Ministério do Desenvolvimento Agrário e Agricultura Familiar

Subcomitê Técnico de Privacidade e Proteção de Dados Pessoais

LGPD NO MDA

Jogo Rápido

Boas práticas para instrução processual no SEI a fim de assegurar a proteção de dados pessoais

Com o advento da **Lei Geral de Proteção de Dados Pessoais (LGPD)**, torna-se essencial que as unidades organizacionais do MDA avaliem adequadamente o nível de acesso atribuído aos processos e documentos produzidos e tramitados no **Sistema Eletrônico de Informações (SEI)**, considerando tanto a natureza das informações tratadas quanto o momento apropriado para sua divulgação.

Os documentos que contenham dados pessoais, possuam caráter preparatório ou estejam sujeitos a hipóteses de restrição de acesso previstas na legislação **devem ser corretamente classificados no SEI**, observando-se o nível de acesso compatível com a respectiva fundamentação legal.

Para se certificar sobre a classificação correta dos processos e documentos, verifique o módulo de consulta pública do sistema, disponível no endereço eletrônico:

https://sei.agro.gov.br/sei/modulos/pesquisa/md_pesq_processo_pesquisar.php?acao_externa=protocolo_pesquisar&acao_origem_externa=protocolo_pesquisar&id_orgao_acesso_externo=0.

Dessa forma, é imprescindível que a classificação do nível de acesso seja realizada previamente à inclusão de cada documento, de modo a evitar a divulgação indevida de informações protegidas.

Com base nas experiências e orientações compartilhadas pela Agência Nacional de Proteção de Dados (ANPD) na palestra **"Procedimentos para adequação de processos no SEI à luz da LGPD"**, realizada em junho de 2026, apresentam-se a seguir recomendações de boas práticas para o aperfeiçoamento da instrução processual, com especial atenção à proteção de dados pessoais e à observância dos princípios da LGPD.



A regra é a **transparência**. Os processos devem ser restritos/sigilosos apenas nas hipóteses apresentadas no SEI. Caso se refira a situações preparatórias, o processo deve estar adequado para torna-se público após a sua conclusão.



Os documentos inseridos no processo que possuem dados pessoais devem ser **pseudonimizados (ocultados)**.



Como **boa prática**, sugere-se que o documento com dados pessoais seja inserido da seguinte forma nos processos SEI:

a) Carregue o **documento original em pdf**, caso seja externo ao SEI, com nome na árvore **VERSÃO PRIVADA** e marque a opção de grau de sigilo **RESTRITO**. Se o documento tiver sido gerado no SEI, siga o passo abaixo;

b) Baixe o documento incluído (ou gerado) no SEI e utilize o **Adobe Acrobat Pro** para tarjar ou descaracterizar os dados pessoais e outros dados protegidos por legislações específicas. Lembre-se também de descaracterizar o **QR code gerado ao final da página, o código verificador e o código CRC, localizados ao final do documento**;


A autenticidade deste documento pode ser conferida no site: https://sei.agro.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **53325353** e o código CRC **F60ADB85**.

c) Carregue o **documento tarjado** em seguida no processo, com nome na árvore **VERSÃO PÚBLICA**, com opção de grau de sigilo **RESTRITO**;

d) Quando o processo for tornado público (ou se já for criado como público), modifique a opção de grau de sigilo **restrito** da **VERSÃO PÚBLICA** para a opção **público**;

e) Nesse momento, a **VERSÃO PRIVADA** deverá permanecer com a opção de grau de sigilo **RESTRITO**.

Não marque como restrito o processo ou os documentos que não se enquadrem nas hipóteses legais elencadas no SEI.

Para verificar se os processos instruídos sob sua responsabilidade estão publicados de forma correta, consulte-os no módulo de pesquisa pública do SEI.

Esse tratamento pode ser adotado para conciliar a **transparência pública com a proteção da privacidade** dos titulares de dados pessoais, além de simplificar a gestão dos processos que não se enquadrem em nenhuma das hipóteses de restrição de acesso previstas no SEI.

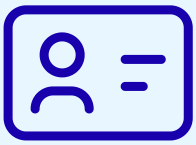
Por exemplo, caso seja solicitado o acesso integral a um processo, com fundamento na **Lei de Acesso à Informação (LAI)**, que ainda não tenha sido classificado com o grau de sigilo "público", com o tratamento prévio, a unidade organizacional, desde que inexistam hipóteses legais de restrição de acesso, não precisará realizar análises individualizadas dos documentos contidos no processo para verificar a possibilidade de disponibilização ao cidadão requerente, reduzindo o retrabalho e conferindo mais celeridade ao atendimento da solicitação.

Utilize ferramentas institucionais para realizar o tarjamento ou a descaracterização de dados pessoais, bem como para converter arquivos entre formatos (por exemplo, de JPEG para Word) e unir documentos em PDF. Evite o uso de ferramentas on-line, pois não há garantias quanto às formas de tratamento, armazenamento e proteção dos arquivos submetidos a esses ambientes.

Observação: Processos instruídos antes de **30/6/2025** poderão ser consultados por meio do módulo de pesquisa pública, mas **sem acesso ao conteúdo dos documentos produzidos antes desta data**.

Dessa forma, quando se tratar de um processo criado antes de 30/6, **os documentos públicos que entrarem após esta data ficarão disponíveis através da pesquisa pública**. Processos abertos antes dessa data estarão identificados com uma **chave azul** ao lado do número do documento.

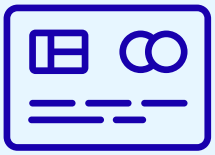
Nos termos do art. 5º, inciso I, da LGPD, considera-se dado pessoal toda informação relacionada à pessoa natural identificada ou identificável. Entre os exemplos mais comuns, estão:



Dados cadastrais e funcionais:

(a depender do caso para servidores)

nome, CPF, RG, CNH, passaporte, título de eleitor, data de nascimento, nacionalidade, estado civil, filiação, número do PIS/PASEP, matrícula funcional, registros profissionais e currículo.



Dados financeiros:

informações bancárias, chave PIX vinculada à pessoa, dados de cartão de crédito, histórico de pagamentos e declaração de imposto de renda.



Dados de contato:

endereço residencial ou comercial, CEP, telefone e e-mail pessoal.



Dados eletrônicos:

endereço IP, login de usuário, identificadores de dispositivos, geolocalização, registros de acesso a sistemas e histórico de navegação vinculado a uma pessoa.



Outros dados

que permitam identificar uma pessoa, como fotografia, voz gravada, assinatura e imagens de câmeras de monitoramento.

Subcomitê Técnico de Privacidade e Proteção de Dados Pessoais

