RESOLUÇÃO CRCSC N.º 453, DE 13 DE DEZEMBRO DE 2021.

Institui a Política de Notificação de Incidentes de Segurança com Dados Pessoais do Conselho Regional de Contabilidade de Santa Catarina.

O **CONSELHO REGIONAL DE CONTABILIDADE DE SANTA CATARINA**, no exercício de suas atribuições legais e regimentais,

Considerando a Lei n.º 13.709, de 14 de agosto de 2018, que trata da Lei Geral de Proteção de Dados Pessoais (LGPD);

Considerando 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;

Considerando que os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista na LGPD em relação aos dados pessoais, mesmo após o seu término,

R E S O L V E:

CAPÍTULO I
DA POLÍTICA E DAS DEFINIÇÕES

Art. 1º Fica instituída a Política de Notificação de Incidentes de Segurança com Dados Pessoais do Conselho Regional de Contabilidade de Santa Catarina (CRCSC).

Art. 2º Para os efeitos desta resolução, entende-se por:

I – Dado pessoal: qualquer informação relacionada a uma pessoa natural identificada ou identificável. Isso significa que um dado é considerado pessoal quando permite a identificação direta ou indireta da pessoa natural;

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 – Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

IV – Tratamento: toda a 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, transparência, difusão ou extração;

V – Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. No caso desta política, o CRCSC.

VI – 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);

VII – Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII – Comitê Gestor de Privacidade e Proteção de Dados (CGPPD): comitê responsável pela avaliação dos mecanismos de tratamento, privacidade e proteção de dados existentes e pela proposição de ações voltadas ao seu aperfeiçoamento com vistas ao cumprimento das disposições da Lei n.º 13.709, de 14 de agosto de 2018, no âmbito do CRCSC;

IX – Autoridade Nacional de Proteção de Dados (ANPD): órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta lei em todo o território nacional;

X – Notificação: ato ou efeito de informar ou de dar a conhecer sobre uma ocorrência e/ou incidente de segurança com dados pessoais.

CAPÍTULO II
DO OBJETIVO

Art. 3º A Política de Notificação de Incidentes de Segurança com Dados Pessoais do CRCSC tem por objetivo descrever os procedimentos necessários para a identificação, comunicação e notificação do incidente de segurança com dados pessoais.

Art. 4º É um incidente de segurança com dados pessoais qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou, ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

CAPÍTULO III
DA COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

Art. 5º A identificação do incidente pode ocorrer das seguintes formas:

I – denúncia por parte de titular ou terceiro;

II – reporte por parte do operador;

III – pelo emprego de ferramentas automatizadas que detectam vazamentos de dados;

Art. 6º Todas as violações de dados pessoais devem ser comunicadas ao Encarregado pelo tratamento de dados pessoais do CRCSC, sem demora injustificada, para registro e avaliação das medidas a tomar.

Art. 7º Em caso de um incidente de segurança com dados pessoais, o operador deverá encaminhar a comunicação ao Encarregado pelo tratamento de dados pessoais do CRCSC, pelo *e-mail* dpo@crcsc.org.br, no prazo de 24 (vinte e quatro) horas, contadas da data do conhecimento do incidente.

Art. 8º No caso do titular ou terceiro, a comunicação de um incidente de segurança com dados pessoais poderá ser enviada ao Encarregado pelo tratamento de dados pessoais do CRCSC, pelo *e-mail* dpo@crcsc.org.br, preferencialmente, em até 48 (quarenta e oito) horas, contadas da data do conhecimento do incidente.

Art. 9º Na comunicação, o operador, terceiro ou titular dos dados pessoais deverá descrever sucintamente o incidente ocorrido, atentando para informações, tais como:

I – descrever a natureza da violação dos dados pessoais incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, bem como as categorias e o número aproximado de registros de dados pessoais em causa;
II – descrever as consequências prováveis da violação de dados pessoais;
III – descrever as medidas adotadas ou propostas para conduzir o caso, o que pode incluir medidas para mitigar os possíveis efeitos adversos da violação dos dados pessoais.

Art. 10. O Encarregado pelo tratamento de dados pessoais do CRCSC será responsável pelo registro e análise inicial do incidente e pela resposta sobre o incidente relatado.

Art. 11. Após o registro e a análise inicial do incidente, o Encarregado pelo tratamento de dados pessoais do CRCSC compartilhará a comunicação com o Comitê Gestor de Privacidade e Proteção de Dados (CGPPD) ou, na sua falta, por Comitê criado no âmbito do CRCSC de equivalente competência, que fará a avaliação das medidas a tomar.

§ 1º Caso necessário, o Comitê Gestor de Privacidade e Proteção de Dados (CGPPD) ou, na sua falta, o Comitê criado no âmbito do CRCSC de equivalente competência poderá acionar o Departamento de Tecnologia da Informação e o Departamento Jurídico do CRCSC.

§ 2º O Comitê Gestor de Privacidade e Proteção de Dados (CGPPD) ou, na sua falta, o Comitê criado no âmbito do CRCSC de equivalente competência não realiza procedimentos de investigação criminal, e eventuais desdobramentos relacionados aos incidentes deverão ser encaminhados às autoridades policiais competentes.

Art. 12. As partes envolvidas devem seguir as orientações do Encarregado pelo tratamento de dados pessoais do CRCSC, pois a adoção de medidas por conta própria pode agravar o problema ou danificar evidências do incidente com dados pessoais.

Art. 13. As partes envolvidas devem manter sigilo sobre a comunicação recebida, pois tornar a informação pública pode prejudicar a investigação do suposto incidente com dados pessoais e a identificação do autor do incidente.

CAPÍTULO IV

DA NOTIFICAÇÃO DE INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

Art. 14. O CRCSC notificará a ANPD e o titular da ocorrência de incidente de segurança com dados pessoais que possa acarretar risco ou dano relevante aos titulares.

§ 1º O CRCSC deverá avaliar internamente a relevância do risco ou dano do incidente de segurança para determinar se deverá comunicar à ANPD e ao titular.

§ 2º Para a avaliação interna, deverão ser analisados os incidentes que envolvam especialmente:

I – dados sensíveis ou de indivíduos em situação de vulnerabilidade, incluindo crianças e adolescentes, ou que tenham o potencial de ocasionar danos materiais ou morais, tais como discriminação, violação do direito à imagem e à reputação, fraudes financeiras e roubo de identidade; e

II – 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 notificação não será necessária se o responsável pelo tratamento puder demonstrar, de forma irrefutável, que a violação da segurança dos dados pessoais não constitui um risco relevante para os direitos e liberdades do titular dos dados.

Art. 15. Caso necessária, a notificação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

I – a descrição da natureza dos dados pessoais afetados;

II – as informações sobre os titulares envolvidos;

III – a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

IV – os riscos relacionados ao incidente;

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

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

Art. 16. Caso não seja possível fornecer todas as informações no momento da notificação preliminar, informações adicionais poderão ser fornecidas posteriormente, sendo que no momento da notificação preliminar deverá ser informado à ANPD se serão fornecidas mais informações posteriormente, bem como quais meios estão sendo utilizados para obtê-las.

Art. 17. A notificação à ANPD será feita por intermédio do Encarregado pelo tratamento de dados pessoais do CRCSC.

Parágrafo único. O Encarregado pelo tratamento de dados pessoais do CRCSC comunicará o incidente com dados pessoais à ANPD, com base nas análises técnicas e jurídicas realizadas pelo Comitê Gestor de Privacidade e Proteção de Dados

(CGPPD) ou, na sua falta, pelo Comitê criado no âmbito do CRCSC de equivalente competência, pelo Departamento de Tecnologia da Informação e pelo Departamento Jurídico do CRCSC.

Art. 18. O Encarregado pelo tratamento de dados pessoais do CRCSC ainda tem como responsabilidade:

I – aprovar e autorizar a divulgação de comunicado aos titulares envolvidos no incidente com dados pessoais;
II – validar quaisquer comunicados ao público, imprensa e usuários;
III – orientar e/ou informar as equipes interessadas a respeito das práticas a serem adotadas com relação ao incidente com dados pessoais;
IV – coordenar todas as ações decorrentes do incidente com dados, com o intuito de mitigar os impactos percebidos;
V – atuar como porta-voz do CRCSC perante a ANPD, demais autoridades competentes e os usuários, supervisionando os contatos e comunicações com o público, decorrentes do incidente com dados pessoais, dentre outras atividades.

Art. 19. Esta Resolução entra em vigor na data de sua publicação.

Contadora **Rúbia Albers Magalhães**
Presidente

Aprovada na 1.404ª Reunião Plenária do CRCSC, realizada em 08 de dezembro de 2021.
Publicada no Diário Oficial da União, Seção 1, n.º 238 páginas 370 e 371, em 20 de dezembro de 2021.