

IV – suporte técnico realizado no exterior;

V – contratação de suboperador estrangeiro.

§2º. A transferência deverá ser registrada no ROPA e indicar:

I – o país ou organismo internacional de destino;

II – o exportador e o importador dos dados;

III – as finalidades;

IV – as categorias de dados e titulares;

V – o mecanismo de transferência utilizado;

VI – os operadores e suboperadores envolvidos;

VII – as medidas de segurança;

VIII – o período de retenção;

IX – os meios para exercício dos direitos.

§3º. Quando utilizado mecanismo contratual, deverão ser adotadas as cláusulas-padrão da ANPD sem alteração, cláusulas reconhecidas como equivalentes, cláusulas específicas previamente aprovadas ou outro mecanismo admitido pela regulamentação.

§4º. A utilização de cláusulas-padrão estrangeiras, por si só, não substitui os mecanismos previstos na regulamentação brasileira.

§5º. A transferência internacional de dados de crianças, adolescentes ou dados sensíveis deverá ser submetida a avaliação reforçada de risco.

CAPÍTULO V

DA GESTÃO DE RISCOS E DO RELATÓRIO DE IMPACTO

Art. 30. As unidades responsáveis deverão identificar, analisar, avaliar e tratar os riscos de privacidade e proteção de dados pessoais associados às suas atividades.

§1º. A avaliação deverá considerar:

I – a natureza, o contexto, a finalidade e a extensão do tratamento;

II – a quantidade e a sensibilidade dos dados;

III – o número e a vulnerabilidade dos titulares;

IV – a possibilidade de identificação ou reidentificação;

V – o uso de tecnologias inovadoras;

VI – o compartilhamento, cruzamento ou enriquecimento de bases;

VII – as consequências de acesso, alteração, perda ou indisponibilidade;

VIII – a probabilidade e a gravidade dos danos;

IX – as medidas técnicas e administrativas existentes.

§2º. Os riscos e as medidas de tratamento deverão ser registrados no ROPA, no RIPD ou em instrumento de gestão de riscos correspondente.

Art. 31. Será obrigatória a elaboração de RIPD quando o tratamento for suscetível de gerar alto risco aos direitos e às liberdades dos titulares.

§1º. Considera-se indicativo de alto risco, entre outras hipóteses:

I – tratamento de dados pessoais sensíveis em larga escala;

II – tratamento sistemático de dados de crianças e adolescentes;

III – monitoramento, rastreamento ou perfilamento sistemático;

IV – decisões automatizadas com efeitos relevantes;

V – cruzamento massivo de bases;

VI – uso de biometria ou reconhecimento facial;

VII – monitoramento de espaços físicos ou digitais;

VIII – utilização de tecnologia inovadora com impacto relevante;

IX – transferência internacional de dados sensíveis ou de grupos vulneráveis;

X – tratamento que possa gerar discriminação, exclusão, prejuízo pedagógico ou restrição de direitos;

XI – compartilhamento continuado, massivo ou interoperável de dados identificáveis;

XII – tratamento cuja falha possa afetar significativamente a continuidade de política pública ou serviço educacional.

§2º. A ANPD, o Controlador, o Colegiado ou o Encarregado poderão determinar a elaboração de RIPD em outras situações devidamente justificadas.

Art. 32. O RIPD deverá conter, no mínimo:

I – identificação da atividade e das unidades envolvidas;

II – descrição das operações de tratamento;

III – finalidade e bases legais;

IV – categorias de dados e titulares;

V – fluxo dos dados;

VI – agentes de tratamento e responsabilidades;

VII – sistemas, ambientes, integrações e fornecedores;

VIII – necessidade e proporcionalidade;

IX – riscos aos direitos e às liberdades dos titulares;

X – medidas de segurança e salvaguardas;

XI – riscos residuais;

XII – plano de ação, responsáveis e prazos;

XIII – manifestação do Encarregado;

XIV – data, versão e critérios de revisão.

§1º. A unidade responsável elaborará as informações operacionais e implementará as medidas de mitigação.

§2º. O Encarregado coordenará ou orientará a elaboração, emitirá manifestação técnica e acompanhará os planos de ação.

§3º. A Astin se manifestará sobre riscos e controles tecnológicos, quando aplicável.

§4º. A Asjur será consultada quando houver controvérsia jurídica, instrumento contratual, transferência internacional, controladoria conjunta ou repercussão jurídica relevante.

§5º. Os tratamentos de alto impacto ou com risco residual elevado serão submetidos ao Colegiado ou à autoridade máxima, conforme a competência.

§6º. O RIPD será revisto quando ocorrer:

I – mudança relevante no tratamento;

II – alteração de finalidade, base legal ou tecnologia;

III – inclusão de nova categoria de dados ou titulares;

IV – novo compartilhamento ou transferência internacional;

V – incidente de segurança relevante;

VI – alteração significativa dos riscos;

VII – determinação da ANPD ou de autoridade competente.

CAPÍTULO VI

DOS OPERADORES, FORNECEDORES E INSTRUMENTOS JURÍDICOS

Art. 33. Os operadores deverão tratar dados pessoais exclusivamente:

I – para as finalidades previstas no instrumento jurídico;

II – segundo as instruções documentadas da Seduc;

III – durante o período autorizado;

IV – com acesso limitado às pessoas que necessitem dos dados;

V – mediante adoção das medidas de segurança exigidas.

§1º. O operador deverá informar imediatamente à Seduc quando considerar que determinada instrução viola a legislação de proteção de dados.

§2º. É vedada a utilização dos dados para finalidade própria, comercial, publicitária, estatística não autorizada ou incompatível com o objeto contratado.

§3º. A contratação de suboperador dependerá de autorização prévia, específica ou geral, conforme o instrumento, e da imposição de obrigações equivalentes.

§4º. O operador permanecerá responsável perante a Seduc pelos atos e omissões dos suboperadores por ele contratados, nos limites da legislação.

Art. 34. Os operadores, fornecedores e unidades da Seduc deverão adotar medidas técnicas e administrativas adequadas aos riscos, incluindo, conforme aplicável:

I – controle de acesso baseado em papéis;

II – princípio do menor privilégio;

III – segregação de funções e ambientes;

