RED IBEROAMERICANA DE PROTECCION DE DATOS

GUIA PARA A IMPLEMENTAÇÃO

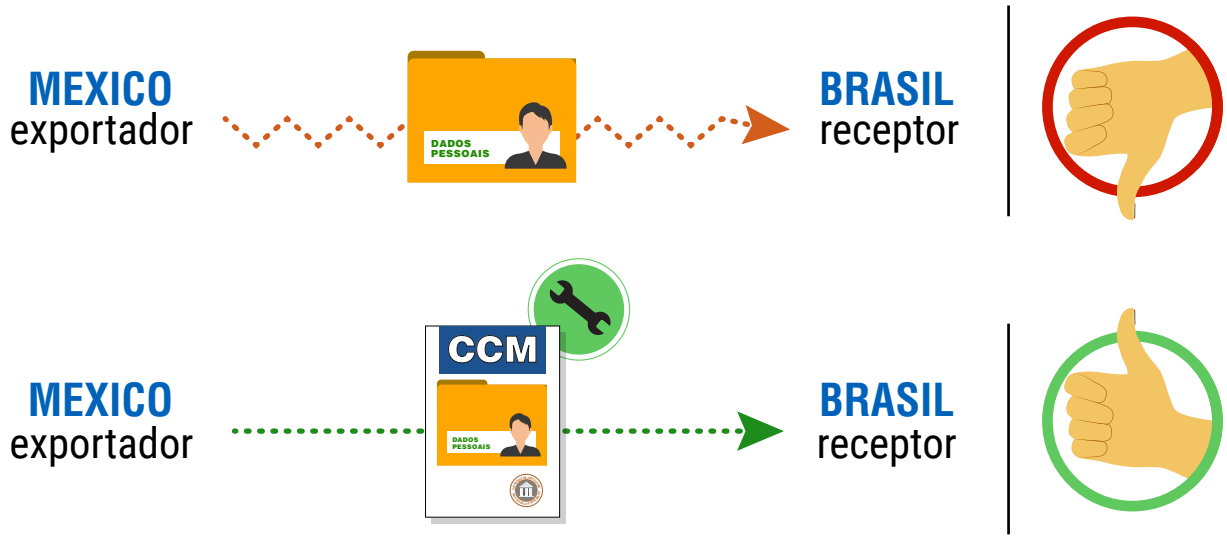
DE CLÁUSULAS CONTRATUAIS MODELO PARA A TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS *(TIDP)*

Índice

1. Introdução

O uso de cláusulas contratuais é uma alternativa para poder realizar transferências internacionais de dados pessoais. A este respeito, o artigo 36(1)(c) das Normas de Proteção de Dados Pessoais para os Estados Ibero-Americanos da Rede Ibero-Americana de Proteção de Dados (RIPD) prevê que "O responsável pelo tratamento e o processador podem realizar transferências internacionais de dados pessoais em qualquer um dos seguintes casos: ... c. O exportador e o destinatário assinam cláusulas contratuais ou qualquer outro instrumento legal que ofereça garantias suficientes e que permita demonstrar o alcance do tratamento dos dados pessoais, as obrigações e responsabilidades assumidas pelas partes e os direitos dos titulares. A autoridade de controle pode validar cláusulas contratuais ou instrumentos legais conforme determinado na legislação nacional dos Estados Ibero-Americanos aplicáveis ao assunto".

Em consonância com o exposto, este guia procura estabelecer os principais aspetos que devem ser tidos em conta quando as transferências internacionais de dados pessoais (doravante TIDP) são efetuadas através da utilização de cláusulas contratuais modelo (doravante CCM). Como tal, este guia apresenta algumas orientações a serem levadas em consideração por aqueles que devem levar as TIDP a jurisdições inadequadas dos países membros da Rede Ibero-Americana de Proteção de Dados Pessoais (RIPD).



Além disso, na América Latina não existem CCMs aprovadas conjuntamente a nível regional. Por esta razão, a RIPD apresenta como anexo a este Guia um modelo de contrato de transferência internacional em duas versões, uma para transferências entre Controladores e outra para transferências de Controladores para Processadores. Estes dois modelos são considerados como um primeiro passo e espera-se que modelos adicionais sejam desenvolvidos em uma etapa posterior para transferências de Processador para Processador e de Processador para Responsável.

O conteúdo substancial de ambos os modelos segue as diretrizes das Normas de Proteção de Dados Pessoais para Estados Ibero-americanos da RIPD[1] (“Normas”).

As CCMs propostas no Anexo também são semelhantes em sua estruturação com as recentes cláusulas contratuais padrão para a transferência de dados pessoais para países terceiros aprovados em junho de 2021 pela Comissão da União Europeia (“UE”)[2], pois em sua essência contêm elementos e princípios.

2. Precisões e limitações

Este Guia é complementar às recomendações, documentos e regulamentos vigentes em cada país da Ibero-América.[3] Os regulamentos de proteção de dados aplicáveis nos países da Ibero-América contêm disposições específicas relacionadas com as TIDP e em vários incluem mesmo uma disposição para o uso de cláusulas contratuais. Em alguns casos, foram desenvolvidos modelos próprios de cláusulas contratuais com base na legislação nacional (ver ponto 3.3. deste Guia).

Este Guia não substitui as regulamentações nacionais nem as diretrizes ou critérios expressos pelas diferentes autoridades de proteção de dados da região no exercício de seus poderes.

1. Cfr. Rede Ibero-Americana de Proteção de Dados -RIPD- (2017). Normas de proteção de dados pessoais para os Estados Ibero-americanos. Disponível em: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

2. Cfr. DECISÃO DE EXECUÇÃO DA COMISSÃO (UE) 2021/914, de 4 de junho de 2021, sobre cláusulas contratuais padrão para a transferência de dados pessoais para países terceiros, em conformidade com o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho. Disponível em: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32021D0914&from=EN#ntr2-L_2021199ES.01003701-E0002

3. Por exemplo, veja os mencionados na seção Documentos consultados deste Guia.

Deve ainda esclarecer-se que, em caso de manifesta contradição entre este documento e qualquer recomendação ou guia da autoridade nacional de proteção de dados, sugere-se seguir a recomendação da referida autoridade no entendimento de que cabe a essa entidade determinar as regras efetivar uma TIDP de acordo com a legislação aplicável.

Em qualquer caso, a aplicação deste Guia e a utilização dos dois modelos contratuais anexos a este Guia devem ser feitas em harmonia com as recomendações, resoluções e determinações das autoridades locais de proteção de dados e, sobretudo, com a legislação local.

Para a elaboração[4] deste documento, bem como as da CCM, foram tomadas como referência as Normas de Proteção de Dados Pessoais dos Estados Ibero-americanos da RIPD[5] para estabelecer os princípios, termos, definições, obrigações do Responsável e do Processador e direitos dos titulares de dados pessoais. O Guia e a CCM não transcrevem literalmente todos os aspectos do mesmo, mas os princípios contidos nas Normas foram tomados como fonte de todos os princípios legais que devem ser aplicados em caso da TIDP. Portanto, este documento deve ser lido em conjunto e de forma abrangente com as Normas acima mencionadas, sem prejuízo de eventuais adaptações que possam ser feitas em nível nacional.

Este Guia não é um conceito jurídico, nem um artigo acadêmico, nem constitui aconselhamento jurídico de qualquer tipo. Tampouco pretende ser uma lista exaustiva de recomendações específicas porque esta é uma questão interna que cada organização deve decidir à luz dos objetivos e da magnitude de cada projeto que envolve a transferência de dados pessoais para jurisdições inadequadas.

4. A Rede Ibero-Americana de Proteção de Dados (RIPD) agradece o trabalho realizado por Pablo Palazzi na elaboração deste guia e seu anexo. A RIPD publicou a versão anterior deste documento para comentários públicos. Comentários e sugestões foram recebidos e analisados das seguintes pessoas e organizações cuja participação agradecemos: (1) SEPD (Autoridade Europeia para a Proteção de Dados); (2) APEP (Associação Profissional Espanhola de Privacidade); (3) Gustavo Parra (Instituto de Transparência, Acesso à Informação Pública e Proteção de Dados Pessoais do Estado do México e Municípios); (4) A Associação Latino-Americana de Internet (ALAI), (5) Daniel Bulnes; (6) Associação de Internet MX; (7) Professora Lourdes Zamudio; (8) Equifax

5. Cfr. Rede Ibero-Americana de Proteção de Dados -RIPD- (2017). Normas de proteção de dados pessoais para os Estados Ibero-americanos. Disponível em: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

3. Antecedentes da TIDP

3.1. Antecedentes internacionais

A Diretiva de Proteção de Dados da União Europeia de 1995[6] foi o primeiro regulamento que implementou regras aplicáveis nas TIDP ao nível do direito comunitário europeu. A referida Diretiva foi revogada e substituída pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação de esses dados (doravante Regulamento Geral de Proteção de Dados, RGPD)[7].

O RGPD contém em seu quinto capítulo uma regulamentação detalhada das transferências internacionais de dados pessoais (Artigos. 44 a 50, RGPD). Art. 46 inc. 2º do RGPD permite a TIDP quando são adotadas garantias adequadas, entre as quais estão as cláusulas padrão de proteção de dados aprovadas pela Comissão Europeia ou por alguma autoridade de controle.

Através da Decisão 2001/497/CE da Comissão[8] e depois através da Decisão 2010/87/UE da Comissão Europeia[9], aprovou dois modelos que contêm cláusulas contratuais padrão para facilitar a transferência de dados pessoais de um Responsável estabelecido na UE para outro Responsável ou Processador estabelecido em um terceiro país que não oferece um nível adequado de proteção.

As cláusulas contratuais padrão das Deliberações mencionadas foram atualizadas em junho de 2021 para adequá-las ao RGPD, processo que incluiu consulta pública[10]. A nova decisão[11] aprova um modelo mais completo adaptado às alterações regulamentares e às novas formas de tratamento de dados pessoais.

---

6. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (DO L 281 de 23.11.1995 , pág. 31). Disponível em https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ%3AL%3A1995%3A281%3ATOC

7. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/ 46/CE, DO L 119 de 4.5.2016, p. 1. Disponível em https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC

8. Decisão 2001/497/CE da Comissão, de 15 de junho de 2001, relativa às cláusulas contratuais padrão para a transferência de dados pessoais para um país terceiro previstas na Diretiva 95/46/CE. Disponível em https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ%3AL%3A2001%3A181%3ATOC

9. Decisão 2010/87/UE da Comissão, de 5 de fevereiro de 2010, relativa às cláusulas contratuais padrão para a transferência de dados pessoais para processadores de dados estabelecidos em países terceiros de acordo com a Diretiva 95/46/EC do Parlamento Europeu e do Conselho. Disponível em https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ%3AL%3A2010%3A039%3ATOC

10. Essas novas cláusulas contratuais receberam comentários, contribuições e sugestões de toda a comunidade internacional e constituem um texto que reflete as mais importantes normas internacionais, incluindo os mais recentes desenvolvimentos jurisprudenciais sobre o assunto.

11. DECISÃO DE EXECUÇÃO DA COMISSÃO (UE) 2021/914, de 4 de junho de 2021, sobre cláusulas contratuais padrão para a transferência de dados pessoais para países terceiros, em conformidade com o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho . Disponível em https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32021D0914&from=EN#ntr2-L_2021199ES.01003701-E0002

Convém mencionar também o "Acordo de Comércio Eletrônico MERCOSUL"[12] (vinculante para a República Argentina, a República Federativa do Brasil, a República do Paraguai e a República Oriental do Uruguai) assinado em 28 de janeiro de 2021.

A arte. 6.2 do referido Contrato prevê que as partes devem adotar ou manter leis, regulamentos ou medidas administrativas para a proteção das informações pessoais dos usuários que participam do comércio eletrônico. Para tanto, levarão em consideração as normas internacionais existentes nesta matéria.

Também, pelo art. 6.7 do Acordo prevê que as partes se comprometam a aplicar um nível adequado de proteção aos dados pessoais que recebem de outra Parte por meio de uma regra geral ou regulamento autônomo específico ou por acordos mútuos, gerais ou específicos, ou em quadros internacionais mais amplos, admitindo para o setor privado a **implementação de contratos** ou autorregulação.

A arte. 7º do regulamento do MERCOSUL estabelece o princípio da não discriminação em matéria de transferência internacional de dados pessoais.

Em 9 de abril de 2021, a Comissão Jurídica Interamericana da Organização dos Estados Americanos aprovou os Princípios Atualizados sobre Privacidade e Proteção de Dados Pessoais[13].

O princípio n. 11 refere-se ao fluxo de dados transfronteiriço e fornece o seguinte: "Reconhecendo seu valor para o desenvolvimento econômico e social, os Estados Membros devem cooperar entre si para facilitar o fluxo transfronteiriço de dados pessoais para outros Estados quando eles fornecem um nível adequado de proteção de dados de acordo com estes Princípios. Da mesma forma, os Estados membros devem cooperar na criação de mecanismos e procedimentos que assegurem que os responsáveis e encarregados do tratamento de dados que operem em mais de uma jurisdição, ou os transmitam para uma jurisdição diferente da sua, possam garantir e ser efetivados responsável pelo cumprimento destes Princípios.

Por outro lado, a Convenção n. 108 do Conselho da Europa com as modificações do Protocolo de 2001[14] prevê em seu art. 2 intitulado "Transferência de dados pessoais para destinatários não sujeitos à jurisdição das Partes da Convenção" que "Cada Parte deverá prever que a transferência de dados pessoais para um destinatário sujeito à jurisdição de um Estado ou organização que não seja Parte à Convenção só será cumprida se o referido Estado ou organização assegurar um nível adequado de proteção".

O artigo 2.2 estabelece que "o artigo 2(1) do presente Protocolo não se aplica e as Partes podem autorizar a transferência de dados pessoais: ... b) se forem fornecidas pelo responsável pela transferência garantias suficientes, que podem resultar, em particular, de cláusulas contratuais, pelo responsável pela transferência e se tais garantias forem consideradas adequadas pelas autoridades competentes de acordo com a legislação nacional".

12. Ver MERCOSUR/CMC/DEC. Nº 15/20, disponível em https://normas.mercosur.int/public/normativas/4018 e https://normas.mercosur.int/simfiles/normativas/82753_DEC_015-2020_ES_Acuerdo%20Comercio%20Electronico.pdf

13. OEA, Princípios atualizados sobre privacidade e proteção de dados pessoais, com anotações (CJI/RES. 266 (XCVIII-O/21)). http://www.oas.org/es/sla/ddi/proteccion_datos_personales_trabajos_actuales_CJI.asp

14. Disponível em https://rm.coe.int/1680080626

3.2. Red Iberoamericana de Protección de Datos

A RIPD com base no artigo 1, alínea a) do Regulamento da Rede Ibero-Americana de Dados Pessoais e com o objetivo de desenvolver e dispor de regulamentos que garantam o direito à proteção e privacidade de dados nos países da região; tem se preocupado com a regulamentação legal da TIDP desde o seu início. Assim, no marco do III Encontro Ibero-Americano sobre Proteção de Dados, realizado em Cartagena das Índias (Colômbia) em 2004[15], os membros da RIPD emitiram várias conclusões onde era evidente sua preocupação com a TIDP.

Nessa reunião, os membros da RIPD concluíram que "A transferência internacional de dados pessoais deve estar sujeita a um regime de garantias para evitar que os princípios que regem o direito fundamental à proteção de dados sejam violados pela mera transferência desses dados a outro país. A Diretiva de Proteção de Dados da União Europeia consagrou este princípio e deu à Comissão Europeia o poder de decidir que um país que estabeleceu legislação de proteção de dados de acordo com os padrões europeus e criou uma autoridade de controle independente é um destino seguro para dados pessoais da UE Estados Membros".

No mesmo documento, os membros da RIPD esclareceram que "Na ausência desse reconhecimento, é possível, entre outras opções, utilizar cláusulas contratuais padrão [...] Sua utilização permite estabelecer as garantias necessárias que compensam a falta de legislação adequada no país de destino, dando às pessoas cujos dados são transferidos a possibilidade de exigir o cumprimento das cláusulas do contrato que as afetam, bem como a reparação no caso de serem prejudicadas pelo não cumprimento".

A Declaração de Cartagena das Índias conclui afirmando que "Assim, os participantes do III Encontro Ibero-Americano de Proteção de Dados esperam que nos países ibero-americanos se estabeleçam normas sobre proteção de dados e se estabeleçam mecanismos de controle independentes que promovam uma efetiva implementação do direito fundamental à proteção de dados pessoais que, ao mesmo tempo, facilita o livre fluxo de dados pessoais entre países".

No âmbito da XVIII Reunião Ibero-Americana sobre Proteção de Dados[16] realizada on-line em 4 de dezembro de 2020 em Montevidéu (Uruguai), os membros da RIPD estabeleceram em sua Declaração Final (ponto 7 da conclusão) que: "[…] o tratamento dos dados pessoais como motor da economia mundial requerem regras claras e transparentes que permitam fluxos de dados internacionais seguros, com base na consideração do nível de proteção fornecido pelos países ou organizações que são destinatários desses fluxos, em tratados internacionais ou em normas contratuais entre emitentes e destinatários que garantem a validade dos princípios de proteção de dados, o exercício dos direitos pelos titulares e o cumprimento das obrigações correspondentes aos responsáveis, encarregados do tratamento e outros terceiros".

15. RIPD, Declaração de Cartagena das Índias, maio de 2004, ponto III - "Transferências internacionais de dados. Perspectivas europeias e ibero-americanas" em https://www.redipd.org/sites/default/files/inline-files/declaracion_2004_III_encuentro_es.pdf

16. RIPD, XVIII Encontro Ibero-Americano de Proteção de Dados, https://www.redipd.org/sites/default/files/2020-12/declaracion-final-xviii-encuentro.pdf

Em conclusão, é natural que no desenvolvimento de documentos complementares às Normas e Declarações da RIPD, procuremos desenvolver guias e modelos que facilitem o livre fluxo de dados, mas mantendo a proteção adequada dos dados pessoais dos titulares, como as CCM ou códigos corporativos obrigatórios.

Em 2017, os membros da RIPD aprovaram as Normas de Proteção de Dados Pessoais para os Estados Ibero-americanos.

As Normas Ibero-Americanas procuram estabelecer um conjunto de princípios e direitos comuns de proteção de dados pessoais que os Estados Ibero-Americanos podem adotar e desenvolver em sua legislação nacional, a fim de ter regras homogêneas na região. Por outro lado, as Normas Ibero-Americanas incluem as melhores práticas nacionais e internacionais no campo no momento de sua emissão. Entre os objetivos das Normas Ibero-Americanas estão os seguintes que de alguma forma justificam a adoção da CCM para a região: (i) facilitar o fluxo de dados pessoais entre os Estados Ibero-Americanos e além de suas fronteiras, a fim de contribuir para o crescimento econômico e desenvolvimento social da região e (ii) promover a cooperação internacional entre as autoridades de controle dos Estados Ibero-Americanos, com outras autoridades de controle não pertencentes à região e autoridades e organismos internacionais na matéria.

Artigo 36 inc. 1, letra "c" das Normas estabelece que "O responsável e o processador podem realizar transferências internacionais de dados pessoais em qualquer um dos seguintes casos: … c. O exportador e o destinatário **assinam cláusulas contratuais ou qualquer outro instrumento legal que ofereça garantias suficientes** e que permita demonstrar o alcance do tratamento dos dados pessoais, as obrigações e responsabilidades assumidas pelas partes e os direitos dos titulares. A autoridade de controle pode validar cláusulas contratuais ou instrumentos legais conforme determinado na legislação nacional dos Estados Ibero-Americanos aplicáveis ao assunto".

Das Normas Ibero-Americanas emerge o seguinte:
+ O Exportador e o Importador podem firmar cláusulas contratuais.
+ Estas cláusulas contratuais devem oferecer garantias suficientes que permitam demonstrar: (i) o âmbito do tratamento dos dados pessoais, (ii) as obrigações e responsabilidades assumidas pelas partes e (iii) os direitos dos Titulares.
+ A respectiva autoridade de controle poderá validar cláusulas contratuais ou instrumentos legais conforme determinado na legislação nacional dos Estados Ibero-Americanos aplicáveis ao assunto.

3.3. Regulamentos Ibero-Americanos sobre TIDP

De acordo com as referidas normas internacionais e com as Normas, um grande número de países ibero-americanos regulamenta a transferência internacional de dados pessoais, na falta de continuidade no nível de proteção.

É o caso dos seguintes países:

Argentina (art. 12 lei n. 25.326 de proteção de dados pessoais, art. 12 do decreto regulamentar n. 1558/2001 e Disposição 60).
Brasil (artigos. 33 a 35 da Lei Geral de Proteção de Dados).

Cabo Verde (art. 20.º, Lei n.º 41/VIII/2013, de 17 de setembro, sobre a Proteção de Dados Pessoais de Pessoas Naturais).
Colômbia (Art. 26 da Lei 1.581 de 2012).
Equador (artigos. 55 a 61 da Lei Orgânica de Proteção de Dados Pessoais).
México (artigos. artigos 65 a 71 da Lei Geral de Proteção de Dados Pessoais detidos por Pessoas Jurídicas e artigos. 36 e 37 da Lei Federal de Proteção de Dados Pessoais detidos por Particulares).
Nicarágua (art.14 da Lei nº 787, Lei de Proteção de Dados Pessoais).
Panamá (artigos. 5 e 33, Lei nº 81, de 26 de março de 2019, de Proteção de Dados Pessoais e artigos. 51 a 53 do Decreto Executivo nº. 285 de 28 de maio de 2021).
Peru (artigos. 11 e 15 da Lei 29.733, Lei de Proteção de Dados Pessoais).
República Democrática de São Tomé e Príncipe ((artigos. 19 e 20, Lei 3/2016, de 2 de maio, Proteção de Dados Pessoais de Pessoas Físicas).
República Dominicana (art. 80 da Lei nº 172-13, de 13 de dezembro de 2013, de Proteção de Dados Pessoais).
Uruguai (art. 23 da Lei nº 18.331 de Proteção de Dados Pessoais, Resolução nº 4/019, de 12 de março de 2019 e Resolução nº 41/021, de 8 de setembro de 2021).

A maioria das legislações acima mencionadas também prevê certas exceções para permitir que a TIDP tenha destinos impróprios (por exemplo, onde existam tratados internacionais). Por outro lado, também é possível recorrer a outras ferramentas para transferência internacional. Por exemplo, as regulamentações da Argentina, Colômbia[17], México[18], Panamá[19], Peru[20] e Uruguai contemplam ou recomendam a possibilidade de utilização da CCM.

Por sua vez, algumas autoridades de proteção de dados, como Uruguai e Argentina, emitiram regulamentos que aprovam diretrizes ou modelos de CCM[21].

17. Colômbia: Em sua nova versão do ano de 2021, o Guia emitido pela autoridade colombiana para a proteção de dados pessoais fornece diretrizes sobre a TIDP e o uso da CCM. Ver Colômbia, SIC, Guia para a implementação do princípio da responsabilidade demonstrada nas transferências internacionais de dados pessoais, p. 17 onde se recomenda a utilização de cláusulas contratuais para a TIDP como forma de demonstrar a responsabilização do Responsável pelo tratamento dos dados pessoais. Disponível em https://www.sic.gov.co/sites/default/files/files/2021/2021%20Gu%C3%ADAs%20para%20implementaci%C3%B3n%20del%20principio%20de%20responsibility%20demonstrada% 202021.pdf

18. México, o artigo 75 do Regulamento da Lei Federal de Proteção de Dados Pessoais de Titularidade Privada (LFPDPPP), sugere as cláusulas contratuais, ao prever "Para este fim, o responsável que transfere os dados pessoais pode usar cláusulas contratuais ou outros instrumentos legais que prevejam, pelo menos, as mesmas obrigações a que está sujeito o responsável pela transmissão dos dados pessoais, bem como as condições em que o titular consentiu no tratamento dos seus dados pessoais. Por outro lado, o Artigo 66 da Lei Geral de Proteção de Dados Pessoais na Posse de Sujeitos Obrigados, que estabelece que "Todas as transferências devem ser formalizadas através da assinatura de cláusulas contratuais, acordos de colaboração ou qualquer outro instrumento legal, de acordo com os regulamentos aplicáveis ao responsável pelo tratamento de dados, que permitam demonstrar o alcance do tratamento de dados pessoais, assim como as obrigações e responsabilidades assumidas pelas partes". Deve-se esclarecer que no México existe uma Lei aplicável a pessoas físicas e outra para Sujeitos Obrigados, que oportunamente são aquelas instituições de natureza pública.

19. Panamá, Art. 53 inc. 2º do Decreto Executivo nº. 285 de 18 de maio de 2021. Disponível em https://www.gacetaoficial.gob.pa/pdfTemp/29296_A/GacetaNo_29296a_20210528.pdf

20. Peru, o artigo 25 do Regulamento LPDP, também considera as cláusulas contratuais, quando afirma que "... o emissor ou exportador pode usar cláusulas contratuais ou outros instrumentos legais que estabeleçam pelo menos as mesmas obrigações a que está sujeito, bem como as condições em que o titular consentiu no tratamento dos seus dados pessoais.

21. Uruguai: Resolução nº 41/021, de 8 de setembro de 2021. Disponível em https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/noticias/changes-regimen-transferencias-internacionales-datos-uruguay e Argentina: Disposição 60/2016 da Direção Nacional de Proteção de Dados Pessoais. Disponível em http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/texact.htm

4. Principais atores da TIDP

Os principais atores envolvidos na TIDP são apresentados a seguir. Isso ajuda a entender o interesse de cada parte em uma TIDP.

As TIDPs ocorrem em um grande número de situações como: transferências bancárias, reservas de passagens aéreas e hotéis, serviços de computação em nuvem, centralização de recursos humanos, operações tradicionais de comércio exterior e comércio eletrônico, entre muitos outros casos

No cenário típico de uma TIDP (seja qual for o motivo) temos os seguintes elementos e atores:

+ Uma entidade que deseja enviar dados para o exterior nomeada: **Exportador de dados.**
+ Uma entidade que deseja receber esses dados nomeada: **Importador de dados**, localizado em outra jurisdição.
+ O Importador recebe os dados para tratá-los com uma determinada finalidade. Mas a TIPD é em si um tratamento de dados: supõe-se que qualquer transferência internacional de dados pessoais TIPD implica o tratamento de dados de acordo com a definição dada pelas Normas[22].
+ O **Titular dos dados pessoais é a** "pessoa singular a quem os dados pessoais se referem"[23] cujas informações devem ser processadas adequadamente. Todos os direitos do Titular devem ser garantidos quando o tratamento for realizado por meio de um TIDP para uma jurisdição caracterizada como não adequada. No caso das Normas, os direitos a serem garantidos são mencionados nos artigos 24 a 32. Uma forma de garantir esses direitos é através do uso da CCM.
+ Por sua vez, o Titular é um **Terceiro Beneficiário** na CCM. Isso significa que o Titular tem direitos que derivam não apenas da lei de proteção de dados pessoais da jurisdição do Exportador de Dados, mas também do contrato de transferência internacional firmado entre as partes (ver ponto 7 deste Guia).
+ Uma **jurisdição inadequada** onde o Importador de Dados está localizado. Esta jurisdição é caracterizada como não adequada para fins da TIDP de acordo com a regulamentação do país do Exportador de Dados ou a interpretação da Autoridade competente. A falta de adequação da jurisdição de destino obriga as partes a adotarem salvaguardas que proporcionem garantias adequadas à proteção dos dados sujeitos a TIDP, por exemplo, através da assinatura da CCM.
+ **A autoridade de proteção de dados** (Autoridade de Controle)[24] deve garantir que aqueles que realizam a TIDP realizam essa atividade, observando o disposto na regulamentação sobre o assunto.
+ **Lei aplicável:** Os regulamentos sobre transferência internacional de dados ou "fluxo de dados transfronteiriço" procuram garantir que o nível de proteção dos dados pessoais dos cidadãos de um país não diminua ou desapareça quando estes devem ser exportados ou transferidos para outro ou outros países[25]. Como consequência da necessidade de proteger os dados pessoais transferidos para uma jurisdição não adequada, é necessário que os dados pessoais estejam sujeitos a uma proteção semelhante àquela existente no momento da coleta.

22. Cf. literal i do art. 2 das Normas de Proteção de Dados Pessoais dos Estados Ibero-americanos (2017).

23. Cfr. Artigo 2.1(h) das Normas de Proteção de Dados Pessoais para os Estados Ibero-Americanos (2017).

24. O Capítulo VII das Normas estabelece os principais aspectos das autoridades de controle e supervisão da proteção de dados.

25. Consulte RIPD, Recomendações para o processamento de dados pessoais por meio de serviços de computação em nuvem. Disponível em https://www.redipd.org/sites/default/files/2021-06/recomendaciones-tratamiento-datos-personales-servicios-nube.pdf

Vejamos um exemplo com o cenário de processamento de dados por meio de serviços de computação em nuvem de acordo com as diretrizes aprovadas pela RIPD sobre o assunto.

Em abril de 2020, a RIPD publicou as "Recomendações para o processamento de dados pessoais por meio de serviços de computação em nuvem"[26]. Neste documento, a RIPD concluiu que o processamento de dados pessoais na nuvem pode envolver a transferência internacional de dados pessoais[27]. As recomendações contêm sugestões para que os prestadores de serviços de computação em nuvem (PSCEN) possam prestar os seus serviços respeitando os direitos de dados pessoais dos Titulares e as regras da TIDP.

Em suas Recomendações, as RIPD afirmam o seguinte: "Se os «datacenters» ou equipamentos de armazenamento PSCEN estiverem localizados fora do país onde está localizada a parte contratante dos serviços de computação em nuvem (CEN), os dados pessoais serão enviados ou exportados de um país para empresas e organizações PSCEN localizadas em um território diferente do o país remetente. É um processo de exportação de dados pessoais".

26. Consulte RIPD, Recomendações para o processamento de dados pessoais por meio de serviços de computação em nuvem. Disponível em https://www.redipd.org/sites/default/files/2021-06/recomendaciones-tratamiento-datos-personales-servicios-nube.pdf

27. RIPD, Recomendações para o tratamento de dados pessoais através de serviços de computação em nuvem, p. 15.

Após esta explicação, o documento especifica: “Neste caso, a empresa contratante dos serviços do CEN será o Exportador e o PSCEN atuará como destinatário da referida exportação de dados. As Normas definem o Exportador como a “pessoa física ou jurídica de natureza privada, autoridade pública, serviços, órgão ou prestador de serviços situado no território de um Estado que realiza transferências internacionais de dados pessoais, de acordo com o disposto nestas Normas “. Assim, o contratante dos serviços do CEN deve observar as regras locais de transferência internacional de dados”.

As mencionadas Recomendações da RIPD concluem que “É importante que o contratante dos serviços do CEN esteja plenamente ciente e, se for o caso, possa aceitar ou limitar os países em que os servidores serão hospedados, além de ser informado das devidas salvaguardas adotadas “.

Tudo isso é explicado com a base da TIDP: “Os regulamentos sobre transferência internacional de dados ou “fluxo de dados transfronteiriço” procuram garantir que o nível de proteção dos dados pessoais dos cidadãos de um país não diminua ou desapareça quando estes devem ser exportados ou transferidos para outro ou outros países. Esta regra é conhecida como princípio da continuidade da proteção de dados, que se baseia no fato de que a transferência internacional de dados não deve afetar a proteção das partes interessadas no que diz respeito ao tratamento de seus dados pessoais. A exportação de informações pessoais não pode se tornar um cenário que reduza o nível de proteção conferido ao titular dos dados no país de onde os dados pessoais são exportados. Essas atividades não devem facilitar, permitir ou tolerar a violação dos direitos dos indivíduos ou a redução das garantias de que dispõem no país exportador. Nesse sentido, devem ser observadas as regras de transferências internacionais que vigoram no país do contratante dos serviços do CEN. No caso das Normas, o artigo 36 prevê as alternativas permitidas para exportar os dados”.

No caso específico analisado, a empresa contratante dos serviços do CEN será a Exportadora de Dados e a PSCEN será a Importadora de Dados. Ambas as partes podem assinar um contrato com base na CCM em que o Importador de Dados atua como Processador usando o respectivo modelo da CCM.

5. Regra geral na TIDP. Exceções e mecanismos de transferência mais usados

5.1. Regra geral

As disposições sobre TIDP contidas nas leis de proteção de dados dos países ibero-americanos visam garantir a continuidade do nível de proteção previsto em suas leis quando houver uma transferência de dados pessoais para um terceiro país considerado inadequado ou que tenha um nível diferente de proteção de dados pessoais.

Os países podem reconhecer outras jurisdições como "adequadas" à sua legislação de dados pessoais, dependendo do nível de proteção garantido pela legislação aplicável. Em virtude do princípio geral de proibição do TIDP, na ausência de uma decisão de adequação ou referência específica no país exportador de dados, o Responsável ou o Processador só poderá transferir dados pessoais para um terceiro país se tiverem sido oferecidas garantias adequadas e em condição de que os Titulares tenham direitos exigíveis e ações judiciais efetivas para proteger seus direitos. Tais garantias podem ser prestadas, entre outros meios, pelas Normas Corporativas Vinculativas (NCV)[28] ou pela CCM.

Em termos gerais, um país é considerado adequado quando possui determinados elementos em seu ordenamento jurídico que permitem concluir que os dados pessoais estão adequadamente protegidos. Por exemplo, de acordo com os regulamentos da União Europeia, os seguintes elementos geralmente são avaliados para determinar o nível de adequação:

- O "Estado de Direito", o respeito aos direitos humanos e aos direitos fundamentais naquele ordenamento jurídico.
- Legislação atual, geral e setorial, sobre dados pessoais.
- As medidas de segurança aplicadas.
- As regras sobre transferências posteriores de dados pessoais para outro país terceiro ou organização internacional observadas nesse país.
- Direitos reconhecidos aos titulares de dados pessoais por meio de recursos administrativos e ações judiciais efetivas.
- A existência e o funcionamento efetivo de uma ou mais autoridades de controle independentes no país terceiro.
- Os compromissos internacionais assumidos pelo país terceiro ou outras obrigações decorrentes de acordos ou instrumentos juridicamente vinculativos, bem como da sua participação em sistemas multilaterais ou regionais, nomeadamente em relação à proteção de dados pessoais.
- O acesso das autoridades públicas do país de destino aos dados transferidos e, de forma mais geral, o regime de exceções às regras de proteção de dados pessoais aplicáveis no país de destino.

28. As Regras Corporativas Vinculativas são uma das salvaguardas apropriadas reconhecidas pela RGPPD e são definidas como "as políticas de proteção de dados pessoais empreendidas por um responsável ou processador estabelecido no território de um Estado-membro para transferência ou conjunto de transferências de dados pessoais a um responsável ou processador em um ou mais países terceiros, dentro de um grupo de empresas ou de um grupo de empresas envolvidas em uma atividade econômica conjunta" (Art. 4. 20) RGPD).

5.2. Exceções

As Normas estabelecem no Art. 36.2 que a legislação nacional aplicável dos Estados Ibero-Americanos pode estabelecer expressamente limites às transferências internacionais de categorias de dados pessoais por razões de segurança nacional, segurança pública, proteção da saúde pública, proteção dos direitos e liberdades de terceiros, bem como por razões de interesse público.

Numerosos regulamentos contêm exceções à regra que proíbe a TIDP para países ou jurisdições inadequados. As regras das jurisdições ibero-americanas mencionadas no ponto 3.3 deste Guia contêm exceções individuais baseadas nesses princípios mencionados nas Normas. As exceções são, por exemplo, o consentimento do envolvido, o interesse público, a execução ou conclusão de um contrato ou os interesses vitais do envolvido.

Um ponto importante a ter em mente é que estas exceções para a TIDP não podem ser aplicadas continuamente para todos os tipos de transferências, mas devem, devido à sua natureza excepcional, ser destinadas a uma transferência específica e direcionada.

5.3. Mecanismos de transferência

C aso o país de destino da TIDP não possua um nível adequado de proteção reconhecido, então a TIDP pode ser realizada por meio de mecanismo de transferência que conceda garantias adequadas, ou pela aplicação de alguma das exceções previstas na regulamentação local.

Os mecanismos TIDP que fornecem garantias adequadas são geralmente os seguintes:

- Cláusulas contratuais modelo (CCM).
- Normas societárias vinculantes (NCV).
- Código de conduta aprovado de acordo com a legislação aplicável.
- Mecanismo de certificação.
- Instrumentos juridicamente vinculativos e executáveis entre autoridades ou órgãos públicos.

A função das CCMs padrão é garantir que haja garantias adequadas de proteção de dados nas transferências internacionais de dados para jurisdições que não possuem um nível adequado de proteção reconhecido. O Exportador de Dados que transfere os dados pessoais para um terceiro país e o Importador de Dados que recebe os dados pessoais podem assinar um acordo para garantir os direitos dos titulares dos dados através da CCM.

Embora as CCM devam, em princípio, ser utilizadas para transferências para jurisdições inadequadas, a RIPD recomenda sua aplicação a todos os tipos de transferências internacionais, quando relevante para garantir a conformidade com os princípios de proteção de dados pessoais.

Finalmente, é importante observar que o uso da CCM não implica, em todos os casos, o pleno cumprimento da legislação ou regulamentos de proteção de dados pessoais das jurisdições afetadas pela transferência e, portanto, exigências específicas devem ser seguidas[29].

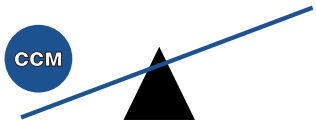
6. A CCM como mecanismo de proteção da TIDP

6.1. Objetivo da CCM

O objetivo da CCM é garantir e facilitar o cumprimento dos requisitos previstos pela lei de proteção de dados do país do Exportador de Dados para a transferência de dados pessoais para um terceiro país que não tenha sido reconhecido com um nível de proteção adequado. A ideia é que a proteção inicialmente concedida aos dados pessoais permaneça presente independentemente de onde esses dados estejam localizados.

É por isso que as transferências subsequentes também são regulamentadas com precauções para evitar a redução do nível de proteção. Os Titulares estão envolvidos através de um conceito universal de direito contratual chamado de Beneficiário de Terceiros. E regulamenta o acesso das autoridades públicas na jurisdição do importador de dados que pode afetar os direitos da pessoa em questão.

6.2. Vantagens e benefícios da CCM



O uso de cláusulas contratuais modelo pode ajudar a superar possíveis limitações nas transferências de dados resultantes de diferenças no nível de proteção entre diferentes países. O instituto do contrato está presente em todos os ordenamentos jurídicos ibero-americanos e serve para comprometer o Importador de Dados a respeitar os dados pessoais do Proprietário, uma vez que os dados pessoais estejam na jurisdição de destino.

29. Por exemplo, no caso do setor público no México, quando são realizadas transferências de dados pessoais que não possuem um nível de proteção adequado, uma Avaliação de Impacto na proteção de dados pessoais deve ser submetida previamente.

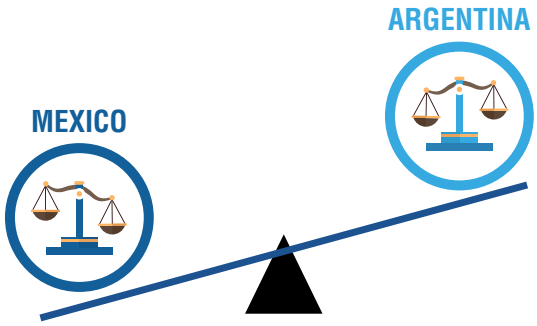
Em outras palavras: as cláusulas modelo ou cláusulas padrão contribuem para construir a convergência em nível contratual, criando um regime autônomo de proteção de dados, sem necessariamente exigir convergência em nível de país (neste caso, podem ir além do nível de proteção em determinados países).

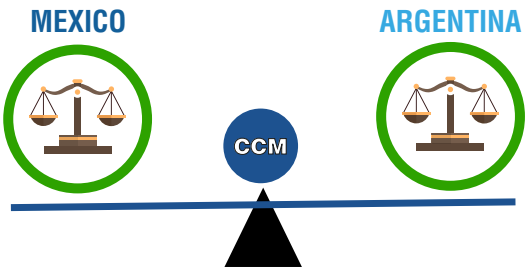
Ao mesmo tempo, a expansão dos princípios de proteção de dados pessoais por meio de redes de contratos internacionais tem um forte impacto na convergência geral na região, pois estabelecem padrões comuns com os quais as empresas se familiarizam. Isso facilita no futuro o alinhamento da legislação nacional com as normas e padrões internacionais de proteção de dados pessoais.

Por outro lado, a utilização da CCM serve para garantir os princípios e deveres na proteção dos dados pessoais. Isso, por sua vez, leva à transparência, segurança jurídica e, portanto, previsibilidade, uma vez que:

(i) através de sua natureza vinculativa e executável como parte de um contrato, podem assegurar a continuidade da proteção quando os dados viajam ao exterior, e o fazem de uma forma que proporciona segurança jurídica;
(ii) ao fazê-lo de forma clara e transparente, ajudam a construir confiança, o que por sua vez dá às empresas que utilizam tais cláusulas uma vantagem competitiva sobre aquelas que têm que recorrer a outros métodos.

As CCM servem para proteger a parte “mais fraca”, que, obviamente, são as pessoas físicas cujos dados pessoais, sob a TIDP, são processados tanto pelo Exportador de Dados quanto pelo Importador de Dados.





Finalmente, o uso da CCM também permite uma solução particularmente econômica para o problema da TIDP; a razão é que as empresas não precisam negociar acordos em cada caso individual com o custo econômico em termos de representação legal e de tempo que isso implica. A existência da CCM permite-lhes contar com o modelo pré-aprovado pela Autoridade de Controlo competente, sabendo que ao fazê-lo cumprem as suas obrigações legais relativas à transferência internacional de dados pessoais com uma solução simples e prática. Essa é uma grande diferença em relação a outras ferramentas, como mecanismos de certificação ou NCVs, que exigem um processo de certificação muitas vezes demorado e caro.

Em comparação com esses mecanismos, as CCMs são um instrumento “pronto para usar” e “pronto para implementar”. Isto é particularmente importante para as pequenas e médias empresas que não podem arcar com outras opções de implementação mais dispendiosas e demoradas.

É por isso que as CCMs são o mecanismo legal mais acessível e usado hoje para TIDP para jurisdições não adequadas. Estima-se que cerca de 80 a 90% das empresas que implementam mecanismos de TIDP utilizam a CCM como solução[30]. Isto, naturalmente, implica que as Partes de uma TIDP usando uma CCM não devem se limitar à exigência formal de sua assinatura, mas devem estar sempre preparadas para serem "responsáveis" por seu processamento de dados pessoais perante a autoridade supervisora competente e aos Sujeitos dos Dados e serem capazes de demonstrar o pleno cumprimento da lei aplicável e das obrigações impostas na CCM.

7. Questões práticas na implementação e execução da CCM

7.1. Aspectos gerais

Dada a multiplicidade de leis existentes na Ibero-América, este Guia baseia-se nas Normas aprovadas na XV Reunião desta Rede, realizada em Santiago do Chile, Chile, em 22 de junho de 2017. Também foram considerados os trabalhos realizados com a CIJ da OEA para a modernização dos princípios de privacidade elaborados pela referida organização, bem como o RGPD e a Convenção 108 modernizada.

As definições da CCM são retiradas das Normas. O mesmo se aplica às obrigações substantivas decorrentes das CCMs. Da mesma forma, foram consultados os modelos de cláusulas contratuais aprovados pela UE, bem como os modelos propostos pelas autoridades neozelandesas.

SANTIAGO DO CHILE
CHILE - JUNHO DE 2017
XV REUNIÃO
RED IBEROAMERICANA DE PROTECCION DE DATOS

30. Um estudo realizado calcula que cerca de 85% utilizam CCM como mecanismos da TIDP. Veja Nigel Cory, Ellysse Dick, Daniel Castro, The Role and Value of Standard Contractual Clauses in EU-US Comércio Digital, ITIF, 17 de dezembro de 2020. Disponível em https://itif.org/publications/2020/12/17/role-and-value-standard-contractual-clauses-eu-us-digital-trade. No mesmo sentido: Laura Bradford, Mateo Aboy, Kathleen Liddell, Cláusulas contratuais padrão para transferências transfronteiriças de dados de saúde após Schrems II, publicadas no Journal of Law and the Biosciences, Volume 8, Issue 1, January-June 2021, https://doi.org/10.1093/jlb/lsab007.

As fontes em que se baseiam as cláusulas da CCM são indicadas abaixo:

Cláusula	Fonte
Cláusula 1.4 - Definições de CCM	Art. 2 das Normas. A definição de anonimato é baseada no Art. 4.3.b das Normas. As definições de Importador de Dados, Transferência Adiante, Lei Aplicável e Terceiro Beneficiário não estão nas Normas. Foi elaborado com base no conteúdo das cláusulas modelo.
Cláusula 6.1 - Princípio de responsabilidade	Artigo 20 das Normas
Cláusula 6.2 - Princípio da finalidade	Artigo 17 das Normas
Cláusula 6.3 - Princípio da Transparência	Artigo 19 das Normas
Cláusula 6.6 y 6.7 Princípios de segurança e confidencialidade	Artigos 21, 22 e 23 das Normas
Cláusula 6.9 - Transferências Adicionais	Cláusula 8.7 da CCM da UE
Cláusula 7 – Direitos do Titular	Artigos 24 a 28 das Normas
Direito a indemnização	Artigo 44 das Normas
Cláusula de acesso por autoridades públicas	Cláusula Contratual Modelo da Nova Zelândia
Cláusula 6.1. do modelo Responsável-Processador	Artigo 34 das Normas

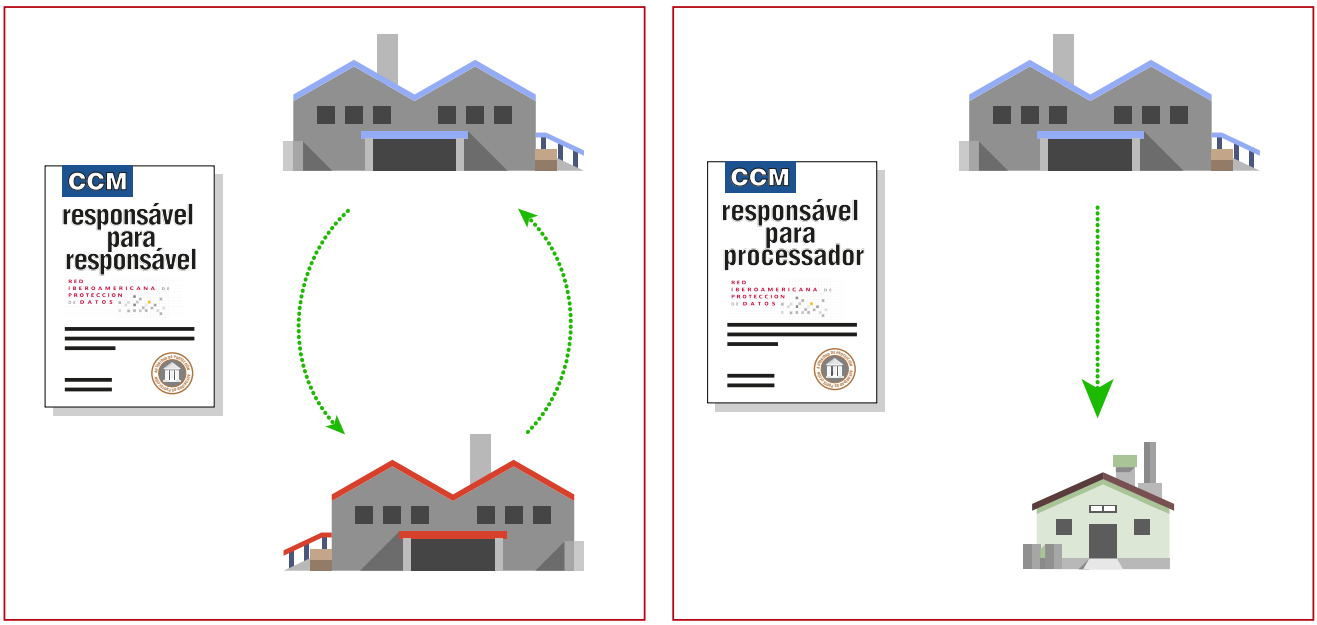
Consequentemente, como primeiro passo recomendado para a adoção das CCMs, sugere-se comparar os requisitos estabelecidos nas Normas com os regulamentos de cada Estado Membro, uma vez que, caso estes últimos prevejam requisitos adicionais, disposições complementares devem ser incluídas nas CCMs.

7.2. Características das CCMs. Forma de uso.

Os dois modelos da CCM incluídos no Anexo a este Guia caracterizam-se pelo seguinte:

• A CCM do Anexo contém dois modelos para as diferentes premissas da TIDP:

i) Responsável para Responsável y ii) Responsável para Processador.



• É incluída uma primeira folha ou capa onde são inseridos todos os dados das partes e do contrato e seus endereços. A ideia é que, em princípio, não seja necessário modificar em nada o texto da CCM.

• As CCMs têm vários anexos para identificar as novas partes que aderem ao contrato após sua assinatura inicial pelo Importador e Exportador de Dados (Anexo A), os dados pessoais envolvidos nas transferências e seus objetivos (Anexo B), as medidas de segurança (Anexo C), a lista de sub-processadores no caso do segundo modelo (Anexo D) e documentação legal adicional que as partes podem desejar incluir, como avisos de privacidade ou políticas de privacidade (Anexo E).

• Com respeito ao Anexo A, cada nova Parte que aderir às CCMs deve assinar um Anexo separado e indicar o tipo de atividade que irá empreender com respeito às TIDP.

• Relativamente ao Anexo B, deve ser possível distinguir claramente a informação aplicável a cada transferência ou categoria de transferências.

• Em relação ao Anexo C, as medidas de segurança devem ser detalhadas com precisão. Não é possível incluir generalidades.

• Com relação ao Anexo D, deve-se mencionar os subdepartamentos caso você tenha optado por listá-los antecipadamente.

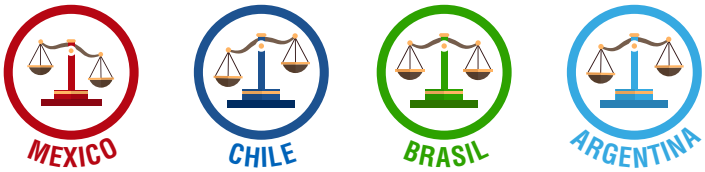
Além disso, considera-se importante ressaltar que o uso de CCMs requer verificação prévia das exigências da transferência no caso específico, e das características das entidades ou pessoas que as realizam, já que as CCMs poderiam eventualmente incorporar elementos adicionais dependendo dessas suposições e das exigências regulatórias aplicáveis em cada um dos países onde tal processamento é realizado.

7.3. Posição das partes. Incorporações de novas partes e utilização da CCM com outros acordos. Modificações.

Embora geralmente se faça referência a cláusulas contratuais padrão ou CCM, o termo refere-se a um modelo de contrato completo que pode ser utilizado tal qual ou modificado em aspectos secundários, desde que sua essência, que é a proteção dos direitos do Titular, não seja alterada de acordo com os regulamentos aplicáveis. É então possível acrescentar estes CCMs como um anexo a um contrato que as partes assinarão ou já assinaram, mas elas devem então realmente executar estes modelos para que sejam válidos e efetivos.

As Partes têm a discrição de incluir em um contrato mais amplo tais cláusulas contratuais padrão, bem como de acrescentar cláusulas ou garantias adicionais, desde que não contradigam, alterem ou modifiquem direta ou indiretamente as cláusulas contratuais padrão ou prejudiquem os direitos fundamentais dos Titulares.

7.4. Lei aplicável às TIDP



A implementação da CCM ocorre quando uma entidade deve transferir dados para outra entidade localizada em outro país que não tenha sido reconhecido como país com nível de proteção adequado pelo país de origem. As Cláusulas Contratuais Modelo podem ser usadas em relação a tais transferências na medida em que o Importador de Dados esteja em um terceiro país que não seja o Exportador de Dados.

Em uma situação normal, cada parte estaria sujeita no processamento de dados pessoais transferidos às leis de seu respectivo país. No entanto, em questões da TIDP através da CCM, a lei aplicável (definida na CCM como "Lei Aplicável") é a lei do país ou jurisdição do Exportador de Dados.

A exportação de informações pessoais não pode se tornar um cenário que reduza o nível de proteção que é conferido ao Titular dos dados no país de onde os dados pessoais são exportados. A TIDP não deve facilitar ou permitir a violação dos direitos dos Titulares ou a redução das garantias de que dispõem os Titulares no país exportador[31]. Isto se baseia na lógica de que os dados são coletados e processados sob a lei do exportador de dados e quando são transferidos ao exterior para um país que foi reconhecido como tendo um nível de proteção adequado, é necessário preservar o nível de proteção que os dados pessoais têm no país de origem.

31. RIPD, Recomendações para o tratamento de dados pessoais através de serviços de computação em nuvem, p. 15.

7.5. Cumprimento das normas gerais de proteção de dados pessoais

1º LEGISLAÇÃO LOCAL

AUTORIDADE LOCAL DE PROTEÇÃO DE DADOS

CLÁUSULAS CONTRATUAIS MODELO

Além de utilizar o CCM para fornecer salvaguardas adequadas para transferências internacionais de dados pessoais, o Exportador de Dados tem que cumprir com suas obrigações gerais como Responsável ou Processador sob a lei de proteção de dados pessoais em vigor em sua jurisdição.

Entre essas responsabilidades estão a obrigação do responsável de comunicar claramente aos Titulares em sua política de privacidade, a existência de transferências internacionais de seus dados pessoais para um terceiro país que não tenha um nível de proteção adequado reconhecido.

Além disso, é importante levar em consideração que, em conformidade com os deveres e princípios e obrigações referentes à proteção de dados pessoais no marco regulatório de cada país, pode haver exigências complementares, como no caso do México, onde existe a obrigação de comunicar a nota de privacidade. Portanto, aqueles requisitos que não são considerados na CCM devem ser adicionados nos anexos correspondentes. De forma a cumprir os princípios de informação e transparência do tratamento de dados pessoais.

7.6. Transferências subsequentes

Se o Importador precisar transferir os Dados Pessoais para outra entidade após receber os dados do Exportador, ocorre uma Transferência subsequente e é necessário continuar protegendo os dados pessoais.

As transferências subsequentes pelo Importador de Dados para um terceiro em outro país terceiro só devem ser permitidas se esse terceiro aderir aos CCMs de teor semelhante e se a continuidade da proteção for assegurada de outra forma ou em situações específicas cobertas pelas CCMs.

Vale lembrar que cada vez que ocorre uma Transferência Subsequente no sentido acima definido, é atualizada a presunção de participação de um terceiro que, fazendo parte do tratamento, adquire responsabilidades em termos de proteção de dados pessoais. Em tal caso, seria necessário o acréscimo às Cláusulas Contratuais Modelo, seja assinando uma nova CCM individual com o Importador de Dados ou através de um instrumento legal específico.

7.7. Beneficiários de terceiros

Na CCM, o Titular é um Terceiro beneficiário do contrato modelo assinado pelas Partes. Em caso de violação de obrigações contratuais pelo Importador de Dados, o Sujeito de Dados poderá, como terceiro beneficiário, reclamar contra o Importador de Dados ou o Exportador de Dados por tal violação. Isso ocorre porque ambas as Partes fazem uma estipulação em favor do Titular[32].

O princípio do Terceiro Beneficiário está contemplado na maioria dos códigos de direito privado latino-americanos. Assim, entre outros, encontramos nos códigos civis da Argentina (art. 1027 do Código Civil e Comercial da Nação), Bolívia (arts. 526 a 529 do Código Civil), Brasil (arts. 436 a 438 do Código Civil), Chile (art. Art. 1449 do Código Civil), Colômbia (art. 1506 do Código Civil), Costa Rica (art. 1026 do Código Civil da Costa Rica), Equador (art. 1465 Código Civil), El Salvador (art. 1320 Código Civil), Guatemala (art. 1531 Código Civil), Honduras (art. 740 Código Comercial), México (arts. 1868-1871 do Código Civil Federal), Nicarágua (art. 1875 Código Civil), Paraguai (art. 732 do Código Civil), Peru (arts. 1457-1459 do Código Civil) e Uruguai (art. 1256 do Código Civil).

7.8. Responsabilidade demonstrada

O artigo 20 das Normas[33] estabelece o princípio de responsabilidade («accountability»). A norma prevê que o responsável implementará os mecanismos necessários para comprovar o cumprimento dos princípios e obrigações estabelecidos nas Normas, bem como prestar contas do tratamento dos dados pessoais em sua posse ao titular e à autoridade de controle, para o qual poderá recorrer a normas, melhores práticas nacionais ou internacionais, esquemas de autorregulação, sistemas de certificação ou qualquer outro mecanismo que considere adequado para tais fins.

32. A estipulação ou contrato em favor de um terceiro é um acordo pelo qual uma parte (chamada de promotor) se compromete a outra (a parte estipuladora) a dar algo a um terceiro (ou beneficiário) ou a fazer ou não fazer algo em favor do terceiro, que, embora não seja parte do contrato, adquire os direitos nele mencionados.

33. Artigo 20 das Normas de Proteção de Dados Pessoais dos Estados Ibero-americanos (2017).

Os mecanismos que uma parte do contrato pode adotar para cumprir com o princípio da responsabilidade comprovada incluem, mas não estão limitados a, o seguinte:

a. Alocar recursos para a implementação de programas e políticas de proteção de dados pessoais.
b. Implementar sistemas de gestão de risco associados ao tratamento de dados pessoais.
c. Desenvolver políticas e programas obrigatórios e executáveis de proteção de dados pessoais dentro da organização do Importador.
d. Implementar um programa de treinamento e atualização para o pessoal sobre as obrigações de proteção de dados pessoais.
e. Revisar periodicamente as políticas e programas de segurança de dados pessoais para determinar quaisquer modificações necessárias.
f. Estabelecer um sistema de supervisão e vigilância interno e/ou externo, incluindo auditorias, para verificar o cumprimento das políticas de proteção de dados pessoais.
g. Estabelecer procedimentos para receber e responder a dúvidas e reclamações dos proprietários.

O anterior se aplicará quando os dados pessoais forem processados por um Processador em nome e por conta do Responsável, bem como na realização da TIDP. O regulamento acima mencionado lista uma série de mecanismos que tanto o Responsável quanto o Processador, conforme o caso, devem ser implementados. Este princípio de responsabilidade demonstrada também se aplica a transferências internacionais de dados pessoais.

No mesmo sentido, a CCM estabelece que as partes devem ser capazes de demonstrar o cumprimento das cláusulas contratuais padrão. Em particular, a CCM exige que o importador de dados mantenha a documentação correspondente às atividades de tratamento sob sua responsabilidade e informe o Exportador de Dados caso, por qualquer motivo, não possa cumprir as cláusulas.

7.9. Impossibilidade de conformidade do Importador

O Importador de Dados deve informar o Exportador de Dados se, após ter entrado na CCM, tiver motivos para acreditar que não poderá cumprir as cláusulas contratuais padrão. Se o Exportador de Dados receber tal comunicação ou descobrir que o Importador de Dados não pode mais cumprir as cláusulas contratuais padrão, ele deverá determinar as medidas adequadas para lidar com a situação, consultando, se for o caso, a autoridade supervisora competente.

As referidas medidas podem consistir em medidas complementares adotadas pelo Exportador e/ou Importador de dados, tais como medidas administrativas, físicas e técnicas para garantir segurança e confidencialidade. Também pode exigir que o Exportador de Dados suspenda a transferência se considerar que não há garantias adequadas ou se assim for ordenado pela Autoridade de Controle competente. Este poder está expressamente previsto na CCM.

***

Glossário do Guia

Anonimização: la aplicação de medidas de qualquer natureza destinadas a evitar a identificação ou reidentificação de uma pessoa física sem esforço desproporcional.

Autoridade de controle competente: Autoridade de proteção de dados pessoais do país do Exportador ou Importador de dados pessoais.

Computação em nuvem: modelo para permitir o acesso a um conjunto de serviços de computação (ex. redes, servidores, armazenamento, aplicativos e serviços) de forma conveniente e sob demanda, que podem ser rapidamente provisionados e liberados com esforço administrativo e interação com o provedor de serviços

Consentimento: expressão livre, específica, inequívoca e informada da vontade do proprietário, através da qual ele aceita e autoriza o tratamento dos dados pessoais que lhe digam respeito.

Dados Pessoais: qualquer informação relativa a uma pessoa singular identificada ou identificável, expressa em forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica ou qualquer outra. Uma pessoa é considerada identificável quando sua identidade pode ser determinada direta ou indiretamente, desde que isso não exija tempo ou atividades desproporcionais.

Dados pessoais sensíveis: aqueles que se referem à esfera íntima do seu titular, ou cujo uso indevido pode dar origem a discriminação ou acarretar um risco grave para o mesmo. A título de exemplo, dados pessoais que possam revelar aspectos como origem racial ou étnica são considerados sensíveis; crenças ou convicções religiosas, filosóficas e morais; filiação sindical; opiniões políticas; dados relativos à saúde, vida, preferência ou orientação sexual, dados genéticos ou dados biométricos destinados a identificar de forma inequívoca uma pessoa singular.

Decisões individuais automatizadas: Decisões que produzem efeitos legais sobre o envolvido ou que o afetam significativamente e que se baseiam unicamente em um tratamento automatizado destinado a avaliar, sem intervenção humana, certos aspectos pessoais relacionados a ele ou a analisar ou prever, em particular, seu desempenho profissional, situação financeira, estado de saúde, preferências sexuais, confiabilidade ou comportamento

Processador: um prestador de serviços que, como pessoa física ou jurídica ou autoridade pública, fora da organização do Responsável, processa dados pessoais em nome e por conta deste.

Padrões: Normas de Proteção de Dados Pessoais para Estados Ibero-americanos aprovadas pela RIPD em 2017.

Exportador de dados: pessoa física ou jurídica de natureza privada, autoridade pública, serviços, órgão ou prestador de serviços situado no território de um Estado que realiza transferências internacionais de dados pessoais, de acordo com o disposto nestas Normas.

Importador de dados: pessoa física ou jurídica privada, autoridade pública, serviços, órgão ou prestador de serviços localizado em um país terceiro que recebe dados pessoais de um Exportador de Dados por meio de transferência internacional de dados pessoais.

Lei Aplicável: é a lei de proteção de dados pessoais da jurisdição do Exportador de Dados.

Medidas administrativas, físicas e técnicas: medidas destinadas a evitar danos, perda, alteração, destruição, acesso e, em geral, qualquer uso ilícito ou não autorizado de Dados Pessoais, mesmo que ocorra acidentalmente, suficiente para garantir a confidencialidade, integridade e disponibilidade dos Dados Pessoais.

Responsável: pessoa singular ou coletiva de natureza privada, autoridade pública, serviços ou organismo que, isoladamente ou em conjunto com outros, determina as finalidades, meios, âmbito e outras questões relacionadas com o tratamento de dados pessoais.

Sub-processador: quando um Processador usa outro Processador para realizar determinadas atividades de tratamento em nome do Responsável..

Beneficiários de terceiros: Titular cujos dados pessoais são objeto de transferência internacional nos termos deste Contrato. O Titular é terceiro beneficiário dos direitos previstos a seu favor na CCM e, portanto, pode exercer os direitos que a CCM reconhece, ainda que não tenha sido celebrado o modelo de contrato entre as partes.

Titular: pessoa singular a quem os dados pessoais dizem respeito.

Transferência subsequente: Transferência de dados feita pelo Importador de Dados para um terceiro localizado fora da jurisdição do Exportador de Dados que cumpra as garantias estabelecidas na CCM.

Processamento: qualquer operação ou conjunto de operações realizadas por meio de procedimentos físicos ou automatizados sobre dados pessoais, relacionados, mas não limitados a obtenção, acesso, registro, registro, organização, estruturação, adaptação, indexação, modificação, extração, consulta, armazenamento, conservação, processamento, transferência, divulgação, posse, exploração e, em geral, qualquer uso ou descarte de dados pessoais.

Violação da segurança de dados pessoais: qualquer dano, perda, alteração, destruição, acesso e, em geral, qualquer uso ilícito ou não autorizado de dados pessoais, mesmo que ocorra acidentalmente.

Acrônimos usados

APD *Autoridade de Proteção de Dados ou Autoridade de Controle.*

Padrões *Padrões de Proteção de Dados Pessoais para Estados Ibero-Americanos aprovados pela RIPD em 2017.*

CEN *Computação em Nuvem.*

CIJ *Comissão Jurídica Interamericana.*

CCM *Cláusulas contratuais modelo.*

OEA *Organização dos Estados Americanos.*

NCV *Regras corporativas vinculantes.*

RGPD *Regulamento Geral de Proteção de Dados ou REGULAMENTO RGPD (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 relativo à proteção de pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e diretiva revogatória 95/46/CE.*

RIPD *Rede Ibero-Americana de Proteção de Dados.*

PSCEN *Provedor de serviços de computação em nuvem*

TDP *Tratamento de dados pessoais.*

TIDP *Transferência internacional de dados pessoais.*

UE *União Europeia.*

Documentos consultados

Referências de países *(ordem alfabética)*

Argentina

- Lei 25.326, Art. 12 lei n. 25.326 de proteção de dados pessoais, art. 12 do decreto regulamentar n. 1558/2001
- Disposição 60/2016 da Direção Nacional de Proteção de Dados Pessoais. Disponível em http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/texact.htm

Brasil

- Arts. 33 a 35 da LGPD.

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm

Cabo Verde

- Art. 20, Lei n.º 41/VIII/2013, de 17 de setembro, sobre a Proteção de Dados Pessoais de Pessoas Naturais.

www.redipd.org/sites/default/files/2020-03/Lei-n-41-VIII-2013-regime-juridico-geral-de-proteccao-de-dados-pessoais-das-pessoas-singulares.pdf

Colombia

- Lei Estatutária 1.581 de 2012 (artigo 26)
- Decreto 1377 de 2013 (artigo 25. contrato de transmissão de dados pessoais)
- Decreto 255 de 2022 (Regras Corporativas Vinculantes)
- Superintendência de Indústria e Comércio (2019-2021) Guia para a implementação do princípio da responsabilidade demonstrada nas transferências internacionais de dados pessoais. Disponível em https://www.sic.gov.co/sites/default/files/files/2021/2021%20Gu%C3%ADas%20para%20implementaci%C3%B3n%20del%20principio%20de%20responsabilidad%20demostrada%202021.pdf
- Superintendência de Indústria e Comércio (2015) Guia para a Implementação do Princípio da Responsabilidade Demonstrada (Accountability). Disponível em https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf

Ecuador

- Arts. 55 a 61 da Lei Orgânica de Proteção de Dados Pessoais. https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf

México

- Arts. 36 e 37 da Lei Federal de Proteção de Dados Pessoais de Titularidade Privada (Publicada no Diário Oficial da Federação em 5 de julho de 2010, disponível no seguinte link eletrônico: http://dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=07/05/2010, sem reformas; texto consolidado em formato de documento portátil, pdf por sua sigla em inglês, pela Câmara dos Deputados de H. Congresso da União, no seguinte link eletrônico: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf.).
- Arts. 67 a 76 do Regulamento da Lei Federal de Proteção de Dados Pessoais de Particulares (Publicado no Diário Oficial da Federação em 21 de dezembro de 2011, disponível no seguinte link eletrônico: http://dof.gob. mx/nota_detalle.php?codigo=5226005&fecha=21/12/2011; sem reformas; texto consolidado em formato de documento portátil, pdf por sua sigla em inglês, pela Câmara dos Deputados do H. Congresso da União, disponível no seguinte link: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf; links consultados pela última vez em 06/10/2021).
- Arts. 65 a 71 da Lei Geral de Proteção de Dados Pessoais de Titulares de Obrigações (Publicada no Diário Oficial da Federação em 26 de janeiro de 2017, disponível no seguinte link eletrônico: http://dof.gob.mx/ nota_detalle.php?codigo=5469949&fecha=01/26/2017, sem reformas; texto consolidado em formato de documento portátil, pdf por sua sigla em inglês, pela Câmara dos Deputados do H. Congresso da União, no seguinte link: http://www.diputa-

dos.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf).

- Artigos 108 a 118 das Diretrizes Gerais para a Proteção de Dados Pessoais do Setor Público (Publicado no Diário Oficial da Federação em 26 de janeiro de 2018, disponível nos seguintes links eletrônicos: https://www.dof.gob. mx /nota_detalle.php?codigo=5511540&fecha=26/01/2018 e http://inicio.inai.org.mx/AcuerdosDelPleno/ACT-PUB-19-12-2017.10.pdf, modificado pela última vez em 25 de novembro de 2020, disponível no link eletrônico https://www.dof.gob.mx/nota_detalle.php?codigo=5605789&fecha=25/11/2020, www.dof.gob.mx/2020/INAI/ACT-PUB-11 -11 -2020-05.pdf, https://home.inai.org.mx/wp-content/documentos/AcuerdosDelPleno/ACT-PUB-11-11-2020.05.pdf).

Nota: As disposições legais específicas sobre transferências são incorporadas, entretanto, a fim de fornecer o contexto completo dos requisitos de transferência para a proteção de dados pessoais, a referência deve ser expandida com artigos adicionais e regulamentos complementares.

Nicaragua

- Art.14 da Lei nº 787, Lei de Proteção de Dados Pessoais.

http://legislacion.asamblea.gob.ni/Normaweb.nsf/xpNorma.xsp?documentId=E5D37E9B4827FC06062579ED0076CE-1D&action=openDocument

Nueva Zelanda

- Comissário de Privacidade da Nova Zelândia, Cláusulas de contrato modelo para envio de informações pessoais para o exterior. Disponível em https://www.privacy.org.nz/responsibilities/disclosing-personal-information-outside-new-zealand/

Panamá

- Arts. 5º e 33º, Lei nº 81, de 26 de março de 2019, de Proteção de Dados Pessoais.
- Arts. 51 a 53 do Decreto Executivo nº. 285 de 18 de maio de 2021, (disponível em https://www.gacetaoficial.gob.pa/pdfTemp/29296_A/GacetaNo_29296a_20210528.pdf).

Perú

- Artigo 15 da Lei nº 29.733. Lei de Proteção de Dados Pessoais. Publicado em julho de 2011.

https://www.redipd.org/sites/default/files/inline-files/Ley-29733.pdf

República Democrática de Santo Tomé y Príncipe

- Arts. 19 e 20, Lei 3/2016, de 2 de maio, Proteção de Dados Pessoais de Pessoas Naturais.

https://www.redipd.org/sites/default/files/2020-03/lei-3-2016-proteccao-de-dados-pessoais.pdf

República Dominicana

- Art. 80 da Lei nº 172-13, de 13 de dezembro de 2013, de Proteção de Dados Pessoais.

https://indotel.gob.do/media/6200/ley_172_13.pdf

Reino Unido

- Cláusulas Contratuais Padrão (SCCs) após o término do período de transição, disponíveis em https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/sccs-after-transition-period/
- Cláusulas contratuais padrão do Reino Unido https://ico.org.uk/media/for-organisations/documents/2620100/uk-sccs-c-p-202107.docx

Uruguay

- Art. 23 da Lei nº 18.331 de Proteção de Dados Pessoais
- Resolução nº 4/019, de 12 de março de 2019.
- Resolução nº 41/021, de 8 de setembro de 2021. Disponível em https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/noticias/cambios-regimen-transferencias-internacionales-datos-uruguay

Referências de algumas organizações

(ordem alfabética)

Concelho Europeu

Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows. (Protocolo Adicional à Convenção para a Proteção das Pessoas no que diz respeito ao Processamento Automático de Dados Pessoais relativo às autoridades de supervisão e fluxos de dados transfronteiriços).

Comitê Europeu de Proteção de Dados (EDPB)

Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Adopted on 10 November 2020. (Recomendações 01/2020 sobre medidas que complementam as ferramentas de transferência para garantir o cumprimento do nível de proteção de dados pessoais da UE Adotada em 10 de novembro de 2020). Disponível em https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

MERCOSUL

MERCOSUR/CMC/DEC. Nº 15/20, disponível em https://normas.mercosur.int/public/normativas/4018 e https://normas.mercosur.int/simfiles/normativas/82753_DEC_015-2020_ES_Acuerdo%20Comercio%20Electronico.pdf

Organização dos Estados Americanos

OEA, Princípios atualizados sobre privacidade e proteção de dados pessoais, com anotações (CJI/RES. 266 (XCVI-II-O/21)). http://www.oas.org/es/sla/ddi/proteccion_datos_personales_Trabajos_Actuales_CJI.asp

Rede Ibero-Americana de Proteção de Dados

Rede Ibero-Americana de Proteção de Dados -RIPD- (2017). Normas de proteção de dados pessoais para os Estados Ibero-americanos. Disponível em: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

RIPD, Declaração de Cartagena das Índias, maio de 2004, ponto III - "Transferências internacionais de dados. Perspectivas Europeias e Ibero-Americanas" em https://www.redipd.org/sites/default/files/inline-files/declaracion_2004_III_encuentro_es.pdf

RIPD, XVIII Encontro Ibero-Americano de Proteção de Dados, https://www.redipd.org/sites/default/files/2020-12/declaracion-final-xviii-encuentro.pdf

RIPD, Regulamento da Rede Ibero-Americana de Dados Pessoais, https://www.redipd.org/sites/default/files/2019-11/reglamento-ripd.pdf

União Europeia

Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (DO L 281 de 23.11.1995, pág. 31). Disponível em https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=O-J%3AL%3A1995%3A281%3ATOC

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/ 46/CE, DO L 119 de 4.5.2016, p. 1. Disponível em https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC

DECISIÓN DE EJECUCIÓN (UE) 2021/914 DE LA COMISIÓN de 4 de junio de 2021 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo. Disponibles en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CE-LEX:32021D0914&from=EN#ntr2-L_2021199ES.01003701-E0002

Decisión 2001/497/CE de la Comisión, de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la

Decisión 2010/87/UE de la Comisión, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ%3AL%3A2010%3A039%3ATOC

DECISIÓN DE EJECUCIÓN (UE) 2021/914 DE LA COMISIÓN de 4 de junio de 2021 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:-32021D0914&from=EN#ntr2-L_2021199ES.01003701-E0002

Sentencia del Tribunal de Justicia de la UE, sentencia del 16 de julio de 2020 en el asunto C-311/18, Data Protection Commissioner/Facebook Ireland Ltd y Maximillian Schrems (“Schrems II”), ECLI:EU:C:2020:559.