PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA
de Santa Catarina

GUIA ORIENTATIVO LGPD

Crianças e Adolescentes no PJSC

MAIO 2023

GUIA ORIENTATIVO LGPD

Crianças e Adolescentes no PJSC

SUMÁRIO

1 INTRODUÇÃO - página 01

2 OBJETIVOS - página 02

3 ASPECTOS GERAIS - página 03

3.1 Principais conceitos - página 03
3.2 Princípios - página 05
3.3 Direitos do titular na LGPD - página 07

4 TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES E O PRINCÍPIO DO MELHOR INTERESSE - página 11

5 BASES LEGAIS - página 12

5.1 Aplicação dos artigos 7º e 11 da LGPD - página 12
5.2 Aplicação do caput do artigo 23 da LGPD - página 16
5.3 Consentimento - página 17

6 TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES PELO PJSC - página 19

6.1 Dúvidas frequentes - página 20

7 MITIGAÇÃO DE RISCOS, ARMAZENAMENTO E ELIMINAÇÃO DE DADOS - página 24

7.1 Mitigação de riscos no tratamento de dados de crianças e adolescentes - página 24
7.2 Armazenamento - página 27
7.3 Eliminação - página 30

8 CONSIDERAÇÕES FINAIS - página 32

REFERÊNCIAS - página 33

GUIA ORIENTATIVO SOBRE O TRATAMENTO DE DADOS PESSOAIS QUE ENVOLVEM CRIANÇAS E ADOLESCENTES NO ÂMBITO DO PODER JUDICIÁRIO CATARINENSE SEGUNDO A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (13.709/2018)

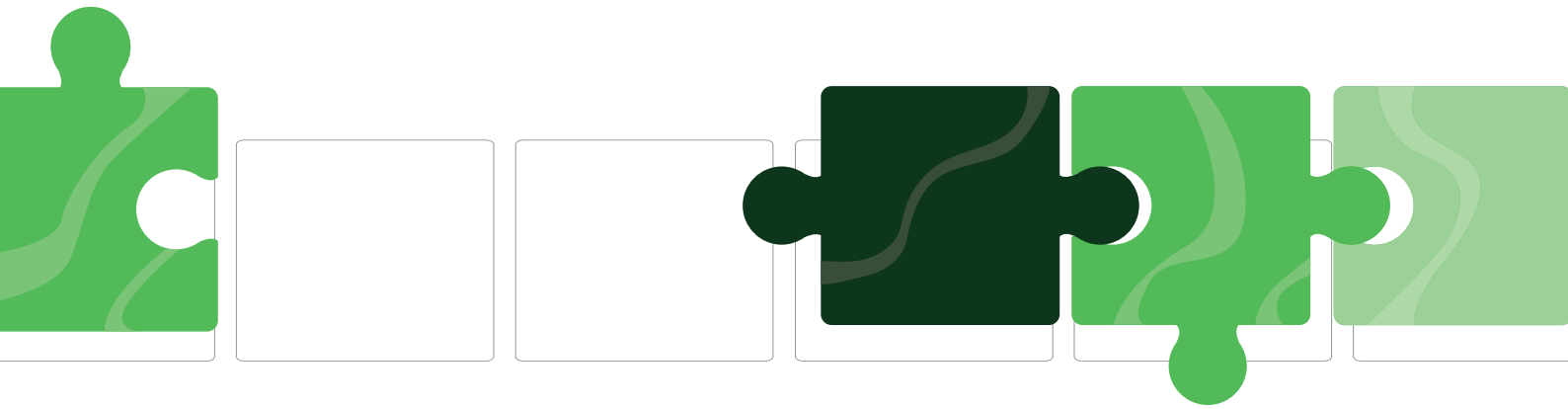
PRESIDENTE DO TRIBUNAL DE JUSTIÇA DE SANTA CATARINA
Desembargador João Henrique Blasi

CORREGEDORIA-GERAL DA JUSTIÇA
Desembargadora Denise Volpato

COORDENADORIA ESTADUAL DA INFÂNCIA E DA JUVENTUDE - CEIJ
Desembargador Álvaro Luiz Pereira de Andrade

COORDENADORIA DA MULHER EM SITUAÇÃO DE VIOLÊNCIA DOMÉSTICA E FAMILIAR - CEVID
Desembargadora Hildemar Meneguzzi de Carvalho

COMITÊ GESTOR DE PROTEÇÃO DE DADOS PESSOAIS - CGPDP
Desembargadora Denise de Souza Luiz Francoski



1.0 INTRODUÇÃO

O presente guia orientativo é resultado de estudo coordenado pela Coordenadoria Estadual da Infância e da Juventude (CEIJ) com a colaboração da Corregedoria-Geral da Justiça (Núcleos II e V), do Comitê Gestor de Proteção de Dados Pessoais (CGPDP), da Comissão Judiciária de Adoção (CEJA) e da Coordenadoria da Mulher em Situação de Violência Doméstica e Familiar (CEVID), no âmbito do tratamento dos dados pessoais de crianças e adolescentes.

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) foi criada com o propósito de proteger e resguardar o direito de privacidade de cada indivíduo. Ela encontra respaldo na Constituição Federal de 1988, em seu artigo 5º, inciso X. A tônica da LGPD, no tocante à infância e juventude, tem como base o melhor interesse e a proteção integral de crianças e adolescentes. O seu artigo 14 está alinhado ao Estatuto da Criança e do Adolescente (ECA).

Nesse sentido, o intuito deste documento é apresentar conceitos e princípios norteadores da LGPD, de modo a orientar e contribuir para o adequado tratamento de dados pessoais que envolvam crianças e adolescentes. Partindo da necessidade de atenção que requer a área da infância e juventude, e da seleção dos principais assuntos que a ela se referem, este guia orientativo foi construído com o objetivo de servir de ferramenta a profissionais que lidam com dados pessoais de crianças e adolescentes em seu dia a dia.

2.0 OBJETIVOS

O objetivo geral deste guia orientativo é fornecer instruções e diretrizes acerca do tratamento de dados pessoais de crianças e adolescentes, com relação à atuação de profissionais no âmbito do Poder Judiciário de Santa Catarina (PJSC).

Os objetivos específicos do guia orientativo, por sua vez, são os seguintes:

a) Elucidar dúvidas referentes às situações em que há necessidade de consentimento de pelo menos um dos pais ou responsável legal para o tratamento de dados pessoais de crianças e adolescentes.

b) Abordar especificidades que devem ser observadas por agentes de tratamento (controlador e operador) nos procedimentos que envolvam dados de crianças e adolescentes, inclusive nos sistemas, programas e projetos desenvolvidos no âmbito do Poder Judiciário catarinense, a exemplo do Programa Busca Ativa, do Cadastro Único Informatizado de Adoção e Abrigo (CUIDA), do Sistema Nacional de Adoção (SNA), do Programa Novos Caminhos e do Cadastro Nacional de Adolescentes em Conflito com a Lei (CNACL).

3.0 ASPECTOS GERAIS

3.1 Principais conceitos

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) é aplicada a qualquer operação de tratamento de dados pessoais realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, com algumas ressalvas dispostas nos seus artigos 3º e 4º.

Destaca-se que a LGPD não alcança diretamente a proteção de dados de pessoas jurídicas.

Os principais conceitos utilizados pela LGPD estão dispostos no seu artigo 5º e podem ser sintetizados da seguinte forma:

TRATAMENTO (art. 5º, X, da LGPD) – Qualquer coisa que se faça com um dado pessoal como coletar, armazenar, reproduzir e compartilhar um dado pessoal.

Exemplo: solicitar dados pessoais para confecção de um estudo social é tratar dados pessoais.

DADO PESSOAL (art. 5º, I, da LGPD) – Qualquer informação que consiga identificar direta ou indiretamente uma pessoa natural.

Exemplo: nome, CPF, RG – Permitem identificar diretamente uma pessoa natural.

Exemplo 2: endereço, IP – Podem permitir a identificação de uma pessoa natural quando cruzada com outras informações.

DADO PESSOAL SENSÍVEL (art. 5º, II, da LGPD) – Trata-se de uma categoria especial de dado pessoal, que pode trazer algum tipo de discriminação ou maior dano ao titular do dado.

Exemplo: são dados relacionados à 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.

Exemplo 2: fotos, registros médicos, impressões digitais.

3.0 ASPECTOS GERAIS

DADO ANONIMIZADO (art. 5º, III, da LGPD) – Refere-se a um dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento, portanto, não podendo ser possível a associação, direta ou indireta a uma pessoa natural.

Exemplo: retirar ou eliminar de um documento original os dados pessoais existentes.

A LGPD não se aplica a dados anonimizados.

TITULAR DOS DADOS (art. 5º, V, da LGPD) – Corresponde a toda pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

AGENTES DE TRATAMENTO (art. 5º, IX, da LGPD) – Associado às figuras do Controlador e do Operador.

CONTROLADOR (art. 5º, VI, da LGPD) – Trata-se da pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais.

Exemplo: no PJSC, o Controlador é o próprio Tribunal, conforme delimitado em suaPolítica Geral de Privacidade e de Proteção de Dados Pessoais.

OPERADOR (art. 5º, VII, da LGPD) – Refere-se à pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Exemplo: são pessoas externas ao quadro funcional do PJSC, como prestadores de serviços externos.

No PJSC, os servidores são como “extensões do Controlador” e não operadores.

ENCARREGADO (art. 5º, VIII, da LGPD) – Diz respeito a pessoa indicada pelo controlador e pelo operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

3.0 ASPECTOS GERAIS

Observe:

Em alguns lugares, o encarregado é conhecido como *Data Protection Officer* (DPO).

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) (art. 5º, XIX, da LGPD) – Corresponde à autarquia de natureza especial, responsável por zelar, implementar e fiscalizar o cumprimento dos dispositivos da LGPD.

BASES LEGAIS (artigos 7º, 11 e 23 da LGPD) – Referem-se às hipóteses legais em que a LGPD autoriza o tratamento de dados pessoais, de dados pessoais sensíveis e de dados pessoais pelo poder público, respectivamente.

Exemplo: consentimento e cumprimento de obrigação legal.

No mais, o presente guia terá enfoque no artigo 14 da LGPD, que dispõe sobre os dados pessoais de crianças e adolescentes.

Por fim, destaca-se que:

CRIANÇA – Pessoa até doze anos de idade incompletos (art. 2º do ECA).
ADOLESCENTE – Pessoa entre doze e dezoito anos de idade (art. 2º do ECA).
INFANTO-JUVENIL – Termo relacionado ou destinado à infância e à juventude.

3.2 Princípios

O artigo 6º da LGPD afirma que todas as atividades de tratamento de dados pessoais precisarão observar, além da **BOA-FÉ**, os seguintes princípios:

FINALIDADE (art. 6º, I, da LGPD) – Corresponde à realização do tratamento para propósitos legítimos (permitido pelo ordenamento jurídico), específicos (delimitado dentro do propósito apresentado), explícitos (claramente revelado) e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

3.0 ASPECTOS GERAIS

Observe:

Para cada tratamento há uma finalidade. Não há possibilidade de tratamento posterior dos dados para finalidade diversa da inicialmente prevista.

ADEQUAÇÃO (art. 6º, II, da LGPD) – Significa a compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

NECESSIDADE (art. 6º, III, da LGPD) – Relaciona-se à limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

Exemplo: porque pedir o CPF e o RG de uma pessoa se apenas um desses dados é suficiente para a sua identificação?

LIVRE ACESSO (art. 6º, IV, da LGPD) – Diz respeito à garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

Observe:

Esse princípio tem vinculação direta com os direitos dos titulares, que serão vistos no próximo tópico.

QUALIDADE DOS DADOS (art. 6º, V, da LGPD) – Refere-se à garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

Observe:

Os dados precisam sempre estar certos e atualizados, sob pena de causar prejuízo ao titular.

TRANSPARÊNCIA (art. 6º, VI, da LGPD) – Corresponde à garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

3.0 ASPECTOS GERAIS

Observe:

Esse princípio também tem vinculação direta com os direitos dos titulares, que serão vistos no próximo tópico.

SEGURANÇA (art. 6º, VII, da LGPD) – Visa à utilização de medidas 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 difusão.

Observe:

Princípio ligado à segurança das informações.

Exemplo: como e onde são armazenados os dados pessoais coletados para fins de um estudo social?

PREVENÇÃO (art. 6º, VIII, da LGPD) – Diz respeito à adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

NÃO DISCRIMINAÇÃO (art. 6º, IX, da LGPD) – Significa a impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS (art. 6º, X, da LGPD) – Refere-se à demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

3.3 Direitos do titular na LGPD

A Lei Geral de Proteção de Dados reservou o seu Capítulo III para abordar os direitos dos titulares de dados.

Relembrando: TITULAR é a pessoa a quem se referem os dados pessoais que são objeto de tratamento.

3.0 ASPECTOS GERAIS

O artigo 17 da LGPD dispõe que toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade.

Já o artigo 18 determina que o titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

CONFIRMAÇÃO DA EXISTÊNCIA DE TRATAMENTO (art. 18, I, da LGPD) – A confirmação da existência de operação realizada com seus dados pessoais.

Exemplo: o TJSC trata dados pessoais referentes a minha pessoa?

ACESSO AOS DADOS (art. 18, II, da LGPD) – Acesso aos dados pessoais tratados, bem como às informações sobre a finalidade daqueles dados, categorias, destinatários, prazo de conservação, etc.

CORREÇÃO DE DADOS INCOMPLETOS, INEXATOS OU DESATUALIZADOS (art. 18, III, da LGPD) – A retificação de seus dados.

Exemplo: atualização de endereço ou inclusão ou retirada de nome de casado(a).

ANONIMIZAÇÃO, BLOQUEIO OU ELIMINAÇÃO (art. 18, IV, da LGPD) – A anonimização, o bloqueio e a eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na lei.

PORTABILIDADE DOS DADOS (art. 18, V, da LGPD) – A transferência dos dados pessoais a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial.

ELIMINAÇÃO DOS DADOS PESSOAIS TRATADOS COM BASE NO CONSENTIMENTO (art. 18, VI, da LGPD) – A eliminação dos dados pessoais tratados com base no consentimento do titular, com a ressalva das hipóteses previstas no art. 16 da LGPD, que aborda sobre a conservação dos dados para certas finalidades.

3.0 ASPECTOS GERAIS

Observe:

O artigo 16 da LGPD determina que os dados tratados com o consentimento podem ser mantidos quando: a) o controlador tem a obrigação legal de manter os dados; b) para estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; c) para transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na LGPD e d) para uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

INFORMAÇÃO SOBRE COMPARTILHAMENTO (art. 18, VII, da LGPD) – Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados.

POSSIBILIDADE DE NÃO FORNECER CONSENTIMENTO (art. 18, VIII, da LGPD) – O titular dos dados tem o direito de ser informado sobre a possibilidade de não fornecer consentimento e informado sobre as consequências da negativa.

Exemplo: o que acontece se eu não der meu consentimento para o tratamento solicitado?

REVOGAÇÃO DO CONSENTIMENTO (art. 18, IX, da LGPD) – O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do § 5º do art. 8º da LGPD.

Observe:

Por conta da possibilidade de revogação do consentimento a qualquer momento é que se recomenda o uso de outras bases legais.

Os parágrafos do artigo 18 da LGPD elencam outros direitos essenciais do titular, veja:

PETICIONAR EM RELAÇÃO AOS SEUS DADOS CONTRA O CONTROLADOR PERANTE A AUTORIDADE NACIONAL;

3.0 ASPECTOS GERAIS

Exemplo: caso o Controlador não solucione o problema do titular, este pode "recorrer" à Autoridade Nacional de Proteção de Dados Pessoais – ANPD.

OPOR-SE A TRATAMENTO REALIZADO COM FUNDAMENTO EM UMA DAS HIPÓTESES DE DISPENSA DE CONSENTIMENTO, EM CASO DE DESCUMPRIMENTO AO DISPOSTO NA LGPD.

EXERCER SEUS DIREITOS PERANTE OS ORGANISMOS DE DEFESA DO CONSUMIDOR.

Exemplo: qualquer pessoa pode procurar o Procon para reclamar da violação de direitos e regras previstas na LGPD.

IMPORTANTE!

- **Os direitos dos titulares não são absolutos. Todas as solicitações devem ser avaliadas e ponderadas se são efetivamente passíveis de cumprimento, sem que sejam frustrados outros direitos.**

- **Sempre que um titular fizer uma solicitação, é importante ter certeza de que ele realmente é quem se diz ser, sob pena de se causar um incidente de proteção de dados.**

4.0 TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES E O PRINCÍPIO DO MELHOR INTERESSE

A Constituição Brasileira de 1988 consagrou um marco no tratamento dos direitos da criança e do adolescente, a partir do qual estes deixaram de ser tratados como serespassivos e objetos de intervenção para se titularizarem sujeitos de direitos, como indivíduos autônomos.

Fundamentado nessa nova acepção, o artigo 227 da Carta Magna legitimou um novo sistema de garantias dos direitos infanto-juvenil, norteado pelo princípio da proteção integral, segundo no qual a construção de todo o ordenamento jurídico deve ser guiada para a proteção dos direitos da criança e do adolescente, com observância à condição peculiar de pessoa em desenvolvimento, destacando ser dever da família, da sociedade e do Estado resguardar os seus bens jurídicos fundamentais até que se tornem plenamente desenvolvidos.

Por outro lado, outro importante princípio que também norteia o sistema de garantias e direitos das crianças e adolescentes é o do melhor interesse, o qual extrai seu fundamento através da proteção integral.

O Princípio do Melhor Interesse estabelece que todas as ações, orientações ou decisões direcionadas à população infanto-juvenil devem pautar-se pelo que é melhor e mais adequado para satisfazer suas necessidades e interesses, visando assim, àproteção integral de seus direitos.

A criança e o adolescente, na nova sistemática jurídica e legislativa, são sujeitos de direitos, detentores de direitos fundamentais e da personalidade, dentre eles, o direito à privacidade, à imagem, à identidade e à integridade biopsíquica.

O sigilo dos dados pessoais do público infanto-juvenil e das informações digitais é uma das facetas de seu direito à vida privada. Considerando a sua especial condição de pessoa em desenvolvimento, o direito à proteção de seus dados é mais rigoroso. Por esse motivo, a legislação trouxe um cuidado particular para o manejo, intervenção e transmissão desses dados, qual seja, o atendimento ao princípio do melhor interesse, previsto no artigo 14 da LGPD: “O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente”.

Logo, todo e qualquer tratamento de dados de crianças e de adolescentes deve atentar à necessidade a que se propõe e obrigatoriamente sempre pautado pela busca do melhor interesse desse

5.0 BASES LEGAIS

5.1 Aplicação dos artigos 7° e 11 da LGPD

Além de apontar os princípios necessários para o devido tratamento de dados pessoais, conforme abordado no ponto 2.2 deste guia, a LGPD elencou as hipóteses taxativas de autorização para o tratamento de dados pessoais.

Essa autorização é denominada de **BASE LEGAL** e está estabelecida nos artigos 7° e 11 da LGPD.

Para que o tratamento de dados pessoais possa ser realizado, necessariamente a finalidade do tratamento deve estar expressa em uma das hipóteses dos artigos 7° e 11 da LGPD.

Observação:

Para o tratamento de dados pessoais, é aplicada a base legal do artigo 7° da LGPD. Em caso de tratamento de dados pessoais sensíveis, é aplicada a base legal do artigo 11 da LGPD.

Inicialmente, cumpre destacar as bases legais dos artigos 7° e 11 da LGPD.

FORNECIMENTO DE CONSENTIMENTO PELO TITULAR (arts. 7°, I, e 11, I da LGPD) – O titular dos dados ou o seu responsável legal deverá concordar com o tratamento de seus dados pessoais para uma finalidade determinada de forma LIVRE, INFORMADA e INEQUÍVOCA.

Exemplo: base legal utilizada para o tratamento de dados pessoais de crianças e adolescentes em audiência especial, para a finalidade de capacitação dos entrevistadores.

CUMPRIMENTO DE OBRIGAÇÃO LEGAL OU REGULATÓRIA PELO CONTROLADOR (arts. 7°, II e 11, II, "a", da LGPD) – Corresponde a uma base legal que dispensa o fornecimento de consentimento pelo titular. O tratamento de dados pessoais está amparado para o cumprimento de uma obrigação legal ou regulatória, como uma lei federal, estadual ou municipal, decreto, resolução do CNJ ou do TJSC, entre outras normas.

Exemplo: base legal utilizada pelo Tribunal de Justiça para o tratamento de dados pessoais para confecção de estudo social.

5.0 BASES LEGAIS

TRATAMENTO E USO COMPARTILHADO DE DADOS NECESSÁRIOS, PELA ADMINISTRAÇÃO PÚBLICA, PARA A EXECUÇÃO DE POLÍTICAS PÚBLICAS PREVISTAS EM LEIS E REGULAMENTOS OU RESPALDADAS EM CONTRATOS, CONVÊNIOS OU INSTRUMENTOS CONGÊNERES (arts. 7°, III e 11, II, "b", da LGPD) – A administração pública pode realizar tratamento e uso compartilhado de dados pessoais para o desenvolvimento de políticas públicas.

A LGPD reservou o seu Capítulo IV para abordar sobre o tratamento de dados pessoais pelo Poder Público.

Exemplo: o Programa Novos Caminhos utiliza essa base legal no tratamento de dados pessoais, pois o seu escopo (finalidade) tem a característica de uma política pública e é respaldado por instrumento formal de cooperação técnica entre as instituições partícipes.

REALIZAÇÃO DE ESTUDOS POR ÓRGÃO DE PESQUISA, GARANTIDA, SEMPRE QUE POSSÍVEL, A ANONIMIZAÇÃO DOS DADOS PESSOAIS (arts. 7°, IV e 11, II, "c", da LGPD) – Conforme dispõe o artigo 5, XVIII, da LGPD, órgão de pesquisa é "órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico".

Essa base legal só será aplicada se o solicitante se enquadrar no conceito de órgão de pesquisa disposto no artigo 5, XVIII, da LGPD. Entretanto, o entendimento será firmado após posicionamento da Autoridade Nacional de Proteção e Dados (ANPD) que irá regulamentar tal discussão.

5.0 BASES LEGAIS

EXECUÇÃO DE CONTRATO OU DE PROCEDIMENTOS PRELIMINARES RELACIONADOS A CONTRATO DO QUAL SEJA PARTE O TITULAR, A PEDIDO DO TITULAR DOS DADOS (art. 7º, V, da LGPD) – Corresponde ao tratamento de dados pessoais para execução de uma obrigação que foi pactuada contratualmente a pedido do titular dos dados.

Observe:

Essa base legal não está prevista para o tratamento de dados pessoais sensíveis.

Exemplo: roaming internacional, compartilhamento de dados entre operadoras parceiras.

PARA O EXERCÍCIO REGULAR DE DIREITOS EM PROCESSO JUDICIAL, ADMINISTRATIVO OU ARBITRAL (arts. 7º, VI e 11, II, "d", da LGPD).

Exemplo: base legal utilizada por partes e advogados para ingressar com demanda judicial em juízo.

PARA PROTEÇÃO DA VIDA OU DA INCOLUMIDADE FÍSICA DO TITULAR OU DE TERCEIRO (arts. 7º, VII e 11, II, "e", da LGPD) – A situação deve ser concreta e real, que envolva risco à vida do titular ou de terceiros, no presente, e não para proteção em momento futuro.

Exemplo: uso de dados pessoais pela polícia em casos de sequestro.

PARA TUTELA DA SAÚDE, EXCLUSIVAMENTE, EM PROCEDIMENTO REALIZADO POR PROFISSIONAIS DE SAÚDE, SERVIÇOS DE SAÚDE OU AUTORIDADE SANITÁRIA (arts. 7º, VIII e 11, II, "f", da LGPD) – Tratamento de dados realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária para a finalidade específica de tutela da saúde.

Exemplo: tratamento de dados pessoais realizado por hospitais para internação e tratamento.

5.0 BASES LEGAIS

QUANDO NECESSÁRIOS PARA ATENDER AOS INTERESSES LEGÍTIMOS DO CONTROLADOR OU DE TERCEIRO, EXCETO NO CASO DE PREVALECEREM DIREITOS E LIBERDADES FUNDAMENTAIS DO TITULAR QUE EXIJAM A PROTEÇÃO DOS DADOS PESSOAIS (art. 7°, IX, da LGPD) –Conforme o artigo 10 da LGPD,

> o legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: I - apoio e promoção de atividades do controlador; e II -proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

Observe:

Aplica-se conjuntamente a essa base legal, os §§ 1° ao 3°, do artigo 10 da LGPD.

Esta base legal não pode ser aplicada para dados pessoais sensíveis, por falta de previsão no artigo 11 da LGPD.

PARA A PROTEÇÃO DO CRÉDITO (art. 7°, X, da LGPD)

Observe:

Não há necessidade de consentimento pelo titular para abertura de cadastro positivo com dados de histórico de crédito.

GARANTIA DA PREVENÇÃO À FRAUDE E À SEGURANÇA DO TITULAR, NOS PROCESSOS DE IDENTIFICAÇÃO E AUTENTICAÇÃO DE CADASTRO EM SISTEMAS ELETRÔNICOS (art. 11, II, "g", da LGPD) – Relaciona-se a uma base legal que autoriza o tratamento de dados pessoais sensíveis para combater fraudes e garantir a segurança do titular.

Exemplo: o uso de biometria como processo de identificação de usuário para área de acesso restrito da empresa.

5.0 BASES LEGAIS

5.2 Aplicação do caput do artigo 23 da LGPD

Conforme abordado no tópico anterior, para que o tratamento de dados pessoais possa ser realizado, necessariamente a finalidade do tratamento deve estar expressa em uma das hipóteses dos artigos 7° e/ou 11 da LGPD.

Todavia, no caso do tratamento de dados realizado pelo Poder Público para sua atividade-fim, há situações em que não são encontradas bases legais adequadas nos artigos 7° ou 11 da LGPD, pois nem sempre a atividade finalística do Poder Público é baseada em lei (cumprimento de obrigação legal ou regulatória) ou em uma política pública.

Nesses casos, a doutrina passou a ver o caput do artigo 23 como uma base legal autônoma, aplicada somente ao Poder Público para atividade-fim.

O *caput* do artigo 23 determina que o tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1° da Lei n° 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que observadas algumas regras dispostas nos artigos 26 a 30 da LGPD.

As pessoas jurídicas de direito público referidas no parágrafo único do art. 1° da Lei n° 12.527/2011, por sua vez, são os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público e as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

Assim, o *caput* do artigo 23 pode ser utilizado pelo Tribunal de Justiça como uma base legal (seja autônoma ou complementar, junto com outra base legal existente nos artigos 7° ou 11 da LGPD, como defende parte da doutrina), para o tratamento de dados pessoais e dados pessoais sensíveis em sua atividade-fim (promover a solução de conflitos pela via judicial).

5.0 BASES LEGAIS

5.3 Consentimento

O consentimento é uma base legal prevista no artigo 7°, I (para dados pessoais) e no artigo 11, I (para dados pessoais sensíveis), ambos da LGPD.

O conceito de consentimento está expresso no artigo 5°, inciso XII da LGPD, como toda manifestação **LIVRE, INFORMADA e INEQUÍVOCA** pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

LIVRE: o titular dos dados pessoais deve ter a liberdade de escolha em conceder ou não o consentimento.

Se o titular estiver em situação em que é obrigado a dar o seu consentimento, este não é livre e, consequentemente, o consentimento não é válido.

INFORMADO: o titular dos dados deve informações suficientes acerca daquilo que será feito com os seus dados pessoais para que possa decidir por consentir ou não.

O titular tem o direito de saber o que acontece caso não forneça o consentimento.

INEQUÍVOCO: o titular dos dados deve expor a sua decisão de forma clara e objetiva.

Em relação ao tratamento de dados pessoais de CRIANÇA E ADOLESCENTE, este deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal, de acordo com o artigo 14, § 1° da LGPD.

A problemática do consentimento, está em sua **volatilidade**.

5.0 BASES LEGAIS

Como já abordado, o titular dos dados pode retirar o seu consentimento a qualquer momento, comprometendo o tratamento de dados realizado pelo Controlador ou Operador.

Ademais, caso haja alteração na finalidade do tratamento de dados, incompatível com o consentimento original, há necessidade de informar o titular dos dados e renovar o consentimento.

Observação:

A grande maioria dos tratamentos de dados realizados pelo PJSC no âmbito de suas atividades-fim não utiliza o consentimento como base legal, mas sim o cumprimento de obrigação legal ou regulatória (arts. 7º, II e 11, II, "a", da LGPD).

6.0 TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES PELO PJSC

No âmbito das atribuições do Poder Judiciário catarinense, o Tribunal de Justiça de Santa Catarina é considerado o controlador, representado por seu presidente, e seus servidores são presumidos controladores por extensão. Já as pessoas físicas e/ou entidades externas, com quem o Poder Judiciário catarinense mantém relação no tratamento de dados, são consideradas os operadores.

Para o tratamento (coleta, armazenamento, reprodução ou compartilhamento) de dados no âmbito do Poder Judiciário catarinense, recomenda-se realizar uma análise de conformidade com base em três critérios: finalidade, necessidade e base legal. Ou seja, o objetivo do tratamento de dados precisa ser legal, específico, claro, sem uso posterior para outro fim, utilizando-se somente o necessário para o que se destina, além de estar enquadrado em uma das hipóteses legais previstas no art. 7° (para dados pessoais) ou no art. 11 (para dados pessoais sensíveis) da LGPD.

O tratamento de dados pessoais realizado pelos servidores do PJSC, em sua grande maioria, está embasado na hipótese de cumprimento de obrigação legal ou regulatória pelo controlador, tendo em vista que os servidores são considerados controladores por extensão e que o tratamento realizado está previsto em lei ou resolução.

O tratamento de dados do público infantojuvenil necessita de uma maior cautela, exigindo-se, principalmente, o atendimento ao princípio do melhor interesse.

No âmbito da atuação jurisdicional, são comuns as dúvidas que envolvem o compartilhamento de dados de crianças e adolescentes, notadamente nas atividades relacionadas à confecção de estudos sociais, avaliações psicológicas e condução de programas e projetos institucionais.

De modo geral, o primeiro passo para o adequado manejo desses dados é a análise do propósito que se deseja alcançar a partir dessa ação.

Para tanto, deve-se valer das seguintes **perguntas norteadoras:**

1 - PARA QUE? É LEGÍTIMO? É ESPECÍFICO? (Princípio da finalidade).

2 - OS DADOS PESSOAIS COLHIDOS SÃO NECESSÁRIOS PARA O QUE SE OBJETIVA (FINALIDADE) OU É POSSÍVEL COLETAR UMA QUANTIDADE MENOR DE DADOS PESSOAIS? (Princípio da necessidade)

3 - A FINALIDADE SE ENCAIXA EM ALGUMA BASE LEGAL PREVISTA NOS ARTIGOS 7 OU 11 DA LGPD? (Base legal).

RESPONDENDO-SE POSITIVAMENTE A ESSAS TRÊS PERGUNTAS, O TRATAMENTO DE DADOS PESSOAIS ESTÁ DE ACORDO COM A LGPD.

6.1 DÚVIDAS FREQUENTES

1) É possível o uso de dados pessoais de crianças e adolescentes, de seus membros familiares ou de outras pessoas obtidos pelo servidor, para elaboração de estudos sociais, avaliação psicológica ou de qualquer outro documento?

Resposta: Sim. É possível o tratamento de dados de crianças e adolescentes quando da elaboração de estudos sociais, avaliação psicológica ou de qualquer outro documento, no âmbito do processo judicial ou no cumprimento de atribuições específicas do cargo. Trata-se de situação em que há uma **finalidade** definida e uma **base legal** adequada, já que se atua em cumprimento de obrigação legal ou regulatória (art. 7º, II, da LGPD) ou para a realização de atividade-fim do Poder Judiciário (caput do art. 23 da LGPD). Contudo, recomenda-se a análise acerca da necessidade de todos os dados coletados, verificando-se se todos são realmente necessários para a finalidade pretendida ou se alguns dados não precisam ser coletados.

2) O consentimento, como meio de autorização para o tratamento de dados pessoais de crianças e adolescentes, é necessário quando da elaboração de estudos sociais, avaliação psicológica ou de qualquer outro documento que envolva criança ou adolescente?

Resposta: Depende da finalidade do tratamento. Quando o tratamento de dados pessoais ocorre, por exemplo, para a elaboração de um estudo social ou de uma avaliação psicológica, há uma finalidade determinada, e a base legal adequada é o cumprimento de obrigação legal ou regulatória, já que se está diante de documentos exigidos e/ou previstos em lei. Veja que a utilização da base legal do cumprimento de obrigação legal ou regulatória (art. 7º, II, da LGPD) dispensa o uso do consentimento.

Contudo, será obrigatório o consentimento, por um dos pais ou responsável legal, se o dado tratado for utilizado para um fim diverso do inicialmente previsto ou em hipótese não prevista em lei ou regulamento.

A título de exemplo, pode-se citar o depoimento especial, em que há a obrigatoriedade do consentimento, por um dos pais ou pelo responsável legal, quando da utilização de imagens do depoimento gravado para fins de aperfeiçoamento ou formação, haja vista a utilização para um objetivo diverso do inicialmente previsto (processo judicial).

Para o preenchimento dos dados de crianças/adolescentes no Sistema Nacional de Adoção (SNA), no Cadastro Único Informatizado de Adoção e Acolhimento (CUIDA) e no Cadastro Nacional de Adolescentes em Conflito com a Lei (CNACL), não há necessidade de consentimento, uma vez que a atividade acontece no âmbito do exercício do cumprimento de obrigação legal, sem apresentar outras finalidades.

6.1 DÚVIDAS FREQUENTES

3) Dados pessoais de crianças e adolescentes podem ser compartilhados por servidores do PJSC com profissionais de instituições públicas, privadas ou da rede de atendimento?

Resposta: Depende da necessidade e da finalidade do compartilhamento.

Algumas situações:

– Primeiro caso: na elaboração de estudo social ou de qualquer outro documento pelo servidor, no âmbito do processo judicial ou no cumprimento de atribuições específicas do cargo, o compartilhamento de dados está embasado no cumprimento de obrigação legal, de modo que é possível o compartilhamento de dados pelo servidor com os profissionais da rede de atendimento para a coleta de informações, cujo destinatário do ato é o magistrado.

– Segundo caso: para a troca de informações acerca dos dados de crianças e adolescentes, a pedido dos profissionais da rede de atendimento, orienta-se que tal pedido seja formalizado por e-mail, no qual se indica a finalidade e a necessidade daquela informação.

– Terceiro caso: o compartilhamento das Guias de Acolhimento e Desligamento geradas no Sistema Nacional de Adoção – SNA e de Guias expedidas no Cadastro Nacional de Adolescentes em Conflito com a Lei (CNACL) está embasado no cumprimento de obrigação legal (art. 7°, II, da LGPD). Apresenta-se como base legal o Estatuto da Criança e do Adolescente, Artigo 101, § 3°, que estabelece que crianças e adolescentes somente poderão ser encaminhados às instituições que executam programas de acolhimento institucional, governamentais ou não, por meio de uma Guia de Acolhimento, expedida pela autoridade judiciária. No que se refere à Guia do CNACL, a base legal é a Resolução n° 165/2012 do Conselho Nacional de Justiça, a qual dispõe sobre as normas gerais referentes aos adolescentes em conflito com a lei nos contextos de internação provisória e de cumprimento de medidas socioeducativas. Estabelece o art. 6° da citada resolução: “A guia de execução, provisória ou definitiva, deverá ser expedida pelo juízo do processo de conhecimento”.

– Quarto caso: o compartilhamento de dados de crianças e adolescentes com pretendentes habilitados à adoção. Nessa hipótese o compartilhamento de dados está embasado no cumprimento de obrigação legal, pois tem fundamento no Estatuto da Criança e do Adolescente, Lei n°. 8.069, de 13 de julho de 1990.

6.1 DÚVIDAS FREQUENTES

4) Dados de crianças e adolescentes inseridos em programas/projetos caracterizados como políticas públicas ou não e conveniados entre o PJSC e outras instituições podem ser tratados?

Resposta: Sim, pois há uma finalidade específica e uma base legal adequada (art. 7º, III, da LGPD). De qualquer forma, recomenda-se sempre verificar se: a) a finalidade do programa/projeto é legítima, específica e explícita; b) todos os dados pessoais tratados são realmente necessários; c) o programa/projeto realmente se caracteriza como uma política pública ou pode ser enquadrado em outra base legal.

Se o programa ou o projeto não se caracteriza como política pública, os dados das crianças e adolescentes poderão ser tratados pelos representantes das entidades parceiras e pelos servidores do PJSC, desde que exista uma base legal que ampare o tratamento.

Ainda, se o programa ou projeto não se caracteriza como política pública, mas o tratamento de dados está previsto em cláusula de termo de cooperação entre o PJSC e as entidades cooperantes, aplica-se a base legal do cumprimento de obrigação legal ou regulatória (art. 7º, II, da LGPD).

5) A imagem de crianças e adolescentes pode ser utilizada nos sistemas institucionais?

Resposta: A imagem da pessoa é um dado pessoal sensível, conforme o conceito existente no inciso II do artigo 5º da LGPD, uma vez que é considerado dado biométrico, e, por isso, cuidados especiais deverão ser tomados. Veja que a finalidade e a base legal para o uso das imagens deverão ser analisadas.

A exemplo da ferramenta Busca Ativa, em que a finalidade é definida pelo impulsionamento das políticas de atendimento às crianças e adolescentes afastados do convívio familiar, no que tange às campanhas de estímulo a adoções, conformeprevisto no artigo 87, inciso VII, da Lei nº 8.069/1990 (Estatuto da Criança e do Adolescente), é possível o uso da imagem. Contudo, mesmo havendo possibilidade do tratamento da imagem de crianças e adolescentes no Busca Ativa a referida disponibilização depende de decisão judicial e de manifestação de interesse do(a) adolescente ou da criança, quando estes(as) forem capazes de manifestar sua vontade para autorizar a utilização de dados e imagens na ferramenta.

6.1 DÚVIDAS FREQUENTES

Os(as) pretendentes habilitados(as) deverão se comprometer a preservar a identidade e a imagem das crianças e dos(as) adolescentes, sendo vedado o repasse e a divulgação das informações, sob pena de responsabilidade administrativa, cível e criminal (art. 2°, § 3°, da Portaria n° 114 do CNJ).

A depender do caso e da finalidade pretendida, deve-se verificar a possibilidade de uso de artifícios que não permitam a identificação da criança e do adolescente (como tarjas pretas nos olhos ou imagens borradas).

6) O uso da imagem de criança ou de adolescente, para publicidade de programas e para projetos institucionais requer o consentimento de um dos pais ou responsável legal?

Resposta: É conveniente o consentimento do responsável legal e o uso somente de imagens que não permitam a identificação da criança ou do adolescente. Não sendo possível a identificação, é desnecessário o consentimento pois não incidiria LGPD.

A título de exemplo, o Programa Novos Caminhos, para publicação de notícias no seu site oficial, e em publicidade do Programa, orienta que o dado do jovem seja anonimizado, de forma que não possa ser identificado. Porém, caso seja necessário a identificação, dever-se obter o consentimento do responsável legal.

7) Dados de crianças e adolescentes para fins de adoção podem ser tratados com as entidades internacionais?

Resposta: Sim. Os procedimentos necessários para a apresentação e a formalização de uma adoção internacional, quando envolvem os Organismos de Adoção Internacional devidamente credenciados pela Autoridade Central Administrativa Federal (ACAF), observam os princípios da finalidade, necessidade e legalidade, além de primar pelo princípio do melhor interesse, uma vez que prezam pela convivência familiar de crianças e adolescentes aptos à adoção, que não apresentaram pretendentes habilitados para seu perfil em território nacional. Esses organismos são entidades sem fins lucrativos, que realizam a intermediação dos procedimentos de adoção internacional, no Brasil e no exterior, nos termos da Convenção de Haia de 1993 Relativa à Proteção das Crianças e à Cooperação Internacional em Matéria de Adoção Internacional.

Conheça mais:

Programa Novos Caminhos (https://www.tjsc.jus.br/web/infancia-e-juventude/acoes-e-projetos/novos-caminhos)
Programa Busca Ativa https://cgjweb.tjsc.jus.br/buscaativa
Sistema Nacional de Adoção e Acolhimento https://www.cnj.jus.br/sna

7.0 MITIGAÇÃO DE RISCOS, ARMAZENAMENTO E ELIMINAÇÃO DE DADOS

7.1 Mitigação de riscos no tratamento de dados de crianças e adolescentes

Conforme anteriormente mencionado, um dos objetivos deste guia orientativo é abordar as especificidades que devem ser observadas pelos agentes de tratamento (controlador e operador) nos procedimentos que envolvem dados de crianças e adolescentes, especialmente ao lidar com os sistemas e programas geridos pelo Poder Judiciário catarinense.

Nesse aspecto, dispõe a LGPD, em seu art. 6º, inciso VIII, acerca do princípio da prevenção, o qual determina que as atividades de tratamento de dados pessoais devem adotar medidas para prevenir a ocorrência de danos em virtude da manipulação desses dados.

Essa premissa adquire especial relevância sobretudo pela natureza especialíssimados dados de crianças e adolescentes, o que exige dos agentes de tratamento uma maior cautela no manejo das informações.

Nesse contexto, o tratamento dos dados deve ser realizado (a) no melhor interesse da criança ou adolescente (art. 14, caput), (b) mediante o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal (art. 14, § 1º) e (c) de acordo com a obrigação dos controladores de manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos do titular dos dados pessoais (art. 14, § 2º).

No Poder Judiciário catarinense, consoante já manifestado, a maior parte do tratamento de dados, no âmbito de sua atividade fim, ocorre para o cumprimento de obrigação legal ou regulatória e independe do consentimento do titular ou dos responsáveis legais (arts. 7º, II, e 11, II, “a”, da LGPD), contudo, é imprescindível a implementação de diretrizes que assegurem a efetividade da proteção das informações no transcorrer das suas atividades-fim.

Sabe-se que os dados podem circular por diversas plataformas, especialmente nas varas de família, oficialatos da infância e juventude, conselhos tutelares, instituições de acolhimento, hospitais, clínicas médicas, delegacias de polícia, entre outros atores de proteção, o que requer máxima atenção de controladores e de operadores ao lidar com os dados sensíveis de crianças e adolescentes disponibilizados em sistemas e cadastros variados.

7.0 MITIGAÇÃO DE RISCOS, ARMAZENAMENTO E ELIMINAÇÃO DE DADOS

A manipulação dos dados de maneira inadequada pode levar a circunstâncias de exposição de informações que acarretam riscos às liberdades civis e aos direitos fundamentais dos seus titulares. Saber lidar com os dados de maneira cautelosa, desde sua coleta até o descarte, é uma atitude baseada na prevenção e fundamental para o resguardo de todos.

O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, evidenciando-se (a) o modo pelo qual é realizado; (b) o resultado e os riscos que razoavelmente dele se esperam e (c) as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado (art. 44, LGPD).

Dessa forma, qualquer informação relativa a crianças e adolescentes deve ser categorizada de maneira especial a fim de possibilitar a proteção dos dados sensíveis de acessos não autorizados e de situações acidentais ou ilícitas, em perfeito atendimento ao princípio da segurança, insculpido no art. 6º, inciso VII, da Lei de Proteção.

Nesse sentido, é aconselhável aos controladores e aos operadores a criação de regras de boas práticas e de governança que estabeleçam procedimentos, normas de segurança, ações educativas e treinamentos aos seus membros e colaboradores, e que visem à mitigação de riscos no tratamento de dados pessoais.

O princípio da governança está previsto no art. 46 da LGPD, o qual determina 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.

Evidencia-se que os riscos de se realizar o tratamento de dados pessoais são variados. A título exemplificativo, pode-se citar a ocorrência de dados expostos indevidamente, vazados ou descartados incorretamente. Por essa razão, deve-se sempre considerar a probabilidade de alguma dessas irregularidades acontecerem.

No aspecto, a elaboração de um relatório de impacto à proteção de dados pessoais pode consistir no ponto de partida para a implementação de um projeto de proteção de dados pessoais.

7.0 MITIGAÇÃO DE RISCOS, ARMAZENAMENTO E ELIMINAÇÃO DE DADOS

Referido relatório consiste em documento que contém a descrição dos processos de trabalho em que há o tratamento de dados pessoais de crianças e adolescentes eque podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco (art. 5º. XVII, LGPD).

Além disso, é fundamental que seja feito o adequado controle de acesso dos usuários aos sistemas informatizados onde estão guardados os dados sensíveis de crianças e adolescentes.

Controle de acesso é o procedimento pelo qual uma pessoa é autorizada a acessar determinado sistema com um nível de acesso às informações específico e limitado ao exercício de sua função ou atuação, bem como a possibilidade de que os acessos sejam auditados, caso necessário.

Assim, para que os riscos de vazamento ou tratamento inadequado dos dados de crianças e adolescentes sejam reduzidos ao máximo, é importante que cada unidade organizacional do PJSC possua um servidor responsável por fazer o controle dos usuários que têm acesso aos sistemas específicos, com informações sobre o processo de autorização, vigência, nível e término da permissão de acesso, com a documentação respectiva desses dados, indicando se há possibilidade de auditoria ou não, para cada sistema informatizado, nos termos dos artigos 23 e 24 da Resolução TJ n. 15, de 4 de julho de 2018.

Além disso, caso ocorra algum incidente de segurança da informação, que corresponde ao vazamento (compartilhamento ilegal) ou mau uso dos dados de crianças e adolescentes, o servidor responsável pela guarda dos sistemas informatizados e pelo controle de acesso ou qualquer outra pessoa que tiver notícia do incidente tem o dever funcional de comunicar imediatamente ao Núcleo de Segurança Cibernética e a Equipe de Prevenção, Tratamento e Resposta a Incidentes de Segurança Cibernética no âmbito do Poder Judiciário do Estado de Santa Catarina, órgãos do Comitê de Governança de Segurança da Informação, conforme o previsto na Resolução GP n. 38 de 20 de outubro de 2021.

Aconselha-se que a análise de riscos seja realizada, levando-se em consideração os diversos procedimentos adotados, os fluxos dos dados entre órgãos e entidades, por onde as informações entram, qual o caminho que percorrem e qual o destino delas, independentemente de se encontrarem armazenadas em meio digital ou físico. Orienta-se, ainda, que

7.0 MITIGAÇÃO DE RISCOS, ARMAZENAMENTO E ELIMINAÇÃO DE DADOS

Para que isso ocorra de modo eficiente, faz-se necessário o envolvimento de todos os agentes do órgão que participam do fluxo de tratamento de dados, a fim de possibilitar uma visão ampla das peculiaridades dos procedimentos realizados, bem como permitir a averiguação do ciclo de vida dos dados dos caminhos percorridos, dos meios de armazenamento e das formas de descarte.

Dessa forma, para que a gestão da segurança do sistema de tratamento de dados seja adequadamente realizada, é imperioso proceder ao levantamento dos possíveis riscos que abranjam as atividades realizadas pelo órgão ou entidade, de maneira a viabilizar que as medidas de prevenção sejam satisfatórias às possíveis ameaças.

É indubitável que a adequação à LGPD oportuniza aos agentes não só transmitir segurança aos titulares dos dados acerca do adequado tratamento que suas informações estão recebendo, mas também que o próprio órgão ou entidade não permaneça em um local de vulnerabilidade.

7.2 Armazenamento

Armazenamento é uma das atividades realizadas quando se trata dados pessoais, conforme o conceito de tratamento definido no art. 5º, X, da LGPD.

Em relação ao período de armazenamento dos dados, cumpre destacar que este deve respeitar a finalidade específica da coleta (art. 6º, I, da LGPD) e a autorização elencada em uma das bases legais previstas na legislação protetiva (arts. 7º, 11 e caput do 23 da LGPD).

Além disso, 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 (art. 46, da LGPD).

Ainda, 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 (art. 47, da LGPD).

7.0 MITIGAÇÃO DE RISCOS, ARMAZENAMENTO E ELIMINAÇÃO DE DADOS

Nesse sentido, compilamos pequenas e relevantes práticas a serem aplicadas nas atividades rotineiras nas quais ocorram a manipulação de dados pessoais. Destaca-se que estes cuidados são aplicáveis a todos os níveis de tratamento e aos seus respectivos agentes, bem como para qualquer volume de dados.

Recomendações de boas práticas a serem adotadas:

1. Acesso a computadores mediante senha individualizada – Sugere-se que o acesso a qualquer dispositivo eletrônico ou terminal de computador por servidores/colaboradores ocorra mediante login e senha pessoais, devendo ser vedado o compartilhamento de credenciais entre colegas de trabalho.

2. Restrição de acesso aos departamentos da entidade/órgão – A fim de evitar vazamentos e o uso indevido de dados pessoais, recomenda-se restringir ao máximo o acesso de pessoas externas ou de outros departamentos nos locais em que são tratados maiores volumes de dados pessoais ou dados pessoais sensíveis, a exemplo dos oficialatos da infância e juventude e das salas de guarda de documentos e sistemas de armazenamento de dados.

3. Uso de armários e gavetas – Preferencialmente, aconselha-se a guarda de documentos físicos que contenham dados pessoais em armários e gavetas que possuam chaves, as quais devem permanecer na posse somente de pessoas autorizadas a acessar esses documentos.

4. Utilização de aparelho celular ou outros dispositivos móveis – Objetivando aperfeiçoar a segurança no uso do aparelho celular, para os casos em que seja utilizado para fins institucionais, indica-se o uso de senha individual ou reconhecimento por biometria.

5. Aplicativos de mensagens instantâneas – Em situações de utilização de aplicativos de mensagens instantâneas, a exemplo do Whatsapp, Telegram, Messenger, entre outros, para fins corporativos ou funcionais, instrui-se que seja ativada a verificação em duas etapas para acesso ao aplicativo. Ademais, orienta-se que seja evitado o envio de mensagens que contenham dados pessoais, contudo, caso seja imprescindível para a realização do trabalho, recomenda-se a exclusão das mensagens com os referidos dados após concluída a atividade.

7.0 MITIGAÇÃO DE RISCOS, ARMAZENAMENTO E ELIMINAÇÃO DE DADOS

6. <u>Salvamento de dados pessoais em computador particular</u> – Para prevenir vazamento e acesso indevido a dados pessoais que servidores/colaboradores detenham em razão das atividades desempenhadas, orienta-se evitar o salvamento de arquivos com dados pessoais em computadores particulares. Em caso de estrita necessidade, os dados devem ser mantidos no equipamento somente durante a execução do trabalho, e eliminados em seguida.

7. <u>Utilização de meio de comunicação oficial/institucional</u> – Sempre que possível utilizar exclusivamente a ferramenta institucional de comunicação digital – Microsoft Teams – para trocas de mensagens, realização de reuniões e chamadas de vídeo, bem como para compartilhamento e armazenamento de informações e documentos digitais.

8. <u>Segurança cibernética</u> – Deve-se atentar para os requisitos mínimos de segurança cibernética na utilização de computadores, notebooks, tablets, celulares, relógios inteligentes ou qualquer outro dispositivo eletrônico utilizado em serviço, sejam eles pertencentes à instituição ou ao servidor/colaborador. Esses requisitos envolvem a instalação de programas antivírus, bloqueio de e-mails que contenham spam ou links suspeitos, phishing, bloqueio de anúncios em navegadores de internet, firewall, configuração VPN para acesso remoto, entre outros. Orienta-se os usuários, ainda, a não acessarem links suspeitos ou sites com violação de segurança. Para melhor orientação nesse aspecto, pode-se recorrer ao setor responsável pelo suporte à informática no órgão.

No tocante ao compartilhamento, podem ser citadas outras medidas para que o procedimento seja realizado de forma segura, tais como:

1. Evitar o compartilhamento de dados por telefone ou por meios que impossibilitem o controle e o comprometimento da parte que receberá os dados em seguir boas práticas de proteção de dados.

2. Se possível, antes do compartilhamento de dados, averiguar o nível de conhecimento do receptor acerca das boas práticas em termos de LGPD;

3. No caso de trâmite de dados pessoais por e-mail, orienta-se a eliminação periódica das mensagens.

7.0 MITIGAÇÃO DE RISCOS, ARMAZENAMENTO E ELIMINAÇÃO DE DADOS

4. Igualmente, sempre que for possível, formalizar regras de boas práticas em proteção de dados de forma documental e por intermédio de mecanismo que possibilite comprovar a leitura e aceite do receptor, anteriormente ao compartilhamento de informações.

5. Evitar o compartilhamento de informações pessoais em grupos de aplicativos de mensagens instantâneas ao qual vários destinatários têm acesso.

É imperioso consignar que essas cautelas não esgotam os procedimentos e as adequações elencadas na LGPD, no entanto, figuram como boas práticas que demonstram a boa-fé dos agentes de tratamento em zelar pela segurança das informações, minimizando o risco de uso indevido de dados pessoais que estão em posse do controlador.

7.3 Eliminação

Desde a vigência da Lei Geral de Proteção de Dados as empresas e as instituições que manipulam dados pessoais em cadastros ou sistemas estão sujeitas a gerenciar essas informações com segurança e privacidade, desde a obtenção até o descarte desse material, seja em ambiente físico ou virtual.

A etapa do descarte deve ser cuidadosamente observada pelos agentes de tratamento, porquanto pode o material tratado conter informações muitas vezes confidenciais, o que configura verdadeiro portfólio ou dossiê, o qual, aliás, pode guardar valor econômico.

O término do tratamento dos dados é o evento que pode coincidir com a fase do descarte das informações utilizadas. A LGPD estabelece em seu art. 15 as hipóteses de encerramento do tratamento de dados pessoais.

Em regra, os dados pessoais são coletados para que atendam a uma finalidade específica e podem, por exemplo, vir a ser eliminados a partir da verificação de que a finalidade foi alcançada (art. 15, I), ao término de seu tratamento (art. 15, II), a pedido do titular desses dados (art. 15, III), assim como ao cumprimento de uma sanção que havia sido aplicada pela Autoridade Nacional de Proteção de Dados (art. 15, IV).

Ademais, o art. 16 da Norma de Proteção prevê que os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites

7.0 MITIGAÇÃO DE RISCOS, ARMAZENAMENTO E ELIMINAÇÃO DE DADOS

técnicos das atividades, autorizada a conservação das informações para o (I) cumprimento de obrigação legal ou regulatória pelo controlador; (II) estudo por órgão de pesquisa; (III) transferência a terceiro; ou (IV) uso exclusivo do controlador.

Dessa forma, ao atingir seu propósito, os dados devem ser excluídos da base ou dos dispositivos de armazenamento. Contudo, enquanto não alcançado o seu objetivo, a operação de tratamento de dados não estará finalizada (encerrada), de modo que permanece a necessidade do armazenamento seguro das informações (arts. 6º, VII,e 46, LGDP).

Independentemente do formato no qual a informação circula – físico ou digital – o descarte deve ser realizado de maneira segura a fim de se evitar o vazamento de qualquer informação, quer seja um dado sensível ou não, cabendo aos agentes de tratamento fazê-lo apropriadamente.

Entende-se por descarte de forma segura e apropriada aquele que não permiti a reconstrução dos dados após a sua exclusão. Em outras palavras, deve-se atentar para que não seja possível tornar os dados acessíveis e legíveis após o seu descarte, o que poderia colocar em risco o sigilo das informações, tornando-as sujeitas a fraudes e violações.

Algumas simples ações podem ser implementadas de maneira a tornar as informações descartadas ilegíveis e inaproveitáveis, a exemplo de picotar documentos impressos antes de colocá-los na lixeira (pode-se usar fragmentadora), excluir informações contidas na “nuvem”, deletar registros fotográficos, bem como formatar o disco rígido do computador (HD) para garantir que os dados não sejam mais acessados. Contudo, é recomendável que o órgão/entidade crie políticas internas claras e desenvolva uma metodologia própria para a eliminação de dados pessoais.

Conquanto a Lei de Proteção não disponha de regulamentação específica para o descarte ou eliminação de dados pessoais, é incontroverso que o tratamento indevido deste material pode acarretar prejuízo ao titular dos dados, capaz de gerar direitos de reparação a qualquer indivíduo que comprove a lesão provocada essencialmente pelo descarte irregular de informações de cunho particular e restrito.

8.0 CONSIDERAÇÕES FINAIS

Este guia orientativo é resultado do empenho conjunto do grupo de trabalho, formado por membros do Poder Judiciário de Santa Catarina (PJSC), e construído com o intuito de ser utilizado como ferramenta norteadora para aplicação da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) no âmbito da infância e juventude.

Desde o início de sua elaboração, o documento foi pensado de modo a ter uma estrutura dinâmica e está sujeito a atualizações, incluindo entendimentos que venham a se consolidar em razão de futuras interpretações acerca do tratamento de dados de crianças e adolescentes à luz da LGPD.

Em derradeira observação, esclarece-se que dúvidas e sugestões sobre as disposições previstas neste guia orientativo poderão ser encaminhadas por meio de mensagem eletrônica para o endereço do Comitê Gestor de Proteção de Dados Pessoais (CGPDP): cgpdp@tjsc.jus.br

REFERÊNCIAS

Autoridade Central Federal: para adoção e subtração internacional de menores. **Ministério da Justiça e Segurança Pública**. 2017. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-protecao/cooperacao-internacional/acaf/autoridade-central-federal. Acesso em: 15 set. 2022.

ANPD. **Hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes**. Setembro/2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/estudo-preliminar-tratamento-de-dados-crianca-e-adolescente.pdf. Acesso em 10 out.2022.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente. Brasília, DF: Congresso Nacional; 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 21 set. 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm.Acesso em: 26 set. 2022.

CALDAS, RICARDO WAHRENDORFF (Coord.). **Políticas Públicas: conceitos e práticas**. Belo Horizonte: Sebrae/MG, 2008. E-book. Disponível em: http://www.mp.ce.gov.br/nespeciais/promulher/manuais/MANUAL%20DE%20POLITICAS%20P%C3%9ABLICAS.pdf. Acesso em 31 out. 2022.

FGV. Guia de proteção de dados pessoais: crianças e adolescentes. Outubro/2020. Disponível em: https://portal.fgv.br/sites/portal.fgv.br/files/u12834/guia_criancas_e_adolescentes.pdf. Acesso em 10 out. 2022.

INSTITUTO ALANA. **CRIANÇA E CONSUMO**. O melhor interesse de crianças e adolescentes e as bases legais aplicáveis ao tratamento de seus dados pessoais. Novembro/2022. Disponível em: https://criancaeconsumo.org.br/wp-content/uploads/2022/11/alana-anpd-2-acess.pdf. Acesso em 11 nov. 2022.

LATERÇA, Priscilla Silva; FERNANDES, Elora; TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio (Coords.). **Privacidade e Proteção de Dados de Crianças e Adolescentes**. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; Obliq, 2021. E-book

PROJETO GRÁFICO: Núcleo de Comunicação Institucional - NCI/TJSC

PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA
de Santa Catarina