



**MINISTÉRIO DO DESENVOLVIMENTO E ASSISTÊNCIA SOCIAL, FAMÍLIA E COMBATE À FOME**  
**OUVIDORIA-GERAL**  
**DIVISÃO DE TRANSPARÊNCIA E ACESSO À INFORMAÇÃO**

**ORIENTAÇÃO N° 1/2024**  
**PROCESSO n° 71000.078585/2024-05**

**Assunto:** Trata do procedimento de ocultação (tarjamento) de dados pessoais na divulgação de informações por meio de ação de transparência e acesso à informação.

**Referência:** Caso responda este Ofício, indicar expressamente o Processo n° 71000.078585/2024-05.

1. Trata a presente orientação da necessidade de ocultação de dados pessoais quando da disponibilização de informações por meio de transparência ativa e passiva no âmbito do Ministério do Desenvolvimento e Assistência Social, Família e Combate à Fome (MDS), com base na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI) e Lei 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), bem como em outros dispositivos legais que abrangem hipóteses de restrição de acesso a dados ou informações.
2. Inicialmente é importante destacar que, em se tratando de informações públicas, a publicidade é o preceito geral e o sigilo a exceção, devendo a Lei nº 12.527/2011, que regula o direito fundamental de acesso a informações previsto no inciso XXXIII do art. 5 da Constituição Federal de 1988, ser executada através das seguintes modalidades:
  - a) **Transparência Passiva:** ocorre por meio do atendimento aos pedidos de informação direcionados a órgãos e entidades públicos por intermédio da Plataforma Integrada de Ouvidoria e Acesso à Informação - Fala.BR; e
  - b) **Transparência Ativa:** ocorre por meio da publicação proativa na internet de informações de interesse coletivo ou geral, produzidas ou custodiadas por órgãos e entidades.
3. A finalidade principal de ações de transparência é possibilitar o controle social e a fiscalização dos atos da administração pública, sendo fundamental para o exercício da democracia e para trazer a responsabilização e prestação de contas (*accountability*) da atividade governamental. Os conteúdos de divulgação obrigatória em transparência ativa estão estabelecidos no artigo 8º da LAI e em diversas outras normativas posteriores a ela, especialmente as expedidas pela Controladoria-Geral da União (CGU).

4. Da mesma forma que o direito de acesso à informação previsto no inciso XXXIII, da Constituição Federal, de 1988, a proteção de dados pessoais foi reconhecida como um direito fundamental a partir da Emenda Constitucional nº 115, de 2022. Assim, embora a LAI venha a estabelecer que as informações produzidas, acumuladas, custodiadas e geridas pelos órgãos públicos são públicas e devem ser disponibilizadas à sociedade, evidencia-se, também, a garantia legal de restrição de acesso a dado pessoal, este entendido como informação que se refira à intimidade, à vida privada, à honra e a imagem de pessoas. Nesse sentido, dispõe o art. 6º da LAI:

Art. 6º Cabe aos órgãos e entidades do poder público, observadas as normas e procedimentos específicos aplicáveis, assegurar a:

I - *omissis*;

II - *omissis*; e

**III - proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso.**  
(grifo nosso)

5. É importante observar que não há hierarquia entre direitos fundamentais, mas sim uma harmonização entre eles, sempre que possível, inclusive em casos de conflito aparente. Para trazer clareza ao tema, transcreve-se abaixo trechos dos Enunciados 4/2022 e 12/2023, da CGU:

Enunciado CGU 4/2022:

(...)

A LAI, a Lei nº 14.129/2021 (Lei de Governo Digital) e a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) são sistematicamente compatíveis entre si e harmonizam os direitos fundamentais do acesso à informação, da intimidade e da proteção aos dados pessoais, não havendo antinomia entre seus dispositivos.

Enunciado CGU 12/2023:

O fundamento "informações pessoais" não pode ser utilizado de forma geral e abstrata para se negar pedidos de acesso a documentos ou processos que contenham dados pessoais, uma vez que esses podem ser tratados (tarjados, excluídos, omitidos, descaracterizados etc.) para que, devidamente protegidos, o restante dos documentos ou processos solicitados sejam fornecidos, conforme preceitua o § 2º do art. 7º da Lei nº 12.527, de 18 de novembro de 2011, assegurando-se o acesso à parte não sigilosa por meio de certidão, extrato ou cópia com ocultação da parte sob sigilo.

Além disso, a proteção de dados pessoais deve ser compatibilizada com a garantia do direito de acesso à informação, podendo aquela ser flexibilizada quando, no caso concreto, a proteção do interesse público geral e preponderante se impuser, nos termos do art. 31, § 3º, inciso V da Lei n. 12.527, de 2011, e dos arts. 7º, § 3º, e 23, caput, da Lei nº 13.709, de 14 de agosto de 2018.

6. Assim, quando a transparência englobar também a disponibilização de dado pessoal, o interesse público nessa disponibilização se limita apenas na identificação dos agentes públicos ou privados envolvidos nos atos administrativos praticados, como contratos administrativos, notas de empenho, entre outros documentos, onde constam dados pessoais dos envolvidos.

7. A LAI, no entanto, não se trata da única legislação a prever informações com restrição de acesso aplicáveis no âmbito da administração pública. Nesse contexto, a LGPD é a legislação que regula as atividades de tratamento de dados pessoais e visa proteger os direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade da pessoa natural, estipulando regras e limitações para o uso de dados pessoais.

8. Embora esta orientação trate da ocultação de dados pessoais, é importante atentar que há outras situações previstas na LAI em que a restrição de acesso deve ser observada: as hipóteses de informações classificadas e os documentos preparatórios. As informações classificadas são aquelas

cujo sigilo seja imprescindível à segurança da sociedade e do Estado (art. 23 e 24) e os documentos preparatórios são aqueles que servem para fundamentar tomada de decisão (art. 7, § 3º). A LAI não proíbe a entrega de tais documentos, mas garante o seu acesso após a edição do ato relativo à tomada de decisão que os usou como fundamento.

8.1. Por fim, destaca-se que o disposto na LAI não exclui as demais hipóteses legais de sigilo e de segredo de justiça nem as hipóteses de segredo industrial decorrentes da exploração direta de atividade econômica pelo Estado ou por pessoa física ou entidade privada que tenha qualquer vínculo com o poder público.

### **QUAIS INFORMAÇÕES PESSOAIS DEVEM SER PROTEGIDAS**

9. De acordo com o Guia de Boas Práticas da LGPD do Comitê Central de Governança de Dados, o regime de proteção de dados pessoais proporcionado por essa lei é amplo. Nos termos do Guia:

(...) os direitos e salvaguardas sobre dados pessoais da LGPD incidem sobre todos os tipos de dados pessoais, observadas as legislações existentes, inclusive os regimes existentes de transparência e acesso à informação. **Ou seja, a tutela da lei se estende não mais apenas aos dados pessoais sensíveis ou diretamente relacionados aos direitos de personalidade, mas, em maior ou menor medida, a todos os dados pessoais.** (p. 20, grifos nossos)

10. Assim, depreende-se que todos os dados pessoais, em alguma medida, são tutelados pela LGPD. Nesse sentido, orienta-se a disponibilização de dados pessoais em transparência apenas nos casos de estrita previsão legal. Caso contrário, deve-se observar a ocultação (tarjamento), para fins de cumprimento de obrigações de transparência ativa e passiva, de todos os dados pessoais, estando seu acesso autorizado a agentes públicos legalmente autorizados e à pessoa a que elas se referirem, conforme art. 31 da LAI.

11. Os tipos de dados pessoais são descritos a seguir:

- a) atributos biográficos: dados de pessoa natural relativos aos fatos da sua vida, tais como nome civil ou social, data de nascimento, filiação, naturalidade, nacionalidade, sexo, estado civil, grupo familiar, endereço e vínculos empregatícios;
- b) atributos biométricos: características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, conforme Art. 2º, inciso II do Decreto 10.046/2019;
- c) atributos genéticos: características hereditárias da pessoa natural, obtidas pela análise de ácidos nucleicos ou por outras análises científicas; e
- d) dados cadastrais: informações identificadoras perante os cadastros de órgãos públicos.

12. Pontua-se que o número de inscrição no Cadastro de Pessoas Físicas (CPF) é dado pessoal cuja divulgação deve dar-se preferencialmente mediante procedimentos de descaracterização, por meio da ocultação dos três primeiros dígitos e dos dois dígitos verificadores. Excepcionalmente, o CPF poderá ser divulgado sem necessidade de descaracterização quando se tratar de Microempreendedor individual (MEI) ou Empresário Individual (EI) que eventualmente utilize seu CPF como dado cadastral em contratos com a administração pública.

13. Além dos tipos de dados e informações trazidos acima, deve-se tarjar rostos de pessoas em fotos e documentos e assinatura física à caneta em processos digitalizados. Quando houver rubrica com identificação de nome do servidor e/ou nº de SIAPE, ela também deverá ser tarjada.

14. Para os documentos oriundos do Sistema Eletrônico de Informações – SEI, deve-se ocultar, também a figura de QR Code, código verificador e código CRC. Esse procedimento impede que os originais possam ser acessados na íntegra por meio da plataforma de conferência de autenticidade do SEI.

15. Em caso de dúvidas sobre informações pessoais a ser divulgada em transparência, orienta-se a consultar o Guia de Transparência Ativa (GTA) da CGU e os Guias Orientativos da Autoridade Nacional de Proteção de Dados (ANPD), que traz a relação de informações a ser divulgada em transparência ativa, sua base legal e as orientações referentes ao que deve ser divulgado. Ademais, os enunciados da CGU devem ser consultados regularmente para conhecimento dos assuntos que devem ser públicos.

16. Por fim, é importante frisar que esta orientação trata da proteção de dados pessoais de pessoas naturais identificadas ou identificáveis, não se aplicando a dados de pessoas jurídicas.

### **QUEM DEVE REALIZAR O TARJAMENTO**

17. Recomenda-se que a unidade responsável pela produção do documento seja a mesma que realizará as atividades de tarjamento nos casos necessários, limitando, assim, a quantidade de agentes públicos que terão acesso a tais informações, quando não essenciais às suas funções laborais. Esta, ainda, detém maiores condições, experiência e conhecimento para identificar as informações que devem - e que não devem - ser disponibilizadas em transparência ativa, na medida em que, durante seus trabalhos, esteve em constante contato com seu conteúdo.

18. Ademais, a despeito da recomendação acima, deve-se ressaltar que todos os agentes que atuam no ciclo de vida dos dados pessoais, na forma do art. 47 da LGPD, detém responsabilidade por zelar por seu devido tratamento, de modo que a atuação de determinada unidade não exime as demais unidades envolvidas do dever de apontar eventuais equívocos nesse processo de tratamento, realizando as devidas interlocuções para solucioná-las.

19. No que tange à transparência passiva, a ocultação de dados pessoais e de dados pessoais sensíveis deverá ser realizada antes do encaminhamento da informação ao Sistema de Informação ao Cidadão - Divisão de Transparência e Acesso à Informação (SIC/DTAI).

### **COMO O TARJAMENTO DEVE SER FEITO**

20. Recomenda-se a utilização de software homologado pela Subsecretaria de Tecnologia da Informação do MDS que realize tarjamento seguro de dados ou informações em PDF. É importante que o software esteja instalado no computador para evitar o risco de vazamento de informação encontrado em soluções on-line.

21. Sugere-se a adoção da ferramenta PDF24 ou Adobe Acrobat Pro para fins de tarjamento de dados pessoais e/ou dados pessoais sensíveis.

22. O tarjamento (no PDF24) deve ser realizado de acordo com as seguintes etapas:

- a) com a ferramenta aberta, selecionar “Caixa de Ferramentas (toolbox)” e escolher a opção “Censurar PDF”;
- b) arrastar o arquivo em formato PDF a ser tarjado para a área indicada;
- c) com o arquivo aberto utilizar o pincel “Desenho livre” ou forma de retângulo e tarjar as áreas desejadas na cor preta;
- d) deve-se observar que o documento não aparece integralmente na tela, devendo ser selecionada a página do documento em que as informações serão tarjadas;
- e) salvar o arquivo tarjado;
- f) voltar ao menu “Caixa de Ferramentas (toolbox)” e escolher a opção “OCR PDF”;
- g) adicionar o arquivo tarjado, clicar em “Iniciar” e esperar o status conversão = Estado 100%;

h) após a conversão, o arquivo final será automaticamente salvo com no local indicado em "diretório de saída", com a adição do sufixo "\_ocred" ao nome. Este é o arquivo que deve ser utilizado.

23. Após a conclusão do processo, orienta-se que haja verificação de que os dados a serem tarjados estão efetivamente como tal. Para isso, deve-se selecionar um trecho de texto contendo a informação tarjada, copiar e colar em um bloco de notas ou software de edição de texto, e observar se o tarjamento permanece ou se a informação que deveria ser ocultada foi revelada.

24. Alternativamente, o tarjamento pode ser realizado através da ferramenta 'Tarjamento de documentos PDF' disponibilizada pela CGU na plataforma Fala.BR, observadas as instruções de tarjamento descritas no manual da ferramenta.

## **DISPOSIÇÕES FINAIS**

25. Cabe ressaltar que as considerações aqui trazidas não desobrigam os agentes públicos do MDS da leitura do texto integral da legislação correlata e que a não-observância dos dispositivos de sigilo de informações pessoais em ações de transparência pode ensejar em responsabilização do agente, nos termos do Capítulo V da LGPD.

26. Abaixo disponibiliza-se relação de material de consulta a ser utilizado como suporte para a garantia da proteção de dados pessoais que são produzidas, acumuladas, custodiadas ou geridas pelo órgão:

I - Lei nº 12.965, de 23 de abril de 2014, o Marco Civil da Internet, que colocou a proteção dos dados pessoais como princípio no uso da internet (art. 3º, inciso III);

II - Lei nº 13.460, de 26 de junho de 2017, que, ao dispor sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública, asseverou o direito de os usuários de serviços públicos terem suas informações pessoais protegidas, nos bancos de dados públicos;

III - Lei nº 14.129 de 29 de março de 2021, que dispõe sobre princípios, regras e instrumentos para o Governo Digital e traz o respeito a privacidade dos dados pessoais e dos dados sensíveis como requisito para a abertura de dados (art. 29, § 1º, VIII);

IV - Guia de Transparência Ativa (GTA) para órgãos e entidades do poder executivo federal, elaborado pela Controladoria-Geral da União, acessível em: <https://www.gov.br/acessoinformacao/pt-br/central-de-conteudo/publicacoes>;

V - Guia de Boas Práticas da Lei Geral de Proteção de Dados (LGPD), acessível em: <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias>;

VI - Enunciados e Boletins Informativos das Decisões da Controladoria-Geral da União, acessíveis em: <https://www.gov.br/acessoinformacao/pt-br/entendimentos-e-estudos-sobre-a-lai/boletins-enunciados-e-estudos-da-lai>; E

VII - Guias orientativos da Autoridade Nacional de Proteção de Dados, acessíveis em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes>.

27. Por oportuno, informa-se que as obrigações legais aqui abordadas serão objeto de monitoramento periódico por parte da Ouvidoria-Geral do MDS, por meio da DTAI, sem prejuízo da atuação da Assessoria Especial de Controle Interno, na qualidade de órgão setorial do Sistema de Integridade, Transparência e Acesso à Informação da Administração Pública Federal (Sitai), instituído pelo Decreto nº 11.529, de 16 de maio de 2023.

28. Assuntos relacionados à proteção de dados pessoais não esclarecidos por meio dessa orientação deverão ser direcionados à Ouvidora-Geral, na qualidade de Encarregada pelo tratamento de dados pessoais no MDS, pelo e-mail [ouvidoria.gabinete@mds.gov.br](mailto:ouvidoria.gabinete@mds.gov.br).

29. Assuntos relacionados ao processo de ocultação de dados pessoais deverão ser direcionados à DTAI por meio do e-mail [ouvidoria.dtai@mds.gov.br](mailto:ouvidoria.dtai@mds.gov.br).

Atenciosamente,

**NATALIA GIOVANNA MARSON**  
ANALISTA TÉCNICA DE POLÍTICAS SOCIAIS

De acordo. Submeto à consideração superior.

**IVAN TUYOSHI MORI KAKIMOTO**  
COORDENADOR-GERAL DE GESTÃO DA OUVIDORIA

Aprovada. Encaminhe-se.

**ELIANA PINTO**  
OUVIDORA-GERAL



Documento assinado eletronicamente por **Natalia Giovanna Marson, Chefe de Projeto II**, em 13/12/2024, às 12:40, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 da Presidência da República. .



Documento assinado eletronicamente por **Ivan Tuyoshi Mori Kakimoto, Coordenador(a)-Geral**, em 13/12/2024, às 14:26, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 da Presidência da República. .



Documento assinado eletronicamente por **Antonia Eliana Pinto, Ouvidor(a)-Geral**, em 13/12/2024, às 14:28, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 da Presidência da República. .

---



A autenticidade deste documento pode ser conferida no site <https://sei.cidadania.gov.br/sei-autenticacao>, informando o código verificador **16168824** e o código CRC **B3721F7B**.

---