RESOLUÇÃO CD/ANPD Nº X, DE XX DE XXXXXXXXXX DE 2023

Aprova o Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais.

O CONSELHO DIRETOR DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD), com base nas competências previstas no art. 55-J, inciso XIII, da Lei nº 13.709, de 14 de agosto de 2018, no art. 2º, inciso XIII, do Anexo I do Decreto nº 10.474, de 26 de agosto de 2020, no art. 5º, inciso I do Regimento Interno da Autoridade Nacional de Proteção de Dados (ANPD), aprovado pela Portaria nº 1, de 8 de março de 2021,

CONSIDERANDO o que consta nos autos do Processo nº 00261.000098/2021-67; e

CONSIDERANDO a deliberação tomada no Circuito Deliberativo nº XX/2023, resolve:

Art. 1º Aprovar o Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais 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 - na comunicação à ANPD e ao titular da ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, prevista no *caput* dos arts. 6º e 9º do Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais, aprovado pela Resolução CD/ANPD nº X, de XX de XXXXXXX de 2023." (NR)

Art. 3º Esta Resolução entra em vigor em 1º de xxxxxx de 2023.

WALDEMAR GONÇALVES ORTUNHO JUNIOR

Diretor-Presidente

ANEXO
REGULAMENTO DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Este Regulamento tem por objetivo normatizar o processo de comunicação de incidente de segurança com dados pessoais 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 O processo de comunicação de incidente de segurança com dados pessoais atenderá aos seguintes objetivos:

I - proteger os direitos dos titulares;

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

III - incentivar o princípio da responsabilização e da prestação de contas pelos agentes de tratamento;

IV - promover a adoção de regras de boas práticas e de governança e 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 regulatórias, de fiscalização e sancionadora 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 com dados pessoais, como a publicação no sítio da Internet e nas redes sociais do controlador ou em outros meios de grande alcance;

II - autenticidade: propriedade pela qual se assegura que o dado pessoal foi produzido, expedido, modificado ou destruído 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, como identificação pessoal, autenticação em sistemas, financeiro, saúde, educação e judicial;

IV - comunicação do incidente de segurança: ato do controlador que comunica à ANPD e ao titular de dados a ocorrência de incidente de segurança com dados pessoais 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, sistemas, órgãos ou entidades não autorizadas e nem credenciadas;

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

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

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

XII - medidas de segurança relacionadas a dados pessoais: medidas técnicas e administrativas adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração ou comunicação;

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

XIV - procedimento de apuração de incidente de segurança: procedimento realizado pela ANPD para apurar a ocorrência de incidente de segurança com dados pessoais capaz de acarretar risco ou dano relevante ao titular que não tenha sido comunicado pelo controlador;

XV - procedimento de comunicação de incidente de segurança: procedimento no âmbito da ANPD que abrange a comunicação do incidente com dados pessoais capaz de

acarretar risco ou dano relevante ao titular e a avaliação da necessidade de determinação de adoção de providências;

XVI - processo de comunicação de incidente de segurança com dados pessoais: processo instaurado no âmbito da ANPD, com o objetivo de verificar a ocorrência de incidentes de segurança com dados pessoais capazes de acarretar risco ou dano relevante aos titulares de dados, podendo abranger o procedimento de apuração de incidente de segurança e o procedimento de comunicação de incidente de segurança; e

XVII - relatório de tratamento de incidente: relatório fornecido pelo controlador que contém cópias, em meio físico ou digital, de documentos, dados e informações relevantes para descrever o incidente e as ações adotadas para o seu tratamento, tais como, evidências e cronologia do incidente, metodologia de investigação e ferramentas utilizadas, e medidas de segurança adotadas.

CAPÍTULO III
DA COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA

Seção I
Dos critérios para comunicação de incidentes de segurança

Art. 4º O controlador deverá comunicar à ANPD e ao titular os incidentes de segurança com dados pessoais que possam acarretar risco ou dano relevante aos titulares.

Art. 5º Para fins deste Regulamento, considera-se que um incidente de segurança com dados pessoais pode acarretar risco ou dano relevante aos titulares quando tiver potencial de afetar significativamente interesses e direitos fundamentais dos titulares e envolver pelo menos um dos seguintes critérios:

I - dados sensíveis;

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

III - dados financeiros;

IV - dados de autenticação em sistemas; ou

V - dados em larga escala.

§ 1º São considerados incidentes que têm potencial de afetar significativamente interesses e direitos fundamentais dos titulares aqueles que possam:

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

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

§ 2º Para aplicação deste Regulamento, os incidentes de segurança com dados pessoais em larga escala serão assim caracterizados quando abrangerem número significativo de titulares, considerando, ainda, o volume de dados envolvidos 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 ao titular.

Seção II
Da comunicação do incidente à ANPD

Art. 6º A comunicação do incidente de segurança com dados pessoais à ANPD deverá ser realizada pelo controlador, no prazo de três dias úteis, ressalvada a existência de legislação específica, contados do conhecimento do incidente de segurança, sempre que o incidente possa acarretar risco ou dano relevante aos titulares afetados, e deve 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 de segurança para a proteção dos dados pessoais adotadas antes e após o incidente;

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

V - os motivos da comunicação do incidente não ter sido realizada no prazo, se for o caso;

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

VII - a data e a hora do conhecimento do incidente de segurança;

VIII - os dados do encarregado, quando aplicável, ou do comunicante, acompanhado, nesta hipótese, de procuração ou outro instrumento com poderes para representar o controlador junto à ANPD;

IX - os dados de identificação do controlador e, se cabível, declaração de tratar-se de agente de tratamento de pequeno porte;

X - as informações sobre o operador, quando aplicável;

XI - a declaração de que foi realizada a comunicação aos titulares, nos termos do art. 10 deste Regulamento;

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

XIII - o total de titulares cujos dados são tratados pela organização e na atividade de tratamento afetada pelo incidente.

§ 1º Excepcionalmente, as informações poderão ser complementadas, no prazo de vinte dias úteis, a contar do momento em que o controlador tomou conhecimento do incidente, prorrogável uma vez, por igual período, mediante solicitação fundamentada a ser avaliada pela ANPD.

§ 2º A comunicação do incidente de segurança deverá ocorrer por meio de formulário eletrônico, disponibilizado pela ANPD.

§ 3º A comunicação do incidente de segurança não será admitida quando apresentada por pessoa sem legitimidade.

§ 4º Caso o controlador seja representado por advogado, este poderá efetuar a comunicação sem procuração, obrigando-se a apresentá-la no prazo de até quinze dias úteis, a contar da data da comunicação, sob pena desta não ser admitida.

§ 5º Nas hipóteses de não admissão da comunicação do incidente previstas nos §§ 3º e 4º, a ANPD poderá apurar a ocorrência do incidente de segurança por meio do procedimento de apuração de incidente de segurança, sem prejuízo da instauração de processo administrativo sancionador para avaliar o descumprimento do previsto nos arts. 6º e 9º deste Regulamento.

§ 6º O prazo constante no *caput* deste artigo conta-se 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 do incidente ao titular de dados pessoais

Art. 9º A comunicação do incidente de segurança com dados pessoais ao titular deverá ser realizada pelo controlador, no prazo de três dias úteis contados do conhecimento do incidente de segurança, sempre que o incidente possa acarretar risco ou dano relevante aos titulares afetados, e deve conter as seguintes informações:

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

II - os riscos ou impactos ao titular;

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

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

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

§ 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 se mostre inviável ou não seja possível determinar, 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 na sua página na Internet, em aplicativos, em suas mídias sociais e em canais de atendimento ao titular, de modo que a comunicação permita o conhecimento amplo, com direta e fácil visualização pelo período de, no mínimo, seis meses.

§ 4º A ANPD determinará que o controlador faça nova comunicação, caso a primeira não contenha todas as informações necessárias ou tenha se utilizado de meios inadequados, ou ainda que comunique o incidente de segurança ao titular, caso a comunicação não tenha sido realizada.

§ 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 reduzir os efeitos do incidente.

§ 6º O prazo constante no *caput* deste artigo conta-se 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 DE INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

Art. 10. O controlador deverá manter o registro de incidentes de segurança com dados pessoais, inclusive daqueles não comunicados à ANPD e aos titulares, pelo prazo mínimo de cinco anos, contados a partir da data do registro, exceto se constatadas obrigações adicionais que demandem maior prazo de manutenção.

§ 1º O registro do incidente deve 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 foi 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 COM DADOS PESSOAIS

Seção I
Das disposições gerais

Art. 11. Aplicam-se ao processo de comunicação de incidente de segurança com dados pessoais regido por este Regulamento as disposições das Seções I, II e IV do Capítulo IV do Título I 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. O processo de comunicação de incidente de segurança com dados pessoais pode incluir os seguintes procedimentos:

I - Procedimento de Apuração de Incidente de Segurança; e

II - Procedimento de Comunicação de Incidente de Segurança.

Parágrafo único. O procedimento de apuração de incidente de segurança não é de realização obrigatória, somente sendo iniciado nas hipóteses em que a ANPD tomar conhecimento de um incidente de segurança envolvendo dados pessoais que não tenha sido comunicado pelo controlador nos prazos e nas condições estabelecidas neste Regulamento.

Art. 13. Os processos de comunicação de incidente de segurança com dados pessoais, de que trata este Regulamento, poderão ser analisados de forma agregada, e as eventuais providências deles decorrentes poderão ser adotadas de forma padronizada.

Parágrafo único. Os processos referidos no *caput* serão analisados e, se for o caso, extintos, 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 nº 1, de 28 de outubro de 2021.

Art. 14. Em qualquer fase do processo de comunicação de incidente de segurança com dados pessoais, a ANPD poderá determinar ao controlador a adoção imediata de medidas preventivas necessárias para salvaguardar direitos dos titulares ou para reverter ou mitigar os efeitos do incidente, sem prévia manifestação do controlador.

Parágrafo único. As medidas referidas no *caput* devem estar diretamente relacionadas ao incidente de segurança e à salvaguarda dos direitos dos titulares.

Seção II
Do procedimento de apuração de incidente de segurança

Art. 15. A ANPD poderá apurar, por meio do procedimento de apuração de incidente, a ocorrência de incidentes de segurança com dados pessoais 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 que possa acarretar risco ou dano relevante aos titulares por meio dos critérios dispostos no art. 5º deste Regulamento.

Art. 16. A ANPD determinará ao controlador o envio da comunicação do incidente à Autoridade e aos titulares, quando identificar a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares de dados que não tenha sido comunicado pelo controlador.

§ 1º A ANPD poderá fixar multa diária para assegurar o cumprimento da determinação prevista no *caput*.

§ 2º A ANPD poderá, ainda, instaurar processo administrativo sancionador para apurar o descumprimento do previsto nos arts. 6º e 9º deste Regulamento.

Seção III
Do procedimento de comunicação de incidente de segurança

Art. 17. O procedimento de comunicação de incidente de segurança será iniciado com o recebimento da comunicação do incidente pela ANPD.

Art. 18. 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 com dados pessoais.

Art. 19. Avaliada a gravidade do incidente, a ANPD poderá determinar ao controlador a adoção das seguintes providências para a salvaguarda dos direitos dos titulares, dentre outras:

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

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

§ 1º As providências citadas no *caput* devem estar diretamente relacionadas ao incidente de segurança.

§ 2º A depender da complexidade das providências para a salvaguarda dos direitos dos titulares a serem exigidas ao controlador, as determinações poderão ser feitas em processo administrativo apartado, nos termos do art. 32 do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados, aprovado pela Resolução nº CD/ANPD nº 1, de 28 de outubro de 2021.

§ 3º A ANPD poderá divulgar em sua página na Internet informações relativas a incidentes de segurança com dados pessoais, com o objetivo de trazer maior transparência, segurança e orientações aos titulares afetados, observados os segredos comercial e industrial.

Art. 20. A ANPD poderá determinar ampla divulgação do incidente em meios de comunicação, a ser custeada pelo controlador, para a salvaguarda dos direitos dos titulares, nos termos do art. 48, § 2º, I da LGPD, quando a comunicação realizada pelo controlador se mostrar insuficiente para alcançar parcela significativa dos titulares afetados pelo incidente.

§ 1º A ampla divulgação do incidente em meios de comunicação deverá ser compatível com a abrangência de atuação do agente de tratamento de dados e a localização dos titulares dos dados pessoais afetados no incidente.

§ 2º 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, dentre outros, 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.

Art. 21. Na determinação pela ANPD 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 de dados.

Art. 22. A ANPD realizará o monitoramento do cumprimento das determinações e da implantação das medidas, com base em critérios de priorização.

Art. 23. A ANPD poderá instaurar processo administrativo sancionador caso o controlador não adote as medidas para reverter ou mitigar os efeitos do incidente no prazo e nas condições determinadas pela Autoridade.

Art. 24. 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 com dados pessoais

Art. 25. O processo de comunicação de incidente de segurança com dados pessoais poderá ser declarado extinto nas seguintes hipóteses:

I - Ao final do procedimento de apuração de incidente de segurança:

a) caso não sejam identificadas pela ANPD evidências suficientes da ocorrência do incidente, ressalvada a possibilidade de reabertura caso surjam fatos novos;
b) caso a ANPD considere que o incidente não possui potencial para acarretar risco ou dano relevante aos titulares de dados; ou
c) caso o incidente não envolva dados pessoais.

II - No curso do procedimento de comunicação de incidente de segurança:

a) se a ANPD considerar que o incidente não acarreta risco ou dano relevante aos titulares de dados; ou
b) que não sejam necessárias medidas adicionais para mitigação ou reversão dos efeitos gerados.

Parágrafo único. Na hipótese da alínea b, do inciso I, mesmo com a decisão da extinção do processo de comunicação de incidente de segurança com dados pessoais, a ANPD poderá determinar a adoção de medidas de segurança com o intuito de salvaguardar os direitos dos titulares.

CAPÍTULO VI
DAS DISPOSIÇÕES FINAIS

Art. 26. Ao entrar em vigor este Regulamento, suas disposições se aplicarão aos processos de comunicação de incidentes de segurança em curso, respeitados os atos já praticados.