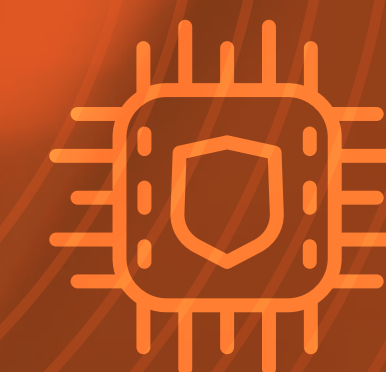


LGPD NO MPF

Cartilha para membros
e servidores de gabinetes





Ministério Público Federal
Gabinete do Procurador-Geral da República
Unidade de Proteção de Dados Pessoais

LGPD NO MPF

Cartilha para membros e
servidores de gabinetes

2ª edição

Brasília - DF
MPF
2024

Organização e Coordenação
Unidade de Proteção de Dados Pessoais

Encarregado de Proteção de Dados
Leonardo Andrade Macedo - Procurador da República

SUMÁRIO

- Apresentação
- 4** Unidade de Proteção de Dados Pessoais do MPF (UPDP/MPF)
- 5** Atribuições do Encarregado e UPDP
- 6** O que são dados pessoais?
- 7** Dados pessoais sensíveis
- 7** Dados pessoais de crianças e adolescentes
- 8** Dicas de proteção de dados pessoais na atividade-fim
- 10** Segurança da informação
- 11** O que significam os termos “ANONIMIZAÇÃO”
E “PSEUDONIMIZAÇÃO”
- 12** Quais dados pessoais utilizar em peças processuais
- 13** Consentimento para tratamento de dados pessoais
- 14** Pílulas do conhecimento

APRESENTAÇÃO

Na “era da informação”, caracterizada pela popularização da tecnologia e pelo aumento do poder computacional, os dados pessoais passam a ser uma valiosa matéria-prima. A partir de dados fornecidos espontaneamente pelos próprios usuários em sites, redes sociais e aplicativos, é possível traçar o perfil de cada indivíduo, seus hábitos de consumo, preferências políticas, vida sexual, condições de saúde, situação financeira, entre outros aspectos, revelando características que não estão claras nem para o próprio titular dos dados. Além disso, esses gigantes bancos de dados pessoais podem chegar a ser negociados illicitamente em ambientes ocultos da internet, servindo como insumo para práticas criminosas diversas.

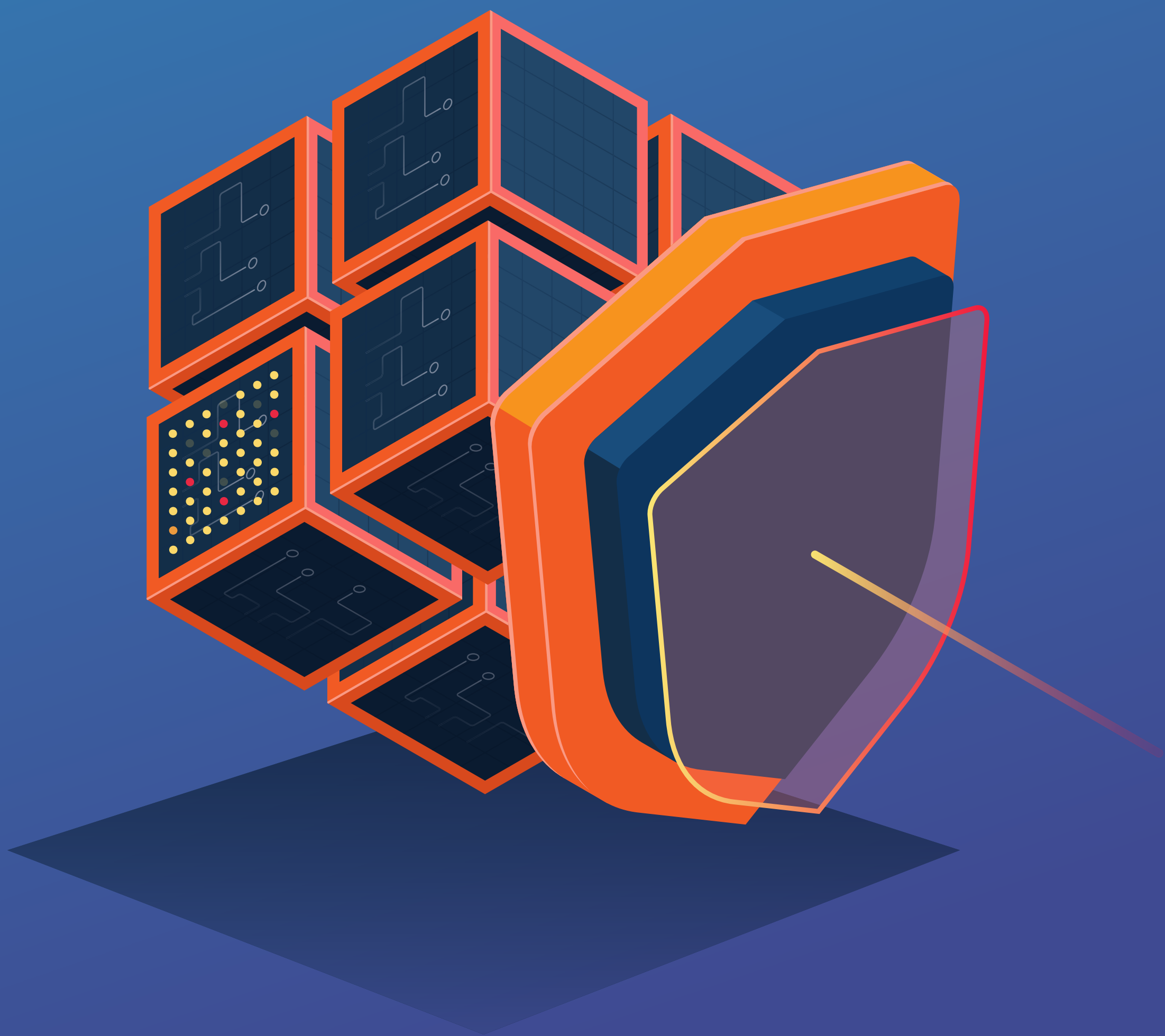
A Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018) visa garantir ao indivíduo maior controle sobre seus dados pessoais (auto-determinação informativa), sem comprometer o desenvolvimento econômico e tecnológico e a inovação. Para isso, a lei exige que qualquer operação de tratamento envolvendo dados pessoais, inclusive o simples armazenamento e a consulta, seja realizada apenas em determinadas hipóteses (as chamadas “bases legais” previstas nos arts. 7º e 11) e conforme os princípios enunciados no art. 6º (boa-fé, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas).

No exercício de sua atividade finalística, cabe ao Ministério Público a defesa desse importante direito fundamental, com os instrumentos de que dispõe, especialmente no âmbito coletivo. Por outro lado, compete também ao Ministério Público, seja na atuação administrativa, seja na atividade-fim, observar e cumprir as disposições da LGPD. Mesmo nas hipóteses excepcionais de não aplicação previstas no seu art. 4º (por exemplo, atividades de investigação e repressão de infrações penais), a lei prevê que deverão ser observados “os princípios gerais de proteção e os direitos do titular”, além da possibilidade de se exigir relatórios de impacto à proteção de dados pessoais (§§ 1º e 3º).

O Ministério Público Federal vem avançando a passos largos no processo de implementação da LGPD, com destaque para a aprovação de sua Política de Privacidade e Proteção de Dados Pessoais (Portaria PGR/MPF nº 661, de 12 de agosto de 2022), a criação da Unidade de Proteção de Dados Pessoais (UPDP) e a disponibilização de canais para exercício dos direitos dos titulares. O MPF também tem investido fortemente na disseminação da cultura de proteção de dados pessoais, promovendo, de forma contínua, planos de capacitação e comunicação voltados para o público interno.

É nesse contexto que apresento esta Cartilha, direcionada a membros e servidores de gabinetes, com alguns conceitos básicos da LGPD, dicas e orientações práticas de como proteger dados pessoais nas atividades finalísticas do MPF. Esta iniciativa é, acima de tudo, uma provocação à reflexão sobre o valor dos dados pessoais nos tempos atuais e um convite ao aprofundamento no tema.

Leonardo Andrade Macedo
Procurador da República
Encarregado de Proteção de Dados Pessoais



A LGPD É UMA REALIDADE NO MPF!

HÁ UM SETOR ESPECIALIZADO PARA APOIAR MEMBROS E SERVIDORES A CUMPRIR A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NO EXERCÍCIO DA ATIVIDADE FINALÍSTICA.

Essa atribuição cabe à Unidade de Proteção de Dados Pessoais (UPDP/MPF), instituída pela Portaria PGR/MPF nº 366, de 18 de maio de 2022. O setor presta apoio e orientação às diversas áreas na implementação das medidas necessárias à proteção dos dados pessoais tratados nas atividades administrativas e finalísticas do Órgão, em cumprimento ao disposto na Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018) e em atos normativos regulamentadores, oriundos da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional do Ministério Público (CNMP).

A UPDP também presta apoio ao Encarregado de Proteção de Dados Pessoais, que é um membro designado pelo procurador-geral da República que tem por atribuições orientar, liderar e coordenar as ações de conformidade à LGPD, além de atuar como canal de contato do MPF com os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD).

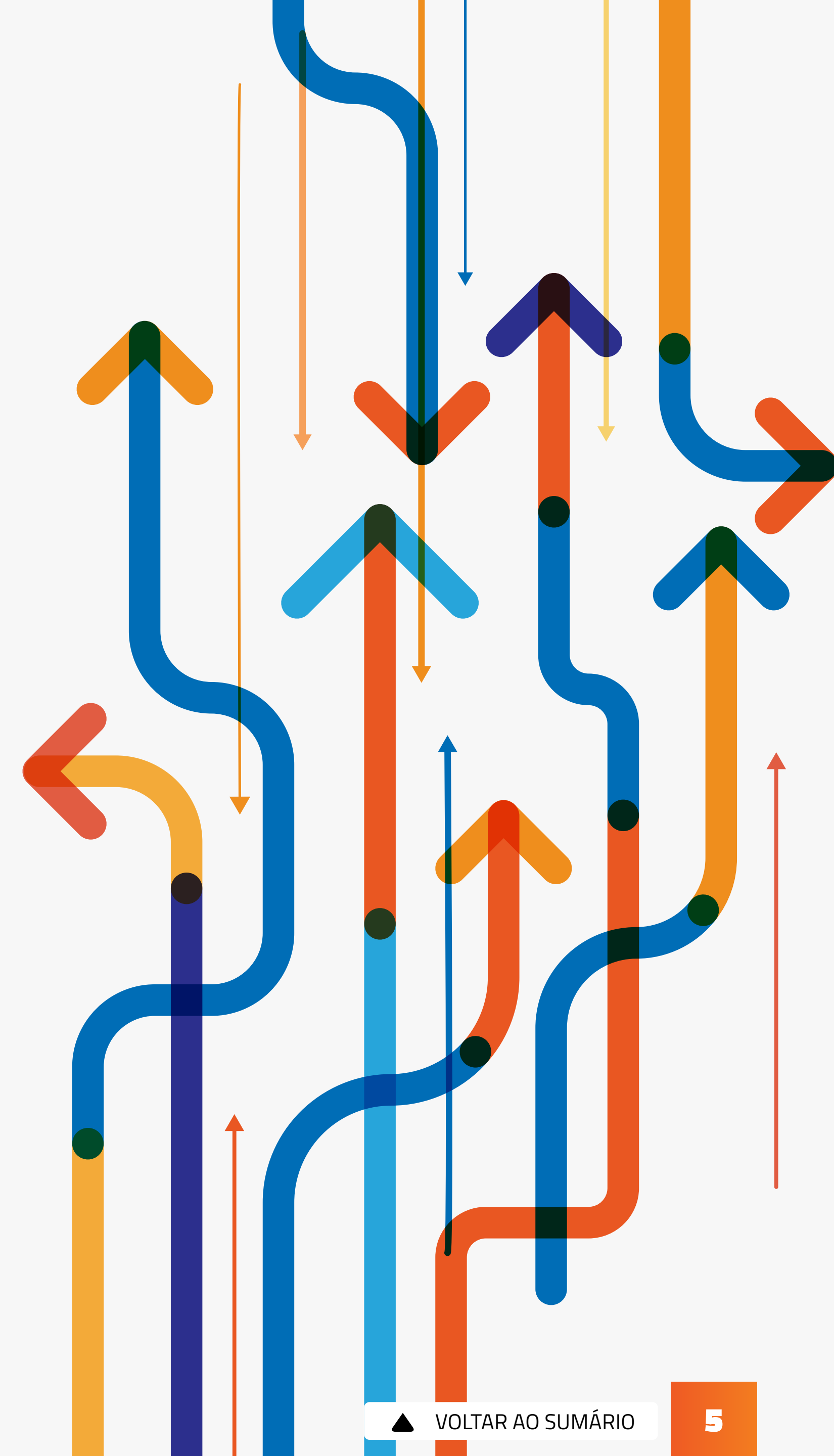
CABE AO ENCARREGADO, ENTRE OUTRAS ATIVIDADES:

- **Orientar** membros, servidores, estagiários e demais colaboradores a respeito das boas práticas a serem tomadas em relação à proteção de dados pessoais.
- **Auxiliar** os diversos setores para que as atividades que abranjam tratamento de dados pessoais ocorram de forma segura, eficaz e controlada.
- **Dirimir** as dúvidas, acompanhar a implementação e indicar os meios para otimizar a Política de Privacidade e Proteção de Dados Pessoais.

QUANTO À UPDP, ALGUMAS DE SUAS ATIVIDADES ESTÃO VOLTADAS A:

- **Apoiar** os diversos setores da Instituição na implementação da LGPD no âmbito do Ministério Público Federal.
- **Orientar** os responsáveis pelo tratamento de dados a respeito de suas obrigações e de outras disposições de proteção de dados.
- **Recomendar** a adoção de medidas técnicas e administrativas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou de qualquer forma de tratamento inadequado ou ilícito.

As atribuições da UPDP e do encarregado constam da Portaria PGR/MPF nº 795/2022.



O QUE SÃO DADOS PESSOAIS?

Dados pessoais englobam toda informação relacionada à pessoa natural identificada ou identificável, ou seja, se uma informação permite identificar, direta ou indiretamente, uma pessoa natural que esteja viva, então ela é considerada um dado pessoal.

São exemplos de dados pessoais:

Nome civil e social, apelido, sexo, data e local de nascimento, filiação, parentesco, IDs (RG, CPF, Previdência, Título de Eleitor, número de Passaporte), naturalidade, nacionalidade, placa de veículos, vínculo empregatício, característica hereditária, dados fiscais, bancários e financeiros, relação de bens, renda, histórico de pagamentos, dados profissionais, endereço residencial, e-mail, números de telefone, dados telefônicos e telemáticos, localização via GPS, fotografias, vídeos de câmeras de segurança, hábitos de consumo, preferências de lazer, informações contidas em aparelhos eletrônicos (IP, IMEI), cookies (rastreadores que monitoram o comportamento do usuário na internet), entre outros.





DADOS PESSOAIS SENSÍVEIS

Essa categoria especial de dados pessoais abrange informações sobre gênero, origem racial ou étnica, 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, prontuário de saúde. Por envolverem maiores riscos, esses dados demandam maior grau de proteção.



ATENÇÃO AOS DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES!

Os dados pessoais de crianças e adolescentes gozam de maior grau de proteção, e só devem ser divulgados em situações excepcionais (maior ônus argumentativo). Nesses casos, o tratamento deve ser feito sempre para a proteção e no melhor interesse desses titulares; e, a depender das circunstâncias, será necessário o consentimento dos responsáveis. Além do uso de iniciais em lugar do nome, podem ser adotadas outras medidas de proteção, como a restrição de acesso a determinados usuários e a imposição de sigilo ao expediente. Também devem ser resguardados dados de eventuais vítimas e testemunhas.

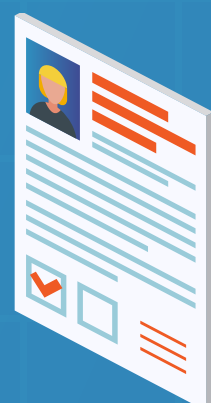
DICAS PRÁTICAS A SEREM OBSERVADAS PELOS MEMBROS E SERVIDORES LOTADOS EM GABINETES NO DESEMPENHO DE SUAS ATIVIDADES:



Adotar cuidado especial ao transportar procedimentos e documentos.



Só compartilhe dados pessoais com terceiros em cumprimento às obrigações legais do MPF (por exemplo: viabilizar acesso do advogado à investigação)



Coletar somente os dados pessoais necessários para atendimento da finalidade específica da atividade.



Evite fazer download de arquivos que contenham dados pessoais para computadores e dispositivos móveis. Abra ou consulte-os diretamente pelo sistema. Se o download for indispensável, ao final do uso, o arquivo deverá ser eliminado completamente da pasta onde foi baixado e, a seguir, da lixeira.

Em casos de exposição, arquivos com informações sigilosas, com ou sem dados pessoais, aumentam o risco de incidentes de segurança da informação.

Para dúvidas sobre como eliminar arquivos, contacte a CENAR via SNP ou pelo nº (61) 3105-8100.



Utilizar técnicas de pseudonimização para evitar a identificação do titular de dados pessoais.



Evitar impressão de documentos que contenham dados pessoais; e, quando impressos, não deixá-los expostos em mesas e/ou bandejas das impressoras. Caso seja necessário, atentar-se para a forma correta de eliminação.



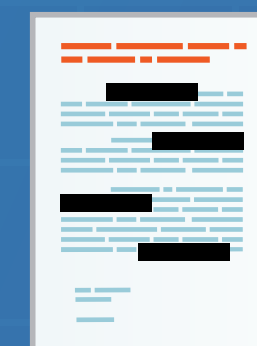
Documentos sigilosos arquivados no Google Drive devem ser mantidos, preferencialmente, na pasta pessoal do usuário (Meu Drive) e protegidos com senha e criptografia.



Para trabalhar com arquivos .pdf (juntar, dividir, extrair tabelas, converter), em vez de lançar dados pessoais em ferramentas em nuvem, utilize o programa PDFSAM Basic (instalado no desktop) ou a suíte LinaPDF (acesso interno ou externo por VPN).



Atente-se para a classificação de sigilo de expedientes que contenham dados pessoais, especialmente sensíveis, de crianças e adolescentes, vítimas e testemunhas.



O mascaramento com tarjas de dados pessoais em documentos deve ser feito de maneira a impedir a pesquisa e o acesso ao conteúdo protegido (**aplicativo PDF24**).



Transcrever para as peças (despachos, petições) apenas os dados pessoais estritamente necessários para a finalidade pretendida.

ATENTE-SE A OUTROS CUIDADOS NECESSÁRIOS PARA A SEGURANÇA DA INFORMAÇÃO:

- ✓ Utilizar, exclusivamente, os sistemas institucionais de comunicação para tratar de assuntos de trabalho.
- ✓ Evitar acessar a rede MPF em locais públicos, entre eles: lan house; aeroportos; shoppings.
- ✓ Nunca sair da estação de trabalho sem bloquear o computador. Em trabalho remoto, redobrar os cuidados quanto à exposição das informações. Sempre que se ausentar, atentar-se em utilizar a tela de bloqueio de vídeo para impedir que estranhos acessem o computador.
- ✓ Negar acesso aos espaços físicos e aos documentos a pessoas não autorizadas.
- ✓ Criar senha institucional forte e diferente das utilizadas em acessos particulares, como em sistemas bancários, provedores de internet e contas de e-mail pessoal. Não compartilhar com outros servidores públicos ou terceiros e não anotar em agendas ou post-it.
- ✓ Utilizar apenas programas certificados pela Secretaria de Tecnologia da Informação e Comunicação do MPF.
- ✓ Não utilizar ferramentas que impliquem o lançamento de informações processuais sensíveis, sigilosas ou pessoais, em banco de dados privado, não passível de fiscalização e controle por parte do Estado.

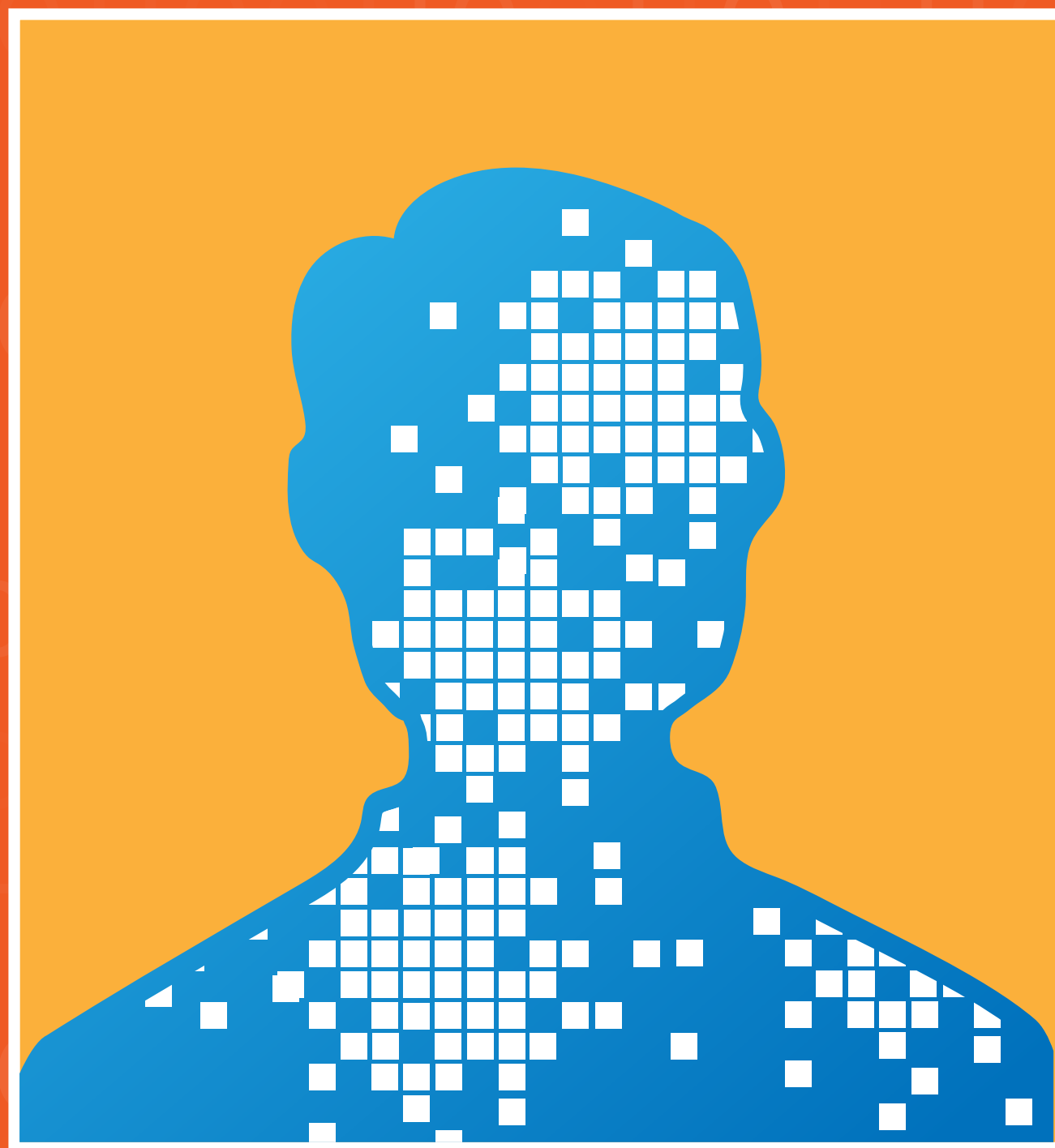


O QUE SIGNIFICAM OS TERMOS “ANONIMIZAÇÃO” E “PSEUDONIMIZAÇÃO”?

São técnicas utilizadas para manter a privacidade dos titulares de dados pessoais previstas no Manual de Redação (Portaria PGR/MPF nº 406, de 1º de junho de 2023).

ANONIMIZAÇÃO

Os dados relativos ao titular não podem ser identificados, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.



PSEUDONIMIZAÇÃO

O dado pessoal 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.

Por exemplo:



Omitir, tarjar ou mascarar os dados pessoais.



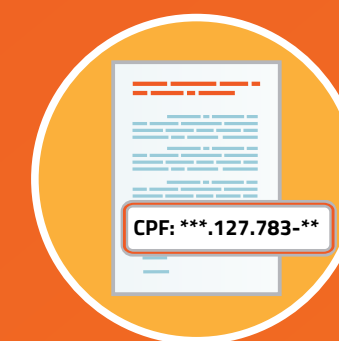
Suprimir os dados pessoais, substituindo-os pela expressão em latim *[omissis]*, grafada entre colchetes e em itálico.



Substituir os nomes próprios por suas iniciais, por pseudônimos ou por expressão genérica que descreva a situação da pessoa na relação fático/processual (por exemplo, investigado, denunciado, réu, vítima, testemunha, representante).



Usar da generalização (por exemplo, servidor público em vez de servidor de determinado órgão; idade ou ano de nascimento da pessoa em vez da data completa; cidade ou estado de domicílio em vez do endereço completo; volume total de transações ou bens em vez de transações ou bens específicos).



Suprimir determinados caracteres (CPF: ***.127.783-**).



PRECISO UTILIZAR TODAS AS INFORMAÇÕES PESSOAIS DOS TITULARES DE DADOS PARA IDENTIFICÁ-LOS EM PEÇAS PROCESSUAIS?

Embora a legislação exija, em peças processuais, a qualificação completa das pessoas (investigados, réus, testemunhas, vítimas etc.), para outros fins, como divulgação e consulta pública de dados das partes e dos advogados, os dados pessoais não são necessários e podem ser pseudonimizados, com a possibilidade de se ter versões diferentes do mesmo documento para cada finalidade.

CUIDADO COM A DIVULGAÇÃO DE DADOS PESSOAIS!

A Política de Comunicação Social do MPF também foi revista para adequá-la à LGPD e, entre outras disposições, passou a prever que “cabe ao setor demandante definir, no contexto da demanda, quais dados pessoais são de interesse público para fins de comunicação social e adotar as medidas adequadas para resguardar os demais dados pessoais, com especial atenção a dados pessoais sensíveis, dados pessoais de crianças e adolescentes e dados de vítimas e testemunhas” (art. 10, § 1º, da Portaria PGR/MPF nº 404, de 1º de junho de 2023).

Portanto, na divulgação de íntegras de peças, vídeos, áudios e outros documentos, eles já devem ser enviados tratados aos órgãos do Sistema Nacional de Comunicação Social, a quem caberá conferir se, de fato, foram adotadas as medidas de proteção dos dados pessoais.

É NECESSÁRIO CONSENTIMENTO DO TITULAR DE DADOS PESSOAIS PARA TODO TIPO DE TRATAMENTO?



Não. O consentimento é apenas mais uma das bases legais que autorizam o tratamento de dados pessoais. Essa hipótese é mais comum no setor privado. No setor público, a base legal mais frequente que autoriza o tratamento de dados pessoais é a prevista no inciso II do art. 7º da LGPD: “cumprimento de obrigação legal ou regulatória pelo controlador”.

CONFIRA OUTRAS BASES LEGAIS NO ART. 7º:

- II – para o cumprimento de obrigação legal ou regulatória pelo controlador;
- III – pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
- IV – para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- V – quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- VI – para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
- VII – para a proteção da vida ou da incolumidade física do titular ou de terceiro;
- VIII – para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência
- IX – quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
- X – para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

GOSTOU DO TEMA E TEM INTERESSE EM SE APROFUNDAR?

Estão disponíveis na plataforma EaD MPF pílulas do conhecimento que abordam diversos conceitos e informações técnicas afetas à LGPD. São 14 sessões sobre os seguintes tópicos:

- Você conhece o valor dos seus dados pessoais?
- Qual o valor dos seus dados pessoais?
- Conheça os princípios da LGPD.
- Proteja seus dados pessoais.
- 4 cuidados com seus dados pessoais.
- O que são dados pessoais?
- Que tal verificar para qual finalidade seus dados serão utilizados?
- O consentimento de dados pessoais agora é lei!
- Quando seus dados pessoais podem ser tratados sem seu consentimento?
- Princípio da transparência na LGPD.
- Fim do tratamento de dados pessoais.
- Tempo de uso dos dados pessoais.
- Por que a LGPD foi criada?
- Webinar LGPD no MPF.

Acesse: <https://ead.mpf.mp.br/> e agregue conhecimentos sobre a LGPD.



TEM DÚVIDAS SOBRE COMO PROTEGER DADOS PESSOAIS EM PROCESSOS?

PROCURE O ENCARREGADO DE PROTEÇÃO DE DADOS OU A EQUIPE DA UPDP/MPF.

ACESSE:



PGR-UPDP@MPF.MP.BR



(61) 3105-6250



WWW.MPF.MP.BR/SERVICOS/LGPD

MPF
Ministério Público Federal