RESOLUÇÃO GPGJ nº 2.548, DE 29 DE AGOSTO DE 2023.

Institui o Plano de Resposta e Remediação de Incidentes de Segurança de Dados do Ministério Público do Estado do Rio de Janeiro.

O **PROCURADOR-GERAL DE JUSTIÇA DO ESTADO DO RIO DE JANEIRO**, no uso de suas atribuições legais,

CONSIDERANDO a previsão constitucional (art. 5º, inc. LXXIX - incluído pela Emenda Constitucional nº 115/22), as disposições da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD), da Lei nº 12.965/2014 (Lei do Marco Civil da *Internet*), da Lei nº 12.527/2011 (Lei de Aceso à Informação), da Lei nº 8.625/1993 (Lei Orgânica Nacional do Ministério Público), da Lei Complementar Estadual nº 106/2003 e da Resolução GPGJ nº 2.434/2021, bem como as boas práticas de governança de dados e segurança da informação;

CONSIDERANDO que os responsáveis pelo tratamento de dados em desconformidade com a lei poderão incidir nas sanções do regime jurídico próprio, da Lei de Improbidade Administrativa, da Lei de Acesso à Informação e da Lei nº 13.709/18;

CONSIDERANDO que o art. 46 da Lei Geral de Proteção de Dados Pessoais estabelece que os agentes de tratamento devem 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, e que tais medidas de segurança deverão ser observadas desde a concepção do produto ou serviço até a sua execução;

CONSIDERANDO que o art. 48 da Lei Geral de Proteção de Dados Pessoais prevê que o controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares;

CONSIDERANDO que o art. 50 da mesma lei estabelece que controladores e operadores, no âmbito de suas competências, poderão formular regras de boas práticas de governança para o tratamento de dados pessoais; e o inciso I do § 2º do referido artigo dispõe que deve ser implementado um Programa de Governança em Privacidade que conte com planos de resposta a incidentes e remediação;

CONSIDERANDO que a Resolução GPGJ nº 2.434/2021 prevê, em seu art. 5º, inciso VII, a elaboração de planos de resposta e remediação de incidentes de segurança de dados;

CONSIDERANDO o que consta no Procedimento SEI nº 20.22.0001.0075052.2022-42,

RESOLVE

Disposições Gerais

Art. 1º - Constitui incidente o evento, ação ou omissão que tenha permitido ou possa vir a permitir acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou, ainda, apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação.

§ 1º - Constitui incidente de segurança qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos ativos ou sistemas de computação ou das redes de computadores;

§ 2º - Caracteriza-se o incidente de segurança com dados pessoais, de acordo com a Autoridade Nacional de Proteção de Dados (ANPD), como 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.

Da Gestão de Incidentes de Segurança

Art. 2º - Caso ocorra incidente que coloque em risco a segurança de dados pessoais, devem ser realizados os seguintes procedimentos:

I - avaliar internamente o incidente com o objetivo de obter informações iniciais sobre impacto do evento, natureza, categoria e quantidade de titulares de dados pessoais afetados; categoria e quantidade de dados afetados, consequências do incidente para os titulares e a entidade, criticidade e probabilidade; além disso, é necessário preservar todas as evidências do incidente;

II - comunicar ao Encarregado de Dados Pessoais do Ministério Público a existência do incidente, caso envolva dados pessoais;

III - comunicar ao controlador do Ministério Público do Estado do Rio de Janeiro, nos termos da LGPD, a existência do incidente, caso envolva dados pessoais;

IV - comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular de dados pessoais, conforme art. 48 da LGPD, a existência do incidente;

V - comunicar à Secretaria de Tecnologia da Informação e de Comunicação (STIC), em caso de incidentes na infraestrutura de tecnologia de informação;

VI - emitir o relatório final com todas as informações coletadas, as ações realizadas para o tratamento efetivo do evento e as considerações necessárias para promover a melhoria contínua no atendimento de incidentes e para atualizar o Relatório de Impacto à Proteção de Dados Pessoais (RIPD).

Art. 3º - É dever do membro, servidor, aluno-residente, estagiário ou terceirizado do Ministério Público que tenha ciência de evento que possa configurar incidente de segurança, comunicá-lo imediatamente ao Comitê Estratégico de Proteção de Dados via procedimento administrativo no Sistema Eletrônico de Informações (SEI), preenchendo o formulário lá disponível.

Art. 4º - É facultado a qualquer interessado que tenha ciência de evento que possa configurar um incidente de segurança, a comunicação ao Comitê Estratégico de Proteção de Dados Pessoais, via procedimento administrativo no Sistema Eletrônico de Informações (SEI), preenchendo o formulário lá disponível.

Art. 5º - Nas hipóteses dos artigos 3º e 4º, o comunicante deverá fornecer as seguintes informações:

I - nome completo, identidade, nº de inscrição no CPF/ CNPJ, conforme o caso, telefone e *e-mail*;

II - descrição resumida do suposto incidente;

III - motivos pelos quais entende que o suposto incidente tenha relação com a gestão de dados do Ministério Público do Estado do Rio de Janeiro;

IV - data do suposto incidente ou data provável, caso não tenha certeza da data;

V - caso o comunicado não tenha sido feito imediatamente após o suposto incidente ou sua ciência, a justificativa para a demora;

VI - apontamento de dados pessoais dos quais seja titular, que o comunicante suspeita tenham sido atingidos pelo incidente, se houver;

VII - se possível for a identificação, o apontamento de dados pessoais de terceiros que o comunicante suspeita tenham sido atingidos pelo incidente, se houver;

VIII - se possível for a identificação, quantidade de titulares de dados pessoais que o comunicante estima tenham sido atingidos pelo incidente;

IX - se possível for, a identificação e a natureza da relação entre os titulares de dados supostamente atingidos e o controlador.

Art. 6º - É dever do operador, em relação ao incidente de segurança, comunicar imediatamente ao Ministério Público, enquanto órgão controlador, no prazo máximo de 24 (vinte e quatro) horas da ciência ou suspeita da ocorrência de qualquer incidente que implique violação ou risco de violação de dados pessoais, realizando-se a notificação via procedimento administrativo no Sistema Eletrônico de Informações (SEI), preenchendo o formulário lá disponível, adotando, no mínimo, as seguintes ações:

I - descrever o incidente e a natureza dos dados pessoais afetados, as categorias e o número de titulares dos dados pessoais em questão;

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

III - informar as medidas técnicas e de segurança utilizadas para a proteção dos dados pessoais;

IV - comunicar o nome e os detalhes de contato do encarregado ou responsável por proteção de dados pessoais do operador;

V - descrever as prováveis consequências e riscos relacionados ao incidente de segurança;

VI - descrever as medidas adotadas ou propostas para solucionar o incidente de segurança; e

VII - descrever as medidas que foram ou serão tomadas para reverter ou mitigar os efeitos das perdas relacionadas ao incidente de segurança.

§ 1º - Qualquer não cumprimento, ainda que suspeito, das disposições legais relativas à proteção de dados pessoais pelo operador, seus funcionários, ou terceiros autorizados, acarretará a imposição de pena de multa de até 2% (dois por cento) do faturamento da empresa, a ser aplicada pela Autoridade Nacional de Proteção de Dados (ANPD), na forma do artigo 52, inc. II, da Lei nº 13.709/18 (Lei Geral de Proteção de Dados Pessoais).

§ 2º - A critério do Encarregado de Dados Pessoais do Ministério Público do Estado do Rio de Janeiro, o operador poderá ser provocado a colaborar na elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), conforme a sensibilidade e o risco inerente dos serviços objeto do eventual contrato firmado entre operador e controlador, no tocante a dados pessoais.

Art. 7º - Caso a comunicação não contenha todos os requisitos previstos nos artigos 5º ou 6º, conforme o caso, desta Resolução, o Comitê Estratégico de Proteção de Dados Pessoais poderá solicitar ao comunicante a complementação das informações no prazo de 24 (vinte e quatro) horas.

Art. 8º - Após verificar o preenchimento dos requisitos do art. 5º ou 6º, conforme o caso, desta Resolução, o Encarregado de Proteção de Dados Pessoais deverá avaliar a veracidade e relevância do incidente, e, caso entenda que há elementos suficientes que possam comprovar a possibilidade de vazamento de dados, enviará o procedimento à Secretaria de Tecnologia da Informação e de Comunicação, para confirmação do possível vazamento e início da fase de triagem, análise e resposta.

Art. 9º - A Secretaria de Tecnologia da Informação e de Comunicação apresentará parecer sobre a possibilidade de comprovação do incidente reportado, e, em caso

de confirmação, apresentará relatório do incidente ao Comitê Estratégico de Proteção de Dados Pessoais, do qual deverão constar:

I - a data e hora da detecção do incidente;

II - a data e hora do incidente e sua duração;

III - qual vulnerabilidade foi 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;

IV - a fonte dos dados pessoais, assim considerado 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*;

V - a extensão do vazamento, assim considerada a descrição dos dados pessoais e as informações afetadas, tais como natureza e conteúdo dos dados pessoais, categoria e quantidade de dados e de titulares afetados;

VI - resumo do incidente de segurança com dados pessoais, com indicação da localização física e meio de armazenamento;

VII - avaliação do impacto ao titular, abrangendo possíveis consequências e efeitos negativos sobre os titulares dos dados afetados;

VIII - avaliação do impacto para a Instituição, abrangendo os impactos que o incidente pode gerar ao Ministério Público, como perda de confiabilidade do cidadão, ações judiciais, danos à imagem da Instituição em âmbito nacional e internacional, e impacto total ou parcial nas atividades desenvolvidas;

IX - resumo das medidas técnicas implementadas até o momento para controlar os possíveis danos;

X - possíveis problemas de natureza transfronteiriça;

XI - outras informações úteis às pessoas afetadas para proteger seus dados ou prevenir possíveis danos.

Parágrafo único - A Secretaria de Tecnologia da Informação e de Comunicação deverá apresentar relatório com a maior brevidade possível e, de preferência, no prazo indicativo de 1 (um) dia útil, contado da data do conhecimento do incidente, sem prejuízo de posterior complementação.

Art. 10 - Recebido o relatório da Secretaria de Tecnologia da Informação e de Comunicação, e coletada as demais informações necessárias, o Encarregado pela Proteção de Dados Pessoais do Ministério Público do Estado do Rio de Janeiro comunicará à Autoridade Nacional de Proteção de Dados (ANPD) a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante.

§ 1º - A avaliação acerca da relevância do risco ou dano será feita com cautela e em atenção aos princípios da prevenção, responsabilização e prestação de contas, de modo que, em caso de dúvida, a comunicação à ANPD deverá ser realizada.

§ 2º - A comunicação será feita, de preferência, no prazo indicativo de 2 (dois) dias úteis, seguindo os termos da Lei Geral de Proteção de Dados Pessoais, salvo circunstâncias excepcionais, contados da data do conhecimento do incidente, sem prejuízo de posterior complementação.

§ 3º - A comunicação deverá conter as informações exigidas no art. 48, § 1º, da Lei nº 13.709/18 e no formulário de informe de incidentes de segurança da ANPD, incluindo:

I - identificação e dados de contato do Ministério Público do Estado do Rio de Janeiro, enquanto entidade controladora, e do Comitê Estratégico de Proteção de Dados Pessoais (CEPDAP);

II - indicação se a notificação é completa ou parcial e, em caso de comunicação parcial, indicar se o caso versa sobre uma comunicação preliminar ou uma comunicação complementar;

III - data e hora da detecção do incidente;

IV - data e hora do incidente e sua duração;

V - circunstâncias em que ocorreu a violação de segurança de dados pessoais, tais como: perda, roubo, cópia e vazamento;

VI - descrição dos dados pessoais e das informações afetadas, tais como natureza e conteúdo dos dados pessoais, categoria e quantidade de dados e de titulares afetados;

VII - resumo do incidente de segurança com dados pessoais, com indicação da localização física e meio de armazenamento;

VIII - possíveis consequências e efeitos negativos sobre os titulares dos dados afetados;

IX - medidas de segurança, técnicas e administrativas, de caráter preventivo, tomadas pelo controlador de acordo com a LGPD;

X - resumo das medidas implementadas até o momento para controlar os possíveis danos;

XI - possíveis problemas de natureza transfronteiriça;

XII - outras informações úteis às pessoas afetadas para proteger seus dados ou prevenir possíveis danos.

§ 4º - Caso não seja possível fornecer todas as informações no momento da comunicação preliminar, informações adicionais poderão ser fornecidas posteriormente, sendo que no momento da comunicação preliminar, deverá ser informado à ANPD se serão fornecidas mais informações posteriormente, bem como quais meios estão sendo utilizados para obtê-las, ressaltando-se que a ANPD também poderá requerer informações adicionais a qualquer momento.

Art. 11 - O Comitê Estratégico de Proteção de Dados Pessoais (CEPDAP) comunicará aos titulares a ocorrência de incidente de segurança relacionado a dados pessoais que possa acarretar risco ou dano relevante aos direitos e liberdades individuais dos titulares afetados.

§ 1º - Quando da avaliação da relevância do risco ou dano, deverão ser considerados com maior peso as situações em que o incidente:

I - envolver dados sensíveis ou de pessoas em situação de vulnerabilidade, como crianças e adolescentes; e

II - tiver potencial de ocasionar danos materiais ou morais, tais como discriminação, violação do direito à imagem e à reputação, fraudes financeiras e roubo de identidade.

§ 2º - Ainda no momento da avaliação da relevância do risco ou dano, deverá ser considerado o volume de dados envolvidos, o quantitativo de indivíduos afetados, a boa-fé e as intenções dos terceiros que tiveram acesso aos dados após o incidente e a facilidade de identificação dos titulares por terceiros não autorizados.

§ 3º - A comunicação aos titulares será realizada em prazo razoável e deverá indicar o seguinte:

I - as informações objeto do incidente;

II - se o titular de dados pessoais pode ser vítima de fraude em razão do incidente;

III - se o incidente foi devidamente comunicado às autoridades;

IV - a existência de medidas que o titular possa tomar em benefício da sua proteção;

V - onde o titular pode obter mais informações sobre o incidente.

§ 4º - Se, pela natureza do incidente, não for possível identificar individualmente os titulares afetados, devem ser comunicados todos os presentes na base de dados comprometida.

§ 5º - A depender da gravidade do incidente e do número de titulares afetados, o Comitê Estratégico de Proteção de Dados Pessoais (CEPDAP) poderá recomendar a divulgação do fato no sítio eletrônico, nas redes sociais e em outros meios de comunicação oficiais do Ministério Público, bem como a articulação junto à Ouvidoria para informe à sociedade civil.

Art. 12 - O Comitê Estratégico de Proteção de Dados Pessoais (CEPDAP) comunicará ao Conselho Nacional do Ministério Público os incidentes de segurança ocorridos no Ministério Público que possam acarretar risco ou dano relevante aos titulares de dados pessoais.

Art. 13 - O Comitê Estratégico de Proteção de Dados Pessoais (CEPDAP) elaborará documentação com a avaliação interna do incidente, medidas tomadas e análise de risco, para fins de cumprimento do princípio de responsabilização e prestação de contas, observando-se o art. 6º, inc. X, da LGPD.

Art. 14 - Ao Encarregado pelo Tratamento de Dados Pessoais caberá a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), conforme o art. 7º, inciso IX, da Resolução GPGJ nº 2.434/21, nas seguintes situações:

I - para o tratamento de dados pessoais realizados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, observando-se as exceções previstas no art. 4º, inciso III, da LGPD;

II - quando houver infração à LGPD em decorrência do tratamento de dados pessoais por órgãos públicos, conforme dispõem os arts. 31 e 32 da LGPD, combinados;

III - a qualquer momento, sob determinação da ANPD, como preceitua o art. 38 da LGPD;

IV - quando constatar a possibilidade de ocorrer impacto na privacidade dos dados pessoais.

Disposições Finais e Transitórias

Art. 15 - No prazo de 6 (seis) meses, a contar da publicação deste Plano, a Secretaria de Tecnologia da Informação e de Comunicação (STIC) elaborará protocolos técnicos específicos de prevenção e resposta a incidentes de segurança.

Art. 16 - Esta Resolução entra em vigor na data da sua publicação, produzindo efeitos a partir de 1º de outubro de 2023.

Rio de Janeiro, 29 de agosto de 2023.

Luciano Oliveira Mattos de Souza

Procurador-Geral de Justiça