DIÁRIO OFICIAL DA UNIÃO
Publicado em: 24/01/2025 | Edição: 17 | Seção: 1 | Página: 57
Órgão: Ministério da Previdência Social/Instituto Nacional do Seguro Social

# RESOLUÇÃO CEGOV/INSS Nº 47, DE 21 DE JANEIRO DE 2025

Institui a Política de Proteção de Dados Pessoais no INSS.

O COMITÊ ESTRATÉGICO DE GOVERNANÇA DO INSTITUTO NACIONAL DO SEGURO SOCIAL - CEGOV/INSS, no uso das atribuições que lhe foram conferidas pelo art. 5º da Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019, e considerando o disposto no Decreto nº 9.203, de 22 de novembro de 2017, bem como o contido no Processo Administrativo nº 35014.153223/2024-80, resolve:

Art. 1º Esta Resolução, institui, no âmbito do INSS, a Política de Proteção de Dados Pessoais - PPDP, atendendo aos preceitos da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais - LGPD.

CAPÍTULO I

Das Disposições Iniciais

Art. 2º Esta Política estabelece as diretrizes para a proteção de dados pessoais sob a responsabilidade do INSS, abrangendo todas as atividades de tratamento realizadas, tanto em meios digitais quanto físicos. Aplica-se a qualquer pessoa ou entidade que, em nome do INSS ou em suas dependências, realize operações de tratamento de dados pessoais.

Art. 3º A finalidade desta Política é adequar os conceitos, princípios e diretrizes da proteção de dados pessoais, visando garantir a efetividade dos direitos dos titulares de dados nas operações de tratamento sob responsabilidade do INSS, além de assegurar a conformidade com a legisla



Parágrafo único. A presente Política deverá ser observada quando da elaboração dos documentos abaixo relacionados, no que couber:

I - contratos e outros documentos, que dispõem sobre obrigações de confidencialidade em relação às informações mantidas pelo INSS;

II - políticas e normas de procedimentos de segurança da informação, bem como termos e condições de uso, que tratem sobre confidencialidade, integridade e disponibilidade das informações do INSS; e

III - normas internas e conjuntas a respeito da proteção de dados pessoais, que vierem a ser elaboradas e atualizadas.

Art. 4º São destinatários desta Política:

I - os agentes públicos do INSS;

II - os terceiros, sejam eles pessoas naturais ou jurídicas, que atuam para ou em nome do INSS em operações que envolvam tratamento de dados pessoais e sejam realizadas no escopo das atividades conduzidas pelo INSS;

III - os agentes de tratamento de dados pessoais externos ao INSS que, de qualquer forma, se relacionem com a instituição; e

IV - os titulares de dados pessoais, cujos dados são tratados pelo INSS.

Parágrafo único. Para fins do disposto nesta Política, serão considerados colaboradores, os servidores de carreira ou em exercício no INSS, ocupantes de cargo em comissão, contratados, terceirizados, estagiários, que realizem operações de tratamento de dados pessoais em nome do Instituto ou em suas dependências.

Art. 5º Além dos conceitos definidos pela legislação vigente voltada à proteção de dados pessoais, as informações abarcadas pela presente Política incluem todos os dados coletados, retidos, processados e compartilhados pelo ou em nome do INSS, em qualquer tipo de suporte, repositório e mídia. Isso inclui, mas não se limita, a dados pessoais registrados em documentos em meio físico (papel), mantidos em bases de dados, sistemas e dispositivos portáteis.

CAPÍTULO II

Dos Conceitos e Princípios

Art. 6º Para os fins desta Política, consideram-se os conceitos existentes no art. 5º da LGPD, bem como as seguintes definições:

I - ativos organizacionais: referem-se a todos os recursos, capacidades e informações que a instituição possui e que envolve o tratamento de dados pessoais. Inclui meios de armazenamento, transmissão e processamento, sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

II - compartilhamento de dados: obedecidas as normas e regulamentações conjuntas ou específicas, é justamente a operação de tratamento pela qual órgãos e entidades públicos conferem permissão de acesso a dados, nas formas de acesso estabelecidas, ou transferem uma base de dados pessoais a outro ente público ou a entidades privadas, visando ao atendimento de finalidade pública;

III - operações de tratamento de dados pessoais: referem-se à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; e

IV - Relatório de Impacto à Proteção de Dados Pessoais - RIPD: 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.



Parágrafo único. As operações previstas no inciso III do caput, encontram-se d Guia de Boas Práticas - Lei geral de Proteção de Dados - LGPD.

Art. 7º A aplicação desta Política observará a boa-fé e os princípios definidos no art. 6º da LGPD, a saber: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

CAPÍTULO III

Das Diretrizes

Art. 8º Para os efeitos desta Política, a proteção dos dados pessoais seguirá as seguintes diretrizes:

I - realização do tratamento de dados pessoais para o atendimento de sua finalidade pública, com o objetivo de executar suas competências e atribuições legais do serviço público;

II - registro das operações realizadas de tratamento de dados pessoais, conforme dispuser a Autoridade Nacional de Proteção de Dados - ANPD, com o mapeamento e a análise dos processos organizacionais, com intuito de identificar os ativos organizacionais e as medidas técnicas de segurança existentes ou que serão implementadas nestes ativos com vistas a prover a adequada proteção dos dados pessoais;

III - aderência ao princípio da segurança da informação;

IV - incorporação da proteção de dados pessoais em todos os processos desde a concepção, promovendo, à medida que se fizerem necessárias, revisões desses processos com o objetivo de aferir a redução ou o aumento de riscos relacionados ao tratamento de dados pessoais;

V - desenvolvimento e atualização das políticas e avisos de privacidade, que fornecerão informações sobre o processamento de dados pessoais em cada ambiente físico ou virtual, bem como detalhamento das medidas de proteção de dados adotadas para salvaguardar esses dados pessoais;

VI - respeito aos direitos dos titulares de dados;

VII - capacitação e conscientização dos envolvidos em atividades que realizem tratamento de dados pessoais com base nesta Política e nas boas práticas dela decorrentes; e

VIII - transparência na forma como o INSS realiza o tratamento de dados pessoais.

§ 1º Os dados pessoais coletados e tratados em sítios ou aplicativos mantidos pelo INSS devem ser administrados em conformidade com as diretrizes desta Política, cabendo à Empresa de Tecnologia e Informações da Previdência - Dataprev a responsabilidade quando a gestão dos dados estiver sob sua operação.

§ 2º Normativos específicos devem ser elaborados para a gestão de dados pessoais coletados a partir de sítios e aplicativos.

§ 3º Com respeito ao consentimento do titular e para fins estatísticos e de melhoria dos serviços ofertados, o INSS poderá utilizar arquivos (cookies) para registrar e gravar no computador do usuário as preferências e navegações realizadas nas respectivas páginas.

CAPÍTULO IV

Do Tratamento de Dados Pessoais

Art. 9º A realização de operações de tratamento de dados pessoais deve ter como base legal as hipóteses previstas no art. 7º da LGPD.

§ 1º No tratamento a que se refere o caput, o INSS utilizará como base legal, preferencialmente, as seguintes hipóteses, independentemente do consentimento dos titulares de dados:

I - cumprimento de obrigação legal ou regulatória; e

II - tratamento e uso compartilhado, pela administração pública, de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições da LGPD, acerca do tratamento de dados pessoais pelo poder público.

§ 2º Excetuadas as hipóteses de que trata o § 1º, a utilização das demais hip
refere o caput, como base legal, dependerá de motivação expressa da área responsável, com a indicação
das razões para a sua adoção.



§ 3º Quando o tratamento não decorrer de obrigação legal ou regulatória, mas do atendimento de interesse legítimo do INSS, o tratamento sem o consentimento do titular poderá ser realizado desde que consideradas as disposições do art. 10 da LGPD, observados os arts. 6º e 9º da referida Lei.

§ 4º No tratamento de dados pessoais de Pessoas Expostas Politicamente - PEPs, deverão ser observados os preceitos estabelecidos nos normativos que regulamentam o tema, além do previsto no Decreto nº 10.046, de 9 de outubro de 2019 e na LGPD podendo o INSS editar instruções complementares que disciplinem o assunto no âmbito interno.

Art. 10. No caso de transferência internacional de dados pessoais, deverá ser observado o que consta no Capítulo V da LGPD.

CAPÍTULO V

Do Tratamento de Dados Pessoais Sensíveis

Art. 11. A realização de operações de tratamento de dados pessoais sensíveis deve ter como base legal as hipóteses previstas no art. 11 da LGPD.

Parágrafo único. Nas hipóteses previstas no art. 11, inciso II, da LGPD, fica dispensado o fornecimento de consentimento do titular para o tratamento de dados pessoais sensíveis.

Art. 12. O tratamento de dados de criança e de adolescente deve pautar-se pelo seu melhor interesse e por sua máxima proteção, estando sujeito às disposições estabelecidas no art. 14 LGPD, observadas as hipóteses legais previstas no art. 7º ou no art. 11 da referida lei.

§ 1º Para fins desta Política, conforme art. 2º da Lei nº 8.069, de 13 de julho de 1990, considera-se criança a pessoa até doze anos de idade incompletos e adolescente aquela entre doze e dezoito anos de idade.

§ 2º Quando o tratamento de dados de criança for amparado na hipótese de consentimento, esse deverá ser específico e destacado por pelo menos um dos pais ou pelo responsável legal.

CAPÍTULO VI

Do Tratamento de Dados Pessoais na Realização de Pesquisas

Art. 13. No caso de estudos por órgãos de pesquisa, deve ser garantida, sempre que possível, a anonimização dos dados pessoais, hipótese que dispensa o consentimento do titular do dado. Esta utilização é estrita para realização de estudos por órgão de pesquisa público ou privado.

Parágrafo único. Para os efeitos do caput, órgão de pesquisa é o 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.

Art. 14. O órgão de pesquisa deverá garantir que não serão revelados dados pessoais, em caso de divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa realizada.

Art. 15. O órgão de pesquisa que tiver acesso aos dados pessoais deverá assumir a responsabilidade pela segurança da informação e se comprometer a não transferir os dados a terceiros em circunstância alguma.

CAPÍTULO VII

Dos Direitos dos Titulares de Dados Pessoais

Art. 16. No contexto das suas atividades de tratamento de dados pessoais, o INSS zela para que o titular dos dados pessoais possa usufruir dos direitos a ele assegurados nos termos dos arts. 18 a 20 da LGPD, de forma plena e segura.

§ 1º Para o exercício de direitos mencionados no caput, sem prejuízo de inovação, o INSS dispõe dos seguintes canais de atendimento, conforme o caso:



I - Aplicativo Meu INSS;

II - Portal Meu INSS (web);

III - Central de atendimento 135;

IV - Agências da Previdência Social; e

V - Ouvidoria.

§ 2º O INSS adotará medidas de segurança e governança para assegurar que as solicitações dos titulares sejam tratadas de forma célere e conforme os prazos estabelecidos pela legislação vigente.

Art. 17. Para ter acesso aos serviços disponibilizados pela instituição via Meu INSS (aplicativo ou Portal), para exercício dos direitos do titular, os usuários deverão, de forma livre e consciente, fornecer dados pessoais necessários ao cadastro, credenciamento, identificação e autenticação.

Art. 18. Quando se tratar de dados pessoais migrados de outras bases apenas com opção de consulta pelo INSS, por não serem objeto de tratamento no âmbito da instituição, o exercício de direito, pelos titulares, deve ser realizado diretamente junto ao gestor da base de dados.

Art. 19. Os direitos do titular de dados pessoais previstos na LGPD, em qualquer caso, serão ponderados com o interesse público de conservação de dados históricos, o fomento ao controle social, a preservação da transparência da instituição e das condutas de agentes públicos no exercício de suas atribuições, e com a divulgação de informações relevantes à sociedade.

Art. 20. Nos pedidos de acesso à informação e respectivos recursos, as decisões que tratam da publicidade de dados pessoais serão fundamentadas nos arts. 3º e 31 da Lei nº 12.527, de 18 de novembro de 2011, Lei de Acesso à Informação - LAI.

Parágrafo único. A aplicação da LAI e LGPD, deve ocorrer de forma integrada, tendo por premissa a compatibilidade entre os comandos legais.

CAPÍTULO VIII

Do compartilhamento de dados pessoais

Art. 21. O uso compartilhado de dados pessoais deve ser realizado em conformidade com a LGPD, notadamente com os princípios, as bases legais, a garantia dos direitos dos titulares e outras regras específicas aplicáveis ao Poder Público.

Art. 22. Além da observância ao disposto no art. 21, o uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º da LGPD.

§ 1º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, e as empresas públicas e as sociedades de economia mista, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, nos termos da LGPD.

§ 2º Na hipótese de compartilhamento de dados entre os órgãos e as entidades da administração pública federal direta, autárquica e fundacional e os demais Poderes da União, deverá ser observado o que consta no Capítulo III do Decreto nº 10.046, de 9 de outubro de 2019, e o disposto na LGPD.

§ 3º No âmbito do INSS, além do compartilhamento de dados pessoais observar o disposto na legislação vigente, também se aplicam as disposições das normas conjuntas ou específicas.

Art. 23. É vedado ao INSS compartilhar com entidades privadas dados pessoais constantes de bases de dados, sistemas e repositórios sob a sua gestão ou operacionalização, exceto:

I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na LAI;

II - nos casos em que os dados forem acessíveis publicamente, observadas a finalidade, a boa-fé e os direitos do titular;

III - quando houver previsão legal ou o compartilhamento de dados for contratos, convênios ou instrumentos congêneres comunicados à ANPD; ou



IV - na hipótese de o compartilhamento dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou a proteção e o resguardo da segurança e da integridade do titular dos dados, sendo vedado o tratamento para outras finalidades.

§ 1º Para os efeitos do disposto no caput, quanto ao Sistema Nacional de Informações de Registro Civil - Sirc, o compartilhamento de dados com entidades privadas somente é permitido para fins de estudos e pesquisas, após a autorização do Comitê Gestor do Sistema Nacional de Informações de Registro Civil - CGSirc, vedada a identificação das pessoas a que os dados se referirem, conforme estabelece o art. 7º, § 7º, do Decreto nº 9.929, de 22 de julho de 2019.

§ 2º A comunicação ou o uso compartilhado de dados pessoais com pessoa de direito privado será informado à ANPD e dependerá de consentimento do titular, exceto:

I - nas hipóteses de dispensa de consentimento previstas na LGPD;

II - nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do art. 23, inciso I da LGPD; ou

III - nas exceções previstas nos incisos do caput.

§ 3º As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos da LGPG.

Art. 24. Para fins de compartilhamento de dados do Cadastro Nacional de Informações Sociais - CNIS, aplica-se o disposto na Portaria Conjunta MPS/INSS nº 3, de 16 de janeiro de 2024, ou ato que vier a substituí-la.

§ 1º Conforme art. 4º, inciso V, da Portaria Conjunta MPS/INSS nº 3, de 2024, compete ao Ministério da Previdência Social - MPS, exercer o papel de controlador no tratamento de dados pessoais do CNIS, de que trata o art. 5º, inciso VI da LGPD, podendo contratar ou firmar parcerias com terceiros para

que este exerça esse papel.

§ 2º De acordo com o art. 5º, inciso VI, da Portaria Conjunta MPS/INSS nº 3, de 2024, compete ao INSS exercer o papel de operador no tratamento de dados pessoais do CNIS, de que trata o art. 5º, inciso VII LGPD, podendo contratar ou firmar parcerias com terceiros para que este exerça esse papel.

Art. 25. Para os fins de compartilhamento de dados do Sirc, aplica-se o disposto pelo Decreto nº 9.929, de 22 de julho de 2019, pela Resolução CGSirc nº 4, de 28 de maio de 2019, e pela Resolução CGSirc nº 8, de 2 de dezembro de 2021, ou atos que vierem a substituí-los.

§ 1º Conforme o art. 3º do Decreto nº 9.929, de 2019, o CGSirc exerce o papel de controlador no tratamento de dados pessoais do Sirc e é responsável pelo estabelecimento de diretrizes para o funcionamento, a gestão e a disseminação do referido sistema e pelo monitoramento do uso dos dados nele contidos.

§ 2º De acordo com o § 11 do art. 4º do Decreto nº 9.929, de 2019, ao INSS, que integra o referido Comitê, compete exercer o papel de operador no tratamento de dados pessoais do Sirc, sendo responsável pelo desenvolvimento, a operacionalização e a manutenção do referido sistema, observadas as diretrizes e as deliberações do CGSirc.

Art. 26. O compartilhamento de dados pessoais no INSS deve ser formalizado em atenção às normas gerais que regem os procedimentos administrativos e à obrigatoriedade de registro das operações de tratamento, conforme disposto no art. 37 da LGPD.

Parágrafo único. Recomenda-se a instauração de processo administrativo, do qual constem os documentos e as informações pertinentes, incluindo análise técnica e jurídica, conforme o caso, que exponham a motivação para a realização do compartilhamento e a sua aderência à legislação em vigor.

Art. 27. Respeitadas as normas e regulamentações conjuntas ou específicas, a autorização de acesso ou de compartilhamento de dados deverá ser estabelecida em ato formal, a exemplo de contratos, convênios, acordos ou instrumentos congêneres firmados entre as partes, ou por meio de expedição de decisão administrativa pela autoridade competente, que autorize o acesso aos dados e estabeleça os requisitos definidos como condição para o compartilhamento.



Parágrafo único. Nos termos do art. 5º do Decreto nº 10.046, de 9 de outubro de 2019, é permitida a dispensa quanto à celebração de convênio, acordo de cooperação técnica ou instrumentos congêneres para a efetivação do compartilhamento de dados entre os órgãos e as entidades de que trata o art. 1º do referido Decreto, observadas as diretrizes do seu art. 3º e o disposto na LGPD.

Art. 28. Na formalização, os dados pessoais objeto de acesso e compartilhamento deverão ser indicados, sendo que a autorização concedida deverá indicar o nível de acesso ou o tipo de compartilhamento autorizado, limitando-se ao que for estritamente necessário para a (s) finalidade (s) do tratamento, em conformidade com o princípio da necessidade.

Parágrafo único. A finalidade deve ser específica, com a indicação precisa da iniciativa, ação ou programa que será executado ou, ainda, da atribuição legal que será cumprida pela instituição solicitante, mediante o compartilhamento dos dados pessoais requerido.

Art. 29. Respeitadas as normas e regulamentações conjuntas ou específicas, os atos que autorizarem o acesso ou o compartilhamento de dados pessoais deverão:

I - estabelecer:

a) se for o caso, o período de duração do compartilhamento de dados, além de esclarecer se há a possibilidade de conservação ou se os dados deverão ser eliminados após o término do tratamento; e

b) os requisitos ou padrões mínimos de segurança, técnicos e administrativos, que deverão ser adotados pela instituição solicitante para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão, em atenção ao art. 6º, inciso VII, e ao art. 46 da LGPD;

II - dispor sobre as formas de atendimento ao princípio da transparência, de que trata o art. 6º, inciso VI da LGPD.

Art. 30. O ato que autorizar o acesso ou o compartilhamento de dados pessoais poderá vedar a realização de novo compartilhamento ou, ainda, autorizá-lo sob determinadas condições, observadas as normas aplicáveis.

Art. 31. Respeitadas as normas e regulamentações conjuntas ou específicas, os atos que autorizarem o acesso ou o compartilhamento de dados pessoais poderão, conforme o caso, indicar a remuneração a ser paga pela instituição solicitante ou, simplesmente, prever que não haverá transferência de recursos financeiros, segundo as disposições legais aplicáveis.

Art. 32. O INSS poderá expedir atos regulamentares acerca do fluxo padronizado de tratativas e respectiva formalização, com o estabelecimento de procedimentos, competências, prazos e requisitos essenciais a serem observados nos processos de compartilhamento de dados.

CAPÍTULO IX

Relatório de Impacto à Proteção de Dados Pessoais

Art. 33. A elaboração do RIPD será necessária quando houver operações de tratamento que representem riscos elevados aos direitos dos titulares, devendo ser atualizado periodicamente ou sempre que houver alterações significativas nas operações de tratamento.

Art. 34. O processo de elaboração, revisão e aprovação do RIPD será regulamentado por normativo específico, que deverá:

I - levar em consideração o volume e a sensibilidade dos dados tratados, bem como a capacidade operacional da instituição; e

II - estabelecer critérios para a identificação das operações de tratamento que exigem sua confecção, definir o fluxo de trabalho envolvido e detalhar as responsabilidades atribuídas a cada unidade.

Parágrafo único. Em conformidade com o art. 38 da LGPD, a ANPD poderá, a qualquer momento, solicitar a apresentação do RIPD. Nesses casos, o INSS deverá fornecer o RIPD atualizado, dentro do prazo estipulado na solicitação.



CAPÍTULO X

Dos Agentes de Tratamento e do Encarregado de Dados Pessoais

Art. 35. O controlador de dados pessoais, nos termos do art. 5º, inciso VI, da LGPD, é a União, assumindo o INSS atribuições de controlador mediante o processo de descentralização administrativa e considerando as competências legais e regulamentares da instituição.

§ 1º Conforme previsto pela Portaria Conjunta MPS/INSS nº 3, de 2024, no tratamento de dados pessoais do CNIS, o MPS exerce o papel de controlador, enquanto o INSS o de operador.

§ 2º Com base no art. 3º do Decreto nº 9.929, de 2019, no tratamento de dados pessoais do Sirc, o CGSirc exerce o papel de controlador, enquanto o INSS o de operador.

Art. 36. É operador a pessoa jurídica de direito público ou privado e a pessoa natural que realizar tratamento de dados pessoais em nome do INSS, sob suas instruções, exceto integrantes do quadro funcional efetivo do INSS.

Parágrafo único. Os fornecedores de produtos ou serviços, ao tratarem os dados pessoais a eles confiados pelo INSS, serão considerados operadores.

Art. 37. O encarregado de dados pessoais é pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD ou com outras organizações com atuação na proteção de dados pessoais com as quais o INSS estabeleça acordo de serviço ou de cooperação técnica.

CAPÍTULO XI

Das Funções e Responsabilidades

Art. 38. Observado o disposto no art. 35, ao INSS compete, no exercício das atribuições típicas de controlador, tomar as decisões estratégicas que afetem ou envolvam o tratamento de dados pessoais, além de determinar as medidas necessárias para executar a Política de Proteção de Dados Pessoais no âmbito de sua estrutura organizacional.

Art. 39. São atribuições do controlador:

I - assegurar o cumprimento da Política de Proteção de Dados Pessoais à luz da legislação vigente;

II - observar os fundamentos, princípios da privacidade e proteção de dados pessoais e os deveres impostos pela LGPD, e por normativos correlatos, quando realizar o tratamento de dados pessoais;

III - considerar o preconizado pelos arts. 7º, 11 e 23 da LGPD, Lei Geral de Proteção de Dados Pessoais, antes de realizar o tratamento de dados pessoais;

IV - cumprir o previsto pelos arts. 46 e 50 da LGPD, inclusive formulando regras de boas práticas e de governança, visando a proteção de dados pessoais;

V - garantir infraestrutura física e de pessoal, além de recursos para o cumprimento das exigências estabelecidas na LGPD;

VI - 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;

VII - assegurar ao encarregado aquilo que dispõe o art. 10 da Resolução CD/ANPD nº 18, de 16 de julho de 2024;

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

IX - 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;

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

XI - acompanhar o cumprimento das cláusulas de proteção de dados junto aos contratados e fornecedores;



XII - promover formações de boas práticas para a proteção de dados; e

XIII - adotar 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.

Parágrafo único. É vedado qualquer tratamento de dados pessoais para fins não relacionados com as atividades desenvolvidas pela organização ou por pessoa não autorizada formalmente pelo INSS.

Art. 40. Em consonância com o previsto no art. 38 do Regimento Interno, aprovado pela Portaria PRES/INSS nº 1.678, de 29 de abril de 2024, compete à Coordenação de Proteção de Dados Pessoais, entre outras atribuições:

I - implementar e avaliar a Política Institucional de Proteção de Dados Pessoais e da Privacidade, nos termos da legislação vigente;

II - prover orientação relacionada às boas práticas de proteção de dados pessoais no INSS, de acordo com os objetivos estratégicos e com as leis e regulamentos pertinentes;

III - propor a constituição de grupos de trabalho para tratar de temas, além de soluções específicas sobre proteção de dados pessoais;

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

V - incentivar a conscientização, capacitação e sensibilização das pessoas que desempenham qualquer atividade de tratamento de dados pessoais no âmbito do INSS.

Art. 41. Ao encarregado de dados pessoais compete:

I - receber:

a) reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; e

b) comunicações e requisições da ANPD e adotar providências;

II - orientar os colaboradores da organização a respeito das práticas a serem adotadas em relação à proteção de dados pessoais; e

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

Parágrafo único. Além das disposições constantes no caput, o encarregado deverá prestar assistência e orientação ao agente de tratamento, nos casos previstos no art. 16 da Resolução CD/ANPD Nº 18, de 16 de julho de 2024, ou ato que venha a substituí-la.

Art. 42. Observado o disposto no art. 36, cabe ao operador realizar o tratamento de dados pessoais seguindo as diretrizes estabelecidas e nos moldes definidos pelo INSS e de forma aderente a esta Política, bem como:

I - realizar o tratamento de dados em nome do controlador;

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

III - manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse; e

IV - 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.

Parágrafo único. É proibida a decisão unilateral do operador quanto aos meios e finalidades utilizados para o tratamento de dados pessoais.

Art. 43. Todas as pessoas, exceto os titulares dos dados pessoais, que atuem em qualquer fase do ciclo de vida das informações protegidas, utilizadas ou fornecidas pelo INSS, têm a obrigação de garantir a privacidade e a proteção dos dados, inclusive após o término do tratamento.

CAPÍTULO XII

Da Segurança e das Boas Práticas



Art. 44. O INSS implementará 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, nos termos do Capítulo VII da LGPD.

Art. 45. Com o objetivo de reduzir ou mitigar a existência de incidentes com os dados pessoais do titular, o INSS adotará, no mínimo, as seguintes medidas técnicas e organizacionais de privacidade e proteção de dados:

I - o acesso aos dados pessoais deverá ser limitado às pessoas que realizam o tratamento e revisado, periodicamente, de acordo com os critérios estabelecidos em normativos da instituição, independente da existência de processos automáticos para tanto;

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

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

IV - todos os dados pessoais deverão ser mantidos ou armazenados em ambiente seguro, de modo que terceiros não autorizados não possam acessá-los;

V - as medidas de segurança técnicas e administrativas, para proteção de dados pessoais, deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução, de acordo com o conceito denominado Privacidade desde a Concepção;

VI - deverão ser planejadas e estabelecidas ações voltadas ao mapeamento e análise dos processos organizacionais, com intuito de identificar os ativos organizacionais e as medidas técnicas de segurança a serem implementadas nestes ativos, com vistas a prover a adequada proteção dos dados pessoais; e

VII - deverá ser mantida uma base de conhecimento com documentos que apresentem condutas e recomendações que melhorem o gerenciamento de risco e que orientem na tomada de ações adequadas em caso de comprometimento de dados pessoais.

§ 1º Quanto às medidas ainda não implementadas, deverão ser adotadas as ações possíveis, como medidas de contingência, para proteger os dados, buscando mitigar os eventuais riscos.

§ 2º Outras medidas poderão ser adotadas observando-se o contido na Política de Segurança da Informação do INSS - POSIN-INSS, de que trata a Resolução nº 9 /CEGOV/INSS, de 31 de agosto de 2020, ou outro normativo que possoa vim a substituí-la.

Art. 46. Qualquer ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos dados pessoais dos titulares deverá ser comunicada à ANPD, pelo encarregado de dados pessoais, dentro do prazo previsto pela LGPD.

CAPÍTULO XIII

Da Conscientização, Capacitação e Sensibilização

Art. 47. Os colaboradores que possuem acesso aos dados pessoais no INSS deverão participar de programas de conscientização, capacitação e sensibilização, em matérias de privacidade e proteção de dados pessoais, a serem ofertados ou promovidos pela instituição.

§ 1º A conscientização, capacitação e sensibilização em privacidade e proteção de dados pessoais deverá ser adequada aos papéis e responsabilidades dos colaboradores.

§ 2º Os planos de conscientização, capacitação e sensibilização deverão contemplar a consolidação de material atualizado periodicamente, com instruções e normas de boas práticas envolvendo segurança da informação, a ser disponibilizado a todos os colaboradores, além de medidas que visem a internalização da cultura de proteção de dados pessoais nas unidades do INSS.

§ 3º Os cursos deverão ser destinados a todos os colaboradores, com abordagem e metodologia que respeite as especificidades e características institucionais.

§ 4º As unidades do INSS deverão ser capacitadas de maneira planejada e específicos, a fim proporcionar maior aderência aos temas a elas direcionados.



CAPÍTULO XIV

Dos Contratos, Convênios, Acordos e Instrumentos Congêneres

Art. 48. Os contratos, convênios, acordos e instrumentos congêneres deverão ser celebrados prezando pelo respeito aos princípios da finalidade, adequação, necessidade, transparência, livre acesso, qualidade dos dados, segurança, prevenção, não discriminação e responsabilização.

Art. 49. Respeitadas as normas e regulamentações conjuntas ou específicas, os contratos, convênios, acordos e instrumentos congêneres, que de alguma forma envolvam o tratamento de dados pessoais, deverão incorporar cláusulas específicas em total conformidade com a presente Política de Proteção de Dados Pessoais e que contemplem:

I - requisitos:

a) indispensáveis de segurança da informação, observados os padrões operacionais necessários à luz da POSIN-INSS, ou outro normativo que possa vim a substituí-la; e

b) de proteção de dados pessoais, que os operadores de dados pessoais devem atender;

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

III - dispositivo:

a) para que os dados coletados e seu processamento sejam limitados ao mínimo necessário para atendimento da finalidade do tratamento;

b) que defina a obrigação do operador de dados pessoais notificar o controlador em caso de ocorrência de violação de dados pessoais;

c) que defina que os dados pessoais armazenados ou retidos possuam controles de integridade, permitindo identificar se foram alterados sem permissão;

d) que defina que as operações de processamento realizadas com dados pessoais sejam registradas de modo a identificar a operação realizada, quem realizou, data e hora (auditoria de log); e

e) que estipule sanções administrativas pelo descumprimento de cada um dos requisitos de segurança da informação e de privacidade especificados;

IV - o uso e arquivamento somente pelo tempo necessário para a execução dos serviços acordados, contratados ou conveniados. E, ao seu fim, a eliminação dos dados coletados, excetuando-se os que se enquadrarem no disposto no art. 16, inciso I da LGPD;

V - 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;

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

VII - quando da transferência ou compartilhamento de dados, dispositivo que deixe claro que, uma vez transferidos ou compartilhados os dados pessoais, a responsabilidade por garantir a privacidade e a proteção dos dados recepcionados será do receptor.

Art. 50. O INSS verificará se os terceiros e os processadores de dados pessoais contratados atendem aos requisitos exigidos pelas cláusulas contratuais estabelecidas, no momento da celebração do acordo.

Art. 51. Outros requisitos poderão ser verificados no Guia de Requisitos e Obrigações quanto à Privacidade e Segurança da Informação, da Secretaria de Governo Digital - SGD, que orienta a adequação do processo de contratação de Soluções de Tecnologia da Informação e Comunicação - TIC para contemplar os requisitos mais importantes de privacidade e segurança dos dados.



CAPÍTULO XV

Das Penalidades

Art. 52. 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. 53. Casos de descumprimento desta Resolução deverão ser registrados e comunicados ao superior imediato para ciência e envio ao encarregado de dados pessoais para tomada de providências cabíveis.

CAPÍTULO XVI

Da Avaliação de Conformidade

Art. 54. O cumprimento desta Política, bem como dos normativos que a complementam, deverão ser avaliados, periodicamente, por meio de verificações de conformidade, buscando a certificação do cumprimento dos requisitos de privacidade e proteção de dados pessoais e da garantia de cláusula de responsabilidade e sigilo constantes de termos de responsabilidade, contratos, convênios, acordos e instrumentos congêneres.

Art. 55. O INSS atuará no sentido de que as atividades, produtos e serviços por ele desenvolvidos estejam em conformidade com requisitos de privacidade e proteção de dados pessoais constantes de leis, regulamentos, resoluções, normas, estatutos e contratos jurídicos vigentes.

Art. 56. Os resultados de cada ação de verificação de conformidade deverão ser documentados em relatório de avaliação de conformidade, a ser regulamentado.

CAPÍTULO XVII

Disposições Finais

Art. 57. O INSS poderá expedir instruções complementares, que detalharão suas particularidades e procedimentos relativos à Proteção de Dados Pessoais alinhados às diretrizes emanadas por esta Resolução e aos respectivos Planos Estratégicos Institucionais do INSS.

Art. 58. Esta Resolução deverá ser revisada ordinariamente no período de 3 (três) anos, a partir do início de sua vigência, ou, extraordinariamente, sempre que houver motivação para tanto.

Art. 59. Os casos omissos serão resolvidos pela autoridade máxima da organização.

Art. 60. Esta Resolução entra em vigor na data de sua publicação.

**ALESSANDRO ANTONIO STEFANUTTO**
Presidente do Instituto

**VANDERLEI BARBOSA DOS SANTOS**
Diretor de Benefícios e Relacionamento com o Cidadão

**DÉBORA APARECIDA ANDRADE FLORIANO**
Diretora de Orçamento, Finanças e Logística

**ROBERTO CARNEIRO DA SILVA**
Diretor de Gestão de Pessoas

**ISMÊNIO BEZERRA**
Diretor de Governança, Planejamento e Inovação

**MARCELO GENU BESERRA**
Diretor de Tecnologia da InformaçãoSubstituto