DIÁRIO OFICIAL DA UNIÃO

Publicado em: 26/04/2024 | Edição: 81 | Seção: 1 | Página: 114

Órgão: Ministério da Justiça e Segurança Pública/Autoridade Nacional de Proteção de Dados/Conselho Diretor

RESOLUÇÃO CD/ANPD Nº 15, DE 24 DE ABRIL DE 2024

Aprova o Regulamento de Comunicação de Incidente de Segurança.

O CONSELHO DIRETOR DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD), no uso das competências que lhe são conferidas pelo art. 5º, I, do Regimento Interno da Autoridade Nacional de Proteção de Dados, aprovado pela Portaria nº 1, de 8 de março de 2021, e considerando as competências previstas no art. 55-J, XIII, da Lei nº 13.709, de 14 de agosto de 2018, no art. 2º, XIII, do Anexo I do Decreto nº 10.474, de 26 de agosto de 2020, bem como a deliberação tomada nos autos do processo nº 00261.000098/2021-67, resolve:

Art. 1º Aprovar o Regulamento de Comunicação de Incidente de Segurança na forma do anexo desta Resolução.

Art. 2º O inciso II do art. 14 do Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte, aprovado pela Resolução CD/ANPD nº 2, de 27 de janeiro de 2022, passa a vigorar com a seguinte redação:

"Art. 14. .....

.....

II - no caso da comunicação, à ANPD e ao titular, da ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, nos termos do Regulamento de Comunicação de Incidente de Segurança, aprovado pela Resolução CD/ANPD nº 15, de 24 de abril de 2024;

....." (NR)

Art. 3º Esta Resolução entra em vigor na data da sua publicação.

WALDEMAR GONÇALVES ORTUNHO JUNIOR
Diretor-Presidente

ANEXO

REGULAMENTO DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Este Regulamento tem por objetivo estabelecer os procedimentos para Comunicação de Incidente de Segurança, que possa acarretar risco ou dano relevante aos titulares, nos termos do art. 48 da Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).

Art. 2º São objetivos deste Regulamento:

I - proteger os direitos dos titulares;

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

III - assegurar a efetividade do princípio da responsabilização e da prestação de contas pelos agentes de tratamento;

IV - promover a adoção de regras de boas práticas, de governança, de medidas de prevenção e segurança adequadas;

V - estimular a promoção da cultura de proteção de dados pessoais;

VI - garantir que os agentes de tratamento atuem de forma transparente e estabeleçam uma relação de confiança com o titular; e

VII - fornecer subsídios para as atividades regulatória, fiscalizatória e sancionatória da Autoridade Nacional de Proteção de Dados (ANPD).

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 ANPD ao controlador, nos termos do art. 48, § 2º, I, da LGPD, no âmbito do processo de comunicação de incidente de segurança, 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 pessoa física, equipamento, sistema, órgão ou entidade;

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 controlador que comunica à ANPD 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, inclusive para contratação de serviços e aquisição de produtos;

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 - disponibilidade: propriedade pela qual se assegura que o dado pessoal esteja acessível e utilizável, sob demanda, por uma pessoa natural ou determinado sistema, órgão ou entidade devidamente autorizados;

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

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

XIV- 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, comunicação ou difusão;

XV - natureza dos dados pessoais: classificação de dados pessoais em gerais ou sensíveis;

XVI- procedimento de apuração de incidente de segurança: procedimento instaurado pela ANPD para apurar a ocorrência de incidente de segurança que não tenha sido comunicado pelo controlador;

XVII - procedimento de comunicação de incidente de segurança: procedimento instaurado no âmbito da ANPD após o recebimento de comunicação de incidente de segurança;

XVIII - processo de comunicação de incidente de segurança: processo administrativo instaurado no âmbito da ANPD que abrange o procedimento de apuração incidente de segurança e o procedimento de comunicação de incidente de segurança; e

XIX - 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 Incidente de Segurança

Art. 4º O controlador deverá comunicar à ANPD e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

Art. 5º O incidente de segurança pode acarretar risco ou dano relevante aos titulares quando puder afetar significativamente interesses e direitos fundamentais dos titulares e, cumulativamente, envolver, pelo menos, um dos seguintes critérios:

I - dados pessoais sensíveis;

II - dados de crianças, de adolescentes ou de idosos;

III - dados financeiros;

IV - dados de autenticação em sistemas;

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

VI - dados em larga escala.

§ 1º O incidente de segurança que possa afetar significativamente interesses e direitos fundamentais será caracterizado, dentre outras situações, naquelas em que a atividade de tratamento puder impedir o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade.

§ 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.

§ 3º A ANPD poderá publicar orientações com o objetivo de auxiliar os agentes de tratamento na avaliação do incidente que possa acarretar risco ou dano relevante aos titulares.

Seção II

Da Comunicação de Incidente de Segurança à ANPD

Art. 6º A comunicação de incidente de segurança à ANPD deverá ser realizada pelo controlador no prazo de três dias úteis, ressalvada a existência de prazo para comunicação previsto em legislação específica.

§ 1º O prazo a que se refere o caput será contado do conhecimento pelo controlador de que o incidente afetou dados pessoais.

§ 2º A comunicação de incidente de segurança deverá conter as seguintes informações:

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

II - o número de titulares afetados, discriminando, quando aplicável, o número de crianças, de adolescentes ou de idosos;

III - as medidas técnicas e de segurança utilizadas para a proteção dos dados pessoais, adotadas antes e após o incidente, observados os segredos comercial e industrial;

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

V - os motivos da demora, no caso de a comunicação não ter sido realizada no prazo previsto no caput deste artigo;

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 de quem represente o controlador;

IX - a identificação do controlador e, se for o caso, declaração de que se trata de agente de tratamento de pequeno porte;

X - a identificação do operador, quando aplicável;

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

XII - o total de titulares cujos dados são tratados nas atividades de tratamento afetadas pelo incidente.

§ 3º As informações poderão ser complementadas, de maneira fundamentada, no prazo de vinte dias úteis, a contar da data da comunicação.

§ 4º A comunicação de incidente de segurança deverá ocorrer por meio de formulário eletrônico disponibilizado pela ANPD.

§ 5º A comunicação de incidente de segurança deverá ser realizada pelo controlador, por meio do encarregado, acompanhada de documento comprobatório de vínculo contratual, empregatício ou funcional, ou por meio de representante constituído, acompanhada de instrumento com poderes de representação junto à ANPD.

§ 6º Os documentos de que trata o § 5º deverão ser apresentados juntamente com a comunicação do incidente de segurança, no prazo previsto no caput deste artigo.

§ 7º No caso de descumprimento do previsto no § 6º, a ANPD poderá apurar a ocorrência do incidente de segurança por meio do procedimento de apuração de incidente de segurança.

§ 8º Os prazos constantes no caput e no § 3º deste artigo são contados em dobro para os agentes de pequeno porte, nos termos do disposto no Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), aos agentes de tratamento de pequeno porte, aprovado pela Resolução CD/ANPD nº 2, de 27 de janeiro de 2022.

Art. 7º Cabe ao controlador solicitar à ANPD, de maneira fundamentada, o sigilo de informações protegidas por lei, indicando aquelas cujo acesso deverá ser restringido, a exemplo das relativas à sua atividade empresarial cuja divulgação possa representar violação de segredo comercial ou industrial.

Art. 8º A ANPD poderá, a qualquer tempo, solicitar informações adicionais ao controlador, referentes ao incidente de segurança, inclusive o registro das operações de tratamento dos dados pessoais afetados pelo incidente, o relatório de impacto à proteção de dados pessoais (RIPD) e o relatório de tratamento do incidente, estabelecendo prazo para o envio das informações.

Seção III

Da Comunicação de Incidente de Segurança ao Titular

Art. 9º A comunicação de incidente de segurança ao titular deverá ser realizada pelo controlador no prazo de três dias úteis contados do conhecimento pelo controlador de que o incidente afetou dados pessoais, e deverá conter as seguintes informações:

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

II - as medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

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

IV - os motivos da demora, no caso de a comunicação não ter sido feita no prazo do caput deste artigo;

V - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente, quando cabíveis;

VI - a data do conhecimento do incidente de segurança; e

VII - o contato para obtenção de informações e, quando aplicável, os dados de contato do encarregado.

§ 1º A comunicação do incidente aos titulares de dados deverá atender aos seguintes critérios:

I - fazer uso de linguagem simples e de fácil entendimento; e

II - ocorrer de forma direta e individualizada, caso seja possível identificá-los.

§ 2º Considera-se comunicação de forma direta e individualizada aquela realizada pelos meios usualmente utilizados pelo controlador para contatar o titular, tais como telefone, e-mail, mensagem eletrônica ou carta.

§ 3º Caso a comunicação direta e individualizada mostre-se inviável ou não seja possível identificar, parcial ou integralmente, os titulares afetados, o controlador deverá comunicar a ocorrência do incidente, no prazo e com as informações definidas no caput, pelos meios de divulgação disponíveis, tais como seu sítio eletrônico, aplicativos, suas mídias sociais e canais de atendimento ao titular, de modo que a comunicação permita o conhecimento amplo, com direta e fácil visualização, pelo período de, no mínimo, três meses.

§ 4º O controlador deverá juntar ao processo de comunicação de incidente uma declaração de que foi realizada a comunicação aos titulares, constando os meios de comunicação ou divulgação utilizados, em até três dias úteis, contados do término do prazo de que trata o caput deste artigo.

§ 5º Poderá ser considerada boa prática, para fins do disposto no art. 52, § 1º, IX, da LGPD, a inclusão, na comunicação ao titular, de recomendações aptas a reverter ou mitigar os efeitos do incidente.

§ 6º O prazo constante no caput deste artigo é contado em dobro para os agentes de pequeno porte, nos termos do disposto no Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) aos agentes de tratamento de pequeno porte, aprovado pela Resolução CD/ANPD nº 2, de 27 de janeiro de 2022.

CAPÍTULO IV

DO REGISTRO DO INCIDENTE DE SEGURANÇA

Art. 10. O controlador deverá manter o registro do incidente de segurança, inclusive daquele não comunicado à ANPD e aos titulares, pelo prazo mínimo de cinco anos, contado a partir da data do registro, exceto se constatadas obrigações adicionais que demandem maior prazo de manutenção.

§ 1º O registro do incidente deverá conter, no mínimo:

I - a data de conhecimento do incidente;

II - a descrição geral das circunstâncias em que o incidente ocorreu;

III - a natureza e a categoria de dados afetados;

IV - o número de titulares afetados;

V - a avaliação do risco e os possíveis danos aos titulares;

VI - as medidas de correção e mitigação dos efeitos do incidente, quando aplicável;

VII - a forma e o conteúdo da comunicação, se o incidente tiver sido comunicado à ANPD e aos titulares; e

VIII - os motivos da ausência de comunicação, quando for o caso.

§ 2º Os prazos de guarda previstos neste artigo não se aplicam às entidades previstas no art. 23 da LGPD, desde que sejam observadas as regras aplicáveis aos documentos de guarda permanente previstas na tabela de temporalidade própria ou definidas pelo Conselho Nacional de Arquivos.

CAPÍTULO V

DO PROCESSO DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA

Seção I

Das Disposições Gerais

Art. 11. O processo de comunicação de incidente de segurança tem por objeto a fiscalização de atos relacionados ao tratamento e resposta ao incidente que possa acarretar risco ou dano relevante aos titulares de dados, a fim de salvaguardar os direitos dos titulares.

Parágrafo único. Aplicam-se ao processo de comunicação de incidente de segurança regido por este Regulamento, no que couber, as disposições do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador, aprovado pela Resolução CD/ANPD nº 01, de 28 de outubro de 2021.

Art. 12. A ANPD poderá, a qualquer momento, realizar auditorias ou inspeções junto aos agentes de tratamento, ou determinar a sua realização, para coletar informações complementares ou validar as informações recebidas, com o objetivo de subsidiar as decisões no âmbito do processo de comunicação de incidente de segurança.

Art. 13. O processo de comunicação de incidente de segurança inicia-se:

I - de ofício, no caso de procedimento de apuração de incidente de segurança; ou

II - com o recebimento da comunicação, devidamente formalizada, na forma do art. 6º, §5º, no caso de procedimento de comunicação de incidente de segurança.

Art. 14. Os processos de comunicação de incidente de segurança poderão ser analisados de forma agregada, e as eventuais providências deles decorrentes poderão ser adotadas de forma padronizada, em conformidade com o planejamento da atividade de fiscalização e os critérios de priorização definidos no Relatório de Ciclo de Monitoramento de que trata o art. 20 do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados, aprovado pela Resolução CD/ANPD nº 1, de 28 de outubro de 2021.

Art. 15. No curso do processo de comunicação de incidente de segurança, a ANPD poderá determinar ao controlador, com ou sem a sua prévia manifestação, a adoção imediata de medidas preventivas necessárias para salvaguardar direitos dos titulares, a fim de prevenir, mitigar ou reverter os efeitos do incidente e evitar a ocorrência de dano grave e irreparável ou de difícil reparação.

Parágrafo único. A ANPD poderá fixar multa diária para assegurar o cumprimento da determinação prevista no caput, na forma do Regulamento de Dosimetria e Aplicação de Sanções Administrativas, aprovado pela Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023.

Seção II

Do Procedimento de Apuração de Incidente de Segurança

Art. 16. A ANPD poderá apurar, por meio do procedimento de apuração de incidente de segurança, a ocorrência de incidentes que possam acarretar risco ou dano relevante aos titulares, não comunicados pelo controlador, de que venha a tomar conhecimento.

§ 1º A ANPD poderá requisitar ao controlador informações para apurar a ocorrência do incidente de segurança.

§ 2º A ANPD avaliará a ocorrência do incidente por meio dos critérios dispostos no art. 5º deste Regulamento.

Art. 17. Constatada a ocorrência de incidente de segurança, a ANPD determinará ao controlador o envio da comunicação à Autoridade e aos titulares, observados os prazos e condições descritos nos arts. 6º e 9º deste Regulamento, respectivamente.

§ 1º A ANPD poderá, ainda, instaurar processo administrativo sancionador para apurar o descumprimento do previsto nos arts. 6º e 9º deste Regulamento.

§ 2º Realizada a comunicação de incidente de segurança, na forma do caput, aplicar-se-á o procedimento de comunicação de incidente de segurança estabelecido na Seção III.

Seção III

Do Procedimento de Comunicação de Incidente de Segurança

Art. 18. O procedimento de comunicação de incidente de segurança será iniciado com o recebimento da comunicação do incidente pela ANPD, devidamente formalizada, na forma do art. 6º., §5º.

Parágrafo único. A comunicação do incidente será recebida, exclusivamente, por meio de canal específico, conforme orientação publicada no sítio eletrônico da ANPD.

Art. 19. Após avaliar a gravidade do incidente de segurança, a ANPD poderá determinar ao controlador a adoção de providências para a salvaguarda dos direitos dos titulares, tais como:

I - ampla divulgação do incidente em meios de comunicação; e

II - medidas para reverter ou mitigar os efeitos do incidente.

§ 1º A gravidade do incidente será avaliada com base nas informações obtidas e nos critérios de que trata o art. 5º deste Regulamento.

§ 2º As providências citadas no caput devem estar diretamente relacionadas ao incidente.

§ 3º A ANPD poderá determinar ampla divulgação do incidente em meios de comunicação, às expensas do controlador, para a salvaguarda dos direitos dos titulares, nos termos do art. 48, § 2º, I, da LGPD, quando a comunicação realizada pelo controlador mostrar-se insuficiente para alcançar parcela significativa dos titulares afetados pelo incidente.

§ 4º A ampla divulgação do incidente em meios de comunicação deverá ser compatível com a abrangência de atuação do controlador e a localização dos titulares dos dados pessoais afetados no incidente.

§ 5º A ampla divulgação do incidente poderá ser viabilizada em meio físico ou digital, considerada sempre a necessidade de se atingir o maior número possível de titulares afetados, admitidos os seguintes meios de veiculação:

I - mídia escrita impressa;

II - radiodifusão de sons e de sons e imagens; ou

III - transmissão de informações pela Internet.

§ 6º A ampla divulgação do incidente não se confunde com a sanção de publicização da infração de que trata no art. 52, IV, da LGPD.

§ 7º Na determinação das medidas para reverter ou mitigar os efeitos do incidente, serão consideradas aquelas que possam garantir a confidencialidade, a integridade, a disponibilidade e a autenticidade dos dados pessoais afetados, bem como minimizar os efeitos decorrentes do incidente para os titulares.

Art. 20. Como medida de transparência ativa, a ANPD poderá divulgar, em seu sítio eletrônico, informações estatísticas agregadas relativas aos incidentes de segurança.

Art. 21. A ANPD poderá instaurar processo administrativo sancionador caso o controlador não adote as medidas para reverter ou mitigar os efeitos do incidente de segurança no prazo e nas condições determinadas pela Autoridade.

Art. 22. As providências descritas no art. 19 deste Regulamento não constituem sanções ao agente regulado, sendo equiparadas às medidas decorrentes da atividade preventiva, nos termos do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados, aprovado pela Resolução CD/ANPD nº 1, de 28 de outubro de 2021.

Seção IV

Da Extinção do Processo de Comunicação de Incidente de Segurança

Art. 23. O processo de comunicação de incidente de segurança será declarado extinto nas seguintes hipóteses:

I - caso não sejam identificadas evidências suficientes da ocorrência do incidente, ressalvada a possibilidade de reabertura caso surjam fatos novos;

II - caso a ANPD considere que o incidente não possui potencial para acarretar risco ou dano relevante aos titulares, nos termos do art. 5º deste Regulamento;

III - caso o incidente não envolva dados pessoais;

IV - caso tenham sido tomadas todas as medidas adicionais para mitigação ou reversão dos efeitos gerados; ou

V - realização da comunicação aos titulares e adoção das providências pertinentes pelo controlador, em conformidade com a LGPD, as disposições deste Regulamento e as determinações da ANPD.

Parágrafo único. Na hipótese do inciso II do caput, mesmo com a declaração da extinção do processo de comunicação de incidente de segurança, a ANPD poderá determinar a adoção de medidas de segurança diretamente relacionadas ao incidente, com o intuito de salvaguardar os direitos dos titulares.

CAPÍTULO VI

DAS DISPOSIÇÕES FINAIS

Art. 24. As disposições constantes deste Regulamento aplicam-se aos processos de comunicação de incidentes de segurança em curso quando da sua entrada em vigor, respeitados os atos processuais praticados e consolidados.