras finalidades.

TERMO DE USO - CONSENTIMENTO E POLÍTICA DE PRIVACIDADE.

É o documento que descreve como serão usadas as informações inseridas por usuários, como dados de cadastro, itens postados e mensagens armazenadas. Deve alertar, ainda, se as informações serão compartilhadas com outras Organizações parceiras ou

Modelo de Termo de Consentimento

Termo de Consentimento Senac Bahia

Prezado (a) *titular de dados pessoais*,

O presente Termo de Ciência e Consentimento ("Termo") tem como finalidade o registro da manifestação inequívoca, por meio do qual o *titular dos direitos pessoais* ("*Titular*") concorda com o tratamento de seus dados pelo Senac Bahia.

Assim, aceitando o presente Termo, o *Titular* consente e concorda que o Senac Bahia adote as melhores decisões para o tratamento das informações pessoais. Caso o Termo de Ciência não seja aceito, o titular não poderá prosseguir com a realização do Questionário de Assessment LGPD.

Ainda, o *Titular* declara neste ato que possui capacidade legal e detém as autorizações e permissões necessárias para realizar o presente cadastro e utilizar os serviços disponibilizados pelo Senac Bahia.

utilizadas em pesquisas.

Os contratos devem estar escritos em linguagem clara, precisa e, facilitar a compreensão do Cliente. As regras devem ser facilmente acessíveis.

As cláusulas que limitem direitos dos consumidores deverão ser esclarecidas e estarem acessíveis.

O importante é que o Titular tenha as opções de aceite ou recusa para dar prosseguimento à formalização do "atendimento". Em caso de quaisquer mudanças de conteúdo, os Titulares devem ser avisados para que, novamente, se manifestem sobre as novas regras.

QUANDO NÃO É PRECISO SOLICITAR O CONSENTIMENTO?

Segundo o Art. 8º da LGPD:

- Cumprimento de obrigação legal ou regulatória por parte do controlador;
- Tratamento e uso compartilhado de dados necessários para a execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, por parte da administração pública;
- Realização de estudos por órgão de pesquisa, garantida a anonimização dos dados pessoais, sempre que possível;
- Execução de contrato ou de procedimentos preliminares relacionados a contrato do qual o titular seja parte, a pedido do titular dos dados;
- Exercício regular de direitos em processo judicial, administrativo ou arbitral;
- Proteção da vida ou da integridade física do titular ou de terceiros;
- Tutela de saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- Atendimento aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e

De acordo com o Art. 8º,
"O consentimento poderá ser registrado pela Instituição por preenchimento de formulários, por e-mail, via sistema, entre outros."

liberdades fundamentais do titular que exigam a proteção dos dados pessoais;

- Proteção do crédito, inclusive quanto ao disposto na legislação pertinente;
- Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.



“Antes de COLETAR os dados, o titular precisa ser informado de maneira clara, objetiva e transparente sobre a razão da coleta das informações.

ARTIGO 6

Assim como a maior parte das leis, a LGPD prevê a boa-fé daqueles atingidos por ela. Isso é fundamental porque, quando falamos de certas regras da Lei — como a possibilidade de o titular solicitar a exclusão de seus dados ou um relatório completo de tratamentos —, nem sempre será possível fornecer provas absolutamente incontestáveis de que a Lei foi obedecida.

Isso também vale para o detalhamento quanto ao tratamento a ser feito, presente na solicitação do consentimento ao titular. Até que surjam evidências do contrário, o titular deve presumir que o controlador realmente está utilizando seus dados pessoais somente para os fins acordados. Caso apareçam evidências do contrário, aí sim, caberá à Autoridade Nacional de Proteção de Dados tomar as devidas providências punitivas.

REVOGAÇÃO DO CONSENTIMENTO E PORTABILIDADE DE DADOS

O parágrafo 5º do Art. 8º determina que o consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação.

O titular também tem direito à portabilidade dos dados, ou seja, pode transferir a outro fornecedor de serviço ou produto, mediante requisição expressa a qualquer momento.

A Instituição deverá disponibilizar um canal de atendimento que permitirá ao titular dos dados revogar o consentimento de maneira simples e gratuita, e solicitar os dados que forneceu. Como também, o acesso às informações que estão sob o controle dos seus dados.

Confiar

responsabilidade

Princípios

Princípios da LGPD



PARA O TRATAMENTO DE DADOS, O SENAC DEVERÁ SEMPRE OBSERVAR OS PRINCÍPIOS DA LEI:

1. DA FINALIDADE:

O Titular autoriza e concorda com o tratamento dos dados pelo Senac Bahia com a finalidade específica de armazenamento dos dados pessoais para oferta de serviços do seu portfólio.

2. DA ADEQUAÇÃO:

O Titular tem ciência de que o tratamento dos dados pessoais atende à finalidade exposta pelo provedor de serviços do Senac Bahia.

3. DA NECESSIDADE:

O Titular autoriza o tratamento dos dados pessoais com o objetivo de permitir comunicação referente aos serviços do Senac Bahia.

4. DO CADASTRO E DO LIVRE ACESSO:

Titular é de uso estritamente pessoal e não deverá ser utilizado por terceiros, sendo que a guarda e sigilo das informações contidas no formulário serão utilizadas de forma diligente, de modo a não os colocar à disposição de terceiros. O Titular tem ciência de que poderá consultar, atualizar ou excluir os dados pessoais cadastrados a qualquer tempo.

5. DA QUALIDADE E VERACIDADE DOS DADOS:

O Titular concorda em fornecer informações verdadeiras, exatas, e completas, responsabilizando-se pelo cadastro das informações que serão utilizadas pelo Senac Bahia, bem como por informar

qualquer modificação destas informações, mantendo as informações sempre atualizadas. Caso o Titular se utilize de informações falsas ou desatualizadas, o Senac Bahia se resguarda ao direito de cancelar e encerrar o acesso do usuário aos seus serviços.

6. DA TRANSPARÊNCIA:

Toda informação tratada pela empresa precisa ser de forma clara, precisa e verdadeira, além de facilmente acessível ao titular.

7. DA SEGURANÇA:

O Senac Bahia realizará o tratamento dos dados pessoais do Titular para a finalidade acima exposta, ficando esta responsável em adotar as medidas técnicas e administrativas aptas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

8. DA PREVENÇÃO:

O Senac Bahia adotará as medidas preventivas para a manutenção da proteção e segurança dos dados pessoais do Titular.

9. DA NÃO-DISCRIMINAÇÃO:

Os dados pessoais disponibilizados pelo Titular ao Senac Bahia, em hipótese alguma, serão utilizados para fins discriminatórios, ilícitos ou abusivos.

10. DA RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS:

O Titular poderá requisitar informações relacionadas ao nível de governança da TI pelo e-mail da Controladoria da Instituição dpo@ba.senac.br ou lgpd.ti@ba.senac.br.

Moralidade

Relacionamentos

Confiança

Responsabilidade

Princípios

Quando é aplicável?



APLICÁVEL

A Lei se aplica às pessoas **físicas e jurídicas de direito público e privado** que venham realizar qualquer tipo de tratamento de dados, bem como às pessoas físicas que tenham seus dados coletados por meio físico ou digital.



NÃO APLICÁVEL

A Lei não se aplica ao tratamento de dados realizado para fins **exclusivamente particulares e não econômicos**, para fins exclusivamente jornalísticos, artísticos, acadêmicos, de segurança pública, de defesa nacional, de segurança do Estado ou de atividade de investigação ou repressão de infrações penais, entre outras, conforme expressamente disposto no artigo 4º da lei 13.709/2018.

Fases para adequação



EQUIPES ENVOLVIDAS:

- Encarregado (DPO): Responsável pela mediação entre empresa, titulares e ANPD
- Comitê da LGPD: Órgão de deliberações.
- Equipe da TI: Responsáveis pela Segurança da Informação da Instituição.

Adequação à LGPD

1. CRIAÇÃO DE UM COMITÊ LGPD AO COMPLIANCE ORGANIZACIONAL.

O termo “compliance” diz respeito a “estar em conformidade com”. No âmbito organizacional é usado para garantir que os processos e procedimentos da organização estejam sempre de acordo com leis e obrigações. O comitê LGPD vai garantir que toda a organização - colaboradores, diretoria e parceiros - esteja de acordo com a lei 13.709/2018.

O compliance para a LGPD não deve ser um assunto somente de TI ou do Jurídico. A LGPD, diz respeito aos dados sensíveis de pessoas físicas e, na Instituição Senac muitas áreas lidam com esses dados. Por isso, é importante envolver todas as áreas, para entender em cada uma delas, como estão sendo tratados esses dados sensíveis, quem tem acesso a eles, como são armazenados, entre outros. O primeiro passo do guia de implementação da lei, é a criação de um comitê multidisciplinar, assim terá maiores condições de entender quais são os riscos reais que a Instituição pode estar exposta e como resolvê-los. Será este comitê responsável por levantar:

1. As questões legais;
2. Os requisitos técnicos;
3. As medidas e protocolos de segurança;
4. Investimentos em Hardware e Software;
5. Reformulação dos pedidos de cadastros;
6. Adoção de boas práticas
7. Contratação de serviços e profissionais de TI;
8. Conscientização da equipe interna.



A Lei Geral de Proteção de Dados não foi sancionada para penalizar e sim para assegurar ao indivíduo o controle sobre seus dados e o direito à privacidade!

Nomear um Responsável Geral pelo comitê de LGPD.

O membro responsável deverá acompanhar o andamento de todo o processo, desde o levantamento das informações, priorização e execução do plano de ação. Indica-se também a nomeação de um Responsável pela Execução, que irá acompanhar a execução do plano de ação elaborado. Além disso, pode convidar um representante de cada área, para acompanhar o processo e ser responsável por repassar as informações à sua área e, além disso irá contribuir com o processo de levantamento dos riscos e a manutenção da gestão.

2. LEVANTAMENTO DOS RISCOS.

Identificar os principais GAP's da Instituição e os Riscos identificados em cada processo, são essenciais para priorizar as ações de adequação à lei. A partir dessa ação será possível entender onde estão os principais pontos de atenção em relação à LGPD. O levantamento de riscos, deverá repassar por todos os setores da Instalação elencando detalhes sobre todos os dados sensíveis usados em cada atividade. Deve envolver um responsável por cada setor, onde ele deverá repassar por todas as atividades da sua área, levantando se são usados dados sensíveis e quais são, como são usados, armazenados e diversas outras informações.

Na etapa de levantamento de riscos, também será possível entender sobre terceiros, fornecedores, processos e contratos que podem estar sujeitos a riscos perante a LGPD.

2.1. Fornecedores

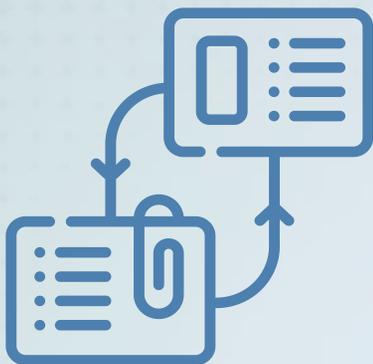
Avaliar com quais fornecedores estão sendo compartilhados dados pessoais e se eles também estão se adequando a lei. Além disso, quais as medidas estão sendo adotadas para proteção desses dados.

2.2. Infraestrutura

Avaliar as medidas de segurança e proteção dos dados que estão sendo usadas na Instituição e seu nível de eficiência. Entender onde os dados são armazenados e as práticas de segurança que estão sendo usadas, nas políticas e regramentos de senhas, firewall, antivírus, entre outros.



“Avaliar e ajustar todos os contratos com fornecedores, parceiros, clientes e colaboradores. Incluir nas cláusulas protetivas em relação a LGPD, sobre posse e tratativa dos dados sensíveis compartilhados.”



2.3. Revisão de processos

Reavaliar todos os processos em que existam dados pessoais. Nessa análise entenda o fluxo dos dados, desde o momento em que a Instituição passa a ter a posse dele até o momento de sua eliminação. Isso envolve atualização, compartilhamento, necessidade de uso, quem tem acesso, entre outras.

Recomenda elaborar um modelo de planilha onde vai encontrar um passo-a-passo descritivo para realizar o levantamento dos dados sensíveis na Instituição apenas para preenchimento, este guiará no levantamento de riscos em cada área.

3. ELABORAÇÃO DE UMA MATRIZ DE RISCO.

Após levantar os riscos, o próximo passo é fazer uma priorização quanto aos maiores impactos diagnosticados na Instituição e por isso deve ter preferência no Plano de Ação.

Os riscos identificados no passo anterior devem ser inseridos em uma matriz que vai estimar a probabilidade daquele risco acontecer e o impacto para o negócio. Para realizar essa priorização, deverá atribuir notas de 1 a 5 com associação ao nível de risco classificados como Extremo, Elevado, Moderado, Leve ou Baixo. Assim, conseguirá começar o plano de ação pelos riscos que mais irão afetar.

Além disso, é necessário criar também uma Planilha de Matriz de Riscos que irá ajudar nessa priorização.

4. ELABORAR PLANO DE AÇÃO.

Montar o Plano de Ação, observando os Riscos Extremos e de níveis Elevados que foram identificados na Matriz de Riscos. Deve-se fazer uma análise bem detalhada, pois caso algum risco não seja classificado como Extremo ou Elevado, mas tenha impacto grave sobre a Instituição, ele também deverá ser considerado no Plano de Ação. Nesse momento, o Responsável pela Execução do plano deverá entrar com as ações para acompanhar o processo que devem mitigar os riscos.

Além dos riscos priorizados, existem alguns “entregáveis” exigidos pela lei, portanto é importante que estejam no plano. Esses documentos são importantes tanto para guiar as ações internas da Instituição, quanto para prestação de contas junto à ANPD (Autoridade Nacional de Proteção de Dados), caso solicitado.

4.1. Mapa de dados Organizacional

Criar o Mapa de Dados que se trata de um documento sigiloso, apenas para uso interno. Ele deverá explicar quais são os dados utilizados pela Instituição, qual a finalidade e como são usados.

4.2. Política de privacidade

Elaborar uma Política de Privacidade institucional sobre como os dados são coletados, armazenados e tratados.

Na Política de Privacidade deve conter informações essenciais, como:

- informações sobre a Instituição responsável pelo tratamento dos dados pessoais e com as respectivas finalidades do tratamento;
- esclarecimento das bases jurídicas quanto ao tratamento;
- divulgação dos prazos de retenção dos dados pessoais;
- informações do contato do Data Protection Officer (DPO) ou encarregado de proteção de dados da organização.

4.3. DPO

Nomear um DPO, que será o guardião da compliance em relação à LGPD na Instituição. O DPO será o responsável por disseminar a cultura de proteção de dados na organização, além de criar normas e procedimentos adequados à lei. Algumas atividades relacionadas ao DPO:

Receber solicitações sobre o assunto;

Interagir com a autoridade nacional do assunto caso necessário;

Realizar treinamento sobre a LGPD internamente.



“Art. 17. 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.”

Confiar

Responsabilidade

Princípios

“A legislação se fundamenta nos valores como:

- O respeito à Privacidade;
- Autodeterminação Informativa;
- A liberdade de expressão, informação, comunicação e de opinião;
- A inviolabilidade da intimidade, da honra e da imagem;
- Ao desenvolvimento econômico, tecnológico e a inovação.”

4.4. Portal do Consentimento

Criar um “Portal de Consentimento”. No Portal, o público da Instituição poderá ter acesso aos seus dados, pedir revisões, exclusões, entre outros. Isso será necessário, visto que a palavra que resume a LGPD é “consentimento”. A Instituição pode reter qualquer dado sensível desde que tenha o consentimento ou alguma base legal que valide essa posse. Após o consentimento, o titular desses dados deve ter transparência indicando os dados retidos pela organização, se está atualizado e, também, deve ter direito de retirar esse consentimento.

5. TRABALHAR A CULTURA DA ORGANIZAÇÃO

A Privacidade deve-se tornar um assunto comum dentro da Instituição. Para isso, é importante que a conscientização dos Colaboradores sobre como a organização está lidando com o tema e como também compartilha as práticas que garantem a integridade dos dados.

Sugestões:

- a. Incluir o assunto no onboarding dos novos Colaboradores, ou seja, no treinamento e/ou integração dos funcionários recém-contratados;
- b. Criar um manual de boas práticas para segurança de dados ou incluir o assunto no código de conduta da Instituição, mas a ideia é disseminar quais são essas práticas, então use dos meios de comunicação direta com os colaboradores e garanta que eles irão acompanhar;



ATENÇÃO COM AS PUNIÇÕES

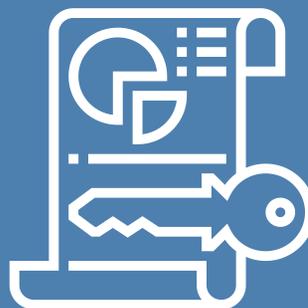
- Processos, sanções administrativas e advertências;
- Multas de até 2% do seu faturamento;
- Apreensão de dados;

c. Realizar treinamentos com a equipe sobre a LGPD e a política de privacidade da Instituição. Muitos colaboradores podem não saber do que se trata essa nova lei, então é importante que todos estejam cientes sobre a atuação e o seu papel para a adequação à lei;

d. Fazer campanhas de comunicação interna destacando os principais pontos da LGPD e da política da Instituição.

6. MANUTENÇÃO

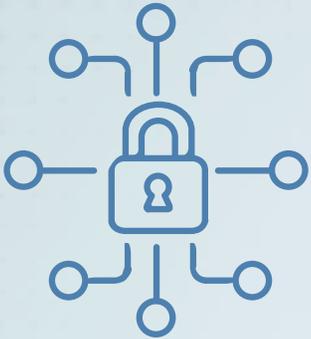
Após a implementação da LGPD, é essencial garantir a manutenção das boas práticas adotadas na organização. Para tal, o DPO será o elo forte na manutenção das políticas implantadas.



“Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição. ”

Responsabilidade

Princípios



DIREITO DOS TITULARES DOS DADOS

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

Bases Legais

BASES LEGAIS PARA TRATAMENTO DE DADOS PESSOAIS NA LGPD

O propósito da base legal é determinar as situações e condições para tratamento de dados pessoais e evitar a sua coleta e seu uso indiscriminado. As bases legais serão atribuídas a cada uma das atividades de tratamento de dados pessoais nas organizações. Por exemplo, na venda de um produto, a instituição coleta os dados pessoais para fazer atividades relacionadas à venda e entrega, como nome, endereço, contatos e cartão de crédito.

Tratamento de dados realizado no Brasil.

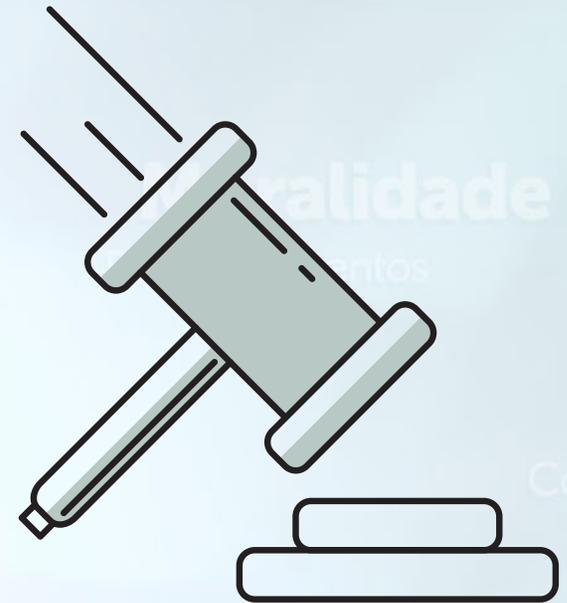
Tratamento de dados que tenha por objetivo a oferta ou fornecimento de bens e/ou serviços no Brasil.

Dados que tenham sido coletados no território nacional.

Dados pessoais são informações relativas a uma pessoa viva e compreendem dados pessoais (indivíduos identificados ou identificáveis)

Também constituem dados pessoais o conjunto de informações distintas que podem levar à identificação de uma determinada pessoa.

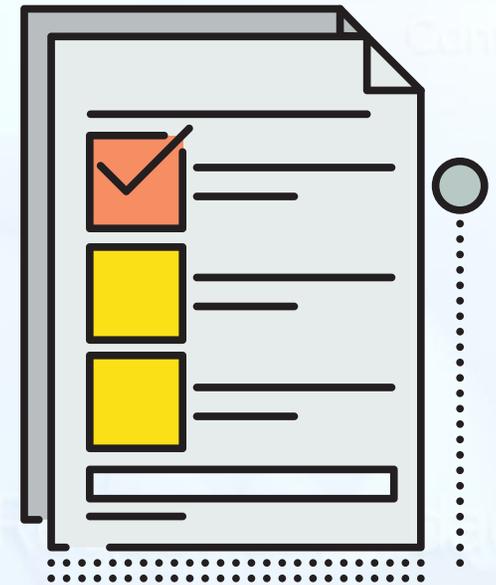
Todo dado pessoal só pode ser tratado se seguir um ou mais critérios definidos pela



LGPD, mas, dentro do conjunto de dados pessoais, há ainda aqueles que exigem um pouco mais de atenção: são aqueles “sobre crianças e adolescentes”; e aqueles “sensíveis”, dados sobre origem racial ou étnica, saúde, dados genéticos ou biométricos, convicção religiosa, orientação sexual e filiação a sindicatos ou organização filosófica ou política;

Os 12 principais Direitos Garantidos pela LGPD aos Titulares dos Dados Pessoais.

1. Acesso aos dados
2. Informação de dados pessoais compartilhados
3. Objeção ao Tratamento dos dados
4. Não Consentimento
5. Restrição do tratamento dos dados
6. Revogação do Consentimento
7. Revisão de decisão automatizada
8. Retificação
9. Portabilidade
10. Eliminação
11. Peticionar contra o Responsável
12. Inversão de ônus da prova



Quem fiscaliza



A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD), CRIADA PELA LEI Nº 13.853/2019, ATUARÁ COMO UMA AGÊNCIA REGULADORA.

Criada em 2018 e sancionada em 2019, a ANPD (Autoridade Nacional de Proteção de Dados) é o órgão federal responsável por fiscalizar e aplicar a LGPD, a Lei Geral da Proteção de Dados. A criação de uma autoridade independente é necessária para que empresas que têm acesso às informações pessoais cumpram a legislação e possam ser auditadas nos casos em que não observarem o devido tratamento destes dados, além disso, uma autoridade nacional poderá deliberar sobre questões que não ficaram tão claras ou que possam gerar algum tipo de questionamento quanto à sua interpretação.

Autoridade nacional: a Autoridade Nacional de Proteção de Dados (ANPD) será o órgão responsável por implementar e gerenciar as regras da LGPD, garantindo que a Lei seja cumprida. A ANPD também é responsável por realizar auditorias, assim como aplicar as devidas sanções em casos comprovados de descumprimento da Lei.

Moralidade
Relacionamentos

Confiança

Responsabilidade

Princípios

Sanções

Artigo 52º

1

ADVERTÊNCIA

Empresas poderão ser advertidas caso desobedeçam à Lei. As advertências exigirão planos de ação com prazo definido para adoção de medidas corretivas.

2

DIVULGAÇÃO

As empresas serão obrigadas a divulgar publicamente casos de vazamento de dados pessoais, para que os titulares e a sociedade saibam que os dados foram comprometidos.

3

MULTA

Em casos graves de descumprimento da Lei, serão aplicadas multas de até 2% do faturamento, limitadas a 50 milhões de reais por infração.

4

BLOQUEIO/ ELIMINAÇÃO

Em casos de solicitação por parte da ANPD devido a alguma infração, haverá a suspensão temporária do tratamento ou a eliminação de dados pessoais de determinado titular.

5

SUSPENSÃO PARCIAL OU TOTAL

Poderá haver a suspensão do Banco de Dados ou o exercício do tratamento de dados até que se desenvolva mecanismos de segurança eficientes.

O operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador. A Autoridade Nacional de Proteção de Dados (ANPD), criada pela Lei nº 13.853/2019, atuará como uma agência reguladora.

Capítulos da Lei

- 1 – Disposições Preliminares
- 2 – Do Tratamento dos Dados Pessoais
- 3 – Dos Direitos dos Titulares
- 4 – Do Tratamento de Dados Pessoais Pelo Poder Público
- 5 – Da Transferência Internacional de Dados
- 6 – Dos Agentes de Tratamento de Dados Pessoais
- 7 – Da Segurança e das Boas Práticas
- 8 – Da Fiscalização
- 9 – Da Autoridade Nacional de Proteção de Dados (ANPD e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade).
- 10 – Disposições Finais e Transitórias.

01	02	03	04	05	06	07	08
09	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	37	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64
65							

 **Artigos sem necessidade de ação**, apenas processo de informação na fiscalização.

 **Artigos focados em segmentos específicos** (transferência internacional, governos, crianças e adolescentes).

 **Artigos de caráter opcional ou sem obrigatoriedade.**

 **Artigos Obrigatórios**

Considerações finais

Neste material, você pode compreender melhor o que é a **Lei Geral de Proteção de Dados Pessoais**. A fim de prevenir a violação e o uso abusivo de dados, as novas regras exigem adequações operacionais e, para o **Senac**, é importante a sua aplicação, de forma clara e direta, de modo que as informações sejam aceitas e compreendidas pelos envolvidos.

A adequação à **LGPD** é uma preocupação de todas as áreas da Instituição e esse processo deve ser feito em três fases: levantamento, execução e monitoramento.

Esperamos que o conhecimento gerado neste e-book contribua para o desempenho de suas atividades.

Bom trabalho!

Referências

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 22 abr. 2021.

Escape das “armadilhas” da LGPD. Disponível em: <https://www.serpro.gov.br/lgpd/noticias/escape-armadilhas-lgpd-lei-geral-de-protecao-de-dados-pessoais>. Acesso em 15 mai.2021.

Lei Geral de Proteção de Dados Pessoais – LGPD. LEI Nº 13.709, de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em 03 mar.2021.

O que muda com a LGPD. Disponível em: <<https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd>>. Acesso em 14 mai.2021.

Termo de consentimento do uso de dados da LGPD. Disponível em: <<https://documentacao.senior.com.br/lgpd/manual-do-usuario/termo-de-consentimento.htm>>. Acesso em 16 mai.2021.

Moralidade

Relacionamentos

Confiança

Responsabilidade

Princípios

Moralidade

Relacionamentos

Confiança

Responsabilidade

Princípios

