

PORTARIA DA SENASP Nº 191, DE 10.11.2020

Institui a Política Geral de Privacidade e Proteção de Dados Pessoais no âmbito da Secretaria Nacional de Segurança Pública do Ministério da Justiça e Segurança Pública.

O SECRETÁRIO NACIONAL DE SEGURANÇA PÚBLICA, no uso das atribuições que lhe foram conferidas pela Portaria nº 77, de 17 de janeiro de 2020, publicada no DOU nº 13, Seção 1, Página 70, de 20/01/2020, combinado com o art. 74, VIII, do Regimento Interno da Secretaria Nacional de Segurança Pública, aprovado pela Portaria nº 151, de 26 de setembro de 2018, do Ministro de Estado da Justiça, publicada no DOU nº 200, Seção 1, Páginas 45-51, de 17/10/2018, e tendo em vista o disposto na Lei 13.709, de 14 de agosto de 2018; na Lei nº 13.675, de 11 de junho de 2018; no Decreto 9.489, de 30 de agosto de 2018; e no Decreto nº 9.876, de 17 de junho de 2019.

CONSIDERANDO que o Controlador é toda pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, nos termos do artigo 5º, inciso VI da Lei 13.709, de 14 de agosto de 2018;

CONSIDERANDO que na Administração Pública, o Controlador é a pessoa jurídica do órgão ou entidade pública sujeita à Lei, representada pela autoridade imbuída de adotar as decisões acerca do tratamento de tais dados.

CONSIDERANDO que Operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador, aí incluídos agentes públicos no sentido amplo que exerçam tal função, bem como pessoas jurídicas diversas daquela representada pelo Controlador, que exerçam atividade de tratamento no âmbito de contrato ou instrumento congênere.

CONSIDERANDO que a Secretaria Nacional de Segurança Pública trata dados pessoais e informações no exercício de suas competências constitucionais, legais e regulamentares e que essas informações devem atender aos padrões de integridade, disponibilidade, confidencialidade, confiabilidade, tempestividade dos sistemas informatizados do Governo Federal, interoperabilidade entre os sistemas eletrônicos governamentais e, quando for o caso, com sigilo resguardado;

CONSIDERANDO o descrito no Art. 35, Seção III da Lei nº 13.675, de 11 de junho de 2018, que determina que o Sistema Nacional de Informações de Segurança Pública, Prisionais e de Rastreabilidade de Armas e Munições, e sobre Material Genético, Digitais e Drogas (Sinesp) tem por finalidade armazenar, tratar e integrar dados e informações dos integrantes do Sistema Único de Segurança Pública (Susp) para auxiliar na formulação, implementação, execução, acompanhamento e avaliação das políticas relacionadas com:

I - segurança pública e defesa social;

II - sistema prisional e execução penal;

III - rastreabilidade de armas e munições;

IV - banco de dados de perfil genético e digitais;

V - enfrentamento do tráfico de drogas ilícitas. CONSIDERANDO que o Sinesp tem por objetivos:

I - proceder à coleta, análise, atualização, sistematização, integração e interpretação de dados e informações relativos às políticas de segurança pública e defesa social;

II - disponibilizar estudos, estatísticas, indicadores e outras informações para auxiliar na formulação, implementação, execução, monitoramento e avaliação de políticas públicas;

III - promover a integração das redes e sistemas de dados e informações de segurança pública e defesa social, criminais, do sistema prisional e sobre drogas;

IV - garantir a interoperabilidade dos sistemas de dados e informações, conforme os padrões definidos pelo conselho gestor.

CONSIDERANDO que a integração das informações e dos dados de segurança pública dos órgãos integrantes do Sistema Único de Segurança Pública (Susp) é de responsabilidade do Sinesp, conforme Artigo 10, inciso VI, Seção II da Lei nº 13.675, de 11 de junho de 2018, cabendo a sua padronização e categorização;

CONSIDERANDO que as informações nos sistemas integrantes da plataforma Sinesp, no âmbito da Secretaria Nacional de Segurança Pública, são armazenadas em diferentes formas, veiculadas por meios físicos e eletrônicos, portanto vulneráveis a incidentes de segurança da informação envolvendo a privacidade de dados pessoais como vazamentos, ataques cibernéticos, acessos não autorizados, mau uso, extravio, sequestro de dados etc.;

CONSIDERANDO que a Política Geral de Privacidade e Proteção de Dados Pessoais (PGPPDP), compreende um conjunto de ações determinadas pela Lei 13.709, de 14 de agosto de 2018, inclusive especificamente no tocante ao tratamento de dados pessoais pelo poder público, que buscam proteger e preservar a privacidade e proteção de dados pessoais e os ativos de informação, assegurando-lhes disponibilidade, integridade, confidencialidade e autenticidade;

CONSIDERANDO a necessidade de aprimorar a interoperabilidade, eficiência, eficácia e efetividade na elaboração, tramitação, utilização e destinação dos documentos, processos e informações produzidas e recebidas pelos órgãos e entidades pertencentes à Administração Pública;

CONSIDERANDO a vantajosidade de utilizar meios eletrônicos para realização dos processos administrativos com segurança, transparência e economicidade, aumentando a produtividade e celeridade na tramitação de processos, ampliando a sustentabilidade ambiental com o uso da tecnologia da informação e comunicação, propiciando a satisfação do público usuário;

CONSIDERANDO a importância da adoção de boas práticas relacionadas à privacidade e proteção de dados pessoais e informações no âmbito da Administração Pública Federal, às quais a Política Geral de Privacidade e Proteção de Dados Pessoais (PGPPDP) deverá estar alinhada;

[Leia a íntegra da Portaria](#)