Portaria PGT nº 1902.2024

Institui a Política de Comunicação de Incidente de Segurança com Dados Pessoais no Ministério Público do Trabalho.

O PROCURADOR GERAL DO TRABALHO, no uso de suas atribuições conferidas pela Lei Complementar nº 75, de 20 de maio de 1993,

CONSIDERANDO que a Emenda Constitucional nº 115/2022 acrescentou o inciso LXXIX ao Art. 5º da Constituição Federal, incluindo a proteção de dados pessoais entre os direitos e garantias fundamentais;

CONSIDERANDO a publicação da Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709, de 14 de agosto de 2018), do Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014), do Regulamento do Marco Civil da Internet (Decreto nº 8.771, de 11 de maio de 2016) e da Lei de Acesso à Informação (Lei nº 12.527, de 18 de novembro de 2011);

CONSIDERANDO que a LGPD dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural;

CONSIDERANDO que, dentre os princípios trazidos pela referida lei, existem o da transparência, o qual recomenda a garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre os tratamentos de dados pessoais realizados, e o princípio da responsabilização e prestação de contas, o qual preconiza que se deva demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas;

CONSIDERANDO a Resolução n.º 281, de 12 de dezembro de 2023, do Conselho Nacional do Ministério Público, que institui a Política Nacional de Proteção de Dados Pessoais e o Sistema Nacional de Proteção de Dados Pessoais do Ministério Público;

CONSIDERANDO que dentre os princípios adotados na resolução supracitada existem o da boa-fé e adequação, o da transparência e o da responsabilização e prestação de contas;

CONSIDERANDO que o Ministério Público do Trabalho trata dados pessoais, tanto nas atividades administrativas, quanto nas atividades finalísticas e que, portanto, é considerado controlador para os fins legais;

CONSIDERANDO que a Resolução CNMP N.º 281/2023 estabelece o dever dos ramos e das unidades do Ministério Público, na qualidade de controladores, de comunicar ao

Conselho Nacional do Ministério Público (CNMP/UEPDAP) e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares;

CONSIDERANDO disposições da LGPD e da Resolução CD/ANPD N.º 15, de 24 de abril de 2024, que aprova o Regulamento de Comunicação de Incidente de Segurança;

CONSIDERANDO a necessidade de instituir, no âmbito do Ministério Público do Trabalho, uma Política de Comunicação de Incidente de Segurança com Dados Pessoais, a fim de orientar todas as pessoas que tratam dados pessoais na Instituição sobre as ações necessárias para assegurar a comunicação tempestiva da ocorrência de incidente de segurança com dados pessoais;

RESOLVE:

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º Fica instituída a Política de Comunicação de Incidente de Segurança com Dados Pessoais do Ministério Público do Trabalho, com o objetivo geral de garantir a comunicação tempestiva à Unidade Especial de Proteção de Dados Pessoais (UEPDAP), à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular de dados pessoais da ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, nos termos da legislação de proteção de dados pessoais em vigor e das respectivas regulamentações e recomendações sobre a matéria.

Art. 2º A política de comunicação de incidente de segurança com dados pessoais atenderá aos seguintes objetivos específicos:

I - proteger os direitos dos titulares;

II - assegurar a adoção das medidas necessárias para mitigar ou reverter os efeitos dos prejuízos;

III – incentivar a adesão às regras de boas práticas e de governança e de medidas de prevenção e segurança adequadas;

IV – promover a cultura de proteção de dados pessoais;

V – atuar de forma transparente, e estabelecer uma relação de confiança com o titular, com a Unidade Especial de Proteção de Dados Pessoais do Conselho Nacional do Ministério Público, com a Autoridade Nacional de Proteção de Dados, e com a sociedade.

CAPÍTULO II
DAS DEFINIÇÕES

Art. 3º Para efeitos deste Regulamento, são adotadas as seguintes definições:

I – ampla divulgação do incidente em meios de comunicação: providência que pode ser determinada pela UEPDAP/CNMP e pela ANPD ao controlador, como a publicação no sítio eletrônico, nas redes sociais do controlador ou em outros meios de comunicação;

II – autenticidade: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada entidade identificável;

III – categoria de dados pessoais: classificação dos dados pessoais de acordo com o contexto de sua utilização, tais como dados de identificação pessoal, dados de autenticação em sistemas, dados financeiros;

IV – comunicação de incidente de segurança: ato do Ministério Público do Trabalho que comunica à Unidade Especial de Proteção de Dados Pessoais, à Autoridade Nacional de Proteção de Dados e ao titular de dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares;

V – confidencialidade: propriedade pela qual se assegura que o dado pessoal não esteja disponível ou não seja revelado a pessoas, empresas, sistemas, órgãos ou entidades não autorizados;

VI – dado de autenticação em sistemas: qualquer dado pessoal utilizado como credencial para determinar o acesso a um sistema ou para confirmar a identificação de um usuário, como contas de login, *tokens* e senhas;

VII – dado financeiro: dado pessoal relacionado às transações financeiras do titular;

VIII – dado pessoal afetado: dado pessoal cuja confidencialidade, integridade, disponibilidade ou autenticidade tenha sido comprometida em um incidente de segurança;

IX - dado protegido por sigilo legal ou judicial: dado pessoal cujo sigilo decorra de norma jurídica ou decisão judicial;

X - dado protegido por sigilo profissional: dado pessoal cujo sigilo decorra do exercício de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem;

XI - incidente de segurança: qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais;

XII - integridade: propriedade pela qual se assegura que o dado pessoal não foi modificado ou destruído de maneira não autorizada ou acidental;

XIII - medidas de segurança: medidas técnicas e/ou administrativas adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, apropriação, comunicação ou difusão;

XIV – natureza dos dados pessoais: classificação de dados pessoais em gerais ou sensíveis;

XV - órgãos de controle: Unidade Especial de Proteção de Dados Pessoais do CNMP e Autoridade Nacional de Proteção de Dados (ANPD);

XVI - relatório de tratamento de incidente: documento fornecido pelo controlador que contém cópias, em meio físico ou digital, de dados e informações relevantes para descrever o incidente e as providências adotadas para reverter ou mitigar os seus efeitos.

CAPÍTULO III
DA COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA

Seção I
Dos critérios para comunicação de incidentes de segurança

Art. 4º O Ministério Público do Trabalho deverá comunicar tempestivamente à Unidade Especial de Proteção de Dados Pessoais e, nos termos da Resolução CNMP N.º 281/2023, à Autoridade Nacional de Proteção de Dados e ao titular, os incidentes de segurança com dados pessoais que possam acarretar risco ou dano relevante aos titulares.

Art. 5º São considerados incidentes de segurança que acarretam risco ou dano relevante aqueles que têm potencial de afetar significativamente interesses e direitos fundamentais dos titulares e que possam:

I - impedir ou limitar o exercício de direitos ou a utilização de um serviço; ou

II - ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou uso indevido de identidade.

§ 1º Os incidentes mencionados no *caput* envolvem pelo menos um dos seguintes critérios:

I - dados sensíveis;

II - dados de crianças, de adolescentes, idosos ou outros grupos considerados vulneráveis;

III - dados financeiros;

IV - dados de autenticação em sistemas;

V – dados protegidos por sigilo legal, judicial ou profissional;

VI - dados de geolocalização; ou

VII - dados em larga escala.

§ 2º 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.

Seção II

Dos envolvidos na comunicação de incidente com dados pessoais

Art. 6º A comunicação do incidente de segurança com dados pessoais é obrigação legal do Ministério Público do Trabalho e deve ser providenciada pelo Encarregado pelo Tratamento de Dados Pessoais, ou pelo Encarregado Adjunto, sempre que o incidente possa acarretar risco ou dano relevante aos titulares afetados.

Subseção I
Do Procurador-Geral do Trabalho

Art. 7° É responsabilidade do Procurador-Geral do Trabalho quanto à comunicação de incidentes com dados pessoais:

I –Determinar que se apurem as responsabilidades pela inobservância da presente política de comunicação de incidentes;

II – Aprovar e determinar a implementação de medidas para salvaguarda dos direitos dos titulares e outras recomendações oriundas da Unidade Especial de Proteção de Dados Pessoais do Conselho Nacional do Ministério Público e da Autoridade Nacional de Proteção de Dados, relacionadas e/ou decorrentes da comunicação de incidentes.

Subseção II
Do Encarregado do Tratamento de Dados Pessoais

Art. 8° É Responsabilidade do Encarregado do Tratamento de Dados Pessoais quanto à comunicação de incidentes de segurança com dados pessoais:

I – providenciar a comunicação de incidente com dados pessoais à Unidade Especial de Proteção de Dados Pessoais, à Autoridade Nacional de Proteção de Dados e ao titular, por meio de formulário específico determinado por cada uma das entidades;

II - fornecer orientações às unidades do Ministério Público do Trabalho para a elaboração do Registro da Operação de Tratamento de Dados Pessoais (ROTDP) e do Relatório de Impacto à Proteção de Dados Pessoais (RIPDP) e recomendar medidas para reverter ou mitigar os efeitos de incidentes;

III – solicitar informações complementares aos operadores envolvidos em incidentes com dados pessoais e às unidades e segmentos do Ministério Público do Trabalho necessárias à instrução da comunicação do incidente;

IV – analisar, em conjunto com o(a) gestor(a) do segmento responsável pelo tratamento dos dados pessoais afetados e com as áreas técnicas envolvidas, o grau de risco e dano do incidente aos titulares de dados pessoais envolvidos.

V – Dar ciência ao Comitê de Proteção de Dados Pessoais e ao Comitê de Gestão de Riscos do Ministério Público do Trabalho da ocorrência do incidente de segurança com dados pessoais.

Subseção III

Dos Operadores

Art. 9° Em qualquer hipótese de incidente de segurança com dados pessoais, independentemente da sua relevância, o operador deverá comunicar imediatamente ao Encarregado pelo Tratamento de Dados Pessoais do Ministério Público do Trabalho a sua ocorrência.

§ 1º A comunicação de que trata o caput deverá conter, no mínimo, as informações especificadas no artigo 17 desta Portaria.

§ 2º Os contratos, acordos e convênios firmados pelo Ministério Público do Trabalho deverão formalmente dispor sobre a necessidade de comunicação prevista no *caput* e no parágrafo primeiro do presente artigo.

Subseção IV
Da Equipe de Prevenção, Tratamento e Resposta à Incidentes Cibernéticos

Art. 10 A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Ministério Público do Trabalho (ETIR), ao detectar ou receber notificação de incidente cibernético com dados pessoais deve notificar imediatamente o Encarregado de Dados e à chefia do segmento responsável pelo tratamento dos dados pessoais afetados.

Parágrafo único: A comunicação de que trata o caput deverá conter, no mínimo, as informações especificadas no artigo 17 desta Portaria.

Art. 11 Após a conclusão do tratamento do incidente cibernético com dados pessoais, a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos deve encaminhar ao Encarregado o relatório preliminar de tratamento de incidente, para embasar a prestação de contas junto à Unidade Especial de Proteção de Dados Pessoais, à Autoridade Nacional de Proteção de Dados e ao titular de dados pessoais, e para fins do registro previsto no Art. 20 desta portaria.

Subseção V
Das Unidades, dos Segmentos e dos Usuários de Informação

Art. 12 É dever de todos os usuários da informação e dos sistemas do Ministério Público do Trabalho comunicar imediatamente ao Encarregado sobre qualquer evento que represente potencial risco à segurança dos dados pessoais tratados pela Instituição em qualquer meio, físico ou digital.

Parágrafo único: Em se tratando de dados pessoais tratados em meio digital, a comunicação referida no *caput* também deverá ser encaminhada à Secretaria de Tecnologia da Informação e Comunicação por meio de sistema próprio de abertura de chamados técnicos do Ministério Público do Trabalho.

Art. 13 As unidades e os segmentos do Ministério Público do Trabalho têm o dever de apoiar o Encarregado, prestando as informações necessárias para a comunicação do incidente, procedendo à avaliação conjunta da gravidade do incidente e dos potenciais impactos aos titulares afetados, na implementação de medidas para reverter ou mitigar os

efeitos do incidente, bem como no atendimento a quaisquer outras solicitações dos órgãos de controle;

§ 1º As unidades e segmentos do Ministério Público do Trabalho devem municiar o Encarregado com as informações elencadas no art. 17, e sempre que necessário, com as informações complementares que forem solicitadas, o que pode incluir a pronta elaboração do Registro de Operação de Tratamento de Dados Pessoais afetados pelo incidente (ROTDP), o Relatório de Impacto à Proteção de Dados Pessoais (RIPDP) e o relatório de tratamento do incidente.

§ 2º As unidades e segmentos do Ministério Público do Trabalho devem atender às solicitações do Encarregado com a celeridade necessária para garantir o cumprimento dos prazos estabelecidos pelas normas e pelos órgãos de controle.

Art. 14 Além das providências previstas no Art. 13, a Secretaria de Tecnologia da Informação e Comunicação (SETIC), a Secretaria de Segurança Institucional (SSI) e a Secretaria de Comunicação Social (SECOM) devem apoiar o Encarregado de Dados na efetivação da comunicação do incidente.

Art. 15 Constatada a necessidade da apuração da conduta responsável pelo incidente, inclusive se dolosa ou culposa, a autoridade competente no âmbito do Ministério Público do Trabalho deverá providenciar a apuração da possível falta funcional, instruindo procedimento com todas as informações possíveis e necessárias, garantidos o contraditório e a ampla defesa.

Seção III
Da comunicação do incidente aos órgãos de controle

Art. 16 O Ministério Público do Trabalho deve comunicar o incidente de segurança com dados pessoais à Unidade Especial de Proteção de Dados Pessoais, no prazo de 72 horas, e à Autoridade Nacional de Proteção de Dados, no prazo de três dias úteis, ressalvada a existência de legislação específica e disposições da Resolução CNMP n.º 281/2023, contados do conhecimento do incidente de segurança, sempre que o incidente possa acarretar risco ou dano relevante aos titulares afetados.

Art. 17 A comunicação de incidente de segurança que trata o artigo anterior deve conter as seguintes informações:

I - a descrição da natureza e da categoria de dados pessoais afetados;

II - o número estimado de titulares afetados, discriminando, quando aplicável, o número de crianças, de adolescentes, idosos, ou outros grupos considerados vulneráveis;

III - as medidas técnicas e de segurança utilizadas para a proteção dos dados pessoais, adotadas antes e após o incidente, observados os casos de sigilo legal e institucional, informando se os dados violados estavam protegidos de forma a torná-los ininteligíveis e a impossibilitar a identificação de seus titulares;

IV - os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares;

V - os motivos da demora, no caso de as comunicações não terem sido realizadas nos prazos previsto no artigo 16;

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente sobre os titulares;

VII - a data da ocorrência do incidente, quando possível determiná-la, e a de seu conhecimento pelo controlador;

VIII - os dados do encarregado, ou do encarregado adjunto, quando aplicável, acompanhados do ato formal de nomeação;

IX - os dados de identificação do Ministério Público do Trabalho, enquanto controlador;

X - a identificação do operador, quando aplicável;

XI - a descrição do incidente, incluindo a causa principal, caso seja possível identificá-la;

XII – o total de titulares cujos dados são tratados nas atividades de tratamento afetadas pelo incidente, sempre que possível; e

XIII - a declaração de que foi realizada a comunicação aos titulares, sempre que aplicável.

§ 1º O procedimento adotado para efetivar a comunicação do incidente de segurança com dados pessoais deve observar as orientações contidas nos respectivos regulamentos específicos e portais na internet dos órgãos de controle.

§ 2º Na hipótese de o Encarregado não dispor de todas as informações necessárias à comunicação do incidente, ou não conseguir notificar a todos os titulares no prazo recomendado, deverá realizar uma comunicação preliminar aos órgãos de controle, com a devida justificativa da impossibilidade de realizar a comunicação completa, e posteriormente protocolar as informações complementares no mesmo processo, observando os prazos estabelecidos.

§ 3º O Encarregado deve acompanhar o andamento do processo de comunicação de incidente com dados pessoais e providenciar o atendimento tempestivo de todas as solicitações formuladas pelos órgãos de controle, até que o processo seja declarado extinto.

Art. 18 Cabe ao Encarregado pelo Tratamento de Dados Pessoais, enquanto representante do Ministério Público do Trabalho, a precaução de solicitar aos órgãos de controle, de maneira fundamentada, o sigilo de informações protegidas por lei ou resguardadas pelo sigilo institucional compartilhadas na comunicação do incidente, indicando aquelas cujo acesso deverá ser restringido.

Seção IV
Da comunicação do incidente ao titular de dados pessoais

Art. 19 A comunicação do incidente de segurança com dados pessoais ao titular deve ser realizada pelo Ministério Público do Trabalho no prazo de três dias úteis, contados do conhecimento do incidente de segurança, sempre que possa acarretar risco ou dano relevante aos titulares afetados, e deve conter no mínimo as seguintes informações:

I - a descrição da natureza e da categoria de dados pessoais afetados;

II - os riscos ou impactos ao titular;

III - as medidas que foram ou que serão adotadas pelo Ministério Público do Trabalho para reverter ou mitigar os efeitos do incidente, quando cabíveis;

IV - a data do conhecimento do incidente de segurança;

V - o contato para obtenção de informações e dados do Encarregado, quando aplicável; e

VI - recomendações ao titular, aptas a reduzir os efeitos do incidente, quando cabíveis.

§ 1º A comunicação do incidente aos titulares de dados deverá utilizar linguagem simples e de fácil entendimento, e ocorrer de forma direta e individualizada, caso seja possível identificá-los e haja disponibilidade de um meio de contato.

§ 2º Considera-se comunicação de forma direta e individualizada no âmbito do Ministério Público do Trabalho, preferencialmente, o e-mail institucional ou, alternativamente, expedição de notificação via serviço postal.

§ 3º Caso a comunicação direta e individualizada se mostre inviável ou não seja possível determinar, parcial ou integralmente, os titulares afetados, a comunicação da ocorrência do incidente deve ser realizada por meio de publicação em página específica no sítio eletrônico do Ministério Público do Trabalho, na qual deverão estar disponibilizadas as comunicações coletivas pelo período de, no mínimo, três meses.

§ 4º Nos casos previstos no § 3º, o Ministério Público do Trabalho poderá disponibilizar a mesma publicação em aplicativos e sistemas, em suas mídias sociais e no canal de atendimento ao titular, de modo que permita o conhecimento amplo, com direta e fácil visualização.

§ 5º O Ministério Público do Trabalho deverá atender às solicitações dos órgãos de controle referentes à comunicação de incidente de segurança com dados pessoais ao titular, tais como a cientificação dos titulares em caso de incidente que não tenha sido comunicado, a complementação de informações sobre o incidente ou a realização de ampla divulgação do incidente em meios de comunicação de larga escala.

§ 6º A comunicação ao titular poderá ser atrasada, restrita ou omitida, se se tratar de atividade institucional sigilosa ou protegida por lei, e nas hipóteses tratadas no art. 77 da Resolução CNMP N.º 281/2023.

CAPÍTULO IV
DO REGISTRO DE INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

Art. 20 O Encarregado pelo Tratamento de Dados Pessoais do Ministério Público do Trabalho deverá manter o Registro Geral de Incidentes de Segurança com Dados Pessoais (RGIDP), inclusive daqueles que não demandem comunicação aos órgãos de controle e aos titulares, pelo prazo estabelecido na tabela de temporalidade e destinação final de documentos de arquivo da atividade meio do Ministério Público do Trabalho, contado a partir da data do registro.

§ 1º O registro do incidente deve conter, no mínimo, as informações relacionadas no art. 17, e ainda, a comprovação das comunicações realizadas ou os motivos da ausência de comunicação, quando for o caso.

§ 2º Aos documentos mencionados no *caput* e parágrafo primeiro deste artigo aplicam-se as hipóteses de sigilo legal e institucional, podendo o acesso a eles ser restringido.

§ 3º A destinação final dos registros de incidentes de segurança com dados pessoais será de guarda permanente.

CAPÍTULO IV
DO PROCESSO DE GESTÃO E COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

Art. 21 Em observância às disposições da legislação de proteção de dados pessoais em vigor e considerando o caráter interdisciplinar da matéria, o Comitê Estratégico de Proteção de Dados Pessoais do Ministério Público do Trabalho deverá aprovar, num prazo de 120 (cento e vinte) dias, a contar da data de publicação desta política, um Processo de Gestão e Comunicação de Incidentes de Segurança com Dados Pessoais (PGI-DP).

§ 1º O processo mencionado no *caput* deverá definir os papéis e as responsabilidades dos atores envolvidos na gestão e na comunicação de incidentes de segurança com dados pessoais, o fluxo das atividades, as interações e comunicações, o detalhamento dos procedimentos a serem executados, além dos modelos de relatórios e de formulários utilizados.

§ 2º O Processo de Gestão e Comunicação de Incidentes de Segurança com Dados Pessoais do Ministério Público do Trabalho deve observar as disposições da legislação e desta política e deve comportar a possibilidade de integração com os processos de gestão e tratamento de incidentes de segurança da informação e de cibersegurança existentes ou que venham a ser instituídos no âmbito do Ministério Público do Trabalho ou determinados em atos normativos vinculantes provenientes do CNMP.

CAPÍTULO V
DISPOSIÇÕES FINAIS

Art. 22 Esta política deverá ser revisada a cada 2 anos ou sempre que houver atualizações nas regulamentações e legislação correlatas.

Art. 23 Esta portaria entra em vigor na data de sua publicação.

(assinado e datado eletronicamente)

JOSÉ DE LIMA RAMOS PEREIRA
Procurador-Geral do Trabalho