MINISTÉRIO PÚBLICO DO TRABALHO
Procuradoria Geral do Trabalho - CNPJ 26.989.715/0055-03
Secretaria Operacional da Chefia de Gabinete do Procurador Geral do Trabalho
SAUN Quadra 5, Lote C, Torre A - Asa Norte - Brasília/DF - CEP 70040-250
Tel. (61) 3314-8500 - portal.mpt.mp.br

Portaria n° 546.2026

Institui a Política de Gestão de Riscos de Privacidade no âmbito do Ministério Público do Trabalho.

O **PROCURADOR-GERAL DO TRABALHO**, no uso das atribuições conferidas pela Lei Complementar n° 75/1993,

CONSIDERANDO que a Emenda Constitucional n° 115/2022 incluiu a proteção de dados pessoais entre os direitos e garantias fundamentais, impondo aos órgãos públicos o dever de adotar medidas administrativas e técnicas voltadas à preservação da privacidade e da autodeterminação informativa;

CONSIDERANDO a necessidade de assegurar o cumprimento da Lei n° 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), que estabelece princípios, fundamentos e obrigações específicos para o tratamento de dados pessoais pela Administração Pública;

CONSIDERANDO o disposto na Resolução CNMP n° 281/2023, que disciplina a proteção de dados pessoais no âmbito do Ministério Público brasileiro, especialmente quanto à governança, à gestão de riscos, à segurança e à prevenção de incidentes;

CONSIDERANDO a edição da Política de Proteção de Dados Pessoais do MPT, que define diretrizes gerais para o tratamento de dados pessoais e estabelece a necessidade de instrumentos complementares destinados à gestão de riscos, avaliações de impacto e mecanismos de governança;

CONSIDERANDO a Política de Segurança Institucional de Dados Pessoais, que determina a obrigatoriedade de diretrizes específicas de gestão de riscos em privacidade para suportar a implementação das medidas de segurança institucional;

CONSIDERANDO a Política de Comunicação de Incidentes de Segurança com Dados Pessoais, que determina a integração entre a comunicação de incidentes e o processo institucional de gestão de riscos, bem como a necessidade de revisão e aperfeiçoamento contínuo dos controles organizacionais;

CONSIDERANDO a Política de Gestão de Riscos no âmbito do Ministério Público do

Trabalho, que estabelece diretrizes gerais, papéis, responsabilidades, objetivos e comprometimentos institucionais em relação à gestão de riscos, inclusive aqueles relacionados ao tratamento de dados pessoais;

CONSIDERANDO que a ausência de diretrizes normativas específicas sobre gestão de riscos em privacidade e proteção de dados pessoais pode gerar assimetrias de procedimentos, fragilidades de governança, inconsistências no tratamento de dados pessoais e maior exposição a incidentes e responsabilizações administrativas, civis e reputacionais;

CONSIDERANDO que o cenário tecnológico atual, marcado por transformação digital, interoperabilidade sistêmica, contratação de serviços em nuvem, uso de biometria, automação, inteligência artificial e elevado fluxo de dados pessoais, exige mecanismos estruturados de avaliação e mitigação de riscos;

CONSIDERANDO a necessidade de adoção de metodologia padronizada de gestão de riscos baseada em boas práticas internacionais, tais como as normas ISO 31000, ISO/IEC 27005, ISO/IEC 27701 e ISO/IEC 29134, amplamente reconhecidas por orientar organizações públicas e privadas na análise e mitigação de riscos de privacidade;

CONSIDERANDO a importância de operacionalizar os princípios de privacidade desde a concepção (Privacy by Design) e privacidade por padrão (Privacy by Default), assegurando que todo sistema, processo, projeto ou contratação que envolva dados pessoais incorpore salvaguardas técnicas e organizacionais adequadas;

CONSIDERANDO que a implementação de uma Política de Gestão de Riscos em Privacidade contribui para fortalecer a governança institucional, aumentar a maturidade organizacional em privacidade, proteger direitos fundamentais, prevenir incidentes e garantir a prestação de contas institucional;

CONSIDERANDO, por fim, a necessidade de consolidar, uniformizar e aprimorar as práticas internas de avaliação, mitigação e monitoramento de riscos relacionados ao tratamento de dados pessoais no âmbito do Ministério Público do Trabalho;

RESOLVE:

CAPÍTULO I – DISPOSIÇÕES PRELIMINARES

Art. 1° Instituir a Política de Gestão de Riscos de Privacidade que estabelece diretrizes, princípios, responsabilidades e procedimentos para a gestão de riscos de privacidade de dados pessoais no âmbito do Ministério Público do Trabalho, em conformidade com a Política de Proteção de Dados Pessoais e a Política de Gestão de Riscos do MPT.

§ 1° A gestão de riscos de privacidade integra o Sistema de Governança da Gestão de Riscos do MPT e deve ser incorporada a todos os processos, sistemas e projetos que envolvam tratamento de dados pessoais.

§ 2° Esta Política também se aplica à organização estendida, compreendendo fornecedores, operadores, suboperadores e terceiros envolvidos no tratamento de dados.

Art. 2° Para os fins desta política, além dos termos e definições constantes na Política de Gestão de Riscos do MPT, consideram-se:

I - Risco de privacidade: possibilidade, considerada em termos de probabilidade e impacto, de ocorrência de eventos, falhas ou vulnerabilidades — decorrentes de fatores estruturais, técnicos, humanos, processuais ou operacionais — que possam comprometer a confidencialidade, integridade, disponibilidade ou os direitos e liberdades dos titulares em razão do tratamento institucional de dados pessoais, causando impacto adverso aos titulares ou à instituição, inclusive de natureza reputacional;

II - Impacto sobre o titular: avaliação dos efeitos potenciais do risco sobre os titulares, independentemente da probabilidade de ocorrência;

III - Proprietário do risco de privacidade: agente que tem a responsabilidade de garantir que os riscos de privacidade sejam gerenciados de forma apropriada, possuindo autoridade necessária para tomar decisões para esse gerenciamento;

IV - Controle: medida técnica ou administrativa que visa detectar ou prevenir as causas e recuperar ou atenuar os impactos dos riscos de privacidade;

V - Registro de Operações de Tratamento de Dados Pessoais (ROTDP): inventário destinado a registrar os processos e as operações de tratamentos de dados pessoais realizadas no âmbito do MPT, nos termos do art. 37, da LGPD;

VI - Relatório de Impacto à Proteção de Dados Pessoais (RIPDP): documento destinado a identificar riscos e avaliar impactos de operações de tratamento de dados pessoais, nos termos do art. 37, da LGPD;

VII - Risco-chave: risco de privacidade que, pela sua gravidade, probabilidade ou impacto institucional, requer supervisão do CEPDAP e ciência pelo CGR;

VIII - Ativo de informação: qualquer recurso físico ou digital que armazena, processa, protege e transmite dados pessoais.

CAPÍTULO II – FINALIDADES E OBJETIVOS

Art. 3° Esta Política tem por tem por finalidade estabelecer estrutura, critérios, metodologia, papéis e responsabilidades para o gerenciamento de riscos de privacidade relacionados ao tratamento de dados pessoais no âmbito do Ministério Público do Trabalho.

Art 4° Constituem objetivos desta Política:

I - adotar metodologia uniforme e integrada de gestão de riscos relacionados ao tratamento de dados pessoais;

II - orientar unidades e agentes públicos sobre responsabilidades no ciclo de gestão de riscos de privacidade;

III - integrar o Registro de Operações de Tratamento de Dados Pessoais (ROTDP) ao processo de gestão de riscos;

IV - definir critérios para Relatórios de Impacto à Proteção de Dados Pessoais (RIPD);

V - assegurar integração entre riscos de privacidade, segurança da informação, segurança institucional e comunicação de incidentes;

VI - assegurar alinhamento da gestão de riscos com o planejamento institucional, inclusive estratégico, tático e operacional;

VII - promover comunicação e consulta contínua com partes interessadas;

VIII - assegurar melhoria contínua do processo de gestão de riscos e da aplicação dos controles;

IX - identificar tanto ameaças quanto oportunidades decorrentes de inovações que aumentem a proteção ou a eficiência no tratamento de dados;

X - prevenir danos aos titulares e impactos adversos à instituição;

XI - fortalecer a governança e estimular a adoção de boas práticas em privacidade.

CAPÍTULO III – DOS PRINCÍPIOS

Art. 5° São princípios da gestão de riscos de privacidade de dados pessoais no MPT:

I - os princípios previstos na LGPD, na Resolução CNMP n.° 281/2023 e na Política de Proteção de Dados Pessoais;

II - proteção dos direitos dos titulares dos dados pessoais;

III - avaliação contínua e integrada dos riscos de privacidade em todos os processos institucionais;

IV - responsabilidade e definição de papéis para todos os envolvidos no tratamento de dados pessoais;

V - segurança, prevenção, proporcionalidade, minimização de dados e transparência;

VI - privacidade e segurança técnica desde a concepção e por padrão (Privacy by Design e Privacy by Default);

VII - responsabilização e prestação de contas;

VIII - razoabilidade e relação custo-benefício na definição de controles;

IX - melhoria contínua do processo de gestão de riscos.

CAPÍTULO IV – GOVERNANÇA E RESPONSABILIDADE

Art. 6° A gestão de riscos em privacidade será executada segundo a seguinte estrutura:

I - Procurador-Geral do Trabalho:

a) zela para que a Política de Gestão de Riscos em Privacidade esteja alinhada à Política de Gestão de Riscos do Ministério Público do Trabalho e suas diretrizes estratégicas;

b) delibera sobre riscos sistêmicos relevantes em matéria de privacidade;

c) declara o nível de apetite ao risco aplicável ao risco de privacidade.

II - Comitê Estratégico de Proteção de Dados Pessoais (CEPDAP):

a) direciona e alinha esta política aos objetivos estratégicos institucionais, assegurando a promoção e a proteção do direito fundamental à privacidade;

b) avalia o impacto da não proteção de direito fundamental à privacidade na estratégia do MPT;

c) monitora os resultados e o desempenho das ações de tratamento dos riscos de privacidade relacionados à estratégia do MPT;

d) propõe melhorias e providências corretivas em gestão de riscos de privacidade em nível estratégico e de alta governança.

III - Comitê de Gestão de Riscos (CGR):

a) conduz a governança dos riscos corporativos;

b) define diretrizes, metodologias e critérios para avaliação e tratamento dos riscos de privacidade;

c) encaminha ao Comitê Estratégico de Proteção de Dados Pessoais (CEPDAP) os riscos de privacidade que estão acima dos níveis de tolerância ao risco.

IV - Encarregado pelo Tratamento de Dados Pessoais:

a) coordena a aplicação desta Política;

b) acompanha o resultado das análises de risco de privacidade;

c) monitora os riscos de privacidade acima do nível de apetite ao risco, orientando sobre ações de tratamento para redução do nível de risco;

d) garante o uso do Registro de Operação de Tratamento de Dados Pessoais (ROTDP) no processo de gestão de riscos de privacidade e orienta, supervisiona a elaboração, revisão e aprovação de Registro de Impacto à Proteção de Dados (RIPD);

e) articula-se com SETIC, Secretaria de Polícia, SIGR, unidades e segmentos que tratam dados pessoais;

f) presta contas e subsidia com informações relevantes o CEPDAP.

V - Secretaria de Integridade e Gestão de Riscos (SIGR):

a) elabora e aplica a metodologia do processo de gestão de riscos de privacidade;

b) presta apoio técnico aos órgãos e segmentos do MPT na execução do processo de gestão de riscos;

c) integra os riscos de privacidade com as demais categorias de riscos institucionais.

VI - Secretaria de Tecnologia da Informação e Comunicação (SETIC):

a) avalia riscos tecnológicos;

b) implementa controles de segurança da informação;

c) participa da avaliação de sistemas, serviços e contratações.

VII - Secretaria de Polícia do Ministério Público do Trabalho:

a) avalia fatores de riscos físicos, humanos e comportamentais;

b) integra riscos de privacidade aos riscos institucionais amplos.

Art. 7° Aos órgãos e segmentos do MPT responsáveis pelo tratamento de dados pessoais compete:

I - realizar o Registro de Operação de Tratamento de Dados Pessoais – ROTDP dos processos de trabalho, incluindo os sistemas que os suportam, que tratam dados pessoais;

II - conduzir o processo de gestão de riscos de privacidade no âmbito de seus objetos de riscos de privacidade;

III - definir e executar plano de tratamento de riscos de privacidade;

IV - encaminhar à Secretaria de Integridade e Gestão de Riscos os relatórios de gestão de ricos;

V - encaminhar ao Órgão Encarregado pelo Tratamento de Dados Pessoais os relatórios de gestão de riscos e o RIPDP, no caso de exigência legal ou determinação normativa.

§ 1° São considerados proprietários dos riscos os Procuradores-Chefes, Coordenadores Nacionais, Secretários, Diretores, chefes de gabinete e demais chefias de unidade e segmentos relativos aos processos, atividades, sistemas, serviços, projetos, contratações e demais objetos de gestão sob sua responsabilidade.

§ 2° Compete ao proprietário do risco executar todas as atividades do processo de gestão de riscos estabelecidas nesta Política, descritas no artigo 6°, para os objetos de gestão sob sua responsabilidade e que envolvam o tratamento de dados pessoais.

§ 3° Na hipótese de dúvida quanto à identificação do proprietário responsável por determinado risco dentro de uma mesma unidade, caberá à chefia comum imediata deliberar sobre a alocação da responsabilidade.

§ 4° Quando a dúvida envolver risco compartilhado por mais de uma unidade — seja no nível regional ou no nível da PGT — o caso será submetido ao Comitê de Proteção de Dados Pessoais (CEPDAP), que decidirá sobre a atribuição da responsabilidade, podendo solicitar manifestação técnica do Encarregado, do SIGR, da SETIC ou da Secretaria de Polícia, conforme o caso.

§ 5° A responsabilidade pela gestão de riscos prevista neste artigo não substitui, limita ou exclui as atribuições previstas na Política de Proteção de Dados Pessoais (PPDP), na Política de Segurança Institucional de Dados Pessoais (PSIDP), na Política de Comunicação de Incidentes (PCISP), nem as responsabilidades estabelecidas no marco legal aplicável.

CAPÍTULO V – OBJETOS DE GESTÃO DE RISCOS

Art. 8° Constituem objetos de gestão de riscos em privacidade e proteção de dados pessoais:

I - processos de trabalho;

II - atividades e rotinas administrativas;

III - sistemas, soluções tecnológicas, bancos de dados, serviços digitais e demais ativos de informação;

IV - projetos institucionais, inclusive de transformação digital e inovação;

V - contratações de bens e serviços, especialmente de TI;

VI - iniciativas que envolvam tratamento de dados pessoais em larga escala;

VII - unidades organizacionais e sua cadeia de responsabilidades;

VIII - demais estruturas, fluxos, artefatos ou recursos que impactem o tratamento de dados pessoais.

Parágrafo único. Considera-se incidente com dados em larga escala aquele que abranger número significativo de titulares, considerando, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica de localização dos titulares.

CAPÍTULO VI – PROCESSO DE GESTÃO DE RISCOS

Art. 9° O processo de gestão de riscos de privacidade seguirá o processo geral de gestão de riscos definido na Política de Gestão de Riscos do MPT adicionados com as seguintes especificidades:

I - nas fases de estabelecimento do contexto e identificação dos riscos, considerar os seguintes itens do ROTDP:

a) existência de operadores envolvidos no tratamento dos dados pessoais;

b) finalidade e fundamentação do tratamento de dados pessoais;

c) escopo do tratamento de dados pessoais;

d) natureza do tratamento de dados pessoais;

e) titulares dos dados pessoais;

f) compartilhamento de dados pessoais;

g) acesso por outros processos ou sistemas internos do MPT;

h) transferência internacional de dados pessoais;

i) inventário dos dados pessoais;

j) segurança e proteção de dados pessoais;

k) ocorrências de violações.

II - na fase de análise dos riscos considerar os seguintes critérios para avaliação de impacto:

a) titular: avalia a extensão do impacto direto que a concretização do risco pode causar aos titulares dos dados pessoais, incluindo consequências individuais ou coletivas que possam: afetar a segurança, liberdade, dignidade, integridade física, psíquica, material ou moral dos titulares; impedir ou limitar o exercício de direitos ou a utilização de um serviço; ou ocasionar danos tais como discriminação; violação do direito à imagem e à reputação; fraudes financeiras ou uso indevido de identidade;

b) exposição: avalia a gravidade da exposição ou divulgação não autorizada de dados pessoais, sejam eles comuns ou sensíveis, considerando o volume, a abrangência e o tipo de dados afetados, além da vulnerabilidade dos titulares envolvidos, como crianças, adolescentes, idosos, pessoas com deficiência, povos originários, entre outros grupos historicamente mais expostos a riscos sociais;

c) segurança da informação: avalia os impactos de um risco de privacidade sob a perspectiva da disponibilidade, integridade, confidencialidade e autenticidade;

d) reputação: avalia o impacto do risco sobre a imagem pública, a credibilidade e a confiança no MPT, considerando que uma reputação sólida é fundamental para sua legitimidade e capacidade de atuação eficaz;

e) conformidade: avalia o impacto de um risco sobre a capacidade do MPT de manter-se alinhado com normas, regulamentos e legislações aplicáveis, garantindo a adesão aos mais altos padrões de transparência e responsabilidade.

§ 1° A gestão de riscos deverá considerar, além dos riscos, as oportunidades de aprimoramento das práticas de privacidade, reconhecidas como riscos positivos.

§ 2° As etapas de identificação, análise e avaliação de riscos poderão ser realizadas por meio de oficinas facilitadas, conduzidas com participação das unidades responsáveis, SETIC, Secretaria de Polícia, SIGR, Encarregado e outros especialistas.

§ 3° Os planos de ação e de gestão das unidades administrativas deverão incorporar os riscos de privacidade e respectivos tratamentos identificados nos processos sob sua responsabilidade.

Art. 10 Serão considerados riscos-chave aqueles que, em função de sua gravidade ou potencial impacto institucional, exigem conhecimento e supervisão pelo CEPDAP e pelo Procurador-Geral do Trabalho.

Parágrafo único. Enquadram-se como riscos-chaves todo risco capaz de causar danos relevantes aos titulares de dados pessoais, conforme descrito no art. 9°, II, “a”, dentre outros, riscos de incidentes envolvendo: vazamentos de dados pessoais significativos; dados sensíveis; dados de crianças, adolescentes, idosos ou outros grupos considerados vulneráveis; dados financeiros; dados de autenticação em sistemas; dados protegidos por sigilo legal, judicial ou profissional; dados de geolocalização ou falhas sistêmicas que impactem toda a instituição.

Art. 11 O Encarregado pelo Tratamento de Dados Pessoais e a Secretaria de Integridade e Gestão de Riscos (SIGR) podem definir processos prioritários, sistemas críticos e operações de alto risco para a finalidade prevista no artigo 7°.

CAPÍTULO VII – DO REGISTRO E DA DOCUMENTAÇÃO DA GESTÃO DE RISCO

Art. 12 As etapas do processo de gestão de riscos em privacidade deverão ser devidamente registradas e documentadas, de forma clara e rastreável, observando os princípios de responsabilização e prestação de contas.

§ 1° O MPT manterá Registro de Riscos em Privacidade, integrado ao Sistema de Governança da Gestão de Riscos, contendo, no mínimo, a identificação do risco, o objeto de gestão, a análise de impacto e probabilidade, o nível de risco, as medidas de tratamento, o risco residual, o responsável, o status e a data de revisão.

§ 2° Os Relatórios de Impacto à Proteção de Dados Pessoais constituem instrumentos específicos de documentação da gestão de riscos e deverão ser mantidos em procedimentos formais, com controle de versões, histórico de revisões e aprovação formal.

§ 3° Os registros de riscos e documentos correlatos deverão ser mantidos

atualizados, protegidos contra acesso não autorizado e disponibilizados, quando necessário, aos órgãos de governança, controle interno, auditoria e autoridades competentes.

CAPÍTULO VIII – DAS BOAS PRÁTICAS DE GOVERNANÇA

Art. 13 O projeto, processo, sistema, serviço ou contratação que envolva tratamento de dados pessoais, sobretudo na área de TI, deverá considerar o processo de gestão de riscos previsto no Capítulo VI e a privacidade por concepção e por padrão (privacy by design, privacy by default) e a consequente busca pela adoção das medidas associadas às boas práticas em privacidade.

Art. 14 As contratações de bens e serviços em geral devem conter medidas proporcionais ao nível de risco em privacidade envolvido, definidas em cláusulas contratuais específicas.

CAPÍTULO IX – RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS (RIPD)

Art. 15 O RIPD será exigido quando:

I - o risco for classificado como alto ou crítico;

II - houver tratamento de dados sensíveis, biométricos ou em larga escala;

III - houver tratamento de dados pessoais de crianças, adolescentes, idosos e outros grupos vulneráveis;

IV - houver monitoramento, vigilância sistemáticas;

V - houver uso de ou tecnologias emergentes;

VI - houver compartilhamento relevante com terceiros;

VII - assim determinar o Encarregado ou normas complementares;

VIII - histórico de incidente de segurança com dados pessoais;

IX - previsão de transferência internacional de dados no processo de tratamento;

X - previsão de uso de dados pessoais para tomada de decisão automatizada com efeito legal;

XI - mudanças, legais ou regulatórias, ou alterações nas regras de negócio que tragam alterações significativas no tratamento de dados pessoais realizado.

§1° O RIPD adotará metodologia conforme ISO/IEC 29134 e ainda atenderá os critérios e recomendações da UEPDAP/CNMP.

§2° A aprovação do RIPD compete ao Encarregado, após manifestação da unidade tratadora e, quando necessário, da SETIC.

CAPÍTULO X – INTEGRAÇÃO COM INCIDENTES

Art. 16 A gestão de riscos se integra e harmoniza com o Processo de Gestão e Comunicação de Incidentes com Dados Pessoais do Ministério Público do Trabalho, previsto na Portaria n° 1.902/2024.

Art. 17 Todo incidente registrado deverá:

I - compor o histórico de riscos da unidade;

II - motivar novo ciclo de análise do risco;

III - alimentar ações de melhoria contínua;

IV - gerar atualização do RIPD, quando aplicável.

CAPÍTULO XI – MONITORAMENTO, AUDITORIA E REVISÃO

Art. 18 O monitoramento contínuo dos riscos é responsabilidade das unidades tratadoras de dados pessoais, que deverão acompanhar a eficácia dos controles implementados, registrar eventos e comunicar desajustes ao Encarregado e às áreas técnicas competentes.

Art. 19 O monitoramento observará:

I - periodicidade mínima anual;

II - revisões extraordinárias após incidentes ou mudanças tecnológicas;

III - integração com auditorias internas.

Art. 20 A revisão desta Política será coordenada pelo Encarregado, submetida ao CEPDAP e encaminhada ao Procurador-Geral do Trabalho para aprovação, observado o prazo máximo de 24 meses ou menores períodos em caso de mudanças

tecnológicas, legais ou institucionais relevantes.

CAPÍTULO XII – DISPOSIÇÕES FINAIS

Art. 21 Os casos omissos serão resolvidos pelo Procurador-Geral do Trabalho, ouvido o CEPDAP.

Art. 22 Esta Política entra em vigor na data de sua publicação.

GLÁUCIO ARAÚJO DE OLIVEIRA