

Política de Proteção de Dados Pessoais

Laboratório Nacional de Astrofísica

Ministério da Ciência, Tecnologia e Inovação

1. Objetivos

A Política de Proteção de Dados Pessoais tem por objetivo estabelecer diretrizes, princípios e conceitos a serem seguidos por todas as pessoas e entidades que se relacionam com o Laboratório Nacional de Astrofísica (LNA) que em algum momento realizam operações de tratamento de dados pessoais, visando o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD) e outras normas vigentes.

2. Escopo

Instituir a Política de Proteção de Dados Pessoais (PPDP), no âmbito do LNA, com a finalidade de estabelecer princípios e diretrizes para a implementação de ações que garantam a proteção de dados pessoais, e no que couber, no relacionamento com outras entidades públicas ou privadas.

Esta Política regula a proteção de dados pessoais, em que o LNA 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.

3. Termos e Definições

Glossário

AGENTES DE TRATAMENTO: o controlador e o operador.

CONTROLADOR: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

OPERADOR: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

ENCARREGADO: pessoa indicada pelo controlador e operador, para atuar como canal de comunicação entre o controlador, os titulares dos dados pessoais e a Autoridade Nacional de Proteção de Dados (ANPD).

DADO PESSOAL: informação relacionada a pessoa natural identificada ou identificável.

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.

TITULAR: pessoa natural a quem se referem os dados pessoais que são objetos de tratamento.

TRANSFERÊNCIA INTERNACIONAL DE DADOS: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

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.

USO COMPARTILHADO DE DADOS: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais.

4. Declarações da PPDP/LNA

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

Art. 2º. Esta Política de Proteção de Dados Pessoais aplica-se a todas as unidades organizacionais do LNA, e deverá ser observada por todos os usuários de informação, seja servidor ou equiparado, empregado, prestador de serviços ou pessoa habilitada pela administração, por meio da assinatura de Termo de Responsabilidade.

Art. 3º. 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 I - DAS DISPOSIÇÕES GERAIS

Art. 4º São objetivos da Política de Proteção de Dados Pessoais:

- 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 LNA;
- 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;
- VII - promover a formulação de 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. 5º. O LNA 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. 6º São responsabilidades do LNA:

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) relacionados às operações de tratamento, e atualizá-lo quando necessário;

III - realizar o desenvolvimento e a atualização das políticas/avisos de privacidade, que tem por finalidade o fornecimento de informações sobre o tratamento de dados pessoais em cada ambiente físico ou virtual.

CAPÍTULO II - TRATAMENTO DE DADOS PESSOAIS

Art. 7º. 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. 8º. As unidades organizacionais do LNA devem adotar mecanismos para que os titulares de dados pessoais usufruam dos direitos assegurados pela LGPD e normativos correlatos.

Art. 9º. O tratamento de dados pessoais sensíveis deve ocorrer somente nos termos da seção II do capítulo II da LGPD e são estabelecidos procedimentos de segurança no tratamento destes dados conforme orientações da LGPD e demais normativos.

Art. 10. O tratamento de dados pessoais de crianças e de adolescentes deve ser realizado nos termos da seção III do capítulo II da LGPD, desde que observado e prevalecente o seu melhor interesse.

Art. 11. O uso compartilhado de dados pessoais deve ocorrer em estrita observância ao art. 26 da LGPD. As operações remanescentes de uso compartilhado de dados devem seguir o disposto no Art. 27 da LGPD.

Art. 12. A transferência internacional de dados pessoais deve observar o disposto no Capítulo V da LGPD.

CAPÍTULO III - CONSCIENTIZAÇÃO, CAPACITAÇÃO E SENSIBILIZAÇÃO

Art. 13. Os servidores do LNA 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 IV - SEGURANÇA E BOAS PRÁTICAS

Art. 14. Considerando a necessidade de mitigar incidentes com dados pessoais, devem ser adotadas as seguintes medidas técnicas e organizacionais:

I - o acesso aos dados pessoais deve estar limitado às pessoas que realizam o tratamento;

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

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

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

Art. 15. Qualquer ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos dados pessoais dos titulares deve ser comunicada à Autoridade Nacional de Proteção de Dados (ANPD) dentro do prazo previsto pela LGPD.

Art. 16. As unidades organizacionais do LNA devem 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 V - AUDITORIA E CONFORMIDADE

Art. 17. O cumprimento desta Política, bem como dos normativos que a complementam devem ser avaliados periodicamente por meio de verificações de conformidade, buscando a certificação do cumprimento dos requisitos de privacidade e proteção de dados pessoais.

Art. 18. As atividades, produtos e serviços desenvolvidos no LNA 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. 19. Os resultados de cada ação de verificação de conformidade devem ser documentados em relatório de avaliação de conformidade.

CAPÍTULO VI - FUNÇÕES E RESPONSABILIDADES

Art. 20. 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 LNA.

Art. 21. Compete ao Comitê de Proteção de Dados Pessoais (CPDP) ou estrutura equivalente (a ser implementada):

- I - promover a proteção de dados pessoais e a adequação do LNA 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 Política de Proteção de Dados Pessoais e das demais normas internas de privacidade e proteção de dados pessoais, além de propor atualizações e alterações;
- IV - a responsabilidade por gerenciar a implementação da LGPD dentro da organização e a administração da Política de Proteção de Dados Pessoais;
- V - incentivar a conscientização, capacitação e sensibilização das pessoas que desempenham qualquer atividade de tratamento de dados pessoais dentro do LNA.

Art. 22. O Comitê de Proteção de Dados Pessoais (CPDP) ou estrutura equivalente, a ser implementada, é constituído no mínimo por:

- I - gestor de Segurança da Informação;
- II - o encarregado pelo tratamento de dados pessoais;
- III - um representante do departamento de tecnologia da informação;
- IV - um representante da ouvidoria;
- V - um representante de cada unidade finalística.

Art. 23. A presidência do Comitê de Proteção de Dados Pessoais (CPDP) ou estrutura equivalente, a ser implementada será exercida pelo titular/representante da Diretoria do LNA.

Art. 24. A responsabilidade pelas decisões relacionadas ao tratamento de dados pessoais é do LNA que no exercício das atribuições típicas de controlador determina as medidas necessárias para executar a Política de Proteção de Dados Pessoais dentro de sua estrutura organizacional.

Art. 25. 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;
- II - considerar o preconizado pelos art. 7º, art. 11 e art. 23 antes de realizar o tratamento de dados pessoais;
- III - cumprir o previsto pelos art. 46 e art. 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;
- VII - criar e manter atualizados os avisos ou políticas de privacidade;
- VIII - requerer do titular a ciência com o termo de uso para cada serviço ofertado que trate dados pessoais.

§ 1º É vedado qualquer tratamento de dados pessoais para fins não relacionados com as atividades desenvolvidas pela organização ou por pessoa não autorizada formalmente pelo LNA.

Art. 26. São considerados operadores de dados pessoais as pessoas naturais ou jurídicas de direito público ou privado, que realizam operações de tratamento de dados pessoais em nome do controlador. Quaisquer fornecedores de produtos ou serviços que realizam o tratamento de dados pessoais a eles confiados são considerados operadores.

Art. 27. 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;

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

Art. 28. Compete ao encarregado de proteção de dados:

- I - receber reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- II - receber comunicações e requisições da ANPD e adotar providências;
- III - orientar os colaboradores da organização a respeito das práticas a serem adotadas em relação à proteção de dados pessoais;
- IV - executar as demais atribuições determinadas pelo agente de tratamento ou estabelecidas em normas complementares.

Art. 29. O encarregado de proteção de dados prestará assistência e orientação ao agente de tratamento na elaboração, definição, e implementação de:

- I - registro e comunicação de incidente de segurança;
- II - registro das operações de tratamento de dados pessoais;
- III - relatório de impacto à proteção de dados pessoais;
- IV - mecanismos internos de supervisão e de mitigação de riscos;
- V - medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais;
- VI - processos e políticas internas que assegurem o cumprimento da LGPD;
- 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;
- X - produtos e serviços que adotem padrões de design compatíveis com os princípios previstos na LGPD;
- XI - outras atividades e tomada de decisões estratégicas referentes ao tratamento de dados pessoais.

Art. 30. Compete ao agente de tratamento:

- I - prover os meios necessários para o exercício das atribuições do encarregado, incluindo 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;
- IV - assegurar aos titulares meios céleres, eficazes e adequados para viabilizar a comunicação com o encarregado e o exercício de direitos;
- V - garantir ao encarregado acesso direto às pessoas de maior nível hierárquico dentro da organização.

CAPÍTULO VII - CONTRATOS, CONVÊNIOS, ACORDOS E INSTRUMENTOS CONGÊNERES

Art. 31. Os contratos, convênios, acordos e instrumentos similares atualmente em vigor, que de alguma forma envolvam o tratamento de dados pessoais, precisam incorporar cláusulas específicas em total conformidade com a presente Política de Proteção de Dados Pessoais e 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;
- V - diretrizes específicas sobre o uso de subcontratados pelo operador para execução contratual que envolva tratamento de dados pessoais.

Art. 32. As unidades organizacionais do LNA devem 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.

CAPÍTULO VIII - PENALIDADES

Art. 33. Ações que violem a Política de Proteção de Dados Pessoais 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. 34. Casos de descumprimento desta Política serão registrados e comunicados ao responsável para ciência e tomada das providências cabíveis.

CAPÍTULO IX - DISPOSIÇÕES FINAIS

Art. 35. Os integrantes do Comitê de Proteção de Dados Pessoais (CPDP) ou estrutura equivalente, a ser implementada, poderão expedir instruções complementares, no âmbito de suas competências, que detalharão suas particularidades e procedimentos relativos à Proteção de Dados Pessoais.

Art. 36. As dúvidas sobre a Política de Proteção de Dados Pessoais e seus documentos serão submetidas ao Comitê de Proteção de Dados Pessoais ou estrutura equivalente, a ser implementada.

Art. 37. Esta política será revisada no período de dois anos, a partir do início de sua vigência.

Art. 38. Os casos omissos serão resolvidos pela autoridade máxima da organização ou CPDP.

Art. 39. Esta política entra em vigor na data de sua publicação.

Referências Bibliográficas

- BRASIL. Autoridade Nacional de Proteção de Dados. Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Abril de 2022.
- BRASIL. Autoridade Nacional de Proteção de Dados. Resolução CD/ANPD Nº 18, de 16 de julho de 2024.
- BRASIL. Presidência da República. Lei nº 13.709, de 14 de agosto de 2018 (LGPD). Lei Geral de Proteção de Dados Pessoais.
- BRASIL. Presidência da República. Gabinete de Segurança Institucional. Portaria nº 93, de 26 de setembro de 2019. Glossário de Segurança da Informação.
- BRASIL. Presidência da República. Gabinete de Segurança Institucional. Instrução Normativa nº 01, maio de 2020. Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.
- DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO DA SECRETARIA DE GOVERNO DIGITAL. Guia do Framework de Privacidade e Segurança da Informação. Novembro 2022.
- MINISTÉRIO DA ECONOMIA. Portaria Nº 218. Maio 2020. Política de Segurança da Informação do Ministério da Economia.
- INFORMATION COMMISSIONER'S OFFICE. Data Protection Policy 2021.