

DIÁRIO OFICIAL DA UNIÃO

Publicado em: 16/06/2026 | Edição: 110 | Seção: 1 | Página: 2

Órgão: Presidência da República/Advocacia-Geral da União

PORTARIA NORMATIVA AGU Nº 226, DE 15 DE JUNHO DE 2026

Institui a Política de Proteção de Dados Pessoais da Advocacia-Geral da União e dá outras providências.

O ADOVADO-GERAL DA UNIÃO, no uso das atribuições que lhe confere o art. 4º, caput, incisos I, XIII e XVIII, da Lei Complementar nº 73, de 10 de fevereiro de 1993, tendo em vista o disposto na Lei nº 13.709, de 14 de agosto de 2018, e o que consta no Processo Administrativo nº 00400.003171/2023-82, resolve:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Fica instituída a Política de Proteção de Dados Pessoais da Advocacia-Geral da União, com a finalidade de:

I - estabelecer regras e procedimentos para a gestão da proteção de dados pessoais de modo a assegurar:

- a) a proteção da privacidade;
- b) a autodeterminação informativa; e
- c) a observância dos princípios previstos no art. 6º da Lei nº 13.709, de 14 de agosto de 2018;

II - definir o modelo de governança da proteção de dados pessoais no âmbito da Advocacia-Geral da União; e

III - disseminar a cultura de proteção de dados pessoais, de forma a promover a conscientização sobre os riscos, as responsabilidades e as boas práticas no tratamento de dados pessoais.

§ 1º O disposto nesta Portaria Normativa se aplica:

I - aos órgãos previstos no art. 2º do Anexo I ao Decreto nº 12.540, de 30 de junho de 2025; e

II - à Procuradoria-Geral da Fazenda Nacional e à Procuradoria-Geral do Banco Central nos casos em que houver utilização dos sistemas mantidos pelos órgãos de que trata o inciso I.

§ 2º Sem prejuízo do disposto no § 1º, as Consultorias Jurídicas junto aos ministérios e as Procuradorias Federais junto às autarquias ou fundações públicas deverão:

I - observar a Política de Proteção de Dados Pessoais dos órgãos e das entidades a que estejam administrativamente vinculados; e

II - comunicar à Secretaria de Governança e Gestão Estratégica sempre que houver questões administrativas disciplinadas de maneira distinta na Política de Proteção de Dados Pessoais dos órgãos e das entidades a que estejam administrativamente vinculados e que possam gerar impactos nas referidas Procuradorias e Consultorias.

Art. 2º A Política de Proteção de Dados Pessoais da Advocacia-Geral da União será pautada pela boa-fé e pela observância dos princípios constantes do art. 6º da Lei nº 13.709, de 14 de agosto de 2018.

Art. 3º Para os efeitos desta Portaria Normativa e de suas normas complementares, aplicam-se as definições:

- do art. 5º da Lei nº 13.709, de 14 de agosto de 2018;



II - do Glossário de Segurança da Informação, aprovado pela Portaria GSI/PR nº 93, de 18 de outubro de 2021; e

III - do Glossário de Proteção de Dados Pessoais e Privacidade, elaborado pela Agência Nacional de Proteção de Dados.

Art. 4º São objetivos da Política de Proteção de Dados Pessoais da Advocacia-Geral da União:

I - definir as competências e responsabilidades quanto à proteção de dados pessoais;

II - estabelecer medidas técnicas e administrativas para o cumprimento das normas de proteção de dados pessoais e dos meios de avaliação para demonstrar a eficácia dessas medidas;

III - estabelecer processos de trabalho que promovam a redução dos riscos no tratamento de dados pessoais;

IV - definir regras de segurança, de boas práticas e de governança com objetivo de assegurar a proteção de dados pessoais;

V - garantir o usufruto dos direitos dos titulares dos dados pessoais;

VI - definir procedimentos para o registro de todas as operações de tratamento de dados pessoais;

VII - promover a criação de programas de treinamento e conscientização das responsabilidades e dos procedimentos adequados para a proteção de dados pessoais; e

VIII - promover a construção de uma cultura institucional de proteção aos dados pessoais.

Art. 5º São diretrizes da Política de Proteção de Dados Pessoais da Advocacia-Geral da União:

I - limitação do tratamento de dados pessoais às situações indispensáveis para o atingimento das finalidades institucionais da Advocacia-Geral da União, sempre na persecução do interesse público;

II - limitação do tratamento aos dados pessoais estritamente necessários à sua finalidade;

III - garantia da segurança dos dados pessoais custodiados pela Advocacia-Geral da União;

IV - garantia aos titulares de transparência e facilidade de acesso às informações relacionadas ao tratamento de dados pessoais;

V - atuação preventiva para mitigação dos riscos no tratamento de dados pessoais;

VI - respeito às especificidades e à autonomia das unidades da Advocacia-Geral da União; e

VII - alinhamento estratégico da Política de Proteção de Dados Pessoais com:

a) o Plano Estratégico da Advocacia-Geral da União;

b) as normas de proteção de dados pessoais da administração pública federal, especialmente da Agência Nacional de Proteção de Dados; e

c) as melhores práticas de proteção de dados pessoais.

Art. 6º A Política de Proteção de Dados Pessoais da Advocacia-Geral da União, suas atualizações e normas complementares deverão ser divulgadas amplamente, a fim de promover seu conhecimento e sua observância no âmbito da Advocacia-Geral da União.

CAPÍTULO II

DA GESTÃO DA PROTEÇÃO DE DADOS PESSOAIS

Seção I

Dos instrumentos de gestão

Art. 7º A gestão da proteção de dados pessoais da Advocacia-Geral da União será realizada por meio dos seguintes instrumentos:

I - definição de competências e responsabilidades;

II - documentação relacionada ao tratamento de dados pessoais;

III - regras para o tratamento de dados pessoais em contextos específicos;



IV - gestão de riscos;

V - regras para o tratamento de violações de dados pessoais;

VI - contratos, convênios, acordos e instrumentos congêneres;

VII - monitoramento; e

VIII - transparência e acesso à informação.

Seção II

Das competências e responsabilidades

Subseção I

Do controlador

Art. 8º No âmbito da Advocacia-Geral da União, as funções do controlador serão exercidas pela Secretaria de Governança e Gestão Estratégica.

Parágrafo único. Compete ao controlador decidir sobre o tratamento de dados pessoais, devendo:

I - observar os fundamentos, os princípios da proteção de dados pessoais e os deveres impostos pela Lei nº 13.709, de 14 de agosto de 2018, e por normativos correlatos no momento de decidir sobre o tratamento ou de realizá-lo;

II - orientar a elaboração do inventário de dados pessoais para serviços e processos de trabalho, conforme disposto no art. 12 desta Portaria Normativa;

III - coordenar a elaboração dos Relatórios de Impacto à Proteção de Dados Pessoais - RIPD nas hipóteses previstas no art. 13 desta Portaria Normativa, com apoio das unidades responsáveis pela atividade, pelo sistema, pelo serviço ou pelo projeto ao qual o relatório diz respeito;

IV - atuar na proteção dos dados pessoais ao longo de todo o seu ciclo de vida, especialmente quanto à sua eliminação após o cumprimento da finalidade e da base legal do tratamento, conforme registrado no inventário de dados pessoais, ressalvadas as hipóteses de conservação autorizadas pelo art. 16 da Lei nº 13.709, de 14 de agosto de 2018;

V - orientar sobre o armazenamento e o descarte seguro dos dados pessoais custodiados pela Advocacia-Geral da União;

VI - elaborar avisos, orientações técnicas e disseminar boas práticas para a adequada aplicação desta Portaria Normativa;

VII - orientar sobre a coleta do consentimento do titular, quando este for necessário, assim como sobre o procedimento para sua revogação;

VIII - elaborar termos de consentimento e avisos de privacidade, conforme disposto no art. 14 desta Portaria Normativa;

IX - informar aos titulares dos dados as alterações nos termos de consentimento, na forma do art. 8º, § 6º, da Lei nº 13.709, de 14 de agosto de 2018;

X - orientar a atuação dos operadores no tratamento de dados pessoais de forma a garantir o cumprimento desta Portaria Normativa;

XI - informar, de forma clara e atualizada, as hipóteses de tratamento de dados pessoais realizadas pela Advocacia-Geral da União, mediante divulgação em seu sítio eletrônico ou em portal específico do serviço ou atendimento, com a indicação:

a) da base legal;

b) da finalidade;

c) dos procedimentos; e

d) das práticas adotados no tratamento;

XII - orientar sobre o processo adequado para a anonimização e a pseudonimização de dados pessoais, quando necessário e possível;



XIII - auxiliar a Ouvidoria quanto ao atendimento dos requerimentos dos titulares sobre o tratamento dos seus dados pessoais, nos termos do art. 18 da Lei nº 13.709, de 14 de agosto de 2018;

XIV - comunicar à Agência Nacional de Proteção de Dados e ao titular dos dados a ocorrência de incidente de segurança com dados pessoais, quando necessário, nos termos do art. 24 desta Portaria Normativa;

XV - divulgar eventual delegação das suas competências, especificando os poderes transferidos e informando a identificação e as informações de contato do delegado;

XVI - fornecer informações de identidade e contato do encarregado de forma clara e objetiva para a divulgação pela Assessoria de Comunicação no sítio eletrônico da Advocacia-Geral da União;

XVII - prover os meios necessários para o exercício das atribuições do encarregado, respeitando sua autonomia técnica;

XVIII - fornecer informações sobre o tratamento de dados pessoais para a gestão de página específica no sítio eletrônico da Advocacia-Geral da União e na rede privada de computadores - intranet, nos termos do art. 31 desta Portaria Normativa;

XIX - elaborar boletim informativo do andamento das atividades de proteção de dados pessoais na Advocacia-Geral da União, bem como de cursos disponíveis, eventos e novidades normativas da área;

XX - elaborar proposta:

a) de normas complementares à Política de Proteção de Dados Pessoais da Advocacia-Geral da União;

b) do Programa de Governança em Privacidade que contemple o planejamento, a execução e o monitoramento das atividades para cumprimento das regras de proteção de dados pessoais no âmbito da Advocacia-Geral da União, conforme disposto no art. 50, § 2º, inciso I, da Lei nº 13.709, de 14 de agosto de 2018; e

c) do Plano de Atendimento às Demandas dos Titulares de Dados Pessoais.

Subseção II

Do encarregado

Art. 9º Compete ao encarregado, assegurada sua autonomia técnica, além das atividades determinadas no art. 41 da Lei nº 13.709, de 14 de agosto de 2018:

I - observar os fundamentos, os princípios da proteção de dados pessoais e os deveres impostos pela Lei nº 13.709, de 14 de agosto de 2018, e por normativos correlatos no exercício das suas funções;

II - auxiliar na elaboração e atualização anual dos inventários de dados pessoais por cada processo de trabalho, a fim de manter registro das operações relacionadas ao seu tratamento no âmbito da Advocacia-Geral da União;

III - auxiliar na elaboração e atualização anual dos relatórios de impacto à proteção de dados pessoais;

IV - declarar ao controlador qualquer situação que possa configurar conflito de interesse, responsabilizando-se pela veracidade das informações prestadas, nos termos da Resolução CD/ANPD nº 18, de 16 de julho de 2024;

V - disponibilizar canal de comunicação aos titulares de dados pessoais no sítio eletrônico da Advocacia-Geral da União, por meio da Plataforma Integrada de Ouvidoria e Acesso à Informação - Fala.Br, para apresentação de reclamações e solicitações, bem como prestar os esclarecimentos e adotar as providências cabíveis;

VI - atuar como canal de comunicação entre a Advocacia-Geral da União e a Agência Nacional de Proteção de Dados;

VII - receber solicitações e comunicações da Agência Nacional de Proteção de Dados e adotar as providências cabíveis;

VIII - auxiliar o controlador no exercício das funções elencadas no art. 8º desta Portaria Normativa;



IX - divulgar eventual delegação das suas competências, especificando os poderes transferidos e informando a identificação e as informações de contato do delegado;

X - representar a Advocacia-Geral da União em eventos organizados por órgãos ou entidades externos, quando a temática do evento for privacidade, proteção de dados pessoais e, especialmente, a própria atuação do encarregado;

XI - aprovar as Avaliações de Impacto à Proteção de Dados Pessoais e os Relatórios de Impacto à Proteção de Dados Pessoais nos termos do art. 13 desta Portaria Normativa.

Parágrafo único. O encarregado pelo tratamento de dados pessoais no âmbito da Advocacia-Geral da União e seu substituto serão designados em ato específico do Advogado-Geral da União.

Subseção III

Do operador

Art. 10. Será considerado operador qualquer fornecedor de produtos ou serviços, que, por qualquer motivo, realize o tratamento de dados pessoais a ele confiados pela Advocacia-Geral da União e em nome desta, incluídas as empresas prestadoras de serviços terceirizados.

§ 1º Os operadores devem, ao realizar o tratamento de dados pessoais, observar as normas estabelecidas nesta Portaria Normativa, suas normas complementares e demais orientações do controlador.

§ 2º São atribuições do operador, além das previstas no art. 39 da Lei nº 13.709, de 14 de agosto de 2018:

I - manter canal de comunicação de fácil acesso e que permita comunicação imediata para interlocução com o controlador e o encarregado;

II - apresentar evidências da aplicação de medidas técnicas adequadas de segurança aos dados pessoais, quando solicitadas pelo controlador e pelo encarregado;

III - manter os registros de tratamento de dados pessoais atualizados, na forma determinada pelo controlador;

IV - descartar, de forma irrecuperável, ou devolver à Advocacia-Geral da União todos os dados pessoais e as respectivas cópias, após o término do tratamento pelo cumprimento da finalidade ou por encerramento do vínculo legal ou contratual, exceto nas hipóteses previstas no art. 16 da Lei nº 13.709, de 14 de agosto de 2018, que autorizem a conservação dos dados, sempre cientificando o controlador;

V - notificar o controlador em caso de ocorrência de incidente de segurança que possa acarretar risco, comprometimento ou dano potencial ou efetivo ao titular de dados pessoais;

VI - auxiliar o controlador a prestar informações sobre o tratamento de dados pessoais ao titular que as solicite;

VII - auxiliar o controlador a realizar a Avaliação de Impacto à Proteção de Dados Pessoais e a elaborar o Relatório de Impacto à Proteção de Dados Pessoais, quando solicitado, conforme disposto no art. 13 desta Portaria Normativa; e

VIII - promover, dentro da sua estrutura, ações de conscientização sobre o tratamento de dados pessoais junto aos seus colaboradores.

§ 3º É vedado ao operador decidir sobre o tratamento de dados pessoais sem a concordância do controlador, especialmente na definição:

I - das tecnologias de tratamento a serem utilizadas;

II - dos meios de armazenamento e de transferência;

III - da forma de arquivamento ou descarte; e

IV - da comunicação e do uso compartilhado.

Subseção IV

Dos demais responsáveis



Art. 11. Os membros, servidores, estagiários e terceirizados que possuem acesso a dados pessoais no desempenho de suas funções deverão assegurar a sua proteção, mesmo após o término do tratamento, observando as medidas técnicas e administrativas determinadas pelo controlador, tais como:

I - regras de armazenamento e descarte seguros dos documentos;

II - controles de acesso físico e lógicos aos documentos que contenham dados pessoais;

III - uso de senhas fortes;

IV - técnicas de anonimização e pseudonimização dos dados pessoais em documentos, como o tarjamento e a criptografia;

V - aposição de sigilo aos processos administrativos que ensejem classificação;

VI - tratamento apenas dos dados estritamente necessários para o desempenho de seus processos de trabalho;

VII - bloqueio de tela do computador ao se ausentar da estação de trabalho presencial ou remota; e

VIII - cautela com documentos físicos que contenham dados pessoais e estejam acessíveis em cima de mesa, armário ou gaveteiro.

Parágrafo único. A Secretaria de Governança e Gestão Estratégica deverá elaborar orientações, cartilhas e informes direcionados aos responsáveis referidos no caput deste artigo, a respeito do tratamento dos dados pessoais, assegurada a sua proteção.

Seção III

Da documentação relacionada ao tratamento de dados pessoais

Subseção I

Dos inventários de dados pessoais

Art. 12. Todo tratamento de dados pessoais deverá ser registrado por meio do inventário de dados pessoais elaborado pelos líderes de privacidade referidos no art. 37 desta Portaria Normativa.



§ 1º Os registros serão realizados segundo modelo disponibilizado pelo controlador e conterão:

I - a identificação do serviço ou processo de negócio de tratamento de dados pessoais;

II - a identificação dos agentes de tratamento e do encarregado;

III - as fases do ciclo de vida do tratamento;

IV - a forma como os dados pessoais são coletados, retidos, armazenados, processados, usados, compartilhados e eliminados;

V - o escopo e a natureza dos dados pessoais;

VI - a finalidade do tratamento de dados pessoais;

VII - a categoria de dados pessoais tratados;

VIII - as categorias de dados pessoais sensíveis tratados;

IX - a frequência e a totalização das categorias de dados pessoais tratados;

X - as categorias dos titulares de dados pessoais;

XI - a existência de compartilhamento de dados pessoais;

XII - os controles de privacidade e de segurança da informação adotados;

XIII - a existência de transferência internacional de dados pessoais; e

XIV - os contratos de serviços e as soluções de tecnologia da informação que tratam dados pessoais.

§ 2º O inventário de dados pessoais deverá ser apresentado ao controlador e atualizado anualmente, conforme cronograma divulgado pelo controlador até o quinto dia útil do mês de fevereiro de cada ano.

§ 3º Caso surja novo processo de trabalho, os líderes de privacidade deverão elaborar inventário de dados pessoais e submeter ao controlador, ainda que fora do período estabelecido no § 2º deste artigo.

§ 4º A Equipe Técnica de Privacidade e Proteção de Dados Pessoais prevista no art. 36 desta Portaria Normativa deve averiguar a conformidade do tratamento registrado nos inventários de dados pessoais com a presente Portaria Normativa, a Lei nº 13.709, de 14 de agosto de 2018, e demais regras de tratamento de dados pessoais, manifestando-se pela sua aprovação ou reprovação.

§ 5º Em caso de reprovação do inventário de dados pessoais, a Equipe Técnica de Privacidade e Proteção de Dados Pessoais deverá reencaminhar o documento ao líder de privacidade responsável pela sua elaboração, indicando as correções que devem ser realizadas.

§ 6º O encarregado poderá solicitar ao controlador e aos líderes de privacidade informações sobre a elaboração dos inventários de dados pessoais.

Subseção II

Dos Relatórios de Impacto à Proteção de Dados Pessoais

Art. 13. O controlador coordenará a elaboração de Relatório de Impacto à Proteção de Dados Pessoais - RIPD.

§ 1º O RIPD será elaborado pela Equipe Técnica de Privacidade e Proteção de Dados Pessoais prevista no art. 36 desta Portaria Normativa, com apoio dos líderes de privacidade.

§ 2º O RIPD deverá ser elaborado nas seguintes hipóteses:

I - solicitação específica da Agência Nacional de Proteção de Dados;

II - tratamento de dados pessoais em larga escala, considerado:

a) o volume de dados envolvido;

b) a duração;

c) a frequência; e

d) extensão geográfica do tratamento;

III - tratamento de dados pessoais sensíveis, nos termos do art. 11 da Lei nº 13.709, de 14 de agosto de 2018, por exemplo, dados sobre:

a) origem racial ou étnica;

b) convicção religiosa;

c) opinião política;

d) filiação a sindicato ou a organização de caráter religioso, filosófico ou político;

e) dado referente à saúde ou à vida sexual; e

f) dado genético ou biométrico, quando vinculado a uma pessoa natural;

IV - tratamento de dados pessoais de pessoas vulneráveis, como:

a) crianças;

b) adolescentes;

c) pessoas idosas;

d) indígenas; e

e) quilombolas;

V - quando o único fundamento do tratamento for o legítimo interesse da Advocacia-Geral da União, nos termos do art. 10 da Lei nº 13.709, de 14 de agosto de 2018;

VI - implementação de tecnologias emergentes ou inovadoras, considerando-se as que ainda não sejam de uso comum na administração pública; e

VII - em outras hipóteses nas quais a existência de risco relevante ao titular de dados pessoais seja verificada pelo controlador.



§ 3º O RIPD deve seguir as orientações da Agência Nacional de Proteção de Dados e da Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos, e deverá conter:

- I - a identificação dos agentes de tratamento e do encarregado;
- II - a descrição da necessidade de elaborar o relatório;
- III - a descrição do tratamento, que deve incluir natureza, escopo, contexto e sua finalidade;
- IV - as partes interessadas consultadas;
- V - a necessidade e a proporcionalidade de elaboração do relatório;
- VI - a identificação e a avaliação dos riscos à proteção de dados pessoais; e
- VII - as medidas para tratar os riscos avaliados.

§ 4º O RIPD deve ser submetido ao controlador e ao encarregado para aprovação.

§ 5º Caso o encarregado ou o controlador decidam pela reprovação do RIPD, deverão reencaminhar o documento à Equipe Técnica de Privacidade e Proteção de Dados Pessoais, indicando as correções que devam ser realizadas.

Subseção III

Dos termos de consentimento e de responsabilidade e avisos de privacidade

Art. 14. Compete ao controlador, de ofício ou sob demanda de qualquer unidade que trate dados pessoais, verificar a necessidade e, se for o caso, redigir os seguintes documentos:

I - termos de consentimento, dispondo sobre o consentimento livre e informado do titular para o tratamento de seus dados pessoais com a delimitação do contexto e da finalidade;

II - termos de responsabilidade, estabelecendo a responsabilidade do terceiro que receberá dados pessoais compartilhados pela Advocacia-Geral da União; e

III - avisos de privacidade, alertando o titular sobre como o tratamento de dados pessoais será realizado em cada oferta de serviço.

Parágrafo único. Os documentos referidos no caput devem ser elaborados com o apoio das áreas solicitantes e de outras áreas responsáveis pela gestão de consentimento, pelo compartilhamento de dados pessoais, e pelo fornecimento do serviço em relação ao qual o documento se refere.

Seção IV

Do tratamento de dados pessoais em contextos específicos

Art. 15. O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse, tais como:

I - realização e documentação de teste de balanceamento, conforme modelo disponibilizado pela Agência Nacional de Proteção de Dados; e

II - publicação das hipóteses de tratamento de dados pessoais por legítimo interesse na página eletrônica da Advocacia-Geral da União, informando:

- a) justificativa;
- b) finalidade; e
- c) delimitação dos dados tratados.

Art. 16. O tratamento de dados pessoais de crianças e adolescentes deverá ser realizado em seu melhor interesse, a ser avaliado no caso concreto.

§ 1º O controlador deve orientar sobre as práticas adequadas para o tratamento de dados pessoais de crianças e adolescentes.

§ 2º O controlador divulgará as situações de tratamento de dados pessoais de crianças e adolescentes na página eletrônica da Advocacia-Geral da União informando:

- a) justificativa;
- b) finalidade; e



c) delimitação dos dados tratados.

Art. 17. A comunicação e o uso compartilhado de dados pessoais devem ocorrer somente para:

a) cumprimento de obrigações legais;

b) requisições legítimas de órgãos e entidades públicas; ou

c) elevar a efetividade e a celeridade do trabalho executado pela Advocacia-Geral da União, nos termos do art. 26 da Lei nº 13.709, de 14 de agosto de 2018.

§ 1º Nos casos em que o uso compartilhado se der com pessoa jurídica de direito privado o controlador deve informar:

I - à Agência Nacional de Proteção de Dados, nos termos do art. 27 da Lei nº 13.709, de 14 de agosto de 2018, e de sua regulamentação; e

II - ao Comitê de Governança da Advocacia-Geral da União.

§ 2º Nos casos em que for necessário o consentimento do titular, a comunicação e o uso compartilhado só serão possíveis caso haja consentimento específico e claro em termo de consentimento.

§ 3º Poderá haver compartilhamento de dados pessoais para fins acadêmicos, cabendo ao controlador providenciar, sempre que possível, a sua anonimização.

§ 4º Em qualquer caso, a comunicação e o uso compartilhado guardarão nexos com a finalidade original do acesso aos dados pessoais e com a legítima expectativa do titular.

Art. 18. A transferência internacional de dados pessoais somente ocorrerá nas hipóteses previstas no art. 33 da Lei nº 13.709, de 14 de agosto de 2018, notadamente para a cooperação jurídica internacional.

Seção V

Da gestão de riscos

Art. 19. Compete ao controlador definir a metodologia para a gestão de riscos no tratamento de dados pessoais, que deverá:

I - estabelecer critérios objetivos para identificação, avaliação e implementação das medidas técnicas e organizacionais necessárias à mitigação ou eliminação dos riscos à proteção de dados pessoais;

II - considerar o contexto, a escala, o escopo, as hipóteses, a base legal e as finalidades do tratamento;

III - abranger todos os sistemas, serviços e processos em que há tratamento de dados pessoais;

IV - considerar, no mínimo, o seguinte:

a) a natureza, a sensibilidade e o volume dos dados pessoais tratados;

b) o estado da técnica e os custos de implementação;

c) a probabilidade e a gravidade dos riscos a direitos e liberdades dos titulares;

d) a adoção de medidas técnicas e organizacionais que garantam a privacidade desde a concepção e por padrão; e

e) os mecanismos de auditoria, controle e transparência;

V - ser revisada periodicamente ou sempre que houver mudanças significativas nos processos de tratamento; e

VI - seguir, no que couber, a Política de Gestão de Riscos da Advocacia-Geral da União, a ser estabelecida em ato específico do Advogado-Geral da União.

Art. 20. Os órgãos previstos no art. 1º, § 1º, desta Portaria Normativa são responsáveis pela implementação e execução da metodologia de gestão de riscos no tratamento de dados pessoais referida no art. 19, devendo atuar em conjunto com o controlador:

I - no levantamento dos riscos; e

II - na definição e efetivação das medidas mitigadoras.



Art. 21. Os resultados do processo de gestão de riscos no tratamento de dados pessoais devem ser utilizados para orientar a tomada de decisões gerenciais, incluindo:

- I - alocação de recursos; e
- II - atribuição de responsabilidades.

Art. 22. A gestão de riscos deve constituir parte integrante e obrigatória do RIPD, previsto no art. 13 desta Portaria Normativa.

Art. 23. A Secretaria de Governança e Gestão Estratégica disponibilizará repositório de conhecimento na rede interna da Advocacia-Geral da União com condutas, recomendações e boas práticas destinadas a:

- I - aprimorar o gerenciamento de risco; e
- II - orientar as ações adequadas em caso de comprometimento de dados pessoais.

Seção VI

Do tratamento de violações de dados pessoais

Art. 24. Na hipótese de ocorrência de incidente de segurança que resulte em violação de dados pessoais, o controlador deverá:

I - comunicar à Agência Nacional de Proteção de Dados, por intermédio do encarregado, a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante ao titular dos dados pessoais, conforme procedimento e prazo determinado na Resolução CD/ANPD nº 15, de 24 de abril de 2024;

II - informar aos titulares a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante, conforme procedimento e prazo determinado na Resolução CD/ANPD nº 15, de 24 de abril de 2024; e

III - manter registro de todas as ocorrências de incidente de segurança, inclusive daqueles não comunicados à Agência Nacional de Proteção de Dados e aos titulares.

Parágrafo único. O registro das ocorrências de incidentes de segurança deve ser mantido pelo prazo mínimo de cinco anos, contado da data do registro, exceto se constatadas obrigações adicionais que demandem prazo maior de manutenção, sob decisão do controlador.

Art. 25. Para mitigar a ocorrência de incidente de segurança com dados pessoais, o controlador e os operadores devem atuar para adoção dos seguintes requisitos de proteção, sem prejuízo da adoção de outras medidas que considerarem necessárias:

I - adotar padrões compatíveis com os princípios previstos na Lei nº 13.709, de 14 de agosto de 2018, na concepção e no desenvolvimento de processos, produtos e serviços, incluindo:

- a) a privacidade por padrão; e
- b) a limitação da coleta de dados pessoais ao mínimo necessário para a realização de suas finalidades;

II - implementar mecanismos:

a) de controle de acesso aplicáveis a todos os usuários, com níveis de permissão definidos conforme a necessidade de utilização do sistema e de acesso a dados pessoais; e

b) que dificultem a transferência de dados pessoais de estações de trabalho para dispositivos de armazenamento externo, como unidades de armazenamento portáteis;

III - utilizar autenticação multifator para acessar sistemas ou base de dados que contenham dados pessoais;

IV - implementar soluções de pseudonimização e anonimização, como a criptografia, para cifrar dados pessoais;

V - permitir somente o uso dos sistemas e aplicativos institucionais para tratamento de dados pessoais, evitando a utilização de aplicações de uso pessoal para este fim;



VI - buscar instituir acordos de confidencialidade ou sigilo com os operadores dos dados pessoais; e

VII - armazenar documentos físicos ou digitais que contenham dados pessoais em ambiente seguro, de modo que terceiros não autorizados não possam acessá-los.

Art. 26. A resposta aos eventos e incidentes de segurança da informação que envolvam dados pessoais deve seguir:

I - as orientações da Agência Nacional de Proteção de Dados; e

II - o plano de resposta a incidentes de segurança da informação, previsto no art. 21, § 2º, da Portaria Normativa AGU nº 166, de 12 de março de 2025.

Art. 27. As violações das regras de proteção de dados pessoais serão registradas, analisadas e tratadas por meio da coleta de evidências, e de investigação e intermediação da comunicação entre a Advocacia-Geral da União, a Agência Nacional de Proteção de Dados e os titulares dos dados pessoais violados.

Parágrafo único. O controlador deverá comunicar à Polícia Federal ou ao Ministério Público os eventos ou incidentes de segurança da informação que envolvam dados pessoais quando identificados indícios de ocorrência de conduta que possa ensejar responsabilização criminal.

Art. 28. A Política de Proteção de Dados Pessoais da Advocacia-Geral da União deverá respeitar, no que couber, a Política de Segurança da Informação da Advocacia-Geral da União, instituída pela Portaria Normativa AGU nº 166, de 12 de março de 2025.

Seção VII

Dos contratos, convênios, acordos e instrumentos congêneres

Art. 29. Os contratos, convênios, acordos e instrumentos congêneres, que, de alguma forma, envolvam o tratamento de dados pessoais, deverão dispor de cláusulas específicas disciplinando as regras e os procedimentos para o tratamento, prevendo, no mínimo:

I - requisitos mínimos de segurança da informação e proteção de dados pessoais, especialmente os previstos no art. 25 desta Portaria Normativa;

II - obrigação do operador de não processar os dados pessoais para finalidades diversas das determinadas pelo controlador;

III - orientações para o operador sobre o armazenamento, a devolução ou o descarte seguro de dados pessoais após conclusão de serviço ou rescisão de qualquer contrato, mediante solicitação do controlador;

IV - diretrizes específicas sobre o uso de subcontratados pelo operador para execução contratual que envolva tratamento de dados pessoais;

V - obrigatoriedade de notificação entre as partes em caso de suspeita de incidentes que envolvam os dados pessoais compartilhados;

VI - restrição da transferência internacional de dados pessoais às hipóteses previstas no art. 33 da Lei nº 13.709, de 14 de agosto de 2018 com a obrigatoriedade de notificação entre as partes;

VII - previsão de penalidades em caso de descumprimento das cláusulas estabelecidas; e

VIII - necessidade de cumprimento desta Portaria Normativa, especialmente do disposto no art. 10.

§ 1º Nos casos de contratação de fornecedores por contratos de adesão, poderão ser elaborados termos de responsabilidade ou acordos de processamento de dados específicos para os serviços da Advocacia-Geral da União, contendo orientações de como deve ocorrer o tratamento dos dados pessoais.

§ 2º Eventuais alterações nos contratos, convênios, acordos e instrumentos congêneres serão implementadas nos contratos em vigor por meio de termo aditivo e, como padrão, nos novos contratos.

§ 3º A Consultoria-Geral da União deve atualizar os modelos de contratos, convênios, acordos e instrumentos congêneres conforme o disposto no caput.



Seção VIII

Do monitoramento contínuo

Art. 30. O cumprimento da Política de Proteção de Dados Pessoais da Advocacia-Geral da União deverá ser monitorado continuamente pela Secretaria de Governança e Gestão Estratégica.

§ 1º O monitoramento incluirá:

- I - verificações de conformidade e certificação dos requisitos de proteção de dados pessoais; e
- II - avaliação das cláusulas de responsabilidade e sigilo constantes de termos de responsabilidade, contratos, convênios, acordos e instrumentos congêneres.

§ 2º A Secretaria de Governança e Gestão Estratégica apresentará resultado do monitoramento da Política de Proteção de Dados Pessoais da Advocacia-Geral da União ao encarregado e ao Comitê de Governança Digital da Advocacia-Geral da União, a cada dois anos.

Seção IX

Da transparência e do acesso à informação

Art. 31. O titular dos dados pessoais poderá apresentar solicitações, reclamações e pedidos de esclarecimentos e informações por meio:

- I - da Plataforma Integrada de Ouvidoria e Acesso à Informação - Fala.BR;
- II - do endereço de correio eletrônico ouvidoriaagu@agu.gov.br; e
- III - da apresentação de manifestação verbal, que será reduzida a termo pela Ouvidoria, diretamente nos endereços da Advocacia-Geral da União.

Subseção I

Do Portal de Tratamento de Dados Pessoais

Art. 32. Fica instituído o Portal do Tratamento de Dados Pessoais, que deverá conter, de forma clara, simples e acessível, as seguintes informações:

- I - identificação da estrutura administrativa que exerce as funções do controlador e informações de contato deste;
- II - identidade e informações de contato do encarregado;
- III - avisos, orientações e consolidações de boas práticas;
- IV - situações de tratamento de dados pessoais pela Advocacia-Geral da União, com informações claras e atualizadas sobre sua previsão legal e finalidade, apresentando de forma destacada as seguintes situações:
 - a) tratamento de dados fundamentados no legítimo interesse;
 - b) tratamento de dados pessoais:
 - 1. sensíveis; e
 - 2. de crianças e adolescentes;
 - c) comunicação e uso compartilhado de dados pessoais; e
 - d) transferência internacional de dados pessoais;
- V - acesso à Plataforma Integrada de Ouvidoria e Acesso à Informação - Fala.Br, com orientações para o seu uso;
- VI - orientações sobre os direitos dos titulares;
- VII - delegações de competências do controlador e do encarregado com a:
 - a) especificação dos poderes transferidos; e
 - b) identificação e informações de contato do delegado;
- VIII - normas complementares à Política de Proteção de Dados Pessoais;



IX - ocorrência de incidentes de segurança que possam acarretar risco ou dano relevante aos dados pessoais custodiados pela Advocacia-Geral da União quando:

a) a divulgação for determinada pela Agência Nacional de Proteção de Dados; ou

b) não for possível identificar individualmente os titulares de dados pessoais afetados pelo incidente e sua comunicação seja essencial para redução dos danos;

X - resultado de monitoramento da Política de Proteção de Dados Pessoais da Advocacia-Geral da União previsto no art. 30, § 2º, desta Portaria Normativa;

XI - modelos de cláusulas relacionadas à Política de Proteção de Dados Pessoais da Advocacia-Geral da União para contratos, convênios, acordos e instrumentos congêneres;

XII - metodologia de avaliação de impacto à proteção de dados pessoais; e

XIII - outras informações definidas pelo controlador.

Art. 33. O controlador disponibilizará as informações referentes ao tratamento de dados pessoais à Assessoria de Comunicação para publicação no Portal do Tratamento de Dados Pessoais, constante do sítio eletrônico da Advocacia-Geral da União.

CAPÍTULO III

DA GOVERNANÇA DA PROTEÇÃO DE DADOS PESSOAIS

Seção I

Disposições gerais

Art. 34. A estrutura de governança da Política de Proteção de Dados Pessoais da Advocacia-Geral da União será composta por:

I - Comitê de Governança da Advocacia-Geral da União;

II - Equipe Técnica de Privacidade e Proteção de Dados Pessoais; e

III - Líderes de Privacidade.

Seção II

Do Comitê de Governança da Advocacia-Geral da União

Art. 35. Compete ao Comitê de Governança da Advocacia-Geral da União instituído pela Portaria Normativa AGU nº 165, de 12 de março de 2025:

I - aprovar:

a) as normas complementares à Política de Proteção de Dados Pessoais da Advocacia-Geral da União;

b) o Programa de Governança em Privacidade;

c) o Plano de Atendimento às Demandas dos Titulares de Dados Pessoais; e

d) os relatórios de acompanhamento da Política de Proteção de Dados Pessoais, previstos no art. 30, § 2º, desta Portaria Normativa; e

II - manifestar-se sobre outras questões relevantes para o tratamento de dados pessoais pela Advocacia-Geral da União, a critério do controlador e do encarregado.

Seção III

Da Equipe Técnica de Privacidade e Proteção de Dados Pessoais

Art. 36. Fica instituída a Equipe Técnica de Privacidade e Proteção de Dados Pessoais, vinculada à Secretaria de Governança e Gestão Estratégica.

§ 1º Os integrantes da Equipe Técnica de Privacidade e Proteção de Dados Pessoais serão designados em ato do Secretário de Governança e Gestão Estratégica, incluindo seu coordenador.

§ 2º Compete à Equipe Técnica de Privacidade e Proteção de Dados Pessoais, dentre outras atribuições determinadas pelo controlador:



I - coordenar a implementação de medidas para efetivação desta Portaria Normativa;

II - estabelecer processo de gestão de riscos de privacidade com vistas a:

a) minimizar possíveis impactos associados aos dados pessoais;

b) reduzir as vulnerabilidades; e

c) evitar ameaças;

III - analisar e responder as notificações e demandas relacionadas ao tratamento de dados pessoais, oferecendo suporte ao controlador e ao encarregado;

IV - participar das atividades da Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR, prevista no art. 50 da Portaria Normativa AGU nº 166, de 12 de março de 2025, sempre que o incidente envolver dados pessoais;

V - auxiliar o controlador na elaboração das minutas dos atos referidos no art. 8º, caput, inciso XX, desta Portaria Normativa;

VI - executar a análise de conformidade sobre os registros elaborados pelos líderes de privacidade;

VII - executar avaliações de impacto à privacidade e elaborar relatórios de impacto à proteção de dados pessoais, nos casos previstos no art. 13 desta Portaria Normativa;

VIII - promover a cooperação com outros órgãos e entidades públicas, bem como participar de fóruns e redes nacionais e internacionais relativos à privacidade e proteção de dados pessoais;

IX - receber comunicações de descumprimento da Política de Proteção de Dados Pessoais da Advocacia-Geral da União e adotar as providências necessárias; e

X - orientar o Departamento de Tecnologia da Informação quanto ao cumprimento das regras de proteção de dados pessoais na contratação e no uso de soluções de tecnologia da informação.

Seção IV

Dos líderes de privacidade

Art. 37. Os líderes de privacidade são responsáveis pela efetivação dos procedimentos previstos nesta Portaria Normativa no âmbito das suas respectivas unidades, devendo:

I - atuar como ponto focal de contato do controlador para prestar informações, auxiliar a solucionar possíveis incidentes e atender a demandas dos titulares;

II - orientar as pessoas que atuem na unidade quanto aos procedimentos adequados para o tratamento de dados pessoais;

III - elaborar o inventário de dados pessoais e auxiliar a Equipe Técnica de Privacidade e Proteção de Dados Pessoais na elaboração dos relatórios de impacto à proteção de dados pessoais; e

IV - fomentar a cultura de proteção de dados na unidade, fiscalizando e notificando o controlador sobre a ocorrência de irregularidades e oportunidades de melhoria.

§ 1º As seguintes unidades da Advocacia-Geral da União devem indicar, no mínimo, um líder de privacidade e seu respectivo suplente:

I - Gabinete do Advogado-Geral da União;

II - Ouvidoria;

III - Assessoria Especial de Comunicação Social;

IV - Secretaria de Controle Interno;

V - Secretaria-Geral de Consultoria;

VI - Secretaria de Governança e Gestão Estratégica;

VII - Secretaria de Gestão Administrativa;

VIII - Secretaria-Geral de Contencioso;

IX - Consultoria-Geral da União;



X - Corregedoria-Geral da Advocacia da União;

XI - Procuradoria-Geral da União;

XII - Procuradoria-Geral Federal; e

XIII - Escola Superior da Advocacia-Geral da União Ministro Victor Nunes Leal.

CAPÍTULO IV

DA DISSEMINAÇÃO DA CULTURA DE PROTEÇÃO DE DADOS PESSOAIS

Seção I

Das medidas de disseminação da cultura de proteção de dados pessoais

Art. 38. A Secretaria de Governança e Gestão Estratégica deve disseminar na Advocacia-Geral da União a cultura de proteção de dados pessoais por meio de medidas de conscientização e capacitação, que serão:

I - disponibilizadas para os membros, servidores, estagiários e demais agentes que possuem acesso a dados pessoais no desempenho de suas funções na Advocacia-Geral da União, conforme suas atribuições e responsabilidades;

II - implementadas em parceria com:

a) a Escola Superior da Advocacia-Geral da União Ministro Victor Nunes Leal; e

b) a Assessoria Especial de Comunicação Social.

§ 1º Além das medidas referidas no caput, fica facultada à Secretaria de Governança e Gestão Estratégica:

I - elaborar cartilhas e informativos com conceitos, orientações e exemplos pertinentes à atuação no tratamento de dados pessoais da Advocacia-Geral da União;

II - realizar capacitações personalizadas com repasse de conhecimento especializado e saneamento de dúvidas; e

III - criar grupo de estudos e debates sobre proteção de dados pessoais.

Seção II

Da Rede de Privacidade

Art. 39. Fica instituída a Rede de Privacidade, composta pelos líderes de privacidade referidos no art. 37 desta Portaria Normativa e coordenada pela Equipe Técnica de Privacidade e Proteção de Dados Pessoais com a função de auxiliar no fomento da cultura de proteção de dados pessoais por meio da:

I - disseminação das regras de proteção de dados pessoais;

II - participação em grupos de trabalho para aprimoramento da atuação da Advocacia-Geral da União na proteção de dados pessoais;

III - participação em debates e na elaboração de proposições para alterações da Política de Proteção de Dados Pessoais da Advocacia-Geral da União e de suas normas complementares, e

IV - organização de ações de conscientização, capacitação e sensibilização.

Parágrafo único. A relação dos membros da Rede de Privacidade será consolidada pelo Secretário de Governança e Gestão Estratégica.

CAPÍTULO V

DISPOSIÇÕES FINAIS

Art. 40. O membro, servidor, estagiário ou terceirizado a serviço da Advocacia-Geral da União observará Política de Proteção de Dados Pessoais da Advocacia-Geral da União e, em caso de ciência de descumprimento, comunicará a Equipe Técnica de Privacidade e Proteção de Dados Pessoais, pelos meios de contato disponibilizados no Portal do Tratamento de Dados Pessoais.



Art. 41. A Política de Proteção de Dados Pessoais da Advocacia-Geral da União deverá ser revisada sempre que as alterações de regulamentação e as atualizações tecnológicas assim determinarem, de forma a manter sua efetividade e atualidade, sob iniciativa do controlador.

Art. 42. O controlador deverá:

I - avaliar os processos, serviços e sistemas em uso pela Advocacia-Geral da União quanto ao cumprimento das determinações desta Portaria Normativa e adotar as providências necessárias para sua adequação; e

II - adaptar às determinações desta Portaria Normativa, no que couber, os inventários de dados pessoais e os relatórios de impacto à proteção de dados pessoais já elaborados e ainda em uso.

Art. 43. A Secretaria de Governança e Gestão Estratégica deverá propor minuta de Plano de Atendimento às Demandas dos Titulares de Dados Pessoais ao Comitê de Governança da Advocacia-Geral da União no prazo de cento e oitenta dias, contados da vigência desta Portaria Normativa.

Parágrafo único: O Plano referido no caput será disponibilizado por meio de manual com informações sobre:

I - os direitos dos titulares de dados pessoais perante a Advocacia-Geral da União;

II - a forma de exercício dos direitos dos titulares de dados pessoais e as etapas e os prazos para resposta às suas solicitações;

III - competências dos órgãos internos; e

IV - canais de comunicação.

Art. 44. A Portaria Normativa AGU nº 165, de 12 de março de 2025, passa a vigorar com a seguinte alteração:

"Art. 6º

.....

II -

.....

h) inovação;

i) governança de processos de trabalho; e

j) proteção de dados pessoais;

.....

IX - deliberar sobre medidas administrativas de governança corporativa, bem como sobre ferramentas e instrumentos utilizados para a consecução dos objetivos estratégicos;

X - exercer a função de:

a) Comitê de Governança Digital, nos termos do art. 5º do Decreto nº 12.198, de 24 de setembro de 2024, conforme dispuser portaria normativa específica do Advogado-Geral da União; e

b) Comitê de Segurança da Informação, nos termos do art. 15, caput, inciso IV, do Decreto nº 9.637, de 26 de dezembro de 2018, conforme dispuser portaria normativa específica do Advogado-Geral da União; e

XI - exercer as competências determinadas no art. 35 da Portaria Normativa AGU nº 226, de 15 de junho de 2026.

....." (NR)

Art. 45. A Portaria Normativa AGU nº 166, de 12 de março de 2025, passa a vigorar com a seguinte alteração:

"Art. 21-A. A gestão de incidentes de segurança da informação que envolvam dados pessoais deve seguir o disposto na Portaria Normativa AGU nº 226, de 15 de junho de 2026." (NR)

Art. 46. Esta Portaria Normativa entra em vigor na data de sua publicação.



Este conteúdo não substitui o publicado na versão certificada.

