NORMA

SELO LGPD

PROTEÇÃO DE DADOS PESSOAIS

INSTITUTO TOTUM

SUMÁRIO

1. OBJETIVO

1.1. Esta norma especifica requisitos para a Concessão de Selo LGPD para as organizações interessadas em demonstrar a conformidade com a Lei Geral de Proteção de Dados.

2. REFERÊNCIAS

2.1. A Norma foi subsidiada pela Lei Nº 13.709 de 14 de agosto de 2019 - Lei Geral de Proteção de Dados Pessoais (LGDP) e sua nova redação dada pela Lei Nº 13.853 de 2019 considerando-se, inclusive, os demais referenciais legais por ela citados.

3. FUNDAMENTOS

Artigo 2º - Capítulo I
3.1. Os fundamentos que disciplinam a Proteção de Dados Pessoais são: a) a autodeterminação informativa; b) a liberdade de expressão, de informação, de comunicação e de opinião; c) a inviolabilidade da intimidade, da honra e da imagem; d) o desenvolvimento econômico, tecnológico e a inovação; e) a livre iniciativa, a livre concorrência e a defesa do consumidor; e f) os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.
Breve explicação (Instituto Totum): ✓ *Os fundamentos acima citados serão verificados durante as auditorias presenciais com a evidenciação de que as atividades de tratamento de dados pessoais da organização não os transgridam em sua prática.*

4. APLICAÇÃO

Artigo 3º - Capítulo I

4.1. A presente norma é aplicada à pessoa natural ou pessoa jurídica de direito público ou privado que realizem quaisquer atividades de tratamento de dados pessoais independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

a) a operação de tratamento seja realizada no território nacional (exceto no caso do requisito 4.2. d);
b) a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados se refira a indivíduos localizados no território nacional; ou
c) os dados tenham sido coletados em território nacional (quando o titular nele se encontre na ocasião da coleta).

Artigo 4º - Capítulo I

4.2. A presente Norma não é aplicável para o tratamento de dados pessoais nos seguintes casos:

a) para pessoas naturais que utilizem os dados pessoais para fins exclusivamente particulares e não econômicos;
b) realizado para fins exclusivamente:
i. jornalístico e artísticos;
ii. acadêmicos (considerar 7.1.1 e 7.2.1.)
c) realizado para fins exclusivos de:
i. segurança pública;
ii. defesa nacional;
iii. segurança do Estado;
iv. atividades de investigação e repressão de infrações penais; ou
d) quando os dados forem provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na Lei Geral de Proteção de Dados.

4.2.1. O tratamento de dados pessoais previsto na alínea c) será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos em Lei.

4.2.2. É vedado o tratamento dos dados a que se refere a alínea c) por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta em 4.2.4.

4.2.3. A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas na alínea c) e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.

4.2.4. Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata a alínea c) poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público.

Breve explicação (Instituto Totum):
Os requisitos do Capítulo 4 desta norma (Aplicação) serão observados em complemento à manifestação de interesse para ratificação do escopo em processo de certificação durante a auditoria presencial.

5. TERMOS E DEFINIÇÕES

Artigo 5º - Capítulo I

5.1. Para os efeitos desta norma aplicam-se os termos e definições abaixo relacionados:

a) **agentes de tratamento:** o controlador e o operador;
b) **anonimização:** utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
c) **autoridade nacional:** órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional;
d) **banco de dados:** conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
e) **bloqueio:** suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;
f) **consentimento**: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
g) **controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
h) **dado anonimizado**: dado relativo à titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
i) **dado pessoal:** informação relacionada a pessoa natural identificada ou identificável;
j) **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;

k) **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);

l) **órgão de pesquisa:** 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;

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

n) **relatório de impacto à proteção de dados pessoais**: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

o) **tratamento:** toda operação realizada com dados pessoais, como as que se referem a:

I. **acesso**: possibilidade de comunicar-se com um dispositivo, meio de armazenamento, unidade de rede memória, registro, arquivo etc., visando receber, fornecer ou eliminar dados;
II. **armazenamento:** ação ou resultado de manter ou conservar em repositório um dado;
III. **arquivamento:** ato ou efeito de manter registrado um dado, embora já tenha perdido a validade ou esgotada a sua vigência;
IV. **avaliação**: ato ou efeito de calcular valor sobre um ou mais dados;
V. **classificação:** maneira de ordenar os dados conforme algum critério estabelecido;
VI. **coleta**: recolhimento de dados com finalidade específica;
VII. **comunicação:** transmitir informações pertinentes a políticas de ação sobre os dados;
VIII. **controle*:*** ação ou poder de regular, determinar ou monitorar as ações sobre o dado;
IX. **difusão**: ato ou efeito de divulgação, propagação, multiplicação dos dados;
X. **distribuição:** ato ou efeito de dispor de dados de acordo com algum critério estabelecido;
XI. **eliminação**: ato ou efeito de excluir ou destruir dado do repositório;
XII. **extração**: ato de copiar ou retirar dados do repositório em que se encontrava;
XIII. **modificação**: ato ou efeito de alteração do dado;
XIV. **processamento:** ato ou efeito de processar dados;
XV. **produção*:*** criação de bens e de serviços a partir do tratamento de dados;
XVI. **recepção*:*** ato de receber os dados ao final da transmissão;
XVII. **reprodução*:*** cópia de dado preexistente obtido por meio de qualquer processo;

XVIII. **transferência**: mudança de dados de uma área de armazenamento para outra, ou para terceiro;

XIX. **transferência internacional de dados:** transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

XX. **transmissão:** movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos etc; e

XXI. **utilização:** ato ou efeito do aproveitamento dos dados.

p) **titular:** pessoa natural a quem se refere os dados pessoais que são objeto de tratamento; e

q) **uso compartilhado de dados:** comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

Breve explicação (Instituto Totum):

Os termos e definições acima especificados servem para harmonização dos conceitos durante o processo de auditoria sempre que necessário.

No anexo I da presente norma outros termos e definições estão dispostos para fins de alinhamentos conceituais.

6. PRINCÍPIOS

Artigo 6º - Capítulo I

6.1. As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

a) **finalidade:** realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

b) **adequação:** compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

c) **necessidade:** 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;

d) **livre acesso:** 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;

e) **qualidade dos dados:** 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;

f) **transparência:** 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;

g) **segurança:** 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;

h) **prevenção:** adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

i) **não discriminação:** impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; e

j) **responsabilização e prestação de contas:** 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.

Para fins desta Norma é considerada <u>boa prática:</u>

BP 1. Definição de uma política com a forma de atendimento aos princípios das atividades de tratamento de dados pessoais, demonstrando o engajamento da Alta Direção da organização que pleiteia a certificação, sendo:

a. documentada;
b. comunicada na organização;
c. aplicada pela organização;
d. comunicada aos operadores de tratamento dos dados, quando for o caso;
e. aplicada pelos operadores de tratamento dos dados, quando for o caso;
f. publicada e
g. atualizada periodicamente.

Breve explicação (Instituto Totum):
Os princípios de tratamento de proteção de dados pessoais serão verificados com relação a sua aplicação, nas auditorias presenciais, em todas as formas de tratamento realizadas durante o ciclo dos dados e informações sob a responsabilidade da organização, podendo incluir, quando for o caso, do operador.

7. TRATAMENTO DE DADOS PESSOAIS

7.1. REQUISITOS PARA O TRATAMENTO DE DADOS PESSOAIS

Artigo 7º - Seção I – Capítulo II

7.1.1. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

a) mediante o fornecimento de consentimento pelo titular;
b) para o cumprimento de obrigação legal ou regulatória pelo controlador;
c) para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
d) quando necessário para a execução de contrato ou de procedimentos preliminares relacionados ao contrato do qual seja parte o titular, a pedido do titular dos dados;
e) para o exercício regular de direitos em processo judicial, administrativo ou arbitral,
f) para a proteção da vida ou da incolumidade física do titular ou de terceiros;
g) para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
h) quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
i) para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

7.1.1.1. O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

7.1.1.2. É dispensada a exigência do consentimento previsto em 7.1.1 a) para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos em 6.1.

7.1.1.3. O controlador que obteve o consentimento referido em 7.1.1 a) que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para este fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta norma, em especial àquelas citadas em 7.1.1. de b) a i).

7.1.1.4. A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta norma, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

7.1.1.5. O tratamento posterior dos dados pessoais a que se referem os requisitos 7.1.1.1. e 7.1.1.2. poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos

e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos em 3.1. e 6.1.

Artigo 8º - Seção I – Capítulo II

7.1.2. O consentimento previsto em 7.1.1.a) deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

7.1.2.1. Caso o consentimento seja fornecido por escrito, esse deverá constar em cláusula destacada das demais cláusulas contratuais.

7.1.2.2. Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade.

7.1.2.3. É vedado o tratamento de dados pessoais mediante vício de consentimento.

7.1.2.4. O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.

7.1.2.5. 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.

7.1.2.6. Em caso de alteração de informação referida em 7.1.3 a), b), c) ou e), o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.

Artigo 9º - Seção I – Capítulo II

7.1.3. O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

a) finalidade específica do tratamento;
b) forma e duração do tratamento, observados os segredos comercial e industrial;
c) identificação do controlador;
d) informações de contato do controlador;
e) informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
f) responsabilidades dos agentes que realizarão o tratamento; e
g) direitos do titular, com menção explícita aos direitos contidos em 8.2.

7.1.3.1. Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

7.1.3.2. Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.

7.1.3.3. Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados em 8.2.

Artigo 10º - Seção I – Capítulo II

7.1.4. 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:

a) apoio e promoção de atividades do controlador; e

b) 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.

7.1.4.1. Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

7.1.4.2. O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

Para fins desta Norma é considerada boa prática:

BP 2. Elaboração de mapeamento ou similar documentado de cada área da organização publicado e atualizado periodicamente, considerando:

a. tipos de dados pessoais existentes;

b. classificação dos dados (pessoais, anonimizados, pseudonimizados, sensíveis e de crianças e adolescentes).

c. para cada tipo de dado pessoal informações de quem são os operadores e controladores;

d. atividade de tratamento realizada, considerando 5.1 o) incisos de I a XXI; e

e. hipóteses que tornam legítimo o tratamento.

Breve explicação (Instituto Totum):
Mediante a identificação de tratamento de dados pessoais será verificado:

- ✓ *o respaldo normativo para a ação conforme as 10 hipóteses especificadas em 7.1.1.*
- ✓ *nos casos em que a organização adotou o consentimento como hipótese de tratamento de dados pessoais serão verificadas as evidências que demonstrem a conformidade com os requisitos expostos em 7.1.2., bem como em 7.1.3.1 e 7.1.3.2.*
- ✓ *nos casos em que a organização adotou o legítimo interesse como forma de permissão de tratamento de dados pessoais, serão verificadas evidências que demonstrem a conformidade com os requisitos expostos em 7.1.4, bem como 7.1.3.3.*
- ✓ *capacidade e preparo para atendimento ao direito do titular dos dados pessoais de acesso facilitado, conforme 7.1.3.*
- ✓ *demais evidências de conformidade aos requisitos do capítulo 7.1., conforme aplicável.*

7.2. TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

Artigo 11º - Seção II – Capítulo II

7.2.1. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

a) quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

b) sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

i. cumprimento de obrigação legal ou regulatória pelo controlador;
ii. tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
iii. realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
iv. exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;
v. proteção da vida ou da incolumidade física do titular ou de terceiros;
vi. tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
vii. garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados em 7.1.3 e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

7.2.1.1. O requisito 7.2.1 se aplica a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.

7.2.1.2. A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.

7.2.1.3. É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado 7.2.1.4., incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir:

a) a portabilidade de dados quando solicitada pelo titular; ou
b) as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este requisito.

7.2.1.4. É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários.

Artigo 12º - Seção II – Capítulo II

7.2.2. Os dados anonimizados não serão considerados dados pessoais, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

7.2.2.1. A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis e a utilização exclusiva de meios próprios.

7.2.2.2. Poderão ser igualmente considerados como dados pessoais, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

Artigo 13º - Seção II – Capítulo II

7.2.3. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro,

conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

7.2.3.1. A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa em nenhuma hipótese poderá revelar dados pessoais.

7.2.3.2. O órgão de pesquisa será o responsável pela segurança da informação prevista, não permitida, em circunstância alguma, a transferência dos dados a terceiro.

7.2.3.3. O acesso aos dados será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.

7.2.3.4. A pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

Breve explicação (Instituto Totum):
Mediante a identificação de tratamento de dados pessoais sensíveis será verificado:

- ✓ *o respaldo normativo para a ação conforme as hipóteses especificadas em 7.2.1.*
- ✓ *evidências de conformidade aos demais requisitos expressos em 7.2.1.*
- ✓ *em todos os casos em que a organização adotar a anonimização de dados pessoais sensíveis, não os considerando como dados pessoais, serão verificados os processos e a adequação aos requisitos expressos em 7.2.2.*
- ✓ *em todas as organizações será verificado durante a auditoria presencial qualquer forma de utilização de dados ou informações advindos de estudos em saúde pública.*
- ✓ *nas organizações que realizam estudos em saúde pública serão verificadas evidências de conformidade com os requisitos expressos em 7.2.3.*

7.3. TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES

Artigo 14º - Seção III – Capítulo II

7.3.1. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, com base, inclusive, na legislação pertinente.

7.3.1.1. O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por, pelo menos, um dos pais ou pelo responsável legal.

7.3.1.2. Os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos mencionados em 8.2.

7.3.1.3. Poderão ser coletados dados pessoais de crianças sem o consentimento citado em 7.3.1.1. quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento citado em 7.3.1.1.

7.3.1.4. Os controladores não deverão condicionar a participação dos titulares (crianças e adolescentes) em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.

7.3.1.5. O controlador deve realizar todos os esforços razoáveis para verificar que o citado em 7.3.1.1. foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.

7.3.1.6. As informações sobre o tratamento de dados deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

Breve explicação (Instituto Totum):
Mediante a identificação de tratamento de dado pessoal de criança ou adolescente serão verificadas as evidências de conformidade com os requisitos expressos em 7.3.1.

7.4. TÉRMINO DO TRATAMENTO DE DADOS

Artigo 15º - Seção IV – Capítulo II

7.4.1. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

a) verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
b) fim do período de tratamento;

c) comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme 7.1.2.5. resguardado o interesse público; ou

d) determinação da autoridade nacional, quando houver violação ao disposto na Lei Geral de Proteção de Dados Pessoais.

Artigo 16º - Seção IV – Capítulo II

7.4.2. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

c) transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos no capítulo 7 desta norma;

d) uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Para fins desta Norma é considerada boa prática:

BP 3. Elaboração de tabela de temporalidade documentada, publicada e atualizada periodicamente com base em processo de avaliação sistemática de impactos e riscos à privacidade e que disponha sobre tempo de guarda, local e autorização de acesso e destinação final de:

a. dados pessoais tratados ou sob o controle da organização;

b. evidências de conformidade com os requisitos desta norma, da organização e qualquer outra regulamentação pertinente; e

c. operações de tratamento de dados pessoais.

Breve explicação (Instituto Totum):

Para cada tipo de dados pessoais identificado serão verificados:

✓ *Se o tratamento dos dados fora finalizado conforme 7.4.1 e demais referências que legitimou o tratamento (7.1.1)*

✓ *Se os dados foram eliminados após o término do tratamento, salvo condições específicas expressas em 7.4.2.*

8. DIREITOS DO TITULAR

Artigo 17º - Capítulo III

8.1. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade.

Artigo 18º - Capítulo III

8.2. 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:

a) confirmação da existência de tratamento;
b) acesso aos dados;
c) correção de dados incompletos, inexatos ou desatualizados;
d) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a Lei Geral de Proteção de Dados Pessoais;
e) portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial
f) eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas em 7.4.2.
g) informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
h) informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
i) revogação do consentimento, conforme 7.1.2.5.

8.2.1. O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto na Lei Geral de Proteção de Dados Pessoais;

8.2.2. Os direitos previstos serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.

8.2.3. Em caso de impossibilidade de adoção imediata da providência de que trata 8.2.2., o controlador enviará ao titular resposta em que poderá:

a) comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou
b) indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

8.2.4. O requerimento referido em 8.2.2. será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.

8.2.5. O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional.

8.2.6. A portabilidade dos dados pessoais a que se refere 8.2. e) não inclui dados que já tenham sido anonimizados pelo controlador.

8.2.7. O direito a que se refere 8.2.1. também poderá ser exercido perante os organismos de defesa do consumidor.

Artigo 19º - Capítulo III

8.3. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:

a) em formato simplificado, imediatamente; ou
b) por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.

8.3.1. Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.

8.3.2. As informações e os dados poderão ser fornecidos, a critério do titular:

a) por meio eletrônico, seguro e idôneo para esse fim; ou
b) sob forma impressa.

8.3.3. Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.

8.3.4. A autoridade nacional poderá dispor de forma diferenciada acerca dos prazos previstos em 8.3. a) e b) para os setores específicos.

Artigo 20º - Capítulo III

8.4. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

8.4.1. O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

8.4.2. Em caso de não oferecimento de informações citadas em 8.4.1. baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

Artigo 21º - Capítulo III

8.5. Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.

Para fins desta Norma é considerada boa prática

BP 4. Elaboração de documentos que determinem responsabilidades e descrevam os procedimentos a serem adotados para atendimento aos direitos dos titulares de dados pessoais sob o controle da organização a partir de requerimento, incluindo os prazos pertinentes.

Breve explicação (Instituto Totum):

✓ *Será verificado nas auditorias a capacidade da organização em atender aos direitos dos titulares em conformidade com os requisitos expressos no capítulo 8.*

9. TRANSFERÊNCIA INTERNACIONAL DE DADOS

Artigo 33º e 36º - Capítulo V

9.1. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:

a) para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto na Lei Geral de Proteção de Dados Pessoais;
b) quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na Lei Geral de Proteção de Dados Pessoais, na forma de:

i. cláusulas contratuais específicas para determinada transferência;
ii. cláusulas-padrão contratuais;
iii. normas corporativas globais;
iv. selos, certificados e códigos de conduta regularmente emitidos;

c) quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;
d) quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiros;
e) quando a autoridade nacional autorizar a transferência;
f) quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;
g) quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade conforme regras de tratamento de dados pessoais pelo poder público;
h) quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou
i) quando necessário para atender as hipóteses previstas em 7.1.1 b), e) e f).

9.1.1. Para os fins de atendimento de 9.1.a), os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, 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, no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.

9.1.2. As alterações nas garantias apresentadas como suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas em 9.1.b) deverão ser comunicadas à autoridade nacional.

Breve explicação (Instituto Totum):

✓ *No caso de a organização realizar transferência internacional de dados pessoais, serão verificadas as evidências de conformidade em relação aos requisitos expressos no capítulo 9.*

10. AGENTES DE TRATAMENTO DE DADOS PESSOAIS

10.1. CONTROLADOR E OPERADOR

Artigo 37º - Seção I – Capítulo VI

10.1.1. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

Artigo 38º - Seção I – Capítulo VI

10.1.2. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

10.1.2.1. O relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Para fins desta Norma é considerada boa prática:

BP 5. Elaboração de Relatório de Impacto à Proteção de Dados Pessoais que demonstre o engajamento da Alta Direção da organização, em periodicidade determinada e que considere, entre outros fatores:

a. tipos de dados pessoais coletados ou tratados;
b. metodologia de coleta dos dados, quando aplicável;
c. práticas adotadas para segurança das informações;
d. análise de riscos das operações de tratamento de dados pessoais;
e. ações de mitigação dos riscos identificados;

f. reclamações;

g. atendimento de reclamações;

h. atendimento aos requerimentos; e

i. ocorrência de incidentes de segurança, suas consequências e medidas de reversão.

Breve explicação (Instituto Totum):

✓ Os registros das operações de tratamento de dados pessoais serão verificados durante toda a auditoria como forma de evidenciar a conformidade com os requisitos desta norma.

✓ Será verificada a capacidade da organização, quando em situação de controladora de dados pessoais, em consolidar o relatório de impacto à proteção de dados pessoais, conforme 10.1.2.1

Artigo 39º - Seção I – Capítulo VI

10.1.3. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

Para fins desta Norma é considerada boa prática

BP 6. Formalização de um processo de auditoria com periodicidade determinada que assegure o cumprimento das orientações sobre o tratamento de dados pessoais pelos operadores e funcionários da organização.

Breve explicação (Instituto Totum):

✓ *Será verificado nas auditorias a suficiência dos mecanismos de garantia dos controladores acerca do cumprimento de suas instruções e atendimento à Lei Geral de Proteção de Dados Pessoais de seus operadores, quando a organização que pleiteia o selo estiver no papel de controlador de dados pessoais.*

✓ *Será verificado nas auditorias a suficiência dos controles de garantia dos operadores acerca do cumprimento das instruções de seus controladores acerca do tratamento de dados, quando a organização que pleiteia o selo estiver no papel de operador.*

10.2. ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS

Artigo 41º - Seção II – Capítulo VI

10.2.1. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

10.2.1.1. A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

10.2.1.2. As atividades do encarregado consistem em:

a) aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
b) receber comunicações da autoridade nacional e adotar providências;
c) orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
d) executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Para fins desta Norma é considerada <u>boa prática:</u>
BP 7. Elaboração de plano de treinamento e conscientização sobre as práticas de proteção de dados pessoais adotadas pela organização, publicado e atualizado periodicamente com evidenciação da realização, considerando:

a. funcionários;
b. terceiros;
c. fornecedores; e
d. operadores.

Breve explicação (Instituto Totum):
✓ *As informações acerca do encarregado designado para tratamento de dados <u>pessoais, quando a organização estiver em situação de controladora de dados pessoais,</u> será verificada na 1ª fase da auditoria.*
✓ *Demais responsabilidades do encarregado designado serão verificadas durante a auditoria.*

11. SEGURANÇA E SIGILO DOS DADOS

Artigo 46º - Seção I – Capítulo VII

11.1. 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.

11.1.1. As medidas citadas em <u>11.1.</u> deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Artigo 47º - Seção I – Capítulo VII

11.2. 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 Lei Geral de Proteção de Dados Pessoais em relação aos dados pessoais, mesmo após o seu término.

Para fins desta Norma é considerada <u>boa prática:</u>

BP 8. Adoção da metodologia *Privacy by Design* para o desenvolvimento de serviços e produtos.

BP 9. Adoção da metodologia *Privacy by Default* para o lançamento de serviços e produtos.

Breve explicação (Instituto Totum):

✓ *Serão verificadas as medidas de segurança técnicas e administrativas da organização para proteção de dados pessoais, desde a concepção do produto ou serviço até o término do tratamento de dados, considerando todas as partes envolvidas e as evidências de eficácia das medidas.*

Artigo 48º - Seção I – Capítulo VII

11.3. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

11.3.1. A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

a) a descrição da natureza dos dados pessoais afetados;
b) as informações sobre os titulares envolvidos;
c) a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
d) os riscos relacionados ao incidente;
e) os motivos da demora, no caso de a comunicação não ter sido imediata; e
f) as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

11.3.2. A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:

a) ampla divulgação do fato em meios de comunicação; e
b) medidas para reverter ou mitigar os efeitos do incidente.

11.3.3. No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

Artigo 49º - Seção I – Capítulo VII

11.4. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na Lei Geral de Proteção de Dados Pessoais e às demais normas regulamentares.

Para fins desta Norma é considerada <u>boa prática:</u>

BP 10. Estruturação de um Programa de Governança em Privacidade, observados a estrutura, a escala e o volume das operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, que demonstre o comprometimento da organização em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais e:

a. considere o conjunto de dados pessoais sob seu controle ou tratados;
b. tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
c. esteja integrado a sua estrutura geral de governança, estabeleça e aplique mecanismos de supervisão internos e externos;
d. conte com planos de resposta a incidentes e remediação;
e. seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas; e
f. possua indicadores capazes de demonstrar a efetividade do programa em especial, em relação a segurança dos dados pessoais e prevenção de ocorrência de incidentes e danos aos titulares de dados pessoais.

Breve explicação (Instituto Totum):

✓ *Será verificado na auditoria a capacidade da organização para reversão de efeitos de incidentes de segurança bem como sua prontidão para as comunicações expressas nos requisitos 11.3.*

✓ *A adequação dos sistemas utilizados na organização para tratamento de dados pessoais com relação ao requisito expresso em 11.4 será verificada durante a auditoria.*

12. MARCO CIVIL DA INTERNET

Artigo 60º – Capítulo X
Artigo 7º - Capítulo II – Lei nº 12.965 (Marco Civil da Internet)
12.1. O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: **a)** inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; **b)** inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; **c)** inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; **d)** informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade; **e)** não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; **f)** informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: **i.** justifiquem sua coleta; **ii.** não sejam vedadas pela legislação; e **iii.** estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; **g)** consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; **h)** exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais;

Artigo 60º – Capítulo X
Artigo 16º - Subseção III – Seção II - Capítulo III– Lei nº 12.965 (Marco Civil da Internet)
12.2. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda: a) dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto em 12.1.; ou

b) de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular, exceto nas hipóteses previstas na Lei que dispõe sobre a proteção de dados pessoais.

Breve explicação (Instituto Totum):
Será verificado nas auditorias a capacidade de a organização assegurar os direitos dos usuários expressos em 12.1., bem como as questões relativas a guarda de dados pessoais de titulares conforme requisitos expressos em 12.2

ANEXO I –TERMOS E DEFINIÇÕES

a) **auditoria:** processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se elas estão de acordo com as disposições planejadas e estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas (em conformidade) à consecução dos objetivos;

b) **biometria:** verificação da identidade de um indivíduo por meio de uma característica física ou comportamental única, através de meios automatizados;

c) **DPO (Data Protection Officer):** profissional responsável por aconselhar e verificar os dados pessoais de terceiros, obedecendo a Lei Geral de Proteção de Dados (LGPD);

d) **gestão de riscos:** processo de natureza permanente, estabelecido, direcionado e monitorado, que contempla as atividades de identificar, avaliar, e gerenciar potenciais eventos que possam afetar a organização ou pessoas naturais, destinado a fornecer segurança razoável quanto à realização de seus objetivos;

e) **incidente:** evento, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação ou dado protegido, remoção ou limitação de uso da informação ou dado protegido ou ainda a apropriação, disseminação e publicação indevida de informação ou dado protegido de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

f) **informação pessoal:** informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem;

g) **interoperabilidade:** característica que se refere à capacidade de diversos sistemas e organizações trabalharem em conjunto (interoperar) de modo a garantir que pessoas, organizações e sistemas computacionais interajam para trocar informações de maneira eficaz e eficiente;

h) **medidas de segurança:** medidas destinadas a garantir sigilo, inviolabilidade, integridade, autenticidade e disponibilidade da informação classificada em qualquer grau de sigilo;

i) **prevenção de perda de dados:** também conhecida como DLP (*Data Loss Prevention*), é a prática de detectar e prevenir vazamentos de dados, exfiltração de dados ou a destruição de dados sensíveis de uma organização. O termo DLP se refere tanto a ações contra a perda de dados (evento no qual os dados são definitivamente perdidos pela organização) como ações contra vazamentos de dados (transferência indevida de dados para fora da fronteira da organização);

j) ***Privacy by Design (PdB):*** significa que todas as etapas do processo de desenvolvimento de um produto ou serviço de uma organização devem ter a privacidade em primeiro lugar, ou seja, o conceito de privacidade deve estar totalmente embutido no projeto e não se aplica a iniciativas onde a privacidade é discutida somente na fase final.

k) ***Privacy by Default (privacidade por padrão)****:* significa que um produto ou serviço, ao ser lançado no mercado, deve vir com as configurações de privacidade no modo mais restrito por padrão, e o usuário deve liberar acesso à coleta de mais informações, caso julgue necessário.

l) **vício de consentimento:**

i. erro: é compreendido como declaração de vontade em desacordo com a realidade, uma vez que o declarante tem uma percepção falsa, errônea ou inexata da realidade.

ii. dolo: incide no ato comissivo ou omissivo de alguém que maliciosamente leva outrem a fazer negócio que lhe é prejudicial ou o emprego de um artifício para induzir alguém à prática de um ato que o prejudica.

iii. coação: traz a ideia de ameaça ou de pressão física ou moral exercida sobre a pessoa, os bens ou a honra de um contratante para obrigá-lo ou induzi-lo a efetivar um negócio.

HISTÓRICO DE ALTERAÇÕES

Nº da Revisão	Data de Alteração	Sumário das Alterações
00	23/01/2020	Emissão Inicial do Documento
01	06/04/2020	Análise em função da Auditoria do TOTUM