🔐 Manual de Boas Práticas no Tratamento de Dados Pessoais

Universidade Federal do Triângulo Mineiro (UFTM)

📜 Base normativa

Com o objetivo de fortalecer a cultura de proteção de dados pessoais e garantir o cumprimento da legislação vigente, este manual apresenta orientações sobre o tratamento de dados no âmbito da UFTM, conforme:

- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);
- Lei nº 12.527/2011 – Lei de Acesso à Informação (LAI);
- Portaria Reitoria/UFTM nº 191/2024 - Dispõe sobre o tratamento de dados pessoais no âmbito da Universidade Federal do Triângulo Mineiro;
- Enunciado CGU nº 4/2022 – Equilíbrio entre transparência e proteção de dados pessoais.

🌟 Apresentação

Este manual tem como finalidade orientar servidores, gestores e demais agentes públicos da UFTM quanto às boas práticas no tratamento de dados pessoais.

📌 A proteção de dados pessoais deve caminhar junto com a transparência pública.

👥 Papel do Gestor de Dados Pessoais (Ponto Focal)

O Gestor de Dados Pessoais é o servidor designado em cada grande área ou unidade da UFTM, responsável por:

- Acompanhar o tratamento de dados pessoais realizado no âmbito da unidade;
- Promover a conformidade com a LGPD nas atividades sob sua responsabilidade;

- Orientar colegas e gestores locais sobre boas práticas de proteção de dados;
- Atuar como interlocutor entre a unidade e o Encarregado de Dados Pessoais.

🧩 Atores do tratamento de dados

- **Controlador:** a UFTM, representada pelo(a) Reitor(a), responsável pelas decisões sobre o tratamento de dados pessoais, incluindo definição de finalidades e meios de tratamento;
- **Operadores:** pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados em nome do controlador, seguindo suas instruções;
- **Encarregado de Dados Pessoais:** servidor designado pela Reitoria para atuar como canal de comunicação com os titulares dos dados e com a Autoridade Nacional de Proteção de Dados (ANPD);
- **Gestores de Dados Pessoais:** pontos focais de apoio à conformidade, conforme designação na Portaria nº 191/2024;
- **Administradores de dados pessoais:** todos os servidores, terceirizados ou unidades que, de alguma forma, realizam operações com dados pessoais (coleta, produção, armazenamento, acesso, compartilhamento, exclusão ou qualquer outra forma de tratamento). Todos são responsáveis por aplicar as boas práticas de proteção de dados e cumprir as normas da LGPD e da Portaria nº 191/2024.

🗂️ Tratamento de dados no SEI

Os processos eletrônicos frequentemente contêm informações pessoais de servidores, discentes, candidatos, pacientes, terceirizados e demais usuários. Para garantir o equilíbrio entre **transparência e proteção de dados**, orienta-se:

- **Princípio da necessidade e minimização de dados:** Inclua **apenas os dados estritamente necessários** à finalidade do processo. Evite expor nomes, CPFs, endereços, telefones e e-mails pessoais quando não forem indispensáveis;
- **Restrição de acesso:** Quando um documento contiver dados pessoais, dados pessoais sensíveis ou informações protegidas, o acesso deve ser **restrito no SEI** (classificação “restrito – dados pessoais”). Ressalta-se que restringir não significa ocultar indevidamente — trata-se de **proteger o dado, não o ato administrativo**;
- **Versão pública com tarjamento:** Para garantir a transparência, deve ser **gerada uma versão pública em PDF**, com **tarjamentos sobre os dados pessoais**. Essa versão deve ser anexada ao processo SEI, permitindo a publicidade do conteúdo institucional sem expor dados protegidos;

- **Responsabilidade compartilhada:** Todos os administradores de dados pessoais (servidores, gestores, terceirizados) têm **responsabilidade legal** pela confidencialidade e segurança dos dados que manipulam.

⚖️ Transparência e Proteção de Dados Pessoais

A **transparência é a regra**, mas deve sempre respeitar os limites da **proteção da intimidade, da vida privada, da honra e da imagem das pessoas**, conforme o art. 31 da LAI e os arts. 6º e 7º da LGPD.

Assim, documentos administrativos devem ser públicos **sempre que possível**, e restritos **apenas quando necessário** à proteção de dados pessoais.

✅ Boas práticas

- Verifique antes de publicar ou tramitar documentos se contêm dados pessoais desnecessários;
- Use identificadores institucionais (ex.: número de matrícula, SIAPE) em vez de CPFs;
- Evite expor contatos pessoais de usuários (telefone, endereço, e-mail particular); Mantenha sigilo sobre informações sensíveis, inclusive em comunicações internas;
- Em caso de dúvida, consulte o(a) Encarregado de Dados Pessoais.

🛠️ Ferramentas de tarjamento

Para operacionalizar a proteção de dados pessoais em documentos públicos, duas ferramentas são recomendadas:

📘 Fala.BR

- Permite ocultar (tarjar) dados pessoais em arquivos PDF antes de disponibilizá-los ao público; identifica automaticamente CPFs, RGs, endereços, e-mails, telefones e dados bancários.
- 📘 Manual oficial: Manual de Tarjamento Fala.BR – CGU (PDF)
- 🌐 Plataforma: https://falabr.cgu.gov.br
- 📰 Notícia: Ferramenta fortalece transparência e proteção de dados

Recomendações:

- Gere o documento em PDF e utilize a ferramenta antes de inseri-lo como público no SEI;
- Revise manualmente as marcações antes de concluir;
- Mantenha a versão íntegra restrita e a versão tarjada pública.

💻 Extensão SEI PRO

- Permite aplicar **tarjas pretas e marcas de sigilo diretamente no editor do SEI**;
- 📄 Tutorial: Briefing – Tarjamento no SEI PRO (CGU)
- 💻 Instalação: Chrome Web Store – SEI PRO
- 🌐 Site oficial: https://sei-pro.github.io/

Recomendações:

- Marque trechos sensíveis antes de salvar;
- Gere duas versões: **restrita** (original) e **pública** (tarjada);
- Revise cuidadosamente, pois o tarjamento é irreversível.

🎯 Mensagem final

Proteger dados pessoais é proteger pessoas.

A responsabilidade é coletiva, e o compromisso com a **transparência e a privacidade** reforça a confiança da sociedade na UFTM.

Essas orientações devem ser compartilhadas com os gestores e agentes de tratamento de dados pessoais de suas grandes áreas.