

DIÁRIO OFICIAL DA UNIÃO

Publicado em: 28/03/2025 | Edição: 60 | Seção: 1 | Página: 10
Órgão: Ministério da Ciência, Tecnologia e Inovação/Observatório Nacional

PORTARIA ON Nº 257, DE 27 DE MARÇO DE 2025

Institui a Política de Proteção de Dados Pessoais do Observatório Nacional.

O DIRETOR DO OBSERVATÓRIO NACIONAL, no uso de suas atribuições estabelecidas no Regimento Interno, aprovado pela Portaria MCTI nº 7.064, de 24 de maio de 2023, e tendo em vista o art. 50 da Lei nº 13.709, de 14 de agosto de 2018, resolve:

Art. 1º Esta Portaria institui a Política de Proteção de Dados Pessoais - PPDP do Observatório Nacional, na forma do anexo.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

JAILSON SOUZA DE ALCANIZ

ANEXO

POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS DO OBSERVATÓRIO NACIONAL

CAPÍTULO I

Das disposições gerais

Art. 1º Fica instituída a Política de Proteção de Dados Pessoais - PPDP, do Observatório Nacional - ON, com a finalidade de estabelecer princípios e diretrizes para a implementação de ações que garantam a proteção de dados pessoais no âmbito interno e, no que couber, no relacionamento com outras entidades públicas ou privadas.

Parágrafo único. A PPDP está em consonância com o Programa de Privacidade e Segurança da Informação - PPSI do Observatório Nacional.

Art. 2º Esta Política regula a proteção de dados pessoais das quais o ON é o agente de tratamento, bem como o meio utilizado para este tratamento, seja digital ou físico, além de qualquer pessoa que realize operações de tratamento de dados pessoais em seu nome ou em suas dependências.

Art. 3º Esta Política aplica-se a todas as unidades organizacionais do ON e deverá ser observada por todos os usuários de informação, sejam servidores ou equiparados, empregados, prestadores de serviços ou pessoas habilitadas pela administração, por meio da assinatura de Termo de Responsabilidade, para acessar os ativos de informação sob responsabilidade do ON.

Art. 4º A aplicação desta Política será pautada pelo dever de boa-fé e pela observância dos princípios previstos no art. 6º da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD).

CAPÍTULO II

Das Definições

Art. 5º Para efeitos da implementação desta Política são consideradas as seguintes definições:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - dado pessoal sensível: dado pessoal sobre 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, quando vinculado a uma pessoa natural;

III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;



IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza operações de tratamento de dados pessoais em nome do controlador;

VIII - encarregado pelo tratamento de dados pessoais: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados pessoais e a autoridade nacional;

IX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional;

X - agentes de tratamento: o controlador e o operador;

XI - comitê de proteção de dados pessoais: órgão colegiado interno responsável por promover e fiscalizar a implementação da PPDP;

XII - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

XIII - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

XIV - consentimento: manifestação livre, informada e inequívoca, pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

XV - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

XVI - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

XVII - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o País seja membro;

XVIII - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos ou entidades públicas, no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

XIX - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

XX - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta, ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

Parágrafo único. Definições adicionais constam da Portaria GSI/PR nº 93, de 18 de outubro de 2021.

CAPÍTULO III

Dos objetivos e responsabilidades

Art. 6º São objetivos específicos da PPDP:



I - estabelecer medidas eficazes para o cumprimento das normas de proteção de dados pessoais e demonstrar a eficácia das mesmas;

II - estabelecer revisões de processos com o objetivo de aferir a diminuição ou aumento de riscos que envolvem o tratamento de dados pessoais;

III - promover a administração dos dados pessoais coletados e tratados, em qualquer meio, físico ou digital, custodiados ou sob orientação direta ou indireta do ON, de acordo com as diretrizes especificadas;

IV - estabelecer a necessidade de criar e manter um registro de todas as operações de tratamento de dados pessoais realizados;

V - promover a adequada gestão do tratamento dos dados pessoais;

VI - promover a criação de programas de treinamento e conscientização para que os colaboradores entendam suas responsabilidades e procedimentos na proteção de dados pessoais; e

VII - promover a formulação regras de segurança, de boas práticas e de governança com objetivo de definir procedimentos e outras ações referentes a privacidade e proteção de dados pessoais.

Art. 7º São responsabilidades do ON:

I - atender ao disposto nos normativos e publicações da Autoridade Nacional de Proteção de Dados Pessoais - ANPD que disciplinam o tratamento e a governança dos dados pessoais;

II - elaborar, quando couber, o Relatório de Impacto de Proteção de Dados Pessoais - RIPD relacionado às operações de tratamento e atualizá-lo quando necessário; e

III - realizar o desenvolvimento e a atualização das políticas e avisos de privacidade, que têm por finalidade o fornecimento de informações sobre o tratamento de dados pessoais em cada ambiente físico ou virtual, bem como, especificar as medidas de proteção de dados adotadas para salvaguardar esses dados pessoais.

CAPÍTULO IV

Do tratamento de dados pessoais

Art. 8º O tratamento de dados pessoais deve ser sempre realizado para o atendimento de sua finalidade pública, conforme o interesse público, com o objetivo de executar competências legais e de cumprir as atribuições legais do serviço público.

Art. 9º O ON deve adotar mecanismos para que os titulares de dados pessoais usufruam dos direitos assegurados pela LGPD e os normativos correlatos e disponibilizar canais de atendimento para garantir esses direitos.

Art. 10. O ON registrará e gravará as preferências e navegações realizadas nas respectivas páginas para fins estatísticos e de melhoria dos serviços ofertados, através de arquivos (cookies), respeitando o consentimento do titular.

Art. 11. O tratamento de dados pessoais sensíveis deve ocorrer somente nos termos da seção II do capítulo II da LGPD e deverão ser estabelecidos procedimentos de segurança no tratamento destes dados, conforme orientações da LGPD e demais normativos.

Art. 12. O tratamento de dados pessoais de crianças e de adolescentes deve ser realizado nos termos da seção III do capítulo II da LGPD, bem como pode ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da mesma Lei, desde que observado e prevalecente o seu melhor interesse, a ser avaliado, no caso concreto, nos termos do art. 14 da Lei.

Art. 13. O uso compartilhado de dados pessoais deve ocorrer em estrita observância ao art. 26 da LGPD.

Parágrafo Único. As operações remanescentes de uso compartilhado de dados devem seguir o disposto no art. 27 da LGPD.

Art. 14. A transferência internacional de dados pessoais deve observar o disposto no capítulo V da LGPD.

CAPÍTULO V



Da conscientização, capacitação e sensibilização

Art. 15. O servidor ou equiparado, empregado, prestador de serviços ou pessoa habilitada pela administração do ON, com acesso a dados pessoais, devem participar de programas de conscientização, capacitação e sensibilização em matérias de privacidade e proteção de dados pessoais, objetivando adequar o tema aos seus papéis e responsabilidades.

CAPÍTULO VI

Da segurança e boas práticas

Art. 16. Considerando a necessidade de mitigar incidentes com dados pessoais, devem ser adotadas as seguintes medidas técnicas e organizacionais de privacidade e proteção de dados:

I - o acesso aos dados pessoais deve estar limitado as pessoas que realizam o tratamento.

as funções e responsabilidades dos colaboradores envolvidos nos tratamentos de dados pessoais devem ser claramente estabelecidas e comunicadas;

II - devem ser estabelecidos acordos de confidencialidade, termos de responsabilidade ou termos de sigilo com operadores de dados pessoais; e

III - todos os dados pessoais devem estar armazenados em ambiente seguro, de modo que terceiros não autorizados não possam acessá-los.

Art. 17. Qualquer ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos dados pessoais dos titulares deve ser comunicada à ANPD, dentro do prazo previsto pela LGPD.

Art. 18. O ON deve manter uma base de conhecimento, com documentos que apresentam condutas e recomendações que melhoram o gerenciamento de risco e orientam na tomada de decisões adequadas em casos de comprometimento de dados pessoais.

CAPÍTULO VII

Da auditoria e conformidade

Art. 19. O cumprimento desta Política, bem como dos normativos que a complementam, deve ser avaliado periodicamente por meio de verificações de conformidade, buscando a certificação do cumprimento dos requisitos de privacidade e proteção de dados pessoais e da garantia das cláusulas de responsabilidade e sigilo constantes de termos de responsabilidade, contratos, convênios, acordos e instrumentos congêneres.

Art. 20. As atividades e serviços desenvolvidos no ON devem observar os requisitos de privacidade e proteção de dados pessoais constantes de leis, regulamentos, resoluções, normas, estatutos e contratos jurídicos vigentes para estarem em conformidade.

Art. 21. Os resultados de cada ação de verificação de conformidade devem ser documentados em relatório de avaliação de conformidade.

CAPÍTULO VIII

Das funções e competências

Art. 22. Qualquer pessoa natural ou jurídica, de direito público ou privado, que tenha interação em qualquer fase do tratamento de dados pessoais, deve assegurar a privacidade e a proteção de dados pessoais que trata, mesmo após o término do tratamento, observando as medidas técnicas e administrativas determinadas pelo ON.

Art. 23. Compete ao Comitê de Proteção de Dados Pessoais - CPDP:

I - promover a proteção de dados pessoais e a adequação do ON à LGPD;

II - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre proteção de dados pessoais;

III - participar da elaboração da PPDP e das demais normas internas de privacidade e proteção de dados pessoais, além de propor atualizações e alterações nestes dispositivos;

IV - gerenciar a implementação da LGPD dentro da organização e a administração da PPDP;



V - incentivar a conscientização, capacitação e sensibilização das pessoas que desempenham qualquer atividade de tratamento de dados pessoais dentro do ON; e

VI - fiscalizar o cumprimento da PPDP.

§ 1º A CPDP poderá expedir instruções complementares, no âmbito de suas competências, detalhando suas particularidades e procedimentos, relativas à proteção de dados pessoais, alinhadas às diretrizes emanadas pelo próprio CPDP e aos respectivos Planos Estratégicos Institucionais do ON.

§ 2º A composição e funcionamento do CPDP serão definidos em norma específica.

Art. 24. Compete ao controlador:

I - observar os fundamentos, princípios da privacidade e proteção de dados pessoais e os deveres impostos pela LGPD e por normativos correlatos no momento de decidir sobre um futuro tratamento ou realizá-lo;

II - considerar o preconizado pelos arts. 7º, 11 e 23 da LGPD antes de realizar o tratamento de dados pessoais;

III - cumprir o previsto pelos arts. 46 e 50 da LGPD buscando à proteção de dados pessoais e sua governança;

IV - indicar um encarregado pelo tratamento de dados pessoais, divulgando a identidade e as informações de contato do encarregado de forma clara e objetiva, preferencialmente no sítio institucional;

V - elaborar o inventário de dados pessoais a fim de manter registros das operações de tratamento de dados pessoais;

VI - reter dados pessoais somente pelo período necessário para o cumprimento da hipótese legal e finalidade utilizadas como justificativa para o tratamento de dados pessoais;

VII - criar e manter atualizados os avisos ou políticas de privacidade, que informarão sobre os tratamentos de dados pessoais realizados em cada ambiente físico ou virtual, e como os dados pessoais neles tratados são protegidos; e

VIII - requerer do titular a ciência com o termo de uso para cada serviço ofertado, informatizado ou não, que trate dados pessoais.

§ 1º A responsabilidade pelas decisões relacionadas ao tratamento de dados pessoais é do ON que, no exercício das atribuições típicas de controlador, determina as medidas necessárias para executar a PPDP dentro de sua estrutura organizacional.

§ 2º É vedado qualquer tratamento de dados pessoais para fins não relacionados com as atividades desenvolvidas pelo ON, ou por pessoa não autorizada formalmente pelo ON.

Art. 25. Compete ao operador:

I - observar os princípios estabelecidos no art. 6º da LGPD, ao realizar tratamento de dados pessoais;

II - seguir as diretrizes estabelecidas pelo controlador; e

III - antes de efetuar o tratamento, verificar se as diretrizes estabelecidas pelo controlador cumprem os requisitos legais presentes nos arts. 7º, 11 e 23 da LGPD.

§ 1º Quaisquer fornecedores de produtos ou serviços que, por algum motivo, realizem o tratamento de dados pessoais a eles confiados, são considerados operadores e devem seguir as diretrizes estabelecidas nesta Política.

§ 2º Não é competência do operador decidir unilateralmente quanto aos meios e finalidades utilizados para o tratamento de dados pessoais.

Art. 26. Compete ao encarregado pelo tratamento de dados pessoais:

I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II - receber comunicações e requisições da ANPD e adotar providências;



III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Parágrafo único: Ao receber comunicações da ANPD, o encarregado adotará as medidas necessárias para o atendimento da solicitação e para o fornecimento de informações pertinentes, dentre outras:

I - encaminhar internamente a demanda para as unidades competentes;

II - fornecer orientação e a assistência necessárias ao agente de tratamento; e

III - indicar expressamente o representante do agente de tratamento perante a ANPD para fins de atuação em processos administrativos, quando esta função não for exercida pelo próprio encarregado.

Art. 27. O encarregado pelo tratamento de dados pessoais prestará assistência e orientação ao agente de tratamento na elaboração, definição, e implementação de:

I - o registro e comunicação de incidente de segurança;

II - o registro das operações de tratamento de dados pessoais;

III - o relatório de impacto à proteção de dados pessoais;

IV - mecanismos internos de supervisão e de mitigação de riscos relativos ao tratamento de dados pessoais;

V - medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;

VI - processos e políticas internas que assegurem o cumprimento da LGPD, e dos regulamentos e orientações da ANPD;

VII - instrumentos contratuais que disciplinem questões relacionadas ao tratamento de dados pessoais;

VIII - transferências internacionais de dados;

IX - regras de boas práticas e de governança e de programa de governança em privacidade, nos termos do art. 50 da LGPD.

X - produtos e serviços que adotem padrões de design compatíveis com os princípios previstos na LGPD, incluindo a privacidade por padrão e a limitação da coleta de dados pessoais ao mínimo necessário para a realização de suas finalidades; e

XI - outras atividades e tomada de decisões estratégicas referentes ao tratamento de dados pessoais.

Art. 28. Compete ao agente de tratamento:

I - prover os meios necessários para o exercício das atribuições do encarregado, neles compreendidos, entre outros, recursos humanos, técnicos e administrativos;

II - solicitar assistência e orientação do encarregado quando da realização de atividades e tomada de decisões estratégicas referentes ao tratamento de dados pessoais;

III - garantir ao encarregado a autonomia técnica necessária para cumprir suas atividades, livre de interferências indevidas, especialmente na orientação a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;

IV - assegurar aos titulares meios céleres, eficazes e adequados para viabilizar a comunicação com o encarregado e o exercício de direitos; e

V - garantir ao encarregado acesso direto às pessoas de maior nível hierárquico dentro da organização, aos responsáveis pela tomada de decisões estratégicas que afetem ou envolvam o tratamento de dados pessoais, bem como às demais áreas da organização.

CAPÍTULO IX



Dos contratos, convênios, acordos e instrumentos congêneres

Art. 29. Os contratos, convênios, acordos e instrumentos similares atualmente em vigor e que, de alguma forma, envolvam o tratamento de dados pessoais, precisam incorporar cláusulas específicas em total conformidade com a presente PPDP, que contemplem minimamente:

I - requisitos mínimos de segurança da informação;

II - determinação de que o operador não processe os dados pessoais para finalidades que divergem da finalidade principal informada pelo controlador;

III - requisitos de proteção de dados pessoais que os operadores de dados pessoais devem atender;

IV - condições sob as quais o operador deve devolver ou descartar com segurança os dados pessoais após a conclusão do serviço, rescisão de qualquer contrato ou de outra forma mediante solicitação do controlador; e

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

Art. 30. O ON deve adotar medidas rigorosas com o propósito de assegurar que os terceiros e processadores de dados pessoais contratados estejam plenamente em conformidade com as cláusulas contratuais estabelecidas, no momento da celebração do acordo entre as partes envolvidas.

CAPÍTULO X

Das penalidades

Art. 31. Ações que violem esta Política poderão acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurados aos envolvidos o contraditório e a ampla defesa.

Art. 32. Casos de descumprimento desta Política serão registrados e comunicados ao CPDP para ciência e tomada das providências cabíveis.

CAPÍTULO XI

Das disposições finais

Art. 33. As dúvidas sobre a aplicação desta Política e seus documentos correlatos serão submetidas à deliberação pelo CPDP.

Art. 34. Os casos omissos serão resolvidos pelo CPDP.

Art. 35. Esta Política será revisada no prazo de 5 (cinco) anos, a partir do início de sua vigência.

Este conteúdo não substitui o publicado na versão certificada.

