# CARTILHA - LEI GERAL DE PROTEÇÃO DE DADOS

# LGPD

Rio PREFEITURA | RIOLUZ

# LGPD NA RIOLUZ

Esta cartilha tem como objetivo auxiliar os servidores e gestores da RIOLUZ em relação à aplicação da Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD). Os servidores deverão atentar para os cuidados que devem tomar quanto ao tratamento de dados pessoais durante a realização de trabalhos que envolvam a utilização dos mesmos como: na nomeação de servidores, na concessão de auxílios ao servidor, na fiscalização e administração de contratos, licenciamento e fiscalizações em geral entre outros, e os gestores em relação às medidas técnicas e administrativas necessárias para que esses dados permaneçam protegidos.

## *O que é a Lei de Proteção de Dados Pessoais (LGPD)?*

Em 14 de agosto de 2018 foi sancionada a Lei nº 13.709 conhecida como Lei Geral de Proteção de Dados (LGPD) que dispõe sobre o tratamento e proteção 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, privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A Lei Geral de Proteção de Dados sedimenta uma necessidade da sociedade atual de promover o uso ético, seguro e responsável dos dados pessoais por parte daqueles que os custodiam. Isso requer que os órgãos públicos implementem uma série de medidas para se adequarem ao disposto nesse novo contexto legal. A implementação dessas medidas deve acontecer de maneira estruturada e planejada, envolvendo todo o órgão público, promovendo uma verdadeira mudança na cultura organizacional.

## O que são dados pessoais e dados pessoais sensíveis?

O dado é considerado pessoal quando permite a identificação, de forma direta, ou indireta, da pessoa à qual o dado se refere, por exemplo: **nome; sobrenome; data de nascimento; CPF; RG; CNH; carteira de trabalho; passaporte; título de eleitor; e-mail, endereço residencial ou comercial; telefone; cookies; e endereço IP.**

Os dados pessoais sensíveis são aqueles dados que podem causar discriminação a uma pessoa, por isso merecem maior proteção, como **origem étnica ou raça, 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.**

A importância de se intercambiar dados pessoais e dados pessoais sensíveis de maneira segura reside na necessidade de impedir que tais dados sejam utilizados para fraudes diversas, divulgados sem autorização do titular, ou usados com intuito de discriminação ou perseguição política.

**Exemplo:**

**DADOS PESSOAIS**

- NOME
- ENDEREÇO
- TELEFONE
- CPF
- GEOLOCALIZAÇÃO
- HISTÓRICO DE INTERNET
- DADOS FINANCEIROS

**Exemplo:**

**DADOS PESSOAIS SENSÍVEIS**

- RAÇA OU ETNIA
- RELIGIÃO
- OPINIÃO POLÍTICA
- DADOS DE SAÚDE
- FILIAÇÃO SINDICAL
- DADOS BIOMÉTRICOS
- DADOS GENÉTICOS
- ORIENTAÇÃO SEXUAL

## O que é tratamento de dados pessoais?

Segundo a Lei, o tratamento de dados pessoais se refere a toda operação realizada com dados pessoais.

Considera-se "tratamento de dados" qualquer atividade que utilize um dado pessoal na execução da sua operação, como, por exemplo:

**coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.**

A Lei então dispõe que mesmo o simples acesso ou consulta a um dado pessoal configura tratamento de dados e, sendo assim, é necessário aplicar os ditames da Lei.

## Quem é o titular dos dados pessoais?

O titular dos dados pessoais é a pessoa natural a quem se referem os dados pessoais que são o objeto de tratamento.

## Quem são os agentes de tratamento?

No âmbito da LGPD, o tratamento dos dados pessoais pode ser realizado por dois agentes de tratamento, o controlador e o operador.

O controlador é definido pela Lei como a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

Na Administração Pública, o controlador será a pessoa jurídica do órgão ou entidade pública sujeita à Lei, representada pela autoridade imbuída de adotar as decisões acerca do tratamento de tais dados.

O operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, aí incluídos agentes públicos no sentido amplo que exerçam tal função, bem como pessoas jurídicas diversas

daquela representada pelo controlador, que exerçam atividade de tratamento no âmbito de contrato ou instrumento congênere.

Além deles, há a figura do Encarregado, que é a pessoa indicada pelo Controlador para atuar como canal de comunicação entre o Controlador, o Operador, os (as) titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Segundo a LGPD, as atividades do encarregado consistem em:

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

## O que é o Comitê de Proteção de Dados Pessoais?

É um grupo formado por servidores de todos os setores da RIOLUZ que tem como atribuições:

- Apoiar o trabalho do encarregado de dados na implantação do Programa de Privacidade e Proteção de Dados Pessoais da RIOLUZ;
- Auxiliar na elaboração dos instrumentos do Programa;
- Fornecer informações acerca dos tratamentos de dados pessoais realizados no âmbito da RIOLUZ;
- Tirar dúvidas e prestar esclarecimentos acerca das atividades realizadas pelas suas áreas e demais setores;
- Reavaliar, em conjunto com os responsáveis pelos sistemas, processos de negócio, serviços e políticas públicas, a efetiva necessidade dos tratamentos de dados pessoais realizados;
- Conscientizar e divulgar a LGPD, visando estimular a mudança de cultura necessária em razão da vigência da norma.

Da esq p/dir: Andrea Vycas, Flávia Meireles, Bárbara Lucariny, Ariel Cavalcanti, Ana Paula Vasconcellos, André Hissa, Carolina Veloso, Tamara Ridolph, Pedro Menezes, Teresa Vasconcellos, e Flávia Cohen.

## O que fazer quando eu tiver que tratar dados pessoais em algum trabalho na RIOLUZ?

Você pode se fazer os seguintes questionamentos: Eu tenho base legal ou regulatória (art. 7º – inciso I) para realizar o tratamento de dados pessoais? (princípio da finalidade)

Se sim, foi dada publicidade de que a RIOLUZ irá realizar tratamento de dados pessoais para as finalidades contidas na base legal? (princípio da transparência) Obs.: As bases legais de tratamento de dados pessoais estão contidas na Política ou Aviso de Privacidade divulgada no site da RIOLUZ . Se não foi dada a publicidade, entre em contato com o encarregado de dados para que ele providencie a atualização da Política ou Aviso de Privacidade, caso necessário.

Se não tiver base legal ou regulatória para realizar o tratamento dos dados pessoais em determinada atividade, o dado não poderá ser coletado. Porém, a lei ainda prevê que você pode tratar os dados pessoais mediante o consentimento do titular (artigo 7º inciso I). Para isso, deverá solicitá-lo formalmente conforme modelo disponibilizado no site lgpd.prefeitura.rio. O consentimento deverá ser arquivado pelo setor que o solicitou.

## Você sabe a diferença entre Aviso e Política de Privacidade?

A principal diferença entre o aviso de privacidade e a política de privacidade é que o aviso é destinado ao público externo, enquanto a política é um documento interno, destinado aos funcionários.

## Tratamento de dados pela Administração Pública

A LGPD prevê nos artigos 6, 7, 9, 11 e 26 que Administração Púbica tem a prerrogativa de tratar dados sem o consentimento do

titular, desde que seja para a execução de políticas públicas, devidamente estabelecida em lei ou para o cumprimento de obrigação legal ou regulatória pelo controlador.

De acordo com o Art. 6º, incisos, I, III, e X: O tratamento de dados deve possuir "propósitos legítimos, específicos, explícitos e informados ao titular", deve ser "limitado ao mínimo necessário para a realização das suas finalidades" e a AP deve "demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais".

Além disso, o titular tem direito ao acesso facilitado às informações sobre o tratamento dos seus dados, que devem ser disponibilizadas de forma clara, adequada e ostensiva, como prevê o Art 9º.

No entanto, após identificar que você pode realizar o tratamento de dados pessoais, de acordo com uma das hipóteses legais previstas no artigo 7º da LGPD, você também deverá se fazer os seguintes questionamentos:

- **Os dados coletados estão adequados para a finalidade para as quais eles serão tratados? (princípio da adequação) , ou seja, o dado coletado em uma determinada atividade é realmente necessário para àquela finalidade. Se não, devemos deixar de coletá-lo.**

- **Eu posso minimizar o uso de dados ao mínimo possível para executar minha atribuição? (princípio da necessidade)**

Além dos princípios da finalidade, adequação, transparência e necessidade, as atividades de tratamento de dados pessoais observam a boa fé e aos seguintes princípios norteadores previstos no artigo 6º da LGPD: livre acesso, qualidade dos dados, segurança, prevenção, não discriminação e responsabilização.

Em relação à segurança dos dados, você deve adotar, no mínimo, as ações previstas nesta cartilha.

## Medidas de segurança no âmbito da LGPD

Nesse momento de transformação digital no qual o Brasil se situa, a oferta de produtos, serviços e informações de governo por meio digital deve vir acompanhada do respectivo desenvolvimento e implementação de medidas de segurança capazes de assegurar a adequada proteção dos dados pessoais que são necessariamente tratados pelos produtos ou serviços ofertados, garantindo assim direitos constitucionais como a privacidade, intimidade e a inviolabilidade da honra e da imagem das pessoas. O conceito de segurança apresentado pela LGPD é pilar fundamental para o entendimento das ações que visam à definição das medidas técnicas e administrativas com a finalidade de proteger os dados pessoais.

O art. 46, VII da LGPD (Lei nº 13.709/2018) define segurança como: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Na RIOLUZ, a aplicação deste artigo é materializado através da Política de Controle de Acessos da Rioluz: Portaria "P" RIOLUZ nº 278 de 04/09/2023 e da realização do gerenciamento dos riscos que geram impacto potencial sobre o titular dos dados pessoais, independentemente de sua natureza, utilizando as informações contidas no inventário de dados que sustentarão a elaboração do RIPD – Relatório de Impacto à Proteção de Dados Pessoais da Rioluz.

## Quais os direitos do titular dos dados?

A Lei Geral de Proteção de Dados (LGPD) garante uma série de direitos aos titulares de dados, que são as pessoas naturais cujos dados são coletados por empresas e organizações. Entre esses direitos, estão:

- Confirmar se os dados estão sendo usados
- Acessar os dados
- Corrigir os dados
- Excluir dados desnecessários
- Bloquear os dados
- Portabilidade dos dados
- Revogação do consentimento
- Informações sobre o compartilhamento de dados
- Informação sobre a possibilidade de não fornecer consentimento
- Anonimização


## Como o titular dos dados pode solicitar seus direitos junto à RIOLUZ?

O Titular de dados poderá entrar em contato por meio dos canais da Central 1746 escolhendo a opção Proteção de Dados ou através do formulário de solicitação do titular de dados disponível no site da Rioluz.

# Quem é responsável por manter os dados protegidos?

O artigo 47 da LGPD determina que o agente de tratamento (controlador ou operador) obriga-se a garantir a segurança dos dados pessoais, mesmo após o seu término.

**O que você deve fazer em caso de um incidente de segurança? Deverá comunicar ao encarregado de dados imediatamente dando todas as informações necessárias em relação ao tratamento inadequado ou ilícito, como data, hora, local, titulares envolvidos, situação.**

ANPD Autoridade Nacional de Proteção de Dados

A ANPD recomenda que sejam aplicadas algumas medidas técnicas dentro da empresa para que a proteção dos dados sejam realizadas, são algumas delas:

- **Controle de acesso**
- **Gerenciamento por senhas**
- **Não permitir o compartilhamento de contas e senhas de funcionários e colaboradores**
- **Utilizar a autenticação multi-fatores**
- **Ter configurações de segurança no local de trabalho de cada colaborador ou empregado**
- **Evitar transferência de dados para outros dispositivos se não os da empresa**
- **Realização de backups regulares**
- **Manter antivírus e sistemas de firewall atualizados e operantes**

# *Seguem algumas dicas práticas para proteger os dados pessoais dentro da RIOLUZ:*

Guardar os dados pessoais com os quais lida em local seguro;

Manter a mesa limpa, sem dados pessoais a mostra;

Picotar dados pessoais quando estes não forem mais necessários;

Não esquecer impressões com dados pessoais na impressora;

Bloquear o computador ao sair de perto da sua estação de trabalho;

Anonimizar dados pessoais em documentos quando os mesmos precisarem ser enviados para terceiros;

Não compartilhar dados pessoais sem que haja base legal prevista para isso;

Utilizar os recursos de proteção que existem nos sistemas como por exemplo, no sistema processo.rio limitando o acesso à lotação ou à pessoa quando o documento possuir dados pessoais e não houver base legal que permita a sua divulgação;

Manter sigilo sobre dados pessoais de cidadãos, servidores, fornecedores, etc, principalmente no que concerne aos dados pessoais sensíveis;

Fazer cursos voltados à privacidade e segurança da informação;

Criar senhas fortes e de preferência únicas para todos os seus sites e aplicativos;

Não compartilhar senhas de acesso; Criptografar HDs e pendrives que contenham dados pessoais;

Evite colocar na nuvem arquivos contendo dados confidenciais ou que considere privados;

Se for necessário, salvar informações na máquina, faça backup regularmente, e criptografe os dados;

Desconfie de links enviados via mensagens eletrônicas, mesmo quando vindo de pessoas conhecidas;

Mantenha seus softwares e aplicativos atualizados; e

Use um serviço de autenticação de dois fatores (2FA) sempre que possível.

# Como proteger dados pessoais em documentos

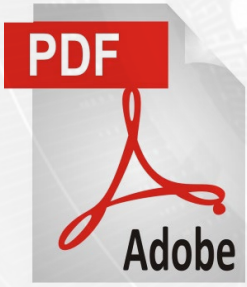
## O que é anonimização e pseudoanonimização?

A anonimização é um processo em que se utiliza 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. Você pode anonimizar dados pessoais fazendo a supressão ou encobrimento de caracteres ou generalização.

Na supressão, por exemplo, você encaminha os dados de uma planilha excluindo as colunas em que se encontram dados pessoais. Na generalização, os dados sãosubstituídos por categorias mais amplas e genéricas. Por exemplo, idades são transformadas em faixas etárias e um CEP é trocado apenas pela cidade ou região do país.

No encobrimento de dados você pode encobrir parcialmente ou totalmente um dado pessoal. Exemplo: CPF nº 023.XXX.448-XX.

A pseudo-anonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.




## Como posso anonimizar dados pessoais?

Caso você não possua o software Adobe Acrobat que já possui a função de anonimização de forma nativa, você poderá anonimizar o arquivo em PDF usando o próprio Adobe Reader. Para isso deverá seguir os seguintes passos:

**1 ABRIR**

Abra o PDF que deseja anonimizar no Adobe Reader

**2 REALÇAR**

Escolha na barra de ferramenta que fica no lado esquerdo da tela, a ferramenta "Realçar texto selecionado" e depois a opção "destaque";

**3 SELECIONAR**

Selecione o trecho que deseja ocultar;

**4 COR**

Se o trecho não ficar ocultado,escolha na barrade ferramenta, a opção "Cor", escolha a cor preta e aumente a opacidade para 100%;

**5 MENU**

Vá até o "Menu" no lado superior esquerdo;

**6 ESCOLHER**

Escolha a impressora Microsoft Print to PDF;

**7 AJUSTAR**

Escolha, na opção "Formulários e Comentários", a opção "Documento e Marcações";

**8 MARCAR**

Na opção "avançado", marque a opção "imprimir como imagem";

**9 IMPRIMIR**

Escolha a opção "imprimir".

**10 COMPLETO**

Pronto, você terá um arquivo PDF com o texto ocultado.

## Como proteger os dados pessoais no Processo.Rio?

Ao criar o expediente ou processo, você poderá classificá-lo com um dos seguintes níveis de acesso:

- Público;
- Limitado ao órgão;
- Limitado de pessoa para lotação;
- Limitado de lotação para pessoa;
- Limitado entre lotações;
- Limitado entre pessoas.

A escolha do nível de acesso dependerá do nível de sensibilidade e de utilização dos dados pessoais tratados. Lembrando sempre que você deve ter base legal para realizar o tratamento do dado bem como o destinatário do expediente/processo.


## O que fazer quando souber que houve um vazamento de dados pessoais?

O vazamento de dados ocorre quando os dados pessoais são indevidamente acessados, coletados e divulgados na internet, ou compartilhados com terceiros. O vazamento de dados pessoais como CPF, e-mail e endereço, por exemplo, pode trazer graves consequências para a vítima.

É comum os criminosos utilizarem esses dados pessoais para realizar fraudes e golpes, como a contratação de empréstimos, serviços e, até mesmo, a realização de compras em nome da vítima. Há casos em que tentam inclusive fazer extorsão, solicitando dinheiro para não usarem ou publicarem os dados roubados.

Em caso de identificar que algum dado pessoal foi vazado, informe ao encarregado de dados da RIOLUZ, no email: **tamara.ridolph@prefeitura.rio**. O encarregado irá comunicar à autoridade nacional e

ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

## *Quais são as penalidades caso haja vazamento?*

Os agentes de tratamento de dados (controlador e operador), em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

1. advertência, com indicação de prazo para adoção de medidas corretivas;
2. multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
3. multa diária, observado o limite total a que se refere o inciso anterior;
4. publicização da infração após devidamente apurada e confirmada a sua ocorrência; bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
5. bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
6. eliminação dos dados pessoais a que se refere a infração;
7. 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;
8. 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;
9. proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

## *O que a RIOLUZ tem feito para proteger os dados pessoais que ela custodia?*

Para acompanhar as ações do Programa de Privacidade e Proteção de Dados Pessoais consulte: https://rioluz.prefeitura.rio/lei-geral-de-protecao-de-dados/.

## Obrigado!

Comitê de Privacidade e Proteção de Dados da Rioluz