MINISTÉRIO DA FAZENDA
Secretaria-Executiva
Comitê de Governança Digital, Segurança da Informação e Proteção de Dados Pessoais
Subcomitê de Proteção de Dados Pessoais

RESOLUÇÃO CGSP /MF Nº 13, DE 27 DE OUTUBRO DE 2026

Aprova a Política de Proteção de Dados Pessoais no âmbito do Ministério da Fazenda.

O COMITÊ DE GOVERNANÇA DIGITAL, SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS DO MINISTÉRIO DA FAZENDA – CGSP/MF, por meio de seu Presidente, no uso da atribuição que lhe confere o art. 2º, caput, inciso I, alínea "b", da Portaria SE/MF nº 1.060, de 26 de junho de 2024, e tendo em vista o disposto no art. 5º, caput, inciso LXXIX, da Constituição Federal, e na Lei nº 13.709, de 14 de agosto de 2018, resolve:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Objeto

Art. 1º Fica aprovada a Política de Proteção de Dados Pessoais no âmbito do Ministério da Fazenda com o objetivo de promover a proteção de dados pessoais em processos de trabalho, serviços e sistemas, em meios físicos ou digitais, inclusive em ambientes de nuvem e em soluções providas por terceiros.

Art. 2º A Política de Proteção de Dados Pessoais visa estabelecer princípios, diretrizes, controles mínimos e responsabilidades para assegurar a conformidade da atuação do Ministério da Fazenda com as disposições da Lei nº 13.709, de 14 de agosto de 2018.

Parágrafo único. A implementação da Política de que trata o caput deverá ser documentada e evidenciada por registros mínimos, conforme diretrizes da governança institucional de proteção de dados pessoais, de modo a permitir rastreabilidade, monitoramento e prestação de contas

Âmbito de aplicação

Art. 3º O disposto nesta Resolução aplica-se:

I - aos órgãos, às unidades administrativas e aos colegiados que integram a estrutura organizacional do Ministério da Fazenda; e

II - a todos os agentes públicos e colaboradores que atuem em nome do Ministério da Fazenda, inclusive contratados, conveniados e demais terceiros, quando houver tratamento de dados pessoais no contexto de atividades, de serviços, de sistemas ou de processos de trabalho de responsabilidade do órgão.

Parágrafo único. A aplicação desta Resolução não afasta o cumprimento de normas específicas sobre sigilo de dados e proteção da informação, e deve respeitar a autonomia técnica das unidades administrativas do Ministério da Fazenda.

Conceitos

Art. 4º Para os fins desta Resolução, aplicam-se as definições da Lei nº 13.709, de 14 de agosto de 2018, e considera-se:

I — agentes de tratamento: controlador e operador;

II - 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;

III - canal institucional de atendimento ao titular de dados pessoais: meio de comunicação oficial disponibilizado pelo Ministério da Fazenda para recepcionar e acompanhar solicitações de titulares de dados pessoais, inclusive as relacionadas aos direitos previstos na Lei nº 13.709, de 14 de agosto de 2018;

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

V - dados pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculados a pessoa natural;

VI - decisão automatizada: decisão tomada unicamente com base em tratamento automatizado de dados pessoais que afete interesses do titular dos dados, inclusive para definição de perfil pessoal, profissional, de consumo e de crédito, ou de aspectos de sua personalidade;

VII - encarregado: pessoa designada pela organização para atuar como canal de comunicação entre o controlador, os titulares de dados e a Agência Nacional de Proteção de Dados – ANPD;

VIII - inventário de dados pessoais – IDP: instrumento institucional destinado ao registro e à organização das operações de tratamento de dados pessoais realizadas no âmbito do Ministério da Fazenda;

IX - inteligência artificial – IA: sistema baseado em máquina que, para objetivos explícitos ou implícitos, permite, a partir das informações recebidas e mediante inferências, a geração de saídas, tais como previsões, conteúdos, recomendações ou decisões, que podem influenciar ambientes físicos ou virtuais, com variados níveis de autonomia e de adaptabilidade;

X - pseudonimização: tratamento por meio do qual um dado pessoal perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro;

XI - 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 as medidas, salvaguardas e mecanismos de mitigação de riscos adotados;

XII - sistemas e soluções: aplicações, serviços, plataformas, bases de dados, repositórios e demais recursos tecnológicos ou físicos utilizados para coletar, armazenar, processar ou compartilhar dados pessoais no âmbito do Ministério da Fazenda;

XIII - solução de IA: sistema que utiliza inteligência artificial para realizar uma ou mais tarefas, seja para atender a necessidades do próprio Ministério da Fazenda ou de terceiros;

XIV - 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; e

XV - governança institucional: modelo de governança estabelecido pelo Comitê de Governança Digital, Segurança da Informação e Proteção de Dados Pessoais do Ministério da Fazenda - CGSP/MF, respeitadas, em sendo o caso, as regras próprias editadas pelos órgãos fazendários que possuam unidade correlata de proteção de dados pessoais, nos termos da Resolução CGSP/MF nº 7, de 14 de janeiro de 2026.

Princípios e diretrizes de proteção de dados pessoais

Art. 5º O tratamento de dados pessoais no âmbito do Ministério da Fazenda observará os princípios previstos no art. 6º da Lei nº 13.709, de 14 de agosto de 2018, e as seguintes diretrizes:

I - responsabilização e prestação de contas:

a) as unidades responsáveis por processo de trabalho que envolva o tratamento de dados pessoais deverão elaborar e manter atualizado o IDP; e

b) as unidades deverão manter evidências mínimas de conformidade, incluindo registros de decisões, relatórios de conformidade, avaliações de risco e medidas de mitigação adotadas, para fins de rastreabilidade e auditoria;

II - prevenção e segurança, com adoção de medidas proporcionais ao risco:

a) as unidades responsáveis por processo de trabalho que envolva o tratamento de dados pessoais deverão adotar medidas técnicas e administrativas para proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas de destruição, de perda, de alteração, de comunicação, de difusão ou de qualquer forma de tratamento inadequado ou ilícito de dados pessoais;

b) os sistemas e soluções utilizados para o tratamento de dados pessoais deverão ser submetidos à avaliação de riscos, com priorização daqueles de maior criticidade, sensibilidade e exposição, para fins de implementação de controles e de planos de tratamento de riscos;

c) o tratamento de dados pessoais deverá limitar-se ao mínimo necessário para o atendimento da finalidade específica do processo de trabalho; e

d) o tratamento de dados pessoais deverá ocorrer em sistemas e meios institucionais autorizados, observadas as diretrizes de segurança da informação e de proteção de dados pessoais;

III - transparência:

a) as unidades responsáveis por serviços e sistemas que realizam o tratamento de dados pessoais deverão elaborar e manter atualizados os avisos de privacidade e os termos de uso, quando aplicáveis, em conformidade com a Lei nº 13.709, de 14 de agosto de 2018; e

b) as unidades deverão assegurar resposta tempestiva e completa às demandas do titular de dados pessoais, nos canais institucionais estabelecidos para tanto, garantindo a rastreabilidade do atendimento e a integridade das informações fornecidas;

IV - melhoria contínua:

a) os processos de tratamento de dados pessoais deverão ser revisados periodicamente, com vistas à atualização do IDP, à correção de lacunas de conformidade, à revisão de riscos e à reavaliação de controles implementados; e

b) as unidades deverão elaborar, registrar e acompanhar planos de ação, com definição de prazos e de responsáveis para a implementação de melhorias decorrentes de diagnósticos, de auditorias, de recomendações da governança institucional de proteção de dados pessoais ou de lições aprendidas com incidentes de segurança no tratamento de dados pessoais;

V - integração à governança institucional:

a) a proteção de dados pessoais deverá ser incorporada ao planejamento institucional, à gestão de riscos, ao planejamento das contratações, ao desenvolvimento e à sustentação de soluções de tecnologia da informação e às rotinas administrativas, com participação das unidades competentes; e

b) decisões e mudanças relevantes que possam impactar o tratamento de dados pessoais deverão ser previamente comunicadas às instâncias de governança competentes, conforme fluxos estabelecidos pela governança institucional de proteção de dados pessoais;

VI - qualidade dos dados pessoais e integridade:

a) as unidades deverão adotar medidas para garantir a exatidão, a clareza, a relevância e a atualização dos dados pessoais, de acordo com a necessidade e a finalidade do tratamento, inclusive por meio

de procedimentos de validação e de rotinas de correção; e

b) os sistemas e processos de trabalho do Ministério da Fazenda deverão, sempre que aplicável, disponibilizar mecanismos para a retificação de dados pessoais incompletos, inexatos ou desatualizados, com rastreabilidade das alterações;

VII — não discriminação e uso ético:

a) é vedado o tratamento de dados pessoais para fins discriminatórios, ilícitos ou abusivos; e

b) nos casos de tratamento automatizado de dados pessoais, inclusive com a utilização de sistemas baseados em inteligência artificial, que possam resultar em decisões que afetem interesses do titular dos dados, as unidades deverão adotar medidas para prevenir vieses e efeitos discriminatórios, registrando as decisões e as salvaguardas adotadas;

VIII - proteção de titulares de dados pessoais em situação de vulnerabilidade:

a) no tratamento de dados pessoais de crianças e adolescentes, idosos e pessoas com deficiência, as unidades deverão adotar medidas adicionais para assegurar a observância do melhor interesse, nos termos da legislação aplicável, e limitar o tratamento ao mínimo necessário para alcançar a finalidade pretendida; e

b) as informações sobre o tratamento de dados pessoais destinadas a titulares em situação de vulnerabilidade deverão ser apresentadas em linguagem clara, simples, acessível e compatível com suas características e com as necessidades do público-alvo, de modo a assegurar a adequada compreensão das informações e o efetivo exercício dos direitos dos titulares de dados.

§ 1º O cumprimento das diretrizes de que trata o caput deverá ser demonstrado por meio de registros e de documentação mínima pelas unidades responsáveis pelo tratamento dos dados pessoais, conforme padrões definidos no âmbito da governança institucional de proteção de dados pessoais.

§ 2º Os controles e as medidas de privacidade e de segurança da informação deverão ser aplicados de forma proporcional ao risco, considerando, no mínimo, a natureza dos dados, o volume, a sensibilidade, a criticidade do processo, os compartilhamentos e a exposição do sistema ou serviço.

§ 3º As unidades do Ministério da Fazenda deverão assegurar que as suas equipes de trabalho sejam capacitadas e conscientizadas de forma contínua quanto às obrigações e às boas práticas de proteção de dados pessoais, conforme as diretrizes previstas nesta Resolução e na legislação pertinente.

CAPÍTULO II
DA GOVERNANÇA, DAS OBRIGAÇÕES E DA ARTICULAÇÃO INSTITUCIONAL

Governança de proteção de dados pessoais

Art. 6º A governança de proteção de dados pessoais no âmbito do Ministério da Fazenda observará o disposto na Resolução CGSP/MF nº 7, de 14 de janeiro de 2026, inclusive quanto à Rede de Proteção de Dados Pessoais, às atribuições dos agentes públicos e à autonomia técnica das unidades.

Art. 7º Para fins de implementação desta Resolução, as unidades do Ministério da Fazenda deverão:

I - manter interlocução com as unidades responsáveis da Rede de Proteção de Dados Pessoais, nos termos da Resolução CGSP/MF nº 7, de 14 de janeiro de 2026, para fins de orientação, de reporte, de monitoramento e de consolidação de evidências no tratamento de dados pessoais;

II - assegurar o encaminhamento tempestivo de informações e de evidências solicitadas no âmbito da governança institucional de proteção de dados pessoais, observadas as hipóteses legais de sigilo aplicáveis;

III - observar os fluxos institucionais relativos à comunicação de incidentes, ao atendimento ao titular de dados e à gestão de riscos relacionados ao tratamento de dados pessoais;

IV - assegurar que o encarregado setorial e os encarregados correlatos disponham de meios humanos, técnicos e administrativos necessários ao exercício de suas atribuições, com garantia de autonomia técnica e prevenção de situações que possam configurar conflito de interesses; e

V - solicitar orientação do encarregado setorial e dos encarregados correlatos quando realizarem atividades e tomarem decisões estratégicas referentes ao tratamento de dados pessoais, mantendo registro mínimo das demandas e das orientações prestadas, observadas as hipóteses legais de sigilo aplicáveis.

Parágrafo único. Deverá ser assegurado ao encarregado setorial e aos encarregados correlatos acesso direto às instâncias responsáveis por decisões estratégicas sobre o tratamento de dados pessoais, conforme os fluxos institucionais de proteção de dados pessoais estabelecidos.

Obrigações dos agentes públicos e dos colaboradores do Ministério da Fazenda

Art. 8º Todo agente público e colaborador que realize, no âmbito do Ministério da Fazenda, o tratamento de dados pessoais no exercício de suas atribuições deverá:

I - observar o disposto na Lei nº 13.709, de 14 de agosto de 2018, nesta Resolução, em normas internas de proteção de dados pessoais e nas orientações expedidas no âmbito da Política de Governança de Proteção de Dados Pessoais do Ministério da Fazenda;

II - tratar dados pessoais de forma compatível com as competências institucionais de sua unidade, com a finalidade do processo de trabalho e com o contexto informado ao titular dos dados, quando aplicável, limitando o tratamento ao mínimo necessário para a consecução de sua finalidade;

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

IV - utilizar sistemas, soluções e canais institucionais autorizados para a realização de operações de tratamento de dados pessoais;

V - restringir o acesso e o compartilhamento de dados pessoais ao estritamente necessário para o exercício de suas atribuições, vedada a divulgação a terceiros ou a outras unidades sem justificativa funcional e em desconformidade com as normas institucionais aplicáveis;

VI - guardar sigilo e confidencialidade quanto aos dados pessoais acessados no exercício de suas atribuições, evitando sua exposição indevida;

VII - adotar medidas de segurança física e lógica no manuseio de dados pessoais, incluindo a proteção de documentos e de mídias, a guarda adequada, o transporte seguro, o controle de impressão e o descarte seguro, quando aplicáveis;

VIII - comunicar imediatamente à equipe de tratamento de incidentes de segurança da informação qualquer suspeita ou ocorrência de incidente de segurança envolvendo dados pessoais, observados os fluxos institucionais de resposta a incidentes, e colaborar com as ações de contenção, de análise e de mitigação de incidentes;

IX - colaborar, quando solicitado, com o mapeamento e a atualização de processos de trabalho e operações de tratamento de dados pessoais, fornecendo informações completas e atualizadas;

X - participar das ações de conscientização e de capacitação em proteção de dados pessoais e segurança da informação definidas pelo Ministério da Fazenda; e

XI - colaborar, quando solicitado, no atendimento às requisições dos titulares de dados pessoais, observando os prazos definidos nas normas pertinentes e assegurando a veracidade e a qualidade das informações.

§ 1º É vedado aos agentes públicos e aos colaboradores do Ministério da Fazenda no tratamento de dados pessoais:

I - utilizar ferramentas, contas, dispositivos, aplicativos ou repositórios não autorizados para o tratamento de dados pessoais;

II - manter bases de dados pessoais sem finalidade legítima, sem registro nos instrumentos institucionais ou sem controles adequados;

III - compartilhar dados pessoais por meios informais ou inadequados que ampliem indevidamente o acesso aos dados ou comprometam a segurança das informações; e

IV - inserir ou manter, de forma deliberada, informações incompletas, inexatas ou desatualizadas sobre dados pessoais em instrumentos institucionais de conformidade.

Art. 9º Na hipótese excepcional de indisponibilidade técnica comprovada de meio institucional autorizado, o tratamento de dados pessoais poderá ser realizado em meio alternativo exclusivamente de forma temporária, justificada e restrita ao mínimo necessário para a continuidade do serviço público, vedada sua utilização para finalidades diversas ou para fins de substituição permanente do meio institucional autorizado para o tratamento.

§ 1º A utilização de meio alternativo para o tratamento de dados pessoais deverá ser formalmente registrada pelo agente público responsável, com indicação da ocorrência, da justificativa, do período de utilização, dos dados pessoais tratados e da identificação do responsável pelo tratamento.

§ 2º O retorno à utilização do meio institucional autorizado para o tratamento de dados pessoais deverá ocorrer imediatamente após a restauração de sua disponibilidade, devendo ser assegurada a migração ou o descarte seguro dos dados eventualmente tratados no meio alternativo, conforme as diretrizes de proteção de dados pessoais previstas nesta Resolução.

§ 3º O tratamento de dados pessoais em meio alternativo deverá observar, no mínimo, controles equivalentes de segurança da informação e de proteção de dados pessoais exigidos para o meio institucional autorizado, vedado o uso de meios pessoais ou não controlados institucionalmente, salvo previsão expressa em norma complementar a esta Resolução.

§ 4º As ocorrências de utilização de meio alternativo para o tratamento de dados pessoais deverão ser submetidas a registro e monitoramento para fins de auditoria, de governança e de prestação de contas.

Obrigações dos titulares das unidades administrativas

Art. 10. Os titulares das unidades administrativas do Ministério da Fazenda deverão assegurar o adequado tratamento de dados pessoais no âmbito de sua competência, devendo, no mínimo:

I - apoiar institucionalmente a implementação desta Resolução e priorizar as ações necessárias para o seu cumprimento, mediante a alocação de recursos humanos, tecnológicos e informacionais compatíveis com o risco e com a criticidade das operações de tratamento de dados pessoais;

II - quando solicitado pela unidade correlata de proteção de dados pessoais, indicar ponto focal para coordenação das ações relacionadas à proteção de dados pessoais e para a interlocução com as instâncias competentes, conforme a Política de Governança de Proteção de Dados Pessoais do Ministério da Fazenda;

III - garantir o cadastramento, a atualização e a qualidade das informações referentes aos processos de trabalho que envolvam o tratamento de dados pessoais nos instrumentos institucionais aplicáveis, inclusive no IDP, assegurando que os registros sejam completos, corretos e atualizados;

IV - assegurar que os tratamentos de dados pessoais sob responsabilidade da unidade sejam submetidos à avaliação de riscos, com registro das análises, das decisões e das medidas adotadas, em articulação com as áreas competentes;

V - assegurar que sistemas, soluções, fluxos e meios utilizados pela unidade para tratar dados pessoais observem as diretrizes institucionais de segurança da informação e de proteção de dados pessoais, incluindo o uso prioritário de sistemas e de canais institucionais autorizados e a eliminação de bases paralelas não justificadas;

VI - assegurar que o compartilhamento de dados pessoais, quando necessário, seja realizado de forma minimizada, segura e documentada, observados os fluxos e requisitos institucionais aplicáveis;

VII - assegurar que a unidade responda de forma tempestiva, completa e tecnicamente adequada às solicitações relacionadas ao tratamento de dados pessoais, inclusive às demandas de titulares de dados, conforme os fluxos institucionais de proteção de dados pessoais, garantindo rastreabilidade do atendimento;

VIII - assegurar a comunicação imediata de suspeitas, de ocorrências ou de incidentes envolvendo dados pessoais aos canais oficiais competentes, e o apoio à contenção, à análise e à mitigação de incidentes, conforme o fluxo institucional de resposta a incidentes;

IX - assegurar a adoção de medidas de transparência sob responsabilidade da unidade, quando aplicável, incluindo a atualização de avisos de privacidade e de termos de uso; e

X - promover e incentivar ações permanentes de conscientização e de capacitação da equipe de trabalho, assegurando que os agentes públicos conheçam e apliquem as disposições desta Resolução no âmbito da unidade.

§ 1º Os titulares das unidades do Ministério da Fazenda deverão estabelecer mecanismos internos de supervisão e de acompanhamento para verificar o cumprimento das obrigações previstas no caput, incluindo a definição de responsáveis, de prazos e o registro das providências adotadas para o tratamento de dados pessoais.

§ 2º Os titulares das unidades do Ministério da Fazenda deverão adotar providências para a correção de não conformidades identificadas no tratamento de dados pessoais, com o registro das justificativas e das medidas corretivas adotadas, e o reporte às instâncias competentes, quando exigido por fluxo institucional de proteção de dados pessoais.

§ 3º O cumprimento das obrigações previstas no caput não afasta a responsabilidade dos agentes públicos e das unidades do Ministério da Fazenda quanto aos atos praticados e às informações prestadas no tratamento de dados pessoais.

§ 4º Para fins de priorização das ações de que trata o caput, o titular da unidade deverá considerar, no mínimo, a sensibilidade dos dados pessoais, o volume tratado, a exposição dos sistemas e serviços, a criticidade do processo de trabalho, a existência de compartilhamentos e o histórico de incidentes ou de não conformidades envolvendo o tratamento de dados pessoais.

CAPÍTULO III
DO INVENTÁRIO DE DADOS PESSOAIS – IDP

Art. 11. Os processos de trabalho que envolvam o tratamento de dados pessoais deverão ser cadastrados e mantidos atualizados no IDP, como registro institucional das operações de tratamento de dados pessoais realizadas no âmbito do Ministério da Fazenda.

§ 1º O IDP constitui instrumento obrigatório de registro das operações de tratamento de dados pessoais para fins de conformidade, de rastreabilidade e de prestação de contas, observado o dever legal de manutenção de registros pelos agentes de tratamento.

§ 2º O cadastramento e a atualização do IDP deverão ocorrer:

I - previamente ao início de novos tratamentos ou à entrada em operação de novos sistemas e soluções que tratem dados pessoais;

II - sempre que houver alteração relevante no tratamento de dados pessoais, incluindo finalidades, categorias de dados, fluxos, compartilhamentos, sistemas utilizados, base legal ou medidas de segurança; e

III - periodicamente, em prazo definido pela governança institucional de proteção de dados pessoais, ainda que não haja alterações relevantes, para confirmação de atualidade.

§ 3º A unidade responsável pelo processo de trabalho deverá assegurar que as informações registradas no IDP sejam completas, corretas, atualizadas e consistentes, buscando validação com as áreas

competentes pela proteção de dados pessoais no âmbito do Ministério da Fazenda, quando necessário.

§ 4º O IDP deverá subsidiar a identificação de operações de tratamento de dados pessoais que demandem avaliação quanto à necessidade de elaboração de Relatório de Impacto à Proteção de Dados Pessoais – RIPD, e apoiar a análise e a resposta a incidentes de segurança envolvendo dados pessoais.

Art. 12. O IDP deverá refletir, no mínimo, os seguintes aspectos:

I - identificação do processo de trabalho e da finalidade do tratamento de dados pessoais;

II - categorias de titulares e de dados pessoais tratados, com indicação de dados pessoais sensíveis, quando aplicável;

III - base legal aplicável ao tratamento de dados pessoais;

IV - origem dos dados pessoais, canais e instrumentos utilizados, com indicação de avisos de privacidade e de informações de transparência, quando aplicáveis;

V - agentes envolvidos no tratamento de dados pessoais;

VI - sistemas, soluções, repositórios e locais de armazenamento, incluindo ambientes de nuvem e soluções de terceiros, quando aplicáveis;

VII - compartilhamentos de dados pessoais, com indicação de destinatários, finalidade do compartilhamento, forma de transferência e salvaguardas adotadas;

VIII - prazos de retenção e critérios de eliminação ou descarte de dados pessoais, quando aplicáveis; e

IX - indicação da existência de avaliação de riscos associada ao tratamento de dados pessoais, com referência aos respectivos instrumentos e registros institucionais, inclusive RIPD, quando aplicável.

Parágrafo único. O IDP deverá apoiar o atendimento a titulares de dados pessoais pelas unidades do Ministério da Fazenda e a demonstração de conformidade no tratamento dos dados, respeitadas as hipóteses legais de sigilo aplicáveis.

CAPÍTULO IV
DO RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS – RIPD

Art. 13. A necessidade de elaboração de RIPD deverá ser avaliada pelo titular da unidade responsável pelo tratamento de dados pessoais no âmbito do Ministério da Fazenda, conforme critérios e fluxos definidos no âmbito da governança institucional de proteção de dados pessoais, observado o disposto no art. 38 da Lei nº 13.709, de 14 de agosto de 2018.

§ 1º A avaliação da necessidade de elaboração do RIPD deverá ocorrer, no mínimo:

I - previamente ao início de novo processo de trabalho ou à entrada em operação de sistema ou solução que envolva tratamento de dados pessoais; e

II - sempre que houver alteração relevante no tratamento de dados pessoais, incluindo finalidades, categorias de dados, base legal, compartilhamentos, tecnologias empregadas, volume, exposição ou controles de segurança.

§ 2º A avaliação de que trata o §1º deverá ser registrada, com indicação do responsável pela decisão, data, justificativa e elementos considerados, devendo ser vinculada ao respectivo registro no IDP.

§ 3º Nos casos em que a avaliação indicar a necessidade de elaboração do RIPD, o relatório deverá conter, no mínimo, os elementos previstos na Lei nº 13.709, de 14 de agosto de 2018, incluindo:

I - a descrição dos tipos de dados coletados;

II - a metodologia utilizada para a coleta e para a garantia da segurança das informações; e

III - a análise do controlador quanto a medidas, salvaguardas e mecanismos de mitigação de

risco adotados.

§ 4º O RIPD deverá ser revisado e atualizado sempre que ocorrerem mudanças relevantes no tratamento de dados pessoais ou incidentes que indiquem necessidade de reavaliação de riscos e salvaguardas adotadas.

§ 5º A elaboração, a revisão e a atualização do RIPD não substituem o dever de manutenção de registros no IDP, nem afastam a obrigação de adoção de medidas de segurança e de prevenção aplicáveis ao tratamento de dados pessoais.

CAPÍTULO V
DOS SISTEMAS INFORMATIZADOS E DA SEGURANÇA E PRIVACIDADE DA INFORMAÇÃO

Sistemas e soluções informatizados

Art. 14. Os sistemas e as soluções utilizados para o tratamento de dados pessoais no âmbito do Ministério da Fazenda deverão ser estruturados e operados em conformidade com os requisitos de segurança da informação, com as boas práticas de governança e privacidade, com os princípios de proteção de dados pessoais e com a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais.

§ 1º Os sistemas e as soluções que tratem dados pessoais deverão ser avaliados quanto aos riscos e aos controles de segurança, em periodicidade definida pela governança institucional de proteção de dados pessoais e conforme a criticidade do tratamento, com o devido registro das evidências, das conclusões e das medidas adotadas.

§ 2º A definição da ordem de precedência para as avaliações periódicas de segurança deverá considerar o nível de risco de cada sistema ou solução, priorizando-se aqueles que apresentem:

I - maior criticidade para a continuidade das atividades institucionais;

II - tratamento de dados pessoais sensíveis ou em larga escala;

III - elevado grau de exposição do ambiente a ameaças de segurança da informação ou de integração com terceiros; e

IV - histórico relevante de incidentes de segurança ou de desconformidades detectadas.

§ 3º Os sistemas e as soluções em fase de desenvolvimento ou de atualização deverão ser avaliados e, se necessário, corrigidos antes da entrada em operação, vedada a implantação sem o prévio tratamento de riscos e implementação de controles mínimos aplicáveis.

§ 4º A avaliação e a manutenção de que trata este artigo deverão estar integradas aos instrumentos institucionais aplicáveis, inclusive ao IDP, de modo a assegurar a rastreabilidade e a prestação de contas.

Art. 15. As medidas de controle de segurança da informação aplicáveis aos sistemas e às soluções que tratem dados pessoais deverão ser proporcionais ao risco e implementadas de forma verificável.

Privacidade desde a concepção e por padrão

Art. 16. A concepção, contratação, aquisição, desenvolvimento, sustentação e evolução de sistemas, serviços e processos de trabalho que envolvam tratamento de dados pessoais no âmbito do Ministério da Fazenda deverão incorporar privacidade desde a concepção - Privacy by Design e por padrão - Privacy by Default, com adoção de medidas técnicas e administrativas desde a fase de concepção do produto ou do serviço até a sua execução, observadas as diretrizes institucionais de proteção de dados pessoais e de segurança da informação.

§ 1º Para fins do disposto no caput, a privacidade desde a concepção e por padrão deverá ser implementada, no mínimo, por meio das seguintes tarefas:

I - definição prévia e documentada de finalidades do tratamento e limitação ao mínimo necessário de dados pessoais, com justificativa vinculada ao IDP;

II - configuração padrão de sistemas e serviços orientada à proteção de dados pessoais, incluindo restrição de acessos, minimização de exposição e desativação de funcionalidades não necessárias ao tratamento;

III - avaliação prévia de riscos e controles aplicáveis, com registro de decisões, planos de ação e evidências, integrada aos instrumentos institucionais de conformidade, incluindo o IDP e, quando aplicável, o RIPD;

IV - incorporação de requisitos de privacidade e segurança ao planejamento do projeto e aos critérios de aceitação, com validação prévia à entrada em operação;

V - manutenção de documentação técnica mínima atualizada, compatível com o risco, incluindo descrição do tratamento de dados pessoais, fluxos de dados, integrações, perfis de acesso e mecanismos de rastreabilidade, quando aplicáveis; e

VI - revisão dos requisitos de privacidade e segurança sempre que houver mudança relevante no tratamento ou ocorrência de incidentes de segurança envolvendo dados pessoais, com atualização da documentação e das evidências.

§ 2º A entrada em operação de novos sistemas, serviços ou atualizações relevantes que tratem dados pessoais dependerá da verificação de conformidade com os requisitos previstos no caput e com os controles mínimos de segurança da informação aplicáveis.

§ 3º As contratações, aquisições e instrumentos congêneres que envolvam soluções com tratamento de dados pessoais deverão prever requisitos de privacidade e proteção de dados pessoais ao longo de todo o ciclo de contratação, incluindo obrigações do fornecedor quanto à segurança, confidencialidade, apoio à auditoria e comunicação de incidentes, conforme orientações institucionais de proteção de dados pessoais e de segurança da informação.

§ 4º A aplicação do disposto neste artigo deverá ser evidenciada por registros mínimos, incluindo responsáveis, decisões e evidências de validação, de modo a permitir rastreabilidade, auditoria e melhoria contínua no tratamento de dados pessoais.

Termos de uso e avisos de privacidade

Art. 17. Os sistemas, serviços e demais canais institucionais do Ministério da Fazenda que envolvam o tratamento de dados pessoais deverão disponibilizar termos de uso e avisos de privacidade claros, acessíveis, atualizados e compatíveis com esta Resolução e com a legislação aplicável.

Parágrafo único. Os termos de uso e os avisos de privacidade de que trata o caput deverão ser apresentados em local de fácil acesso e visualização, e ser editados em linguagem acessível, clara e simples.

Art. 18. Nos avisos de privacidade deverão constar, no mínimo, as seguintes informações:

I - a indicação sobre o tratamento de dados pessoais sensíveis, quando aplicável;

II - a indicação sobre o tratamento de dados pessoais de crianças e adolescentes, quando aplicável;

III - o prazo de retenção dos dados pessoais;

IV - a finalidade do tratamento de dados pessoais;

V - a hipótese legal que fundamenta o tratamento de dados pessoais, nos termos da Lei nº 13.709, de 14 de agosto de 2018;

VI - a previsão legal do tratamento de dados pessoais, com indicação das normas que o fundamentam;

VII - as informações sobre o compartilhamento de dados pessoais com outras instituições, quando aplicável, ou a indicação de sua não ocorrência; e

VIII - as informações sobre transferência internacional de dados pessoais, quando aplicável, ou a indicação de sua não realização.

Parágrafo único. Quando o consentimento for a base legal aplicável para o tratamento de

dados pessoais, o consentimento deverá ser solicitado de forma livre, informada e inequívoca, e o aviso de privacidade deverá indicar o modo de revogação e seus efeitos.

Art. 19. Nos termos de uso deverão constar, no mínimo, as seguintes informações:

I - os termos e as políticas aplicáveis, e as respectivas ciências ou aceitações, quando exigidos;

II - as definições dos principais termos, conceitos e expressões utilizados no serviço;

III - a descrição da finalidade, das funcionalidades e das condições de utilização do serviço;

IV - o arcabouço legal e normativo aplicável à prestação e à utilização do serviço;

V - os direitos do usuário do serviço;

VI - as responsabilidades do usuário do serviço;

VII - as responsabilidades do Ministério da Fazenda;

VIII - no caso dos sítios eletrônicos, portais e aplicativos móveis, o detalhamento dos requisitos técnicos;

IX - os canais de contato para atendimento ao titular dos dados pessoais, esclarecimento de dúvidas e recebimento de manifestações;

X - a forma de comunicação das mudanças no termo de uso;

XI - o foro elegido para a resolução de controvérsias; e

XII - a versão e a data do documento.

Art. 20. Os termos de uso e os avisos de privacidade deverão ser:

I - elaborados previamente à entrada em produção de novos sistemas ou serviços que envolvam o tratamento de dados pessoais; e

II - revisados e atualizados sempre que houver alterações que impliquem impacto no tratamento de dados pessoais, incluindo, mas não se limitando, a modificações de finalidades, categorias de dados tratados, hipóteses de compartilhamento ou canais de coleta e tratamento de dados pessoais.

Parágrafo único. As unidades do Ministério da Fazenda responsáveis pelos sistemas e serviços deverão manter registro mínimo das versões, datas de publicação e principais alterações dos termos de uso e dos avisos de privacidade, de modo a permitir rastreabilidade e prestação de contas.

CAPÍTULO VI
DO CONSENTIMENTO E DOS DIREITOS DOS TITULARES DE DADOS PESSOAIS

Consentimento do titular de dados pessoais

Art. 21. Quando o consentimento do titular for utilizado como base legal para o tratamento de dados pessoais no âmbito do Ministério da Fazenda, sua gestão deverá assegurar registro, rastreabilidade e possibilidade de revogação, nos termos da legislação aplicável e das orientações institucionais de proteção de dados pessoais.

§ 1º O consentimento pelo titular dos dados pessoais deverá ser:

I - vinculado a finalidades específicas e determinadas, sendo nulas as autorizações genéricas para tratamento de dados pessoais;

II - informado, devendo ser apresentado de forma destacada, de modo a permitir compreensão clara pelo titular;

III - inequívoco, sendo coletado por meio que demonstre a manifestação de vontade do titular, com preservação de evidências do ato de consentir; e

IV - livre, vedadas práticas que o condicione de forma indevida ao acesso ao serviço quando

não estritamente necessário à finalidade informada.

§ 2º Caberá ao responsável pelo tratamento de dados pessoais manter a prova de que o consentimento foi obtido em conformidade com o disposto no §1º, mantendo registro mínimo que contenha os seguintes aspectos:

I - identificação do titular dos dados pessoais, data e canal de coleta do consentimento;

II - finalidade autorizada, os dados armazenados e, quando aplicável, o período de validade;

III - vinculação ao aviso de privacidade vigente à época da coleta, com controle de versão e histórico de alterações; e

IV - registro de eventuais revogações, atualizações e comunicações associadas.

§ 3º O titular dos dados pessoais poderá revogar o consentimento a qualquer tempo, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação.

§ 4º Sempre que houver alteração relevante nas informações relacionadas ao tratamento de dados pessoais baseado em consentimento, o titular dos dados deverá ser informado de forma destacada e específica, assegurando a possibilidade de revogação do consentimento, caso discorde da alteração.

§ 5º Caso exista outra base legal aplicável ao tratamento de dados pessoais no âmbito do Ministério da Fazenda, o tratamento não deverá ser realizado com base no consentimento pelo titular.

§ 6º Os sistemas e os serviços do Ministério da Fazenda que utilizem o consentimento pelo titular como base legal para o tratamento de dados pessoais deverão implementar controles para:

I - impedir o tratamento de dados pessoais fora do escopo consentido pelo titular dos dados;

II - garantir a revogação tempestiva do consentimento e a atualização de seu status em todos os fluxos de tratamento de dados pessoais e integrações de sistemas que dependam desta base legal;

III - manter trilhas de auditoria e registros de eventos relacionados à coleta, à alteração e à revogação do consentimento; e

IV - suportar extração de relatórios e de evidências para atendimento ao titular dos dados pessoais e às auditorias internas, respeitadas as hipóteses legais de sigilo aplicáveis.

Direitos dos titulares de dados pessoais

Art. 22. O Ministério da Fazenda assegurará a existência e o funcionamento de canal institucional de atendimento aos titulares de dados pessoais, para recepcionar, registrar, acompanhar e responder solicitações relacionadas aos direitos previstos na Lei nº 13.709, de 14 de agosto de 2018.

§ 1º Sem prejuízo do canal institucional de que trata o caput, os órgãos que integram a Rede de Proteção de Dados Pessoais prevista na Resolução CGSP/MF nº 7, de 14 de janeiro de 2026, deverão manter canal próprio para atendimento às solicitações dos titulares de dados pessoais no âmbito de suas competências.

§ 2º O canal próprio de que trata o § 1º deverá possuir, no mínimo, as seguintes características:

I - ser de fácil acesso, permanente e com acompanhamento contínuo de seu funcionamento;

II - permitir o registro e a rastreabilidade das solicitações recebidas;

III - assegurar mecanismos adequados de identificação e de autenticação do titular dos dados pessoais ou de representante legalmente constituído, quando aplicável; e

IV - manter registros relativos a prazos, encaminhamentos internos, respostas e respectivas evidências.

§ 3º A identidade e as informações de contato dos encarregados setoriais e correlatos e do canal próprio de que trata o § 1º deverão ser divulgadas publicamente, de forma clara e objetiva, em meios oficiais do respectivo órgão, observado o disposto na Lei nº 13.709, de 14 de agosto de 2018, e na Política de

Governança de Proteção de Dados Pessoais do Ministério da Fazenda.

§ 4º As comunicações e as requisições da Agência Nacional de Proteção de Dados – ANPD serão recebidas e tramitadas por meio do canal oficial definido pela própria ANPD, devendo ser tratadas internamente pelos encarregados setoriais e correlatos competentes, nos termos da Política de Governança de Proteção de Dados Pessoais do Ministério da Fazenda, com registro, rastreabilidade e adoção das providências cabíveis.

§ 5º As solicitações dos titulares de confirmação de existência de tratamento ou de acesso a dados pessoais deverão ser atendidas:

I - em formato simplificado, imediatamente; ou

II - por meio de declaração clara e completa, fornecida no prazo de até quinze dias, contado da data do requerimento, contendo, quando aplicáveis, a origem dos dados pessoais, a inexistência de registro de dados pessoais, os critérios utilizados e a finalidade do tratamento, observadas as hipóteses de sigilo e as limitações legais aplicáveis.

§ 6º Na impossibilidade de adoção imediata da providência solicitada pelo titular de dados pessoais, a resposta da unidade deverá, no mínimo:

I - indicar as razões de fato ou de direito que impedem o atendimento imediato da providência; ou

II - quando aplicável, informar que o Ministério da Fazenda não é agente de tratamento dos dados pessoais e indicar, sempre que possível, o agente responsável.

Art. 23. As unidades do Ministério da Fazenda deverão responder às solicitações dos titulares de dados pessoais encaminhadas pelos canais previstos no art. 22, observados os prazos, os fluxos e os padrões definidos no âmbito da governança institucional de proteção de dados pessoais, garantindo qualidade técnica, completude, rastreabilidade e respeito às hipóteses legais de sigilo aplicáveis.

§ 1º Para fins do disposto no caput, as unidades deverão adotar, no mínimo, as seguintes providências:

I – manter ponto de contato interno para coordenar o recebimento, a consolidação e o envio das informações necessárias ao atendimento das solicitações dos titulares de dados pessoais;

II - identificar e validar as informações relativas ao tratamento de dados pessoais com base no IDP e em demais registros institucionais aplicáveis, assegurando sua consistência e atualização;

III - informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados pessoais a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional; e

IV - preservar evidências do atendimento da solicitação e das providências adotadas, de modo a permitir auditoria e prestação de contas.

§ 2º As respostas e as evidências do atendimento das solicitações de que trata o caput deverão ser encaminhadas aos titulares dos dados pessoais, no prazo estabelecido pelo fluxo institucional de proteção de dados pessoais, de forma a permitir resposta tempestiva ao titular e, quando aplicável, o atendimento de requisições recebidas por meio do canal oficial da ANPD.

§ 3º A recusa de atendimento da solicitação do titular de dados pessoais deverá ser fundamentada, com indicação da base legal e da hipótese de sigilo aplicável, devendo ser registrada e tratada conforme o fluxo institucional de proteção de dados pessoais.

§ 4º As unidades do Ministério da Fazenda deverão tratar com prioridade as solicitações de que trata o caput que envolvam risco de dano relevante ao titular ou que se relacionem a incidentes de segurança envolvendo dados pessoais, sem prejuízo da observância dos fluxos institucionais de resposta a incidentes.

CAPÍTULO VII
DOS CONTRATOS E INSTRUMENTOS CONGÊNERES

Art. 24. Os contratos, convênios, instrumentos congêneres e demais ajustes que envolvam o tratamento de dados pessoais no âmbito do Ministério da Fazenda deverão prever cláusulas e requisitos mínimos de proteção de dados pessoais e de segurança da informação.

§ 1º A observância do disposto no caput deve ocorrer desde a fase do planejamento até o encerramento do respectivo ajuste, inclusive quanto às providências posteriores necessárias à proteção de dados pessoais e à segurança da informação, de modo a assegurar a governança, a rastreabilidade e a conformidade com a legislação vigente, e deve contemplar, no mínimo:

I - a identificação dos papéis e responsabilidades das partes no tratamento de dados pessoais, inclusive quanto à atuação como controlador ou operador, conforme o caso;

II - a obrigatoriedade de o operador realizar o tratamento estritamente conforme as instruções documentadas do controlador;

III - a definição de finalidades do tratamento, escopo, categorias de dados e de titulares, duração, fluxos, integrações e locais de armazenamento e processamento, quando aplicável;

IV - o estabelecimento de obrigações de confidencialidade, restrição de acesso, segregação de perfis e controle de credenciais, proporcionais ao risco identificado;

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

VI - a previsão de obrigações de registro e rastreabilidade das operações relevantes e de eventos de segurança, com preservação de evidências e apoio a auditorias e investigações, respeitadas as hipóteses legais de sigilo aplicáveis;

VII - o regramento da subcontratação, quando admitida pela legislação e pelo respectivo instrumento contratual, assegurando que os subcontratados fiquem sujeitos a obrigações de proteção de dados pessoais, segurança da informação, confidencialidade e comunicação de incidentes compatíveis com aquelas aplicáveis ao contratado principal;

VIII - o estabelecimento de obrigação de apoio ao atendimento de direitos do titular de dados pessoais, incluindo prazos de resposta e fornecimento de informações necessárias ao cumprimento de solicitações;

IX - a obrigação de comunicação imediata ao controlador de incidentes e eventos de segurança relacionados a dados pessoais, com fornecimento de informações necessárias à contenção, à análise, à mitigação e eventual comunicação às autoridades e titulares, quando aplicável;

X - o regramento sobre retenção, devolução e eliminação segura de dados pessoais ao término do ajuste, incluindo descarte de cópias residuais e preservação de registros exigidos por obrigação legal; e

XI - a previsão de mecanismos de monitoramento e verificação do cumprimento contratual, incluindo indicadores, evidências mínimas, direito de auditoria e sanções em caso de descumprimento.

§ 2º Quando houver transferência internacional de dados pessoais no âmbito da contratação, o instrumento deverá:

I - prever o mecanismo de transferência internacional aplicável, observadas as disposições da Lei nº 13.709, de 14 de agosto de 2018, e da regulamentação da ANPD, bem como as orientações dos órgãos competentes; e

II - incorporar, nas hipóteses de transferência internacional fundamentada em cláusulas contratuais, as Cláusulas-Padrão Contratuais aprovadas pela ANPD, sem alteração de seu conteúdo, observados os requisitos e as condições estabelecidos na regulamentação aplicável, inclusive quanto à submissão das partes à fiscalização da autoridade brasileira.

§ 3º Os contratos, convênios e instrumentos congêneres vigentes que envolvam tratamento de dados pessoais deverão ser revisados periodicamente e, quando necessário, adequados aos requisitos previstos neste artigo e às orientações institucionais, com registro das providências adotadas e dos responsáveis.

§ 4º A documentação e as evidências de conformidade relativas às contratações e à gestão contratual deverão ser mantidas de forma organizada e rastreável, de modo a permitir auditoria, prestação de contas e monitoramento institucional.

§ 5º O controlador deverá, conforme processos internos e proporcionalmente ao risco do tratamento, avaliar se operadores e demais agentes de tratamento cumprem as obrigações de proteção de dados pessoais e segurança previstas nos instrumentos contratuais, podendo utilizar, entre outros meios, análise de evidências, questionários, relatórios e auditorias.

§ 6º No encerramento de contrato, acordo ou instrumento congênere que envolva tratamento de dados pessoais, deverá ser assegurado encerramento seguro do fluxo de dados e a adoção de providências relativas à devolução, à anonimização, à eliminação ou ao descarte seguro dos dados pessoais tratados, conforme aplicável, com registro e preservação de evidências.

§ 7º A unidade responsável deverá assegurar a atualização das operações correspondentes no IDP quando da entrada em operação, aceitação técnica definitiva ou implementação de produtos e serviços que envolvam tratamento de dados pessoais, conforme aplicável, sem prejuízo dos atos de recebimento, liquidação e pagamento previstos na legislação contratual.

§ 8º A previsão dos requisitos de que trata este artigo deverá observar os modelos, minutas padronizadas e orientações da Advocacia-Geral da União e dos órgãos centrais competentes, quando aplicáveis, admitidas adaptações justificadas em razão das peculiaridades do objeto, da natureza do tratamento de dados pessoais e do risco envolvido.

CAPÍTULO VIII
DO COMPARTILHAMENTO DE DADOS PESSOAIS

Art. 25. O compartilhamento de dados pessoais no âmbito do Ministério da Fazenda deverá observar o disposto na Lei nº 13.709, de 14 de agosto de 2018, no Decreto nº 10.046, de 9 de outubro de 2019, e nas orientações institucionais de proteção de dados pessoais, devendo ser realizado de forma minimizada, segura, motivada e rastreável.

§ 1º O uso compartilhado de dados pessoais pelas unidades do Ministério da Fazenda deverá atender a finalidades específicas de execução de políticas públicas e de cumprimento de atribuição legal, nos termos dos arts. 23 e 26 da Lei nº 13.709, de 14 de agosto de 2018, respeitados os princípios de proteção de dados pessoais.

§ 2º Previamente ao compartilhamento de dados pessoais, a unidade responsável deverá:

I - registrar a operação no IDP, com indicação da finalidade do uso do dado pessoal, base legal aplicável, os dados pessoais a serem compartilhados, a identificação do destinatário, o mecanismo de compartilhamento e as medidas de segurança aplicáveis;

II - avaliar a necessidade e a proporcionalidade da operação, garantindo que serão compartilhados apenas os dados pessoais estritamente necessários ao atendimento da finalidade informada;

III - definir, previamente ao compartilhamento, as responsabilidades e os pontos de contato entre as partes envolvidas, inclusive quanto à gestão de incidentes e ao atendimento aos direitos dos titulares dos dados pessoais; e

IV - assegurar que o mecanismo de compartilhamento de dados pessoais e os controles de segurança sejam compatíveis com o nível de risco da operação e, quando aplicável, alinhados entre as partes envolvidas.

§ 3º O compartilhamento de dados pessoais deverá ser formalizado por instrumento jurídico apropriado quando exigido por lei ou necessário para definir o escopo, as responsabilidades, as salvaguardas e as condições operacionais, observadas as hipóteses legais de sigilo aplicáveis e a vedação de tratamento para finalidades diversas das pactuadas.

§ 4º É vedado ao Ministério da Fazenda transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto nas hipóteses previstas na Lei nº 13.709, de 14 de agosto de 2018, incluindo:

I - execução descentralizada de atividade pública que exija a transferência, exclusivamente para fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011;

II - dados acessíveis publicamente, observadas as disposições da Lei nº 13.709, de 14 de agosto de 2018;

III - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou

IV - quando a transferência dos dados pessoais for destinada exclusivamente à prevenção de fraudes e irregularidades ou à proteção e resguardo da segurança e da integridade do titular dos dados, desde que vedado o tratamento para outras finalidades.

§ 5º Nos casos em que a legislação ou a regulamentação da ANPD exigir a comunicação de operações de compartilhamento de dados pessoais ao setor privado, a providência deverá ser adotada pelo encarregado setorial e correlato, por meio do canal oficial definido pela agência, com registro e rastreabilidade.

§ 6º As unidades deverão assegurar que o órgão ou a entidade destinatária implemente salvaguardas compatíveis com os riscos da operação, e que possuam, quando aplicáveis, controles de segurança equivalentes aos exigidos no âmbito do Ministério da Fazenda, incluindo:

I - controles de acesso, segregação de perfis e rastreabilidade dos dados pessoais;

II - proteção dos canais de comunicação e dos mecanismos de compartilhamento dos dados pessoais;

III - obrigações de confidencialidade e de limitação de uso dos dados pessoais à finalidade estabelecida; e

IV - procedimentos de resposta a incidentes e comunicação tempestiva entre as partes.

§ 7º Quando houver o compartilhamento de dados pessoais, as unidades responsáveis deverão assegurar a atualização dos avisos de privacidade e das informações institucionais pertinentes, quando aplicáveis.

§ 8º O compartilhamento de dados pessoais deverá ser revisto periodicamente e sempre que houver alteração relevante na finalidade, no escopo, no destinatário, nos dados pessoais, nos mecanismos de compartilhamento ou nas medidas de segurança, com a devida atualização do IDP e registro das providências adotadas pela unidade do Ministério da Fazenda.

§ 9º O disposto neste artigo não afasta a observância da legislação específica sobre sigilo e proteção da informação e da regulamentação complementar expedida pela ANPD.

§ 10 As unidades do Ministério da Fazenda deverão assegurar que os dados pessoais necessários ao uso compartilhado estejam disponíveis em formato interoperável e estruturado, observadas as normas e diretrizes pertinentes.

CAPÍTULO IX
DA GESTÃO DE INCIDENTES

Art. 26. Os incidentes de segurança envolvendo dados pessoais no âmbito do Ministério da

Fazenda deverão ser comunicados, registrados, tratados e respondidos conforme o fluxo institucional de gestão de incidentes de segurança da informação, com atuação coordenada das instâncias competentes, para fins de análise, de contenção, de mitigação, de recuperação e de melhoria contínua no tratamento de dados pessoais.

§ 1º Todo agente público ou colaborador do Ministério da Fazenda que identifique ou suspeite da ocorrência de incidente envolvendo dados pessoais deverá comunicá-lo imediatamente à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR, pelos canais institucionais de reporte, fornecendo as informações mínimas para triagem, classificação e contenção do incidente.

§ 2º A resposta a incidentes envolvendo dados pessoais deverá assegurar, no mínimo, a revisão e a atualização de controles, de procedimentos e, quando aplicáveis, dos registros no IDP e no RIPD.

§ 3º Quando o incidente puder acarretar risco ou dano relevante aos titulares dos dados pessoais, o controlador deverá comunicar a ocorrência à ANPD e aos titulares afetados, observado o disposto no art. 48 da Lei nº 13.709, de 14 de agosto de 2018, e na Resolução CD/ANPD nº 15, de 24 de abril de 2024.

§ 4º A comunicação de que trata o § 3º deverá conter, no mínimo, as seguintes informações:

I - a descrição da natureza dos dados pessoais afetados;

II - as informações sobre os titulares de dados pessoais envolvidos;

III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados pessoais, observados os sigilos legais aplicáveis;

IV - os riscos relacionados ao incidente;

V - os motivos da demora, se a comunicação não ter sido imediata; e

VI - as medidas adotadas ou a serem adotadas pela unidade para reverter ou mitigar os efeitos do prejuízo decorrente do incidente.

§ 5º A comunicação de incidente envolvendo dados pessoais à ANPD deverá ser realizada por meio do canal oficial definido pela própria agência, por agente competente, nos termos do fluxo institucional de proteção de dados pessoais, com registro e preservação de evidências do envio e do conteúdo comunicado.

§ 6º A comunicação aos titulares de dados pessoais afetados deverá ser realizada em linguagem clara e adequada, por meio que assegure a efetiva da ciência do titular, observadas as orientações da ANPD e o fluxo institucional de proteção de dados pessoais, incluindo, quando aplicáveis, orientações sobre medidas que possam ser adotadas pelo titular para reduzir ou mitigar os riscos decorrentes do incidente.

§ 7º O registro do incidente de segurança com dados pessoais, tenha ele sido objeto de comunicação à ANPD e aos titulares ou não, deverá ser mantido pelo prazo mínimo de cinco anos, contado da ocorrência do incidente, sem prejuízo da aplicação de prazos superiores ou de guarda permanente previstos em normas arquivísticas, inclusive aquelas definidas em tabela de temporalidade própria ou pelo Conselho Nacional de Arquivos.

§ 8º Na hipótese de o incidente com dados pessoais envolver operador ou terceiro contratado pelo Ministério da Fazenda, deverão ser observadas as obrigações contratuais de comunicação tempestiva, cooperação, fornecimento de informações e evidências, e execução de medidas corretivas, sem prejuízo da adoção das providências institucionais cabíveis.

§ 9º Os incidentes de segurança envolvendo dados pessoais deverão subsidiar, de forma estruturada, a revisão de riscos associados às operações de tratamento, e a atualização de controles, do IDP e, quando aplicável, do RIPD, com registro das medidas adotadas e das lições aprendidas pelas unidades do Ministério da Fazenda.

§ 10. O registro de todos os incidentes relacionados a dados pessoais, que tenham sido comunicados ou não à ANPD e aos titulares, deverá ser consolidado no Registro Geral de Incidentes com

Dados Pessoais - RGI-DP sob gestão do encarregado setorial e correlato, visando assegurar a rastreabilidade e a melhoria contínua dos controles envolvendo dados pessoais no âmbito do Ministério da Fazenda.

CAPÍTULO X
DA CAPACITAÇÃO E DA CONSCIENTIZAÇÃO EM PROTEÇÃO DE DADOS PESSOAIS

Art. 27. O Ministério da Fazenda deverá promover ações permanentes de conscientização e de capacitação em proteção de dados pessoais, integradas às práticas de segurança da informação, com o objetivo de assegurar a aplicação efetiva desta Resolução, prevenir incidentes e mitigar riscos.

§ 1º As ações de conscientização e capacitação de que trata o caput deverão, no mínimo:

I - contemplar conteúdo obrigatório, no ingresso de agentes públicos e colaboradores do Ministério da Fazenda, sobre princípios, deveres e vedações aplicáveis ao tratamento de dados pessoais;

II - ocorrer de forma contínua, incluindo comunicações internas, campanhas e materiais de orientação;

III - abranger práticas sobre tratamento seguro de dados pessoais, minimização, uso de sistemas institucionais, compartilhamento responsável, proteção de documentos, prevenção de incidentes e comunicação de eventos; e

IV - incorporar lições aprendidas de incidentes, auditorias e avaliações de conformidade, com foco na melhoria contínua no tratamento de dados pessoais.

§ 2º Para fins de capacitação específica, deverão ser priorizados os agentes públicos e as atividades com maior exposição a riscos envolvendo dados pessoais, incluindo, quando aplicáveis:

I - gestores de unidades e pontos focais responsáveis por coordenação interna de ações;

II - equipes que desenvolvam, mantenham, operem ou administrem sistemas e soluções que tratem dados pessoais;

III - equipes envolvidas em contratações e gestão contratual com tratamento de dados pessoais por terceiros; e

IV - equipes envolvidas no atendimento a titulares de dados pessoais, no tratamento de incidentes e na gestão de riscos.

§ 3º As unidades do Ministério da Fazenda deverão assegurar a disponibilização das ações de conscientização e de capacitação em proteção de dados pessoais e incentivar a participação dos agentes públicos e colaboradores, em especial dos pontos focais e demais atores previstos na Política de Governança de Dados Pessoais, registrando a participação e, quando aplicável, as evidências de conclusão das atividades de conscientização e capacitação.

§ 4º O Ministério da Fazenda deverá manter registros mínimos das ações de capacitação e de conscientização em proteção de dados pessoais realizadas, incluindo conteúdos, públicos-alvo, datas e indicadores de participação, de modo a permitir rastreabilidade e demonstração de efetividade, observadas as diretrizes desta Resolução.

CAPÍTULO XI
DO CICLO DE VIDA DOS DADOS PESSOAIS

Art. 28. As unidades do Ministério da Fazenda deverão gerir o ciclo de vida dos dados pessoais sob sua responsabilidade, definindo critérios de retenção, de revisão e de eliminação de dados, de modo a assegurar o encerramento do tratamento quando alcançada a sua finalidade ou quando os dados pessoais deixarem de ser necessários ou pertinentes, observado o disposto no art. 15 da Lei nº 13.709, de 14 de agosto de 2018.

§ 1º O término do tratamento de dados pessoais deverá ser identificado e registrado pela unidade responsável, no mínimo, nas seguintes hipóteses:

I - verificação de que a finalidade do tratamento foi alcançada ou de que os dados pessoais deixaram de ser necessários ou pertinentes ao alcance da finalidade específica;

II - término do período de tratamento;

III - comunicação do titular dos dados pessoais, inclusive no exercício do direito de revogação do consentimento, resguardado o interesse público; ou

IV - determinação da ANPD, quando houver violação ao disposto na Lei nº 13.709, de 14 de agosto de 2018.

§ 2º As unidades do Ministério da Fazenda deverão estabelecer critérios e prazos de retenção e de descarte de dados pessoais por processo de trabalho, compatíveis com:

I - a finalidade do tratamento;

II - as obrigações legais ou regulatórias aplicáveis;

III - as hipóteses legais de sigilo; e

IV - os riscos associados ao tratamento.

§ 3º As unidades do Ministério da Fazenda deverão registrar no IDP os critérios e os prazos de que trata o § 2º.

§ 4º As rotinas de retenção e de eliminação de dados pessoais pelas unidades do Ministério da Fazenda deverão abranger, quando aplicáveis, cópias de trabalho, repositórios, integrações e cópias de segurança, respeitados os limites técnicos e as regras institucionais de continuidade dos serviços, recuperação de ambientes tecnológicos e preservação da disponibilidade das informações.

Art. 29. Os dados pessoais deverão ser eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades realizadas pelas unidades do Ministério da Fazenda, autorizada a conservação para as seguintes finalidades:

I - cumprimento de obrigação legal ou regulatória pelo controlador;

II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na Lei nº 13.709, de 14 de agosto de 2018; ou

IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados pessoais.

§ 1º A eliminação dos dados pessoais deverá ser realizada de forma segura e verificável, devendo a unidade do Ministério da Fazenda manter registro mínimo da execução, incluindo escopo, data, responsável e método adotado, preservadas as evidências necessárias à prestação de contas.

§ 2º Na hipótese de impossibilidade técnica de eliminação imediata dos dados pessoais, a unidade do Ministério da Fazenda deverá:

I - adotar salvaguardas compensatórias, tais como restrição de acesso, bloqueio lógico, segregação e monitoramento;

II - registrar a justificativa da impossibilidade técnica de eliminação imediata dos dados pessoais; e

III - definir prazo para regularização.

CAPÍTULO XII
DA ANONIMIZAÇÃO, DA PSEUDONIMIZAÇÃO E DA PUBLICIZAÇÃO DE DADOS PESSOAIS

Art. 30. As unidades do Ministério da Fazenda deverão adotar técnicas de anonimização e, quando aplicável, de pseudonimização, como medidas de mitigação de riscos e de proteção de dados pessoais, especialmente para fins de publicização de informações, de elaboração de relatórios, de estudos, de estatísticas e de compartilhamentos de dados que não demandem identificação do titular.

§ 1º A anonimização deverá ser realizada mediante a utilização de meios técnicos razoáveis e disponíveis na ocasião do tratamento de dados pessoais, por meio dos quais o dado não possa ser associado, direta ou indiretamente, a um indivíduo.

§ 2º Os dados anonimizados não serão considerados dados pessoais para os fins da Lei nº 13.709, de 14 de agosto de 2018, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

§ 3º As unidades do Ministério da Fazenda deverão avaliar e registrar o risco de reversibilidade da anonimização de dados pessoais, considerando fatores objetivos, como o custo e o tempo necessários para reverter o processo de anonimização, o contexto e a finalidade do tratamento.

§ 4º Previamente à publicação ou à divulgação de documentos, relatórios ou bases de dados, a unidade responsável deverá:

I - avaliar a existência de dados pessoais e a necessidade de sua exposição;

II - aplicar a anonimização de dados pessoais ou técnicas equivalentes, caso a identificação do titular seja prescindível;

III - validar o resultado, considerando o risco de reidentificação; e

IV - registrar os critérios e as técnicas empregadas, com preservação de evidências.

§ 5º A pseudonimização poderá ser utilizada como salvaguarda adicional quando houver necessidade de manutenção do vínculo controlado com o titular dos dados pessoais, hipótese em que a informação adicional que permita reidentificação deverá ser mantida separadamente, em ambiente seguro, com controles de acesso restritos e medidas técnicas e administrativas adequadas.

§ 6º As unidades do Ministério da Fazenda deverão observar as orientações e os procedimentos institucionais de proteção de dados pessoais vigentes sobre anonimização e publicização de informações, incluindo padrões técnicos, ferramentas e práticas recomendadas pela unidade correlata de proteção de dados pessoais.

CAPÍTULO XIII
DO USO DE SOLUÇÕES DE INTELIGÊNCIA ARTIFICIAL E DECISÕES AUTOMATIZADAS

Soluções de inteligência artificial

Art. 31. O tratamento de dados pessoais por meio de soluções de inteligência artificial observará o disposto nesta Resolução, na Política de Uso Responsável de Soluções de Inteligência Artificial Generativa do Ministério da Fazenda e nas demais normas institucionais aplicáveis, devendo permanecer sob supervisão e responsabilidade de agente público, observada a Política de Governança de Proteção de Dados Pessoais do Ministério da Fazenda.

§ 1º A utilização de soluções de inteligência artificial que envolvam tratamento de dados pessoais deverá ser precedida de avaliação dos riscos inerentes ao tratamento e da necessidade de elaboração de RIPD.

§ 2º Na avaliação de que trata o § 1º deverão ser considerados, entre outros aspectos:

I - a natureza, a finalidade e o contexto do tratamento de dados pessoais;

II - o tratamento de dados pessoais sensíveis;

III - a possibilidade de produção de inferências sobre os titulares dos dados pessoais;

IV - os impactos significativos aos direitos e às liberdades fundamentais dos titulares dos dados pessoais; e

V - o grau de autonomia, de opacidade e de complexidade da solução de inteligência artificial empregada.

§ 3º A utilização de soluções de inteligência artificial com dados anonimizados deverá ser precedida de avaliação documentada que demonstre, nos termos da Lei nº 13.709, de 14 de agosto de 2018, que o processo de anonimização impede a identificação do titular por meios técnicos razoáveis e disponíveis, considerado o contexto de uso, devendo essa avaliação permanecer registrada para fins de prestação de contas.

Decisões automatizadas

Art. 32. As decisões que afetem interesses do titular não poderão ser delegadas a soluções de tratamento automatizado de dados pessoais, devendo ser assegurada a supervisão e a responsabilidade de pessoa natural no processo decisório.

§1º Nos casos em que o tratamento automatizado for utilizado como subsídio à tomada de decisão, deverá ser assegurado ao titular dos dados pessoais:

I - o direito de solicitar revisão da decisão por pessoa natural; e

II - o fornecimento, mediante solicitação, de informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados, observadas as normas legais de sigilo aplicáveis.

§ 2º As unidades do Ministério da Fazenda deverão manter procedimento interno para gestão de solicitações de revisão que contemple a indicação do responsável pela análise.

§ 3º No caso de limitação ao fornecimento de informações em razão de hipótese legal de sigilo, a unidade do Ministério da Fazenda deverá:

I – registrar formalmente a justificativa para a restrição de fornecimento das informações; e

II - adotar medidas que permitam a verificação interna da ausência de discriminação indevida, para fins de auditoria ou fiscalização pela ANPD.

CAPÍTULO XIV
DISPOSIÇÕES FINAIS

Art. 33. O Ministério da Fazenda deverá instituir, manter, monitorar e revisar periodicamente o Programa de Governança em Privacidade – PGP/MF, com o objetivo de promover a conformidade da atuação das unidades com a legislação de proteção de dados pessoais, com a gestão de riscos à privacidade e com a adoção de medidas organizacionais, técnicas e administrativas voltadas à proteção dos dados pessoais.

Parágrafo único. O PGP/MF deverá ser publicizado em meios institucionais, respeitadas as hipóteses legais de sigilo e as restrições relacionadas à segurança da informação aplicáveis.

Art. 34. O Ministério da Fazenda poderá expedir guias, manuais e demais instrumentos de apoio necessários à operacionalização das disposições desta Resolução.

Parágrafo único. Os documentos de que trata o caput deverão:

I - ser compatíveis com o modelo de governança instituído pela Resolução CGSP/MF nº 7, de 14 de janeiro de 2026;

II - observar as diretrizes da unidade setorial de proteção de dados pessoais no âmbito do Ministério da Fazenda; e

III - manter alinhamento com as normas e com as orientações expedidas pelo CGSP/MF.

Art. 35. O descumprimento das obrigações previstas nesta Resolução sujeita o agente público ou o colaborador do Ministério da Fazenda às medidas administrativas cabíveis, sem prejuízo de outras responsabilidades previstas na legislação pertinente.

Art. 36. Esta Resolução deverá ser publicada em meio oficial e permanecer disponível em local de fácil acesso nas dependências das unidades do Ministério da Fazenda, devendo ser revisada e atualizada periodicamente.

§ 1º A revisão de que trata o caput deverá ocorrer, no mínimo:

I - periodicamente, para verificação da aderência da Política de Proteção de Dados Pessoais do Ministério da Fazenda às boas práticas de proteção de dados pessoais; e

II - sempre que houver alteração relevante no arcabouço normativo aplicável, na Política de Governança de Proteção de Dados Pessoais do Ministério da Fazenda ou em orientações e regulamentações da ANPD que impactem as disposições desta Resolução.

§ 2º As atualizações desta Resolução deverão ser registradas, com histórico de versões que contemple a data, o responsável e a síntese das alterações, de modo a permitir rastreabilidade e prestação de contas, com a devida publicação em meio oficial.

Art. 37. Os casos omissos e as dúvidas surgidas na aplicação desta Resolução serão dirimidos no âmbito do CGSP/MF, observada a Política de Governança de Proteção de Dados Pessoais do Ministério da Fazenda.

Art. 38. Ficam sem efeito em relação ao Ministério da Fazenda as seguintes resoluções do Comitê Estratégico de Privacidade e Proteção de Dados Pessoais do Ministério da Economia - CEPPDP/ME:

I - a Resolução CEPPDP/ME nº 7, de 22 de fevereiro de 2022;

II - a Resolução CEPPDP/ME nº 11, de 24 de junho de 2022;

III - a Resolução CEPPDP/ME nº 12, de 4 de outubro de 2022;

IV - a Resolução CEPPDP/ME nº 13, de 23 de novembro de 2022;

V - a Resolução CEPPDP/ME nº 14, de 24 de novembro de 2022;

VI - a Resolução CEPPDP/ME nº 15, de 6 de dezembro de 2022; e

VII - a Resolução CEPPDP/ME nº 16, de 26 de dezembro de 2022.

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

Documento assinado eletronicamente

THAYSSA MENDES TAVARES PENA

Documento assinado eletronicamente por **Thayssa Mendes Tavares Pena**, **Presidente(a)**, em 28/10/2026, às 16:19, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

A autenticidade deste documento pode ser conferida no site https://colaboragov.sei.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **65416813** e o código CRC **70159459**.