Sumário

PROCURADORIA-GERAL DE JUSTIÇA

RESOLUÇÕES DO PROCURADOR-GERAL DE JUSTIÇA

RESOLUÇÃO GPGJ nº 2.547, DE 29 DE AGOSTO DE 2023.

Institui o Programa de Governança em Privacidade no âmbito 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 a Lei Geral de Proteção de Dados traz um conceito amplo de tratamento, assim considerada "toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração";

CONSIDERANDO que a Lei Geral de Proteção de Dados possui um capítulo dedicado ao tratamento de dados pessoais pelo poder público;

CONSIDERANDO que o Ministério Público do Estado do Rio de Janeiro faz tratamento de dados para atividades relacionadas à segurança pública, investigação e repressão de infrações penais, procedimentos cíveis, contratos administrativos, processo judicial eletrônico, gestão administrativa de membros, servidores e colaboradores;

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 a necessidade de adequação e aprimoramento das atividades institucionais e dos fluxos internos de governança de dados pessoais às exigências da legislação específica;

CONSIDERANDO o que consta no Procedimento SEI nº 20.22.0001.0064216.2022-62,

RESOLVE

Capítulo I

Disposição Preliminar

Art. 1º - Esta Resolução institui, no âmbito do Ministério Público do Estado do Rio de Janeiro, o Programa de Governança em Privacidade.

Parágrafo único - O Programa de Governança em Privacidade tem por fundamentos a proteção de direitos e liberdades fundamentais, o exercício da cidadania, o incremento da confiabilidade do cidadão titular de dados pessoais no Ministério Público do Estado do Rio de Janeiro, e a eficiência no cumprimento das atribuições constitucionais, legais e normativas.

Capítulo II

Objetivo

Art. 2º - O Programa de Governança em Privacidade se aplica ao tratamento de dados de pessoa natural, identificada ou identificável, levado a efeito no âmbito do cumprimento das atribuições do Ministério Público do Estado do Rio de Janeiro, consoante o art. 50 da Lei Geral de Proteção de Dados.

Parágrafo único - As disposições desta Resolução são direcionadas às atividades administrativas, de gestão e finalísticas do Ministério Público do Estado do Rio de Janeiro, e definem diretrizes para a atuação do Encarregado pelo Tratamento de Dados Pessoais do Ministério Público do Estado do Rio de Janeiro e do Comitê Estratégico de Proteção de Dados Pessoais.

Art. 3º - O Programa de Governança em Privacidade não se aplica ao tratamento de dados pessoais realizado pelo Ministério Público do Estado do Rio de Janeiro para fins exclusivamente jornalísticos, artísticos, acadêmicos, de segurança pública, defesa nacional, segurança do Estado ou atividades de inteligência, de segurança orgânica, de investigação e de repressão de infrações penais.

Capítulo III

Princípios Gerais

Art. 4º - A aplicação do Programa de Governança em Privacidade será regida pela boa-fé e pelos princípios da finalidade, adequação, necessidade, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

§ 1º - Nenhuma disposição deste Programa poderá ser interpretada de forma a gerar lesão à ordem jurídica, aos direitos e interesses individuais ou transindividuais, ou comprometer a efetividade, a eficiência e a finalidade das atribuições do Ministério Público do Estado do Rio de Janeiro.

§ 2º - Os direitos dos titulares não poderão ser exercidos de forma a gerar lesão ou ameaça de lesão indevida a terceiros.

§ 3º - As disposições deste Programa deverão ser interpretadas em consonância com os instrumentos de investigação civil no âmbito da tutela coletiva e direitos individuais indisponíveis, especialmente no que diz respeito à possibilidade de imposição de sigilo fundamentado, decorrente de lei ou por necessidade de investigação civil em procedimento administrativo, sobre a integralidade ou sobre determinadas atividades de tratamento de dados pessoais, nos termos das normas vigentes e regulamentação específica.

Art. 5º - Para os fins deste Programa, considera-se:

I - dado pessoal: informação relacionada à pessoa natural identificada ou identificável;

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

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

IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VI - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

VII - controlador: pessoa jurídica de direito público a quem competem as decisões referentes ao tratamento de dados pessoais;

VIII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

IX - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

X - 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;

XI - 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;

XII - relatório de impacto à proteção de dados pessoais: 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 medidas, salvaguardas e mecanismos de mitigação de risco;

XIII - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei Federal nº 13.709/2018 no território nacional.

Capítulo IV

Tratamento de Dados Pessoais

Art. 6º - O tratamento de dados pessoais pelo Ministério Público do Estado do Rio de Janeiro é admitido para o atendimento de sua finalidade pública e a persecução do interesse público, tendo como objetivos a execução de suas competências legais ou o cumprimento das atribuições legais do serviço público.

§ 1º - O tratamento dos dados pessoais será limitado ao mínimo necessário para a realização de sua finalidade.

§ 2º - O tratamento de dados pessoais de crianças no âmbito do Ministério Público do Estado do Rio de Janeiro, além de observar as exigências do *caput* deste artigo e seu §1º, deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou responsável legal.

§ 3º - Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o parágrafo anterior, quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e, em nenhum caso, poderão ser repassados a terceiro sem o consentimento de que trata o §2º deste artigo.

§ 4º - O Ministério Público do Estado do Rio de Janeiro é o controlador dos dados pessoais à sua disposição e a ele compete decidir sobre o tratamento destes dados.

§ 5º - A transparência ativa será cumprida mediante a disponibilização, no sítio eletrônico do Ministério Público do Estado do Rio de Janeiro, de informações claras e atualizadas acerca das hipóteses em que, no exercício de suas competências, realiza o tratamento de dados pessoais, nos termos do inciso I do art. 23 da Lei Geral de Proteção de Dados Pessoais.

§ 6º - A transparência passiva será cumprida mediante a possibilidade de exercício dos direitos do titular perante o Encarregado.

Art. 7º - O compartilhamento de dados pessoais ou seu uso compartilhado pelo Ministério Público do Estado do Rio de Janeiro poderá ser realizado para atender finalidade específica de execução de atribuição legal ou cumprimento de competência legal.

Art. 8º - O Ministério Público do Estado do Rio de Janeiro empregará os esforços necessários para que os dados pessoais sejam mantidos disponíveis, adequados, exatos e atualizados, bem como protegidos por procedimentos internos, com trilhas de auditoria, para registrar utilização, autorizações, acesso, impactos e violações.

Art. 9º - Os sistemas internos do Ministério Público do Estado do Rio de Janeiro devem manter registro das operações de tratamento de dados pessoais realizados por controlador, encarregado e operadores.

Parágrafo único - A utilização de ferramentas de consulta ou pesquisa em bancos de dados pessoais em sistemas do Ministério Público do Estado do Rio de Janeiro deverá ensejar registro no respectivo sistema, que permita a identificação do usuário em eventual auditoria.

Art. 10 - O Centro de Estudos e Aperfeiçoamento Funcional poderá tratar dados pessoais, quando necessário para a execução do contrato de prestação de serviços educacionais ou quando necessário para atender interesses legítimos próprios ou de terceiros, para a finalidade de melhor adequação, desenvolvimento e eficiência das atividades prestadas.

§ 1º - O tratamento dos dados pessoais será limitado ao mínimo necessário para a realização de sua finalidade.

§ 2º - Os dados deverão ser conservados após o término do tratamento caso indispensável para o cumprimento de obrigação legal ou uso dentro das finalidades acadêmicas, administrativas ou educacionais do Centro de Estudos e Aperfeiçoamento Funcional.

Capítulo V

Direitos do Titular

Art. 11 - O Ministério Público do Estado do Rio de Janeiro zelará pelo pleno exercício dos direitos do titular, aplicando-se, no que couber, as disposições dos arts. 18 e 19 da Lei Geral de Proteção de Dados Pessoais.

Art. 12 - O titular dos dados pessoais tem direito a obter as informações sobre o tratamento de seus próprios dados, mediante requerimento expresso dirigido ao Encarregado, ressalvadas as hipóteses do § 5º deste artigo.

§ 1º - As requisições de titulares de dados pessoais inerentes às atividades previstas no art. 41, § 2º, da Lei 13.709/2018, serão recebidas pelo Encarregado, por peticionamento externo, e processadas por meio do Sistema Eletrônico de Informações (SEI).

§ 2º - O solicitante deverá comprovar que é o titular dos dados pessoais quando da solicitação de que trata o *caput* deste artigo.

§ 3º - O Encarregado poderá pedir informações ou documentos complementares para comprovar a identidade do solicitante.

§ 4º - A responsabilidade do Ministério Público do Estado do Rio de Janeiro estará circunscrita ao emprego dos meios razoáveis e disponíveis na verificação da identidade do solicitante.

§ 5º - A solicitação de exercício de direitos do titular poderá ser negada, total ou parcialmente, de maneira fundamentada e por motivo legítimo, quando houver prejuízo ao cumprimento das obrigações legais ou ao desenvolvimento das atribuições institucionais, notadamente as hipóteses relacionadas a procedimentos sob sigilo, direitos de propriedade intelectual de determinados sistemas de processamento de dados, pedidos de exclusão de dados em caso de necessidade de retenção por dever legal ou necessidade de proteção do Ministério Público do Estado do Rio de Janeiro ou de terceiros;

§ 6º - Das decisões proferidas com base neste artigo caberá recurso hierárquico ao Procurador-Geral de Justiça.

Capítulo VI

Transferência Internacional de Dados

Art. 13 - O Ministério Público do Estado do Rio de Janeiro poderá realizar transferência internacional de dados pessoais, quando necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência,

investigação ou persecução, para a proteção da vida e integridade do titular ou de terceiros ou para o cumprimento de atribuição legal, observados os instrumentos de direito internacional e o adequado grau de proteção de dados pessoais conferido pelos países ou organismos internacionais.

Capítulo VII

Agentes de Tratamento de Dados Pessoais

Art. 14 - O Ministério Público do Estado do Rio de Janeiro é o controlador dos dados pessoais tratados no âmbito de suas atividades.

Art. 15 - Os fornecedores de serviços relacionados à Tecnologia da Informação e Comunicação são considerados operadores e devem realizar o tratamento de dados de acordo com o Programa veiculado nesta Resolução, com as instruções fornecidas pelo controlador e com as normas específicas aplicáveis.

§ 1º - O Ministério Público do Estado do Rio de Janeiro pode, a qualquer tempo, requisitar informações dos fornecedores de serviços relacionados à Tecnologia da Informação e Comunicação acerca de tratamentos de dados pessoais efetuados em nome do controlador.

§ 2º - Os fornecedores devem garantir, no mínimo:

I - estrita adoção das instruções e determinações transmitidas pelo controlador;

II - medidas de segurança da informação, técnicas e administrativas, e de confidencialidade, aptas a proteger os dados pessoais de acessos não autorizados ou de situações acidentais ou ilícitas que produzam risco ao titular e ao controlador;

III - manutenção de registros de tratamentos de dados pessoais que realizarem, com condições de rastreabilidade e de prova eletrônica;

IV - possibilidade de realização de auditorias, pelo controlador ou por auditor independente autorizado;

V - comunicação imediata e formal ao controlador sobre eventuais riscos, ameaças ou incidentes de segurança;

VI - assistência, mediante técnicas apropriadas e organizacionais, para o cumprimento das obrigações do controlador perante titulares de dados, autoridades competentes ou terceiros legítimos, fornecendo as informações necessárias para demonstrar a adequação às normas vigentes;

VII - vedação ao compartilhamento de dados pessoais com terceiros não autorizados ou tratamento posterior para novas finalidades não expressamente autorizadas;

VIII - vedação ao atendimento direto a eventual solicitação de exercício de direitos do titular, devendo informar imediatamente tal fato ao Encarregado, por escrito.

Capítulo VIII

Privacidade e Proteção de Dados no âmbito de domínios externos ao MPRJ

Art. 16 - O Ministério Público compromete-se com a adoção de cláusulas gerais de privacidade e proteção de dados ao fazer uso de ferramentas de redes sociais como *Facebook*, *Messenger*, *Twitter*, *Instagram*, *WhatsApp*, *Tik Tok*, dentre outros, bem como ao utilizar *software* da *Microsoft* e seus programas (*Word*, *Teams*, *Excel etc.*), ou ainda serviços de *call center*.

§ 1º - O Ministério Público do Estado do Rio de Janeiro está dispensado de elaborar cláusulas próprias nas hipóteses de os contratos com as plataformas, redes sociais e empresas prestadoras dos serviços supramencionados já preverem a adoção de regramento protetivo.

§ 2º - O cidadão, ao entrar em contato com o Ministério Público do Estado do Rio de Janeiro por intermédio de quaisquer uma dessas ferramentas, deverá ser informado sobre a existência de cláusula ou política de privacidade e proteção de dados:

I - Caso haja cláusula própria elaborada pelo *MPRJ*, deverá constar o aviso por escrito ou veiculado oralmente, no caso de *call center*:

"Política de Privacidade e Proteção de Dados Pessoais

O Ministério Público do Estado do Rio de Janeiro, respeitando seu direito à privacidade e proteção de dados, informa que o acesso a esta ferramenta obedece à Cláusula Geral de Proteção de Dados Pessoais firmada por esta Instituição,

que se encontra disponível no seu sítio eletrônico <LINK para a publicação da cláusula de proteção de dados, a ser incorporada aos contratos firmados pelo Ministério Público>."

II - Caso não haja, o usuário deverá ser cientificado do seguinte:

"Política de Privacidade e Proteção de Dados Pessoais

Esta é uma ferramenta gratuita e o Ministério Público do Estado do Rio de Janeiro não se responsabiliza pelos dados aqui compartilhados, que são tratados nos termos da política de proteção de dados da própria ferramenta. Caso deseje conhecer mais da política de privacidade de dados do MPRJ, acesse o site da Instituição <LINK para a publicação da Política de Privacidade de Dados do MPRJ>."

Capítulo IX

Segurança e Boas Práticas

Art. 17 - O Ministério Público do Estado do Rio de Janeiro aplicará medidas técnicas e organizacionais de segurança da informação e governança institucional aptas a proteger os dados pessoais tratados, com observância das normas técnicas.

Art. 18 - Em caso de incidente ou suspeita de incidente que implique violação de segurança, incidental ou dolosa, a área ou órgão responsável deve comunicar imediatamente ao Encarregado de Proteção de Dados Pessoais, visando à adoção das medidas necessárias para minimizar os efeitos, prezando, em especial, pela integridade dos sistemas e proteção a direitos e garantias fundamentais do titular dos dados pessoais.

§ 1º - Caberá ao Encarregado comunicar ao Procurador-Geral de Justiça e ao titular de dados pessoais a ocorrência de incidente de segurança que acarrete risco ou dano relevante ao titular;

§ 2º - Caberá ao Encarregado deliberar com o Comitê Estratégico de Proteção de Dados Pessoais, de acordo com a relevância e a gravidade do incidente, sobre a necessidade de comunicação à Autoridade Nacional e aos titulares dos dados pessoais, consoante o art. 48 da LGPD.

Art. 19 - A Secretaria de Tecnologia da Informação e de Comunicação - STIC, sob a coordenação do Comitê Estratégico de Proteção de Dados Pessoais - CEPDAP, deverá disponibilizar no sítio eletrônico do Ministério Público do Estado do Rio de Janeiro, de forma ostensiva e de fácil acesso:

I - informações básicas sobre a Lei Geral de Proteção de Dados Pessoais no Ministério Público do Estado do Rio de Janeiro, incluindo: hipóteses em que, no exercício de suas atribuições (bases legais), realiza o tratamento de dados pessoais; informações claras e atualizadas sobre a previsão legal, finalidade, os procedimentos e as práticas utilizadas para a execução das atribuições;

II - as obrigações do Ministério Público do Estado do Rio de Janeiro (controlador) e as exceções à incidência da LGPD; os direitos dos titulares e a indicação do Encarregado;

III - Termos de uso e política de privacidade das plataformas digitais utilizadas pelo Ministério Público do Estado do Rio de Janeiro, como *website* e redes sociais.

Capítulo X

Disposições Finais

Art. 20 - 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

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

ATOS DO PROCURADOR-GERAL DE JUSTIÇA

DE 29.08.2023

Designa o Procurador de Justiça **MARCELO DALTRO LEITE**, com anuência do Procurador de Justiça designado **VICENTE FERREIRA DE ARRUDA COELHO FILHO**, para participar da sessão de julgamento na 18ª Câmara de Direito Privado do Tribunal de Justiça do Estado do Rio de Janeiro, no dia 12 de setembro de 2023, sem prejuízo de suas demais atribuições.

Designa o Promotor de Justiça **SÉRGIO LUIS LOPES PEREIRA** para prestar auxílio à 1ª Promotoria de Justiça Criminal de Maricá, especificamente no Inquérito Policial nº 951-00366/2023, e demais procedimentos investigatórios e/ou ações dele originados, a partir de 29 de agosto de 2023 até ulterior deliberação, sem prejuízo de suas demais atribuições e sem ônus para o Ministério Público.