

Cartilha de **Boas Práticas**

Lei Geral de Proteção de Dados (LGPD)



 **fapdf**

FUNDAÇÃO DE APOIO À PESQUISA DO DISTRITO FEDERAL

APRESENTAÇÃO

Esta Cartilha possui orientações aplicáveis a situações rotineiras do ambiente de trabalho dos servidores, procurando difundir o adequado tratamento de dados pessoais, destacando-se:



- A geração de documentos no SEI;
- Disponibilização de processos e documentos para o público externo;
- Relação da **LAI** e **LGPD**;
- Exemplos de anonimização;
- Uso de estações de trabalho, impressoras e ferramentas oficiais do governo do estado;
- Cuidado com o descarte de documentos.

LGPD NA FAPDF: O QUE VOCÊ PRECISA SABER!

A Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018) garante a privacidade e a segurança no tratamento de informações, equilibrando transparência e proteção de dados.



Direito à Proteção dos Dados Pessoais



Com a Emenda Constitucional nº 115/2022, o direito à proteção dos dados pessoais passou a ser um Direito Fundamental (art. 5º, LXXIX). Os Direitos Fundamentais são aqueles que proporcionam o mínimo necessário para que o indivíduo exista de forma digna em uma sociedade.



Processos Administrativos e Dados Pessoais



Os processos administrativos são, em regra, públicos. Mas e quando há dados pessoais? A publicidade dos processos garante transparência e controle social, mas quando um documento contém dados pessoais ou sensíveis (como CPF, RG, endereço residencial, dados bancários, informações médicas), a proteção deve ser priorizada conforme a LGPD!



No SEI

Marque documentos com dados pessoais ou sensíveis como "RESTRITO" e justifique: ("Informação Pessoal art. 33 §1º, Lei 4990/2012 e art. 23 Lei 13.709/2018"). Isso se aplica a processos contendo documentos como: RG, CPF, comprovante de residência, telefone pessoal)



No site da FAPDF

Antes de publicar documentos, anonimize as informações utilizando exclusivamente o PDF24 Tools. Siga o passo a passo:

- 1) Abra o arquivo no PDF24 Tools;
- 2) Selecione a ferramenta de redação;
- 3) Cubra completamente os dados pessoais com retângulos pretos;
- 4) Salve o documento verificando se os dados estão realmente ilegíveis.



No envio de e-mails

Se for encaminhar e-mails para mais de um destinatário e o conteúdo contiver dados pessoais ou sensíveis, utilize a cópia oculta (CCO) para proteger as informações. Por exemplo: ao enviar resultados de seleção ou documentos com dados pessoais para múltiplos pesquisadores. Além disso, adote a padronização dos emails institucionais conforme a orientação da Ascom, incluindo assinatura padrão com nome, cargo e setor.

Direitos do Titular



A LGPD cria diversos direitos para o titular de dados pessoais, tais como:

- Confirmação de existência de tratamento;
- Acesso aos dados;
- Correção de dados incompletos, inexatos ou desatualizados;
- Revogação do consentimento

O tratamento dos dados pessoais deve levar em conta os seguintes princípios:

finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas

Você, servidor público, também possui esses direitos!

Seja cauteloso com os dados pessoais que você está tratando!

A **LGPD** traz diretrizes sobre o adequado tratamento de **dados pessoais**.

you, como **servidor público** precisa estar atento às **boas práticas** quanto ao tratamento de

tais **dados**, sejam **aqueles** pertencentes a **usuários do serviço público** ou até mesmo **seus próprios**.



O tratamento inadequado de **dados pessoais** pode acarretar em **sanções administrativas, civis e penais**, inclusive na **responsabilização de agentes públicos**.



Pareceres Ad Hoc e Anonimização



E os pareceres Ad Hoc? Devem ser anonimizados? Não! A anonimização é irreversível, ou seja, uma vez removidos os dados do parecerista, não há como recuperá-los. Para garantir transparência, rastreabilidade e auditoria, os dados do avaliador devem ser mantidos acessíveis para fins de prestação de contas e verificação da competência técnica.

O parecer Ad Hoc contém diversos dados pessoais que precisam de proteção especial:

CPF e RG do parecerista

Por isso, ao inserir pareceres Ad Hoc no SEI, siga estas orientações:

- Classifique o documento como "RESTRITO"
- Inclua a justificativa legal: "Informação Pessoal art. 33 §1º, Lei 4990/2012 e art. 23 Lei 13.709/2018"
- Mantenha registro do parecerista no processo para fins de auditoria
- é importante lembrar que, embora o SEI seja um sistema que facilite e registre a tramitação de documentos, a responsabilidade pelo tratamento dos dados e pela garantia de sigilo continua sendo das pessoas e das instituições que manuseiam tais documentos. Cada etapa deve ser cercada de cuidado e observância das normas para garantir o devido sigilo e evitar sanções legais.

A manutenção dos dados do parecerista é fundamental para garantir a legitimidade do processo de avaliação e permitir eventuais verificações pelos órgãos de controle.

Exemplos de Dados Pessoais e Dados Sensíveis

São exemplos de dados pessoais:

- Número de documentos de identificação pessoal (RG, CPF, título de eleitor, matrícula etc.);
- Endereços residenciais;
- Telefones residenciais;
- Telefones celulares pessoais;
- Carteira funcional;
- Passaportes;
- Estado civil;
- Data de nascimento;
- E-mail pessoais



São exemplos de dados sensíveis:

- Informações médicas;
- Origem social, racial ou étnica;
- Filiação sindical ou a organização de caráter religioso, filosófico ou político;
- Dados biométricos (imagem, digitais etc.).

Boas práticas para tratar dados pessoais no SEI!

Na geração de documentos no SEI, atente-se ao **princípio da necessidade**, ou seja, colete ou insira somente os dados pessoais estritamente necessários para o alcance de sua **finalidade**.

Na geração de **documentos públicos** (portarias, designações, e-mails etc.), **atente-se à aplicação de tarjas e/ou descaracterização** dos dados pessoais para evitar exposições desnecessárias, exceto se houver **previsão legal** quanto à **publicidade/exposição** de tais dados.



CPF: 000.000.000-00 **x**

CPF: *****.000.000-**** ✓

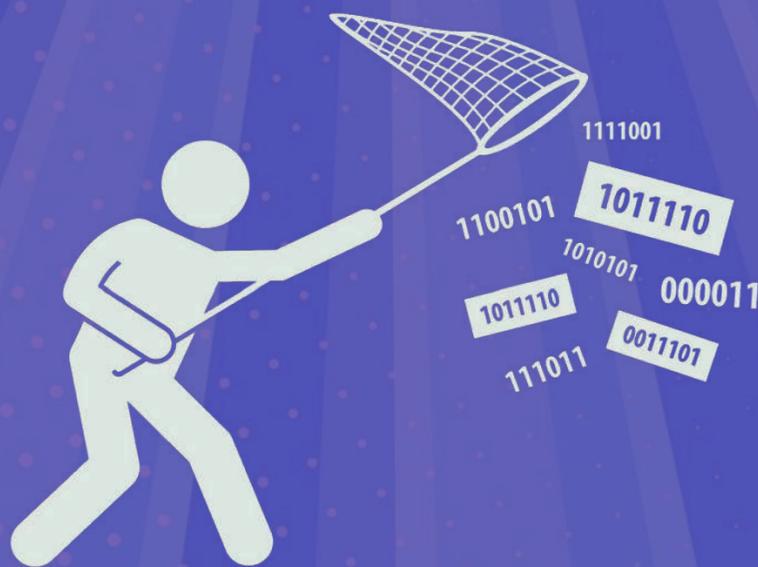
Matrícula: 000000000 **x**

Matrícula: *******000** ✓

Boas práticas para tratar dados pessoais no SEI!

Na geração de processos ou documentos, atente-se à adequada configuração do nível de acesso (público, restrito ou sigiloso). Quando houver o tratamento de dados ou informações pessoais o nível de acesso deve ser restrito sob a hipótese legal de "Informação Pessoal (Art. 31 da Lei nº 12.527/2011)".

Quando for necessário disponibilizar processos ou documentos a usuários externos, recomenda-se que o servidor analise-os previamente, procedendo com a **descaracterização dos dados pessoais existentes**, promovendo o equilíbrio entre a transparência e a proteção dos dados pessoais.



LAI e LGPD

Conhecida como Lei de Acesso à Informação (**LAI**), Lei Federal nº 12.527/2011. A LAI entrou em vigor em maio de 2012 e criou mecanismos que possibilitam a qualquer pessoa, física ou jurídica, sem necessidade de justificativa, o acesso a informações produzidas e custodiadas pelos órgãos e entidades da Administração Pública.

A **LAI** e a **LGPD** são leis sistematicamente compatíveis entre si. Essas duas normas harmonizam os direitos fundamentais de acesso à informação e da proteção de dados pessoais, não havendo oposição entre seus dispositivos.



As decisões que tratam da publicidade de dados de pessoas naturais, relativas a pedidos de informação e respectivo recursos, devem ser fundamentadas nos arts. 3º e 31 da **LAI**, considerando ser mais específica.

(Enunciado CGU nº 4, de 10 de março de 2022)

Boas práticas ao usar os computadores



Ao se ausentar da sua mesa, lembre-se de sempre **bloquear** (☞ + L) sua estação de trabalho. Desta forma você evitará que pessoas não autorizadas visualizem informações restritas, sigilosas ou confidenciais na tela de seu computador.



Evite tirar prints, fotos ou gravar vídeos da tela do computador que contenha algum **dado pessoal à mostra** e encaminhá-los por meio de canais de comunicação não oficiais. Esses dados pessoais são de sua **responsabilidade**.



Boas práticas ao usar a impressora



Ao **imprimir** documentos que contenham **dados pessoais**, lembre-se de **retirá-los** da impressora o mais breve possível. Quando for necessário descartar tais documentos, atente-se em **descaracterizar os dados pessoais**, procedendo, por exemplo, com a fragmentação (trituração) do documento.



Documentos **impressos** contendo **dados pessoais** devem ser **armazenados** em **locais seguros**. Quando deixá-los em sua mesa, por algum instante, lembre-se de **ocultar as informações** de maneira que não seja possível **identificá-las**, virando o anverso das folhas para baixo, por exemplo.



CONTATOS

AUTORIDADE DE MONITORAMENTO

Autoridade: Ivone S. Pita Dezaneti

E-mail projure@fap.df.gov.br

(61) 3462-8841

CHEFE DA UNIDADE DE GOVERNANÇA E GESTÃO (UGG)

Ana Paula Aragão

ugg@fap.df.gov.br

(61) 3462-8853

