DIÁRIO OFICIAL ELETRÔNICO
MINISTÉRIO PÚBLICO DE SERGIPE
Edição nº 1.959
27 de maio de 2024

PORTARIA Nº 1.437/2024
DE 20 DE MAIO DE 2024

Institui o Plano de Comunicação e Resposta de Incidentes de Segurança de Dados Pessoais do Ministério Público do Estado de Sergipe (MPSE), e dá outras providências.

O **PROCURADOR-GERAL DE JUSTIÇA**, no uso de suas atribuições legais conferidas pela Lei Federal nº 8.625, de 12 de fevereiro de 1993, e pela Lei Complementar Estadual nº 02, de 12 de novembro de 1990, e

Considerando que a proteção de dados pessoais é direito fundamental autônomo na Constituição Federal de 1988 (art. 5º, inciso LXXIX);

Considerando que o Ministério Público do Estado de Sergipe deverá observar, no exercício de suas funções, os princípios da Lei Geral de Proteção de Dados (LGPD), dentre os quais se destacam o da segurança, o da prevenção e o da *accountability* (responsabilização e prestação de contas);

Considerando que o princípio da segurança, previsto no art. 6o, inciso VII, da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados), obriga a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

Considerando que o princípio da prevenção, consagrado no art. 6o, inciso VIII, da Lei nº 13.709/2018, impõe a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

Considerando que o princípio da *accountability* (responsabilização e prestação de contas) exige a demonstração, pelo agente, da 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, conforme se extrai do art. 6o, inciso X, da Lei Geral de Proteção de Dados;

Considerando que, de acordo com o art. 46 da Lei nº 13.709/2018, o Ministério Público do Estado de Sergipe, enquanto agente de tratamento de dados, deve "adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito";

Considerando que "a violação ou o vazamento de dados pessoais, voluntária ou acidentalmente, é considerado um incidente de segurança no tratamento, notadamente se ocasionar destruição, perda, alteração, subtração, cópia, transferência, comunicação ou difusão de dado pessoal", nos termos do art. 135 da Resolução nº 281, de 12 de dezembro de 2023, do Conselho Nacional do Ministério Público (CNMP);

Considerando que "todo responsável pelo tratamento de dados pessoais deverá reportar ao Encarregado e ao órgão de tecnologia da informação competente, imediatamente, a ocorrência de incidente de segurança com dados pessoais, com finalidade de permitir a imediata tomada de medidas de contenção e outras necessárias ao controle e à mitigação do dano", por força do disposto no art. 145 da Resolução nº 281/2023, do Conselho Nacional do Ministério Público;

Considerando que o Ministério Público do Estado de Sergipe "ao tomar conhecimento do incidente de segurança relativo ao tratamento de dados pessoais com possibilidade de causar dano relevante aos titulares, comunicará à UEPDAP, sem demora injustificada, sempre que possível no prazo de até 72 (setenta e duas) horas", conforme art. 148 da Resolução nº 281/2023, do Conselho Nacional do Ministério Público;

Considerando que o Ministério Público de Sergipe, na qualidade de controlador, deverá adotar, para além de medidas técnicas, expedientes de ordem administrativas, como a criação de novas rotinas de trabalho, procedimentos de segurança de informação e aumento da transparência e governança, o que exigirá a criação e difusão de uma cultura de proteção de dados dentro da Instituição;

RESOLVE:

CAPÍTULO I

Das Disposições Preliminares

Art. 1º Institui, no âmbito do Ministério Público do Estado de Sergipe, o Plano de Comunicação e Resposta para Incidente de Segurança de Dados Pessoais, na forma desta Portaria.

Parágrafo único. O Plano de Comunicação e Resposta para Incidente de Segurança de Dados Pessoais se aplica a todos os membros, servidores, estagiários, terceirizados e demais colaboradores do Ministério Público do Estado de Sergipe.

Art. 2º Caracteriza-se como incidente de segurança com dados pessoais qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação de dados pessoais, sendo por meio de acesso não autorizado, acidental ou ilícito que resulte em destruição, perda, alteração vazamento ou qualquer forma de tratamento de dados ilícita ou inadequada, que tem a capacidade de pôr em risco os direitos e as liberdades dos titulares dos dados pessoais.

§ 1º Ocorre ainda o incidente de segurança no tratamento de dados pessoais quando se verifica, sem autorização ou de maneira acidental, uma ou mais das seguintes violações ou perdas:

I – da confidencialidade: quando há uso, divulgação ou acesso indevido do dado pessoal;

II – da integridade: quando há alteração do dado pessoal; e

III – da disponibilidade: quando há perda de acesso ou destruição do dado pessoal.

§ 2º Também pode caracterizar risco de violação de dados pessoais, de probabilidade e relevância variáveis, quando o tratamento causar danos físicos, materiais ou morais e imateriais, em especial:

I – quando possa dar origem à discriminação, à usurpação ou subtração da identidade, a perdas financeiras, a prejuízos para a reputação, a perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, à inversão não autorizada da pseudonimização ou a quaisquer outros prejuízos importantes de natureza econômica ou social;

II – quando os titulares possam ficar privados dos seus direitos e liberdades ou impedidos do exercício do controle sobre os respetivos dados pessoais;

III – quando forem revelados, sem autorização, dados pessoais sensíveis;

IV – quando forem avaliados aspectos de natureza pessoal, em particular análises ou previsões de aspectos que digam respeito ao desempenho no trabalho, à situação econômica, à saúde, às preferências ou aos interesses pessoais, à fiabilidade ou comportamento e à localização ou aos deslocamentos das pessoas, a fim de definir ou fazer uso de perfis;

V – quando forem tratados indevidamente dados relativos a pessoas naturais vulneráveis, em particular crianças e adolescentes; ou

VI – quando o tratamento incidir sobre uma grande quantidade de dados pessoais e afetar um grande número de titulares.

CAPÍTULO II

Da Comunicação e da Resposta Interna de Incidente de Segurança de Dados Pessoais

Art. 3º Os membros, servidores, estagiários, terceirizados e colaboradores do Ministério Público do Estado de Sergipe, que identifique ou suspeite da ocorrência de incidente de segurança ou qualquer outra violação de dados pessoais, deverão comunicar, imediatamente, o fato ao Encarregado e, em se tratado de incidente de segurança cibernético, à Diretoria de Tecnologia da Informação e Comunicação – DTIC, com a finalidade de permitir a imediata tomada de medidas de contenção e outras necessárias ao controle e à mitigação do dano.

§1º O Encarregado e a Diretoria de Tecnologia da Informação e Comunicação - DTIC deverão ser informados do incidente de segurança de dados pessoais por meio do Sistema Gerenciador Eletrônico de Expedientes, Documentos e Procedimentos – GED.

Art. 4º Qualquer pessoa, não integrante do Ministério Público do Estado de Sergipe, poderá comunicar ao Encarregado, através do e-mail "encarregado@mpse.mp.br" ou outro canal de comunicação institucional com o público externo, incidente de segurança de dados pessoais.

Art. 5º Em qualquer hipótese de incidente de vazamento de dados pessoais, independentemente da sua relevância, o operador deverá comunicar imediatamente ao Ministério Público do Estado de Sergipe e o Encarregado a sua ocorrência.

Parágrafo único. Os contratos de prestação de serviços de tratamento de dados pessoais, atuais e futuros, deverão conter cláusula determinando a obrigação prevista no *caput* deste artigo.

Art. 6º A comunicação do incidente de segurança de dados pessoais deverá conter:

I – a descrição e a natureza dos dados pessoais afetados;

II – as informações sobre os titulares envolvidos;

III – as medidas técnicas e de segurança utilizadas para a proteção dos dados pessoais, observados os casos de sigilo legal e institucional;

IV – os riscos relacionados ao incidente;

V – os motivos da demora, no caso de a comunicação não ter sido imediata; e

VI – as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Art. 7º Ao ser cientificado da ocorrência de incidente de segurança ou qualquer outra violação de dados pessoais, o Encarregado deverá informar o fato, sem demora, ao Procurador-Geral de Justiça, que designará equipe composta por membros e/ou servidores para atuar na solução do incidente.

§ 1º A equipe designada pelo Procurador-Geral de Justiça adotará, imediatamente, sob a coordenação do Gabinete de Segurança Institucional (GSI) e com o acompanhamento do Encarregado, as seguintes providências de Respostas ao Incidente de Segurança de Dados Pessoais:

I – Contenção e mitigação do incidente de segurança;

II – Erradicação ou mitigação dos danos e das causas do incidente de segurança;

III – Emissão do Relatório Final de Incidente de Segurança de Dados Pessoais, com a descrição das medidas técnicas e de segurança adotadas, dos resultados alcançados e dos efeitos causados pelo incidente de segurança.

§ 2º A equipe designada pelo Procurador-Geral de Justiça avaliará o incidente de segurança com o objetivo de obter informações sobre o impacto do evento, a exemplo:

I – da vulnerabilidade explorada no evento, abrangendo situações como: acesso indevido aos dados pessoais; roubo de dados; ataques cibernéticos; erros de programação de aplicativos e sistemas internos; engenharia social; descartes indevidos; repasse de dados pessoais; roubo, venda e utilização de dados tutelados pela entidade; comprometimento de senhas de acesso; e outras;

II – da fonte dos dados pessoais, isto é, o meio pelo qual foram obtidos os dados pessoais, tais como preenchimento de formulário eletrônico ou não eletrônico por parte do titular, API, uso compartilhado de dados, XML e *cookies*;

III – da categoria de dados pessoais afetados pelo evento, indicando, inclusive, se dados sensíveis e dados pessoais de crianças e adolescentes foram impactados pelo incidente;

IV – da extensão do vazamento, quantificando os titulares e os dados pessoais que tiveram a sua segurança violada no incidente;

V – da avaliação do impacto aos titulares;

VI – da avaliação do impacto ao Ministério Público do Estado de Sergipe, especialmente quanto a eventuais perda de confiabilidade do cidadão; possibilidade de ações judiciais; danos à imagem da Instituição em âmbito local, nacional e internacional; prejuízo à entidade em contratos com fornecedores e impacto total ou parcial nas atividades desenvolvidas pela Instituição.

CAPÍTULO III

Da Comunicação do Incidente à Unidade Especial de Proteção de Dados Pessoais

Art. 8º O Procurador-Geral de Justiça, ao tomar conhecimento do incidente de segurança relativo ao tratamento de dados pessoais com possibilidade de causar dano relevante aos titulares, comunicará à Unidade Especial de Proteção de Dados Pessoais (UEPDAP), vinculada à Comissão de Preservação da Autonomia do Ministério Público, do Conselho Nacional do Ministério Público, sem demora injustificada, sempre que possível no prazo de até 72 (setenta e duas) horas.

§ 1º A comunicação deverá conter, no mínimo:

I – a descrição da natureza do incidente incluindo, se possível, as informações sobre o número aproximado de titulares de dados afetados, bem como a natureza e o número aproximado de registros de dados pessoais em causa;

II – o nome e o contato do Encarregado da proteção de dados pessoais;

III – a descrição das consequências prováveis do vazamento; e

IV – a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados pessoais, observadas as hipóteses de sigilo legal, além das medidas que foram ou que serão adotadas para reverter ou mitigar os prejuízos.

§ 2º A comunicação das informações acerca do incidente de vazamento não importará na remessa dos dados pessoais vazados e das bases nas quais esses se encontram.

§ 3º A comunicação prevista no *caput* deste artigo, em hipóteses de tratamento de dados pessoais para fins de segurança pública, de segurança institucional, de assuntos institucionais e jurídicos ou, ainda, por questão de natureza estratégica, deve ser destinada à Unidade Especial de Proteção de Dados Pessoais (UEPDAP) com a informação classificada como de sigilo absoluto.

CAPÍTULO IV

Da Comunicação do Incidente aos Titulares de Dados Pessoais

Art. 9o Quando o incidente de segurança relativo ao tratamento for suscetível de criar um relevante risco para os direitos e as liberdades das pessoas naturais e, também, quando o Procurador-Geral de Justiça ou o Encarregado entenderem oportuno, os titulares de dados pessoais e a Autoridade Nacional de Proteção de Dados deverão ser informados, sem demora injustificada, a fim de permitir que tomem as precauções necessárias, devendo constar da comunicação a natureza da violação de dados pessoais e as recomendações destinadas a atenuar potenciais efeitos adversos.

§ 1º A comunicação poderá ser atrasada, restrita ou omitida, se se tratar de atividade institucional sigilosa ou protegida por lei, e nas seguintes hipóteses:

I – evitar prejuízo para procedimentos, investigações, inquéritos ou processos administrativos e judiciais;

II – evitar prejuízo para a prevenção, a detecção, a investigação ou a repressão de infrações penais ou para a execução de sanções penais, igualmente, para evitar prejuízo às atividades finalísticas que tenham como objeto a defesa da ordem jurídica, do regime democrático e dos interesses sociais e individuais indisponíveis;

III – proteger a segurança institucional ou a atividade de produção de conhecimento; ou

IV – proteger os direitos e as garantias de terceiros.

§ 2º A comunicação não será exigida se:

I – o Ministério Público do Estado de Sergipe ou a pessoa responsável pelo tratamento de dados pessoais tiver aplicado medidas de proteção adequadas, tanto tecnológicas como administrativas, e essas medidas tiverem sido aplicadas aos dados pessoais afetados pela violação, especialmente medidas que os tornem incompreensíveis para qualquer pessoa não autorizada a acessá-los, como, por exemplo, a criptografia; ou

II – o Ministério Público do Estado de Sergipe ou a pessoa responsável pelo tratamento de dados pessoais tiver tomado medidas subsequentes capazes de assegurar que a ocorrência de relevante risco para os direitos e as liberdades dos titulares referida no *caput* deixou de ser provável.

Art. 10 Na hipótese de a comunicação individual implicar um esforço desproporcional para o Controlador, será feita uma comunicação coletiva ou adotada medida semelhante por meio da qual os titulares dos dados pessoais serão informados de forma igualmente eficaz.

§ 1º Para efetivar a comunicação coletiva devem ser adotadas cautelas necessárias que não acarretem exposição indevida dos dados pessoais a ela correspondentes.

§ 2º O Ministério Público do Estado de Sergipe manterá página específica em seu sítio eletrônico, na qual deverão estar disponibilizadas as comunicações coletivas previstas no *caput* deste artigo.

Art. 11 Para fins de quantificação e qualificação dos danos decorrentes do incidente de segurança no tratamento de dados pessoais, devem ser levados em conta, primordialmente, os seguintes critérios:

I – o tipo de dado pessoal afetado;

II – a confidencialidade do dado e da informação afetados;

III – a natureza do dado pessoal vazado;

IV – a sensibilidade do dado pessoal afetado;

V – o volume de dados pessoais vazados;

VI – a facilidade da identificação do titular de dados pessoais;

VII – o impacto das consequências para o titular de dados pessoais;

VIII – as características pessoais do titular;

IX – as características especiais do tipo de tratamento que estava sendo utilizado no dado pessoal vazado;

X – o número de titulares afetados; e

XI – se a análise conjugada dos dados pessoais vazados implicar uma maior probabilidade de ofensa às liberdades e garantias fundamentais dos titulares.

CAPÍTULO V

Do Registro e do Relatório Final de Incidente de Segurança de Dados Pessoais

Art. 12 O Ministério Público do Estado de Sergipe, por meio da Procuradoria-Geral de Justiça, deverá documentar todos os casos de incidente de segurança de dados pessoais, registrando os fatos relacionados, os respectivos efeitos e a medida de reparação adotada, visando permitir, principalmente, a verificação do cumprimento desta Portaria e das medidas protetivas estabelecidas na Resolução nº 281/2023, do Conselho Nacional do Ministério Público.

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

Art. 13 O registro do incidente de segurança de dados pessoais deverá conter as seguintes informações:

I – a data de conhecimento do incidente pelo Ministério Público do Estado de Sergipe;

II – a descrição das circunstâncias em que o incidente ocorreu;

III – a natureza e categoria dos dados pessoais afetados;

IV – o número dos titulares de dados pessoais impactados;

V – a avaliação do risco e os possíveis danos aos titulares de dados pessoais;

VI – as medidas de correção e mitigação dos efeitos do incidente;

VII – a forma e o conteúdo da comunicação do incidente de segurança à Unidade Especial de Proteção de Dados Pessoais e aos titulares de dados pessoais, quando realizada nos termos desta Portaria;

VIII – os motivos da comunicação do incidente de segurança à Unidade Especial de Proteção de Dados Pessoais e aos titulares de dados pessoais.

Art. 14 A equipe designada pelo Procurador-Geral de Justiça deve preservar, a partir da sua ciência do evento, todas as evidências do incidente de segurança de dados pessoais e de todas as ações realizadas para compreender o evento e reduzir seus efeitos, especialmente:

I – todos os *logs* dos sistemas internos e externos envolvidos no incidente;

II – comunicações e diálogos da equipe com órgãos integrantes da estrutura administrativa do Ministério Público do Estado de Sergipe, bem como com outras Instituições Públicas e Empresas Privadas;

III – todas as medidas adotadas;

IV – eventuais contratações de ferramentas e equipes de especialistas e auditores para atuação pontual no incidente a ser tratado;

V – atas das reuniões relevantes.

Art. 15 Concluída a investigação e a adoção das medidas de comunicação e resposta, o Procurador-Geral de Justiça, ou a equipe por ele designada, elaborarão, no prazo de 05 (cinco) dias, o Relatório Final de Incidente de Segurança de Dados Pessoais, encaminhando-o ao Encarregado.

§ 1º O Relatório Final de Incidente de Segurança de Dados Pessoais deverá conter, no mínimo:

I – as informações sobre o incidente de segurança de dados pessoais, efeitos e sua natureza;

II – as medidas adotadas para a preservação das evidências e os procedimentos adotados para a contenção da crise;

III – as funções e a descrição da atuação das pessoas envolvidas;

IV – os questionamentos do público externo (titulares de dados pessoais, agentes públicos e meios de comunicação), com as respectivas respostas;

V – a descrição das medidas técnicas, de segurança e governança adotadas e dos resultados alcançados;

VI – as medidas futuras que poderão ser adotadas para prevenir novos incidentes de segurança de dados pessoais;

VII – a descrição de estratégias de curto, médio e longo prazo, se preparadas.

§ 2º O Encarregado deverá remeter cópia do Relatório Final de Incidente de Segurança de Dados Pessoais para o Comitê Estratégico de Proteção de Dados Pessoais, para conhecimento.

§ 3º O Relatório Final de Incidente de Segurança de Dados Pessoais deverá ser arquivado no Gabinete do Encarregado.

CAPÍTULO VII

Das Disposições Finais

Art. 16 A Escola Superior do Ministério Público realizará, anualmente, cursos teóricos e práticos para membros e servidores, com o objetivo de treiná-los para atuar na resposta de incidentes de segurança de dados pessoais.

Art. 17 A Coordenadoria de Comunicação Social realizará, anualmente, campanhas internas de conscientização e de boas práticas relacionadas à Lei Geral de Proteção de Dados (Lei nº 13.709/2018), tendo como público-alvo os membros, servidores, estagiários, terceirizados e demais colaboradores do Ministério Público do Estado de Sergipe, com a finalidade de se criar uma cultura de proteção de dados pessoais no âmbito da Instituição.

Art. 18 Constatado que o incidente de segurança de dados pessoais decorreu de ação ou omissão, dolosa ou culposa, de membro ou servidor do Ministério Público do Estado de Sergipe, o Procurador-Geral de Justiça comunicará o fato à autoridade disciplinar para a apuração da possível falta funcional, encaminhando todas as informações possíveis e necessárias que permitam a instauração do devido processo legal, garantidos o contraditório e a ampla defesa.

Art. 19 Os casos omissos desta Portaria serão submetidos a apreciação do Procurador-Geral de Justiça para deliberação.

Art. 20 Esta Portaria entra em vigor na data de sua publicação no Diário Oficial Eletrônico do Ministério Público do Estado de Sergipe (DOFe MPSE).

Art. 21 Ficam revogadas as disposições em contrário.

Dê-se ciência, cumpra-se e publique-se.

Manoel Cabral Machado Neto
Procurador-Geral de Justiça

*** Republicada por incorreção**

Expediente assinado eletronicamente por **Manoel Cabral Machado Neto***, em 27/05/2024 09:35:30, conforme art. 1º, III,"b", da Lei 11.419/2016.

A validade deste documento pode ser conferida no site https://sistemas.mpse.mp.br/mpse/Administrativo/Publico.html#/Expediente/ConsultaPublica informando o número do expediente: **20.27.0229.0010785/2024-88.**