RED IBEROAMERICANA DE PROTECCION DE DATOS

IMPLEMENTATION GUIDE

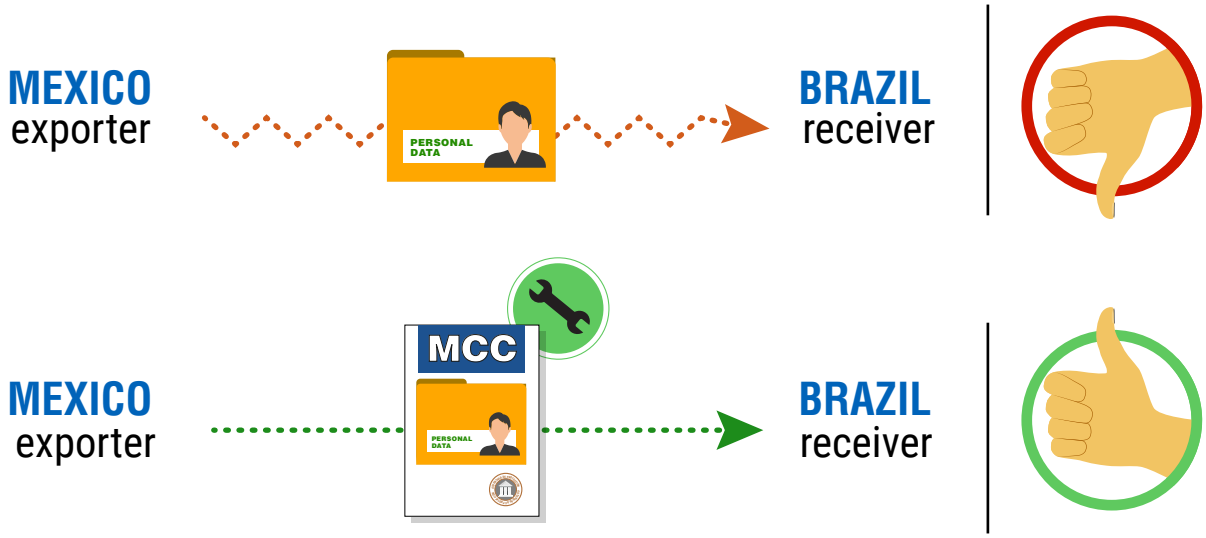
ON MODEL CONTRACT CLAUSES FOR INTERNATIONAL PERSONAL DATA TRANSFERS *(IPDT)*

Index

1. Introduction

The use of contractual clauses is an alternative for international personal data transfers. In this sense, Paragraph c) of Subsection 1 of Article 36 of the Personal Data Protection Standards for the Ibero-American States of the Ibero-American Data Protection Network (IDPN) states that "The party responsible may carry out international personal data transfers in any of the following cases: … c. The exporter and recipient enter into contractual clauses or any other legal instrument that offer sufficient guarantees and demonstrate the scope of personal data processing, the obligations and responsibilities assumed by the parties, and the rights of the Data Subjects. The Supervisory Authority may validate any contractual clauses or legal instruments on the matter, as determined in the applicable national legislation of the Ibero-American States."

In line with the above, this guide seeks to establish the main aspects to be considered when making international personal data transfers (hereinafter, IPDT) by using model contract clauses (hereinafter, MCC). As such, this guide presents some guidelines to be considered by the parties who must carry out IPDTs to inappropriate jurisdictions from the member countries of the Ibero-American Data Protection Network (IDPN).



Similarly, there are no MCC approved jointly in Latin America at the regional level. For this reason, the IDPN presents two versions of an international transfer model contract as an annex to this Guide, one for transfers between Responsible Parties, and another for transfers from Responsible Parties to Processors. These two models are considered to be an initial step, and additional model contracts are expected to be drawn up subsequently for transfers from Controller to Controller and Controller to Recipient.

The substantial content of both models follows the guidelines set forth in the Personal Data Protection Standards for the Ibero-American States of the IDPN[1] ("Standards").

The MCC proposed in the Annex are also similar in their structuring to the recent standard contractual clauses for the transfer of personal data to third countries approved in June 2021 by the European Commission ("UE")[2] since they contain similar elements and principles in essence.

2. Clarifications and limitations

This Guide is complementary to the recommendations, documents, and regulations in force in each Ibero-American country [3]. The data protection regulations applicable in the countries of Ibero-America contain specific IPDT-related provisions and several even include a provision on the use of contractual clauses. In some cases, specific contractual model clauses have been drawn up based on national legislation (see section 3.3. of this Guide).

This Guide does not replace national regulations, or the guidelines or criteria set forth by the different data protection authorities in the region in the exercise of their powers.

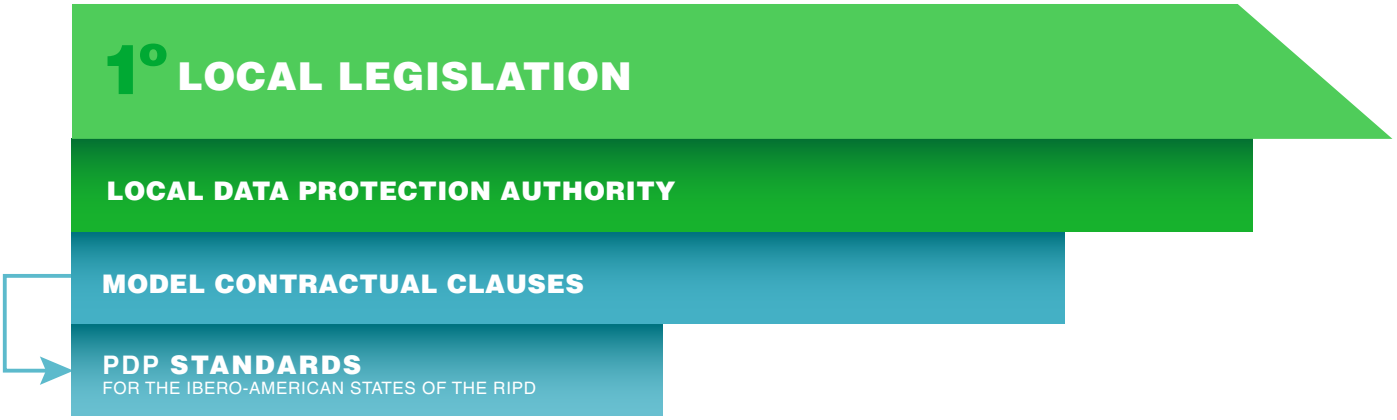
It is also worth noting that, in case of manifest contradiction between this document and any recommendation or guide from the national data protection authority, it is best to follow the recommendation of said authority, in the understanding that said entity has been entrusted to set the rules for effective IPDTs, in accordance with the applicable legislation.

1. Cfr. Ibero-American Data Protection Network -IDPN- (2017). Personal data protection standards for Ibero-American States. Available at: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

2. Cfr. IMPLEMENTATION DECISION (EU) 2021/914 of June 4, 2021 on standard contractual clauses for the transfer of personal data to third countries, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council. Available at: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:-32021D0914&from=EN#ntr2-L_2021199ES.01003701-E0002

3. Por ejemplo, ver las mencionadas en la sección de Documentos consultados de esta Guía.

In any case, the implementation of this Guide and the use of the two contractual models annexed to this Guide shall be in harmony with the recommendations, resolutions, and determinations of local data protection authorities and, above all, with the applicable local legislation.



To draw up[4] this document, as well as those of the MCCs, the Personal Data Protection Standards applicable to the Ibero-American States of the IDPN were taken as a reference[5] to establish the principles, terms, definitions, and obligations of the Controller and the Recipient and rights of Personal Data Subjects. The Guide and the MCCs do not transcribe verbatim all the aspects thereof, but rather took the principles set forth in the Standards as the source of all enforceable legal principles in the event of an IPDT. Therefore, this document must be read jointly and comprehensively with the aforementioned Standards, without prejudice to any eventual adaptations made at the national level.

This Guide is not a legal concept, nor an academic article, nor does it constitute legal advice of any kind. Neither is it intended to be an exhaustive list of specific recommendations because this is an internal matter to be decided by each organization in light of the objectives and the magnitude of each project involving the transfer of personal data to inappropriate jurisdictions.

4. The Ibero-American Data Protection Network (IDPN) appreciates the work undertaken by Pablo Palazzi in the preparation of this Guide and its annex. The IDPN published the previous version of this document for public comments. Comments and suggestions were received and analyzed from the following people and organizations, whom we wish to thank for their participation: (1) EDPS (European Data Protection Supervisor); (2) APEP (Spanish Professional Association of Privacy); (3) Gustavo Parra (Institute of Transparency, Access to Public Information, and Personal Data Protection of the State of Mexico and Municipalities); (4) The Latin American Internet Association (ALAI), (5) Daniel Bulnes; (6) MX Internet Association; (7) Professor Lourdes Zamudio; (8) Equifax.

5. Cfr. Ibero-American Data Protection Network -IDPN- (2017). Personal data protection standards for Ibero-American States. Available at: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

3. IPDT Background

3.1. International background

The European Union Data Protection Directive of 1995[6] was the first to implement IPDT-related rules at the level of a European community law. The aforementioned Directive has been repealed and replaced by Regulation (EU) 2016/679 of the European Parliament and of the Council, dated April 27, 2016, on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter, General Data Protection Regulation, GDPR)[7].

Chapter 5 of the GDPR contains a detailed regulation on international personal data transfers (Art. 44 to 50, GDPR). Art. 46 Section 2 of the GDPR allows for IPDT when adequate guarantees are adopted, such as the standard data protection clauses approved by the European Commission or by some Supervisory Authority.

By means of Commission Decision 2001/497/EC[8] and then by Decision 2010/87/EU of the European Commission[9], two separate models containing standard contractual clauses were approved to facilitate the transfer of personal data by a Controller established in the EU to another Controller or Processor established in a third country that does not offer an adequate level of protection.

The standard contractual clauses of the aforementioned Decisions were updated in June 2021 to adapt them to the GDPR, a process that underwent public consultation[10]. The new decision[11] approves a more complete model adapted to the regulatory changes and the new ways of processing personal data.

It is also appropriate to mention the "MERCOSUR Electronic Commerce Agreement"[12] (binding for the Republic of

6. Directive 95/46/CE of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (DO L 281 of 23.11.1995, p.31). Available at: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ%3AL%3A1995%3A281%3ATOC

7. Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, DO L 119 of 4.5.2016, p. 1. Available at: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC

8. Commission Decision 2001/497/EC of June 15, 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC. Available at: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ%3AL%3A2001%3A181%3ATOC

9. Commission Decision 2010/87/EU of the Commission of February 5, 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council. Available at: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ%3AL%3A2010%3A039%3ATOC

10. These new contractual clauses received comments, contributions, and suggestions from the entire international community, and their text reflects the most relevant international standards, including the latest jurisprudential developments on the matter.

11. (EU) COMMISSION IMPLEMENTING DECISION) 2021/914 of June 4, 2021 on standard contractual clauses for the transfer of personal data to third countries in accordance with (EU) Regulation 2016/679 of the European Parliament and of the Council. Available at: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32021D0914&from=EN#ntr2-L_2021199ES.01003701-E0002

12. See MERCOSUR/CMC/DEC. No. 15/20, available at: https://normas.mercosur.int/public/normativas/4018 y https://normas.mercosur.int/simfiles/normativas/82753_DEC_015-2020_ES_Acuerdo%20Comercio%20Electronico.pdf

Argentina, the Federative Republic of Brazil, the Republic of Paraguay, and the Eastern Republic of Uruguay) entered into on January 28, 2021.

Art. 6.2 of the aforementioned Agreement states that the parties must adopt or maintain laws, regulations, or administrative measures to protect the personal information of users involved in electronic commerce. For such purposes, they shall take the international standards available on this matter into consideration.

Also, Art. 6.7 of the Agreement establishes that the parties agree to apply an adequate level of protection to the personal data received from another Party by means of a general rule or specific autonomous regulation, or by mutual, general, or specific agreements, or in broader international frameworks, admitting the implementation of contracts or self-regulation by the private sector.

Art. 7 of the MERCOSUR regulation sets forth the principle of non-discrimination in matters of international personal data transfers.

On April 9, 2021, the Inter-American Juridical Committee of the Organization of American States approved the Updated Principles on Privacy and the Protection of Personal Data[13].

Principle No. 11 on Cross-Border Data Flows provides as follows: "Recognizing its value for economic and social development, Member States should cooperate with each other to facilitate the cross-border flow of personal data to other States whenever they provide an adequate level of data protection, in accordance with these Principles. Member States should similarly cooperate in the creation of mechanisms and procedures that allow data processing controllers and processors operating in more than one jurisdiction or transmitting them to a jurisdiction other than their own, to guarantee and be effectively made accountable for compliance with these Principles."

On the other hand, Convention No. 108 of the European Council, with the modifications of the 2001 Protocol[14] establishes in its Art. 2 entitled "Transfer of personal data to Processors not subject to the jurisdiction of the Parties to the Convention" that "Each Party shall ensure that the transfer of personal data to a recipient subject to the jurisdiction of a State or organization that is not a Party to the Convention takes place only if said State or organization ensures an adequate level of protection."

For its part, Art. 2.2 states that "Paragraph 1 of Article 2 of this Protocol shall not apply, and the Parties may authorize the transfer of personal data: … b) if sufficient guarantees are provided, which may arise, particularly, from contractual clauses, by the data controller responsible for the transfer, and said guarantees are deemed adequate by the competent authorities in accordance with national law."

13. OEA, Principios Actualizados sobre la Privacidad y la Protección de Datos Personales, con Anotaciones (CJI/RES. 266 (XCVIII-O/21)). http://www.oas.org/es/sla/ddi/proteccion_datos_personales_Trabajos_Actuales_CJI.asp

14. Available at: https://rm.coe.int/1680080626

3.2. Ibero-American Data Protection Network

The IDPN, based on Article 1, subparagraph a) of the Regulations of the Ibero-American Personal Data Network, and with the purpose of developing and adopting regulations that guarantee the right to data protection and privacy in the countries of the region, has been concerned with the legal regulation of IPDTs since their inception. Thus, within the framework of the III Ibero-American Data Protection Meeting held in Cartagena de Indias (Colombia) in 2004[15] the members of the IDPN issued various conclusions evincing their concern about IPDTs.

In that meeting, the members of the IDPN concluded that "The international transfer of personal data must be subject to a system of guarantees to prevent the principles governing the fundamental right to data protection from being violated by the mere transfer of said data to another country. The European Union Data Protection Directive has enshrined this principle and has given the European Commission the power to decide whether a country that has established data protection legislation in accordance with European standards and that has created an independent Supervisory Authority is a secure destination for the personal data originating from EU Member States."

In the same document, the members of the IDPN clarified as follows: "Should this recognition not exist, standard contractual clauses may be used, among other options, […] The use thereof allows the establishment of the necessary guarantees to make up for the lack of adequate legislation in the country of destination by granting the Data Subjects whose data is being transferred the possibility of demanding compliance with the contract clauses that affect them, as well as reparation in the event that any breach thereof causes damages to them."

The Declaration of Cartagena de Indias concludes by noting as follows: "For this reason, the participants in the III Ibero-American Data Protection Meeting hope that Ibero-American countries enact data protection regulations and establish independent control mechanisms to promote the effective implementation of the fundamental right to data protection and, at the same time, to facilitate the free flow of personal data between countries."

Within the framework of the XVIII Ibero-American Data Protection Meeting[16] held online on December 4, 2020 in Montevideo (Uruguay), the members of the IDPN stated in their Final Declaration (conclusion section 7) that "[…] the processing of personal data as a driver of the global economy requires **clear and transparent rules to allow secure international data flows** based on the level of protection provided by the countries or organizations that are the recipients of said flows, in international treaties, or in contractual regulations between issuers and receivers, that guarantee the validity of data protection principles, the exercise of rights by the Data Subjects, and the fulfillment of the obligations of controllers, processors, and other third parties."

15. IDPN, Declaration of Cartagena de Indias, May 2004, section III - "International data transfers. European and Ibero-American perspectives" at https://www.redipd.org/sites/default/files/inline-files/declaracion_2004_III_encuentro_es.pdf

16. IDPN, XVIII Ibero-American Data Protection Meeting, https://www.redipd.org/sites/default/files/2020-12/declaracion-final-xviii-encuentro.pdf

In conclusion, it is natural that in the development of documents additional to the Standards and Declarations of the IDPN, guides and models are sought after to facilitate the free flow of data, while maintaining adequate protection of personal data, such as the MCC or binding corporate codes.

In 2017, the members of the IDPN approved the Personal Data Protection Standards for Ibero-American States.

The Ibero-American Standards lay out a set of common personal data protection principles and rights that Ibero-American States can adopt and develop in their national legislation to ensure homogeneous rules in the region. On the other hand, the Ibero-American Standards include the best national and international practices on the matter at their time of enactment. The objectives of the Ibero-American Standards include the following, which in some way justify the adoption of MCCs for the region: (i) ease the flow of personal data between Ibero-American States and beyond their borders, in order to contribute to the economic and social growth of the region, and (ii) favor international cooperation between the control authorities of the Ibero-American States, with other control authorities outside the region, and with related international authorities and organizations.

Art. 36, subparagraph. 1, letter "c" of the Standards states that "Controllers and processors may carry out international personal data transfers in any of the following cases: … c. The exporter and recipient **sign contractual clauses or any other legal instrument that offers sufficient guarantees** and that conveys the scope of personal data processing, the obligations and responsibilities assumed by the parties, and the rights of the Data Subjects. The Supervisory Authority may validate any contractual clauses or legal instruments on the matter, as determined in the applicable national legislation of the Ibero-American States."

The following emerges from the Ibero-American Standards:
+ The Exporter and the Importer can enter into contractual clauses.
+ These contractual clauses must offer sufficient guarantees to convey: (i) the scope of personal data processing, (ii) the obligations and responsibilities assumed by the parties, and (iii) the rights of the Data Subjects.
+ The respective Supervisory Authority may validate contractual clauses or legal instruments as determined in the applicable national legislation of the Ibero-American States.

3.3. Ibero-American IPDT Regulations

In accordance with the aforementioned international regulations and with the Standards, a large number of Ibero-American countries regulate international personal data transfers, in the absence of continuity in the level of protection.

This is the case for the following countries:

Argentina (Art. 12 of Law No. 25.326 on the protection of personal data, Art. 12 of Regulatory Decree No. 1558/2001, and Provision 60).
Brazil (Art. 33 to 35 of the General Data Protection Law).
Cape Verde (Art. 20, Law No. 41/VIII/2013, of September 17, on the Protection of Personal Data).
Colombia (Art. 26 of Law 1581 of 2012).
Ecuador (Art. 55 to 61 of the Organic Law on the Protection of Personal Data).
Mexico (Art. 65-71 of the General Law on the Protection of Personal Data Held by Obliged Entities and Art. 36 and 37 of the Federal Law on the Protection of Personal Data Held by Private Parties).

Nicaragua (Art.14 of Law No. 787, Personal Data Protection Law).
Panama (Art. 5 and 33, Law No. 81 of March 26, 2019 on the Protection of Personal Data and Art. 51 to 53 of Executive Decree No. 285 of May 28, 2021).
Peru (Art. 11 and 15 of Law 29.733, Personal Data Protection Law).
Democratic Republic of São Tomé and Príncipe (Art. 19 and 20, Law 3/2016 of May 2 on the Protection of Personal Data of Natural Persons).
Dominican Republic (Art. 80 of Law No. 172-13 of December 13, 2013 on the Protection of Personal Data).
Uruguay (Art. 23 of Law No. 18.331 on the Protection of Personal Data, Resolution No. 4/019 of March 12, 2019, and Resolution No. 41/021 of September 8, 2021).

Most of the aforementioned legislations also establish certain exceptions to allow IPDTs to unsuitable destinations (when there are international treaties, for example). On the other hand, it is also possible to resort to other tools for international transfer. For example, the regulations of Argentina, Colombia[17], Mexico[18], Panama[19], Peru[20] and Uruguay contemplate or recommend the possibility of using MCCs.

For their part, some data protection authorities, such as Uruguay and Argentina, have issued regulations approving MCC guidelines or models[21].

17. Colombia: In its updated version of 2021, the Guide issued by the Colombian authority for the protection of personal data provides guidelines on IPDTs and the use of MCCs. See Colombia, SIC, Guide for implementing the principle of accountability in international personal data transfers, p. 17, which recommends the use of contractual clauses for IPDTs as a way of demonstrating accountability by the personal data Processor. Available at: 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

18. Mexico, Article 75 of the Federal Law on the Protection of Personal Data Held by Private Parties (LFPDPPP, by its Spanish acronym) suggests using contractual clauses, as follows: "For this purpose, controllers who transfer personal data may use contractual clauses or other legal instruments containing at least the same obligations applicable to controllers transferring personal data, as well as the conditions under which the Data Subject consented to the processing of their personal data. On the other hand, Article 66 of the General Law on the Protection of Personal Data held by Obliged Entities, which establishes that "Any transfer shall be formalized by signing contractual clauses, collaboration agreements, or any other legal instrument, in accordance with the regulations applicable to the controller, to demonstrate the scope of personal data processing, as well as the obligations and responsibilities assumed by the parties." It is worth clarifying that, in Mexico, there is a Law applicable to individuals and another to Obliged Subjects, which are specifically all institutions of a public nature.

19. Panama, Art. 53 subparagraph 2 of Executive Decree No. 285 of May 18, 2021. Available at: https://www.gacetaoficial.gob.pa/pdfTemp/29296_A/GacetaNo_29296a_20210528.pdf

20. Peru, Article 25 of the Regulations of the LPDP (Personal Data Protection Law) also considers contractual clauses by stating that "... the issuer or exporter may use contractual clauses or other legal instruments that establish at least the same obligations to which they are subject, as well as the conditions under which the Data Subject consented to the processing of their personal data.

21. Uruguay: Resolution No. 41/021 of September 8, 2021. Available at: https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/noticias/cambios-regimen-transferencias-internacionales-datos-uruguay y Argentina: Provision 60/2016 of the National Directorate for Personal Data Protection. Available at: http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/texact.htm

4. Main IPDT stakeholders

Below are the main stakeholders involved in IPDTs. This helps understand the interest of each party in an IPDT.

IPDTs take place in a large number of situations such as: bank transfers, airline and hotel reservations, cloud computing services, centralization of human resources, traditional foreign trade operations, and electronic commerce, among many others.

In the typical scenario of an IPDT (whatever the reason), the following elements and stakeholders are involved:

+ An entity that wants to send data abroad known as: **Data exporter.**
+ An entity that wants to receive those data known as: **Data importer**, located in another jurisdiction.
+ The Importer receives the data to process them for a certain purpose. But the IPDT is in itself data processing: based on the assumption that any international personal data transfer (IPDT) implies data processing according to the definition established by the Standards[22].
+ The **Personal Data Subject** is the "natural person to whom the personal data concerns"[23] whose information must be treated properly. All the rights of the Data Subject must be guaranteed when data processing undergoes an IPDT to a jurisdiction classified as inadequate. In the case of the Standards, the rights to be guaranteed are mentioned in Articles 24 to 32. One way to guarantee these rights is by using MCCs.
+ In turn, the Data Subject is a **Third Party Beneficiary** in the MCCs. This means that the Data Subject has rights deriving not only from the personal data protection law of the Data Exporter's jurisdiction, but also from the international transfer contract entered into between the parties (see section 7 of this Guide).
+ An **inadequate jurisdiction** where the Data Importer is located. This jurisdiction is characterized as inadequate for the purposes of the IPDT according to the regulations of the Data Exporter's country or the interpretation of the competent Authority. The lack of adequacy of the destination jurisdiction forces the parties to adopt safeguards that provide adequate guarantees to protect the data subject to the IPDT, for example, by signing MCCs.
+ The Data Protection Authority (Supervisory Authority)[24] must ensure that the parties who conduct IPDTs do so in adherence with the regulations on said subject.
+ **Applicable Law:** The regulations on international data transfers or "cross-border data flows" seek to ensure that the level of protection of the personal data of the citizens of a country does not diminish or disappear when exported or transferred to another country or to other countries[25]. Given the need to protect the personal data transferred to an inappropriate jurisdiction, it is necessary that they be subject to a level of protection similar to the one at the time of collection.

22. Cfr. Letter i of Art. 2 of the Personal Data Protection Standards for Ibero-American States (2017).

23. Cfr. Letter h) of Article 2.1 of the Personal Data Protection Standards for Ibero-American States (2017).

24. Chapter VII of the Standards establishes the main aspects of data protection control and supervision authorities.

25. See IDPN, Recommendations for the processing of personal data by means of cloud computing services. Available at: https://www.redipd.org/sites/default/files/2021-06/recomendaciones-tratamiento-datos-personales-servicios-nube.pdf

Let us look at an example with the scenario of data processing through cloud computing services according to the relevant guidelines approved by the IDPN.

In April 2020, the IDPN published the "Recommendations for the processing of personal data through cloud computing services"[26]. In this document, the IDPN concluded that the processing of personal data in the cloud may involve the international transfer of personal data[27]. The recommendations contain suggestions for cloud computing service providers (PSCEN, by its Spanish acronym) to provide their services while respecting the personal data rights of the Data Subjects and IPDT rules.

In its Recommendations, the IDPN states the following: "If the PSCEN data centers or storage equipment are located outside the country of the cloud computing service (CEN) contracting party, the personal data shall be sent or exported from a country to companies and PSCEN organizations located in a territory other than the sending country. This is a personal data exporting process."

26. See IDPN, Recommendations for the processing of personal data through cloud computing services. Available at: https://www.redipd.org/sites/default/files/2021-06/recomendaciones-tratamiento-datos-personales-servicios-nube.pdf

27. IDPN, Recommendations for the processing of personal data through cloud computing services, p. 15.

After this explanation, the document specifies as follows: “In this case, the cloud computing service contracting company shall be the Exporter and the PSCEN shall act as the recipient of said data export. The Standards define the Exporter as the “private natural or legal person, public authority, services, body, or service provider located in the territory of a State that carries out international personal data transfers, in accordance with the provisions of these Standards.” Thus, the cloud computing service contracting party must adhere to local rules on international data transfer.”

The aforementioned IDPN Recommendations conclude that “It is important that the cloud computing service contracting party is fully aware and, where appropriate, that it can accept or limit the countries in which the servers are going to be hosted, in addition to being informed of the adequate guarantees adopted.”

All this is explained by the IPDT: “International data transfer or “cross-border data flow” regulations seek to ensure that the level of protection of the personal data of the citizens of a country does not decrease or disappear when exported or transferred to another country or to other countries. This rule is known as the principle of data protection continuity, which is based on the fact that international data transfers must not affect the protection of the parties involved with regard to the processing of their personal data. The export of personal information cannot become a scenario that reduces the level of protection granted to the data Subject in the country from which the personal data is exported. These activities must not facilitate, allow, or tolerate the violation of the rights of individuals or the reduction of the guarantees available to them in the exporting country. In this sense, the international transfer rules applicable in the country of the could computing service contracting party must be complied with. In the case of the Standards, Article 36 establishes the alternatives allowed to export data.”

In the specific case analyzed, the cloud computing service contracting company shall be the Data Exporter and the PSCEN shall be the Data Importer. Both parties could sign a contract based on the MCC where the Data Importer acts as Processor using the respective MCC model.

5. General IPDT rule. Exceptions and most commonly used transfer mechanisms

5.1. General rule

The IPDT provisions in the data protection laws of the Ibero-American countries are intended to guarantee the continuity of the level of protection provided in their laws in the event of personal data transfer to a third country that is considered inadequate or that has a different level of personal data protection.

Countries may recognize other jurisdictions as "adequate" in relation to their personal data legislation depending on the level of protection guaranteed by the applicable legislation. By virtue of the general principle of prohibition of IPDTs, in the absence of a decision of adequacy or specific reference in the data exporting country, the Controller or the Processor can only transfer personal data to a third country if there are adequate guarantees and under the condition that the Data Subjects have enforceable rights and effective legal actions to protect their rights. Such guarantees can be provided, among other means, by binding corporate rules (BCR)[28] or by MCCs.

In general terms, a country is considered adequate when it has certain elements in its legal system to conclude that the personal data are adequately protected. For example, under European Union regulations, the following aspects are usually assessed to determine the level of adequacy:

- The "Rule of Law", the respect for human rights, and the fundamental rights in that legal system.
- Current personal data legislation, both general and sectoral.
- The security measures applied.
- The rules on onward personal data transfers to another third country or international organization applicable in that country.
- The rights granted to Personal Data Subjects through effective administrative resources and legal actions.
- The existence and effective operation of one or more independent control authorities in the third country.
- The international commitments adopted by the third country or other obligations derived from agreements or legally binding instruments, as well as from its participation in multilateral or regional systems, particularly in relation to the protection of personal data.
- The access of public authorities in the country of destination to the data transferred and, more generally, the regime of exceptions to the personal data protection rules applicable in the country of destination.

28. Binding corporate rules are one of the adequate guarantees recognized by the GDPR and which are defined as "the personal data protection policies assumed by a controller or processor established in the territory of a Member State for the transfer or set of transfers of personal data to a controller or processor in one or more third countries, within a business group or a group of companies engaged in a joint economic activity" (Art. 4. 20) GDPR).

5.2. Exceptions

Art. 36.2 of the Standards state that the national legislation of Ibero-American States applicable to the matter may expressly set limits on international personal data transfers for reasons of national security, public safety, protection of public health, protection of the rights and freedoms of third parties, as well as for matters of public interest.

Numerous regulations contain exceptions to the rule that prohibits IPDTs to inadequate countries or jurisdictions. The rules of Ibero-American jurisdictions mentioned in section 3.3 of this Guide contain individual exceptions based on the principles listed in the Standards. These exceptions include the consent of the Data Subject, public interest, the execution or conclusion of a contract, or the vital interests of stakeholders, among others.

An important aspect to bear in mind is that these exceptions to IPDTs cannot be applied continuously to all types of transfers, but rather, due to their exceptional nature, they must be used for a specific and concrete transfer.

5.3. Transfer mechanisms

Should the IPDT destination country not have an adequate recognized level of protection, then the IPDT can be carried out through a transfer mechanism that grants adequate guarantees, or by applying any of the exceptions provided for in local regulations.

The IPDT mechanisms that provide adequate guarantees are usually the following:

- Contractual model clauses (MCC).
- Binding corporate rules (BCR).
- Code of conduct approved in accordance with the applicable law.
- Certification mechanism.
- Legally binding and enforceable instruments between authorities or public entities.

The purpose of the MCCs is to ensure adequate data protection guarantees for international data transfers to jurisdictions that do not have an adequate recognized level of protection. The Data Exporter transferring the personal data to a third country and the Data Importer receiving the personal data can sign an agreement in order to guarantee the rights of the data subjects by means of the MCC.

Although the MCC should be used in principle for transfers to inadequate jurisdictions, the IDPN recommends the implementation thereof to all types of international transfers, where relevant, to ensure compliance with the principles of personal data protection.

Finally, it is important to point out that the use of MCCs does not imply, in all cases, full compliance with the personal data protection legislation or regulations in the jurisdictions affected by the transfer, in which case, the specific requirements would have to be met[29].

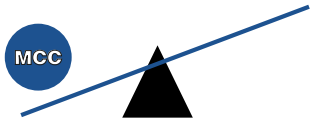
6. MCCs as a protection mechanism of IPDTs

6.1. Purpose of the MCCs

The purpose of the MCCs is to guarantee and facilitate compliance with the requirements provided by the data protection law of the Data Exporting country for the transfer of personal data to a third country that has not been recognized with an adequate level of protection. The idea is that the protection granted initially to the personal data remains in force regardless of where these data are located.

That is why onward Transfers are also regulated with precautions to avoid diminishing the level of protection. Data Subjects are granted intervention by means of a universal concept of contract law known as Third Party Beneficiary. And access by public authorities in the Data Importer's jurisdiction that may affect the rights of Data Subjects is also regulated.

6.2. Advantages and benefits of MCCs



The use of contractual model clauses (MCC) can help overcome possible data transfer limitations arising from the differences in the level of protection between different countries. The introduction of contracts is present in all Ibero-American legal systems and serves to require Data Importers to respect the personal data of the Data Subjects once the personal data is in the destination jurisdiction.

29. For example, in the Mexican public sector, in the event of personal data transfers that do not have an adequate level of protection, an Impact Assessment on the protection of the personal data must be submitted beforehand.

In other words: model clauses or standard clauses contribute to building convergence at the contractual level, creating an autonomous data protection regime, without necessarily requiring convergence at the country level (in this sense, they can go beyond the level of protection in certain countries).

At the same time, the expansion of personal data protection principles through international contract networks has a strong impact on the general convergence in the region, since they establish common standards that companies can become acquainted to. This facilitates the future alignment of national legislation with international norms and standards governing the protection of personal data.

On the other hand, the use of MCCs serves to guarantee the principles and duties pertaining to personal data protection. This, in turn, leads to transparency, legal certainty, and, therefore, predictability, since:

(i) their binding and enforceable nature as part of a contract ensures the continuity of protection when the data travels abroad, and in a way that provides legal certainty;
(ii) adopting clear and transparent measures helps build trust, which, in turn, gives companies that use such clauses a competitive advantage over those that have to resort to other methods.

The MCCs serve to protect the "weaker" party, which, of course, are the natural persons whose personal data, in the case of IPDTs, is processed by both the Data Exporter and the Data Importer.

Finally, the use of MCCs also allows a particularly economical solution to the IPDT problem because companies do not have to negotiate agreements in each individual case with the economic burden of legal representation and time. MCCs allow parties to rely on the model pre-approved by the competent Supervisory Authority, in the understanding that, by doing so, they comply with their legal international personal data transfer obligations with a simple and practical solution. This is significantly different from other tools, such as certification mechanisms or BCRs, which require an often lengthy and costly certification process.

Compared to those mechanisms, MCCs are a "plug and play" and "ready to run" instrument. This is particularly important for small and medium-sized businesses that cannot afford other more expensive options that require more time to implement.

That is why MCCs are the most accessible and widely used legal mechanism today for IPDTs to inadequate jurisdictions. About 80 to 90% of companies that implement IPDT mechanisms use MCCs as a solution[30]. Of course, this implies that the Parties to an IPDT that use a MCC must not limit themselves to the formal requirement of their signature but must always be prepared to "be accountable for" the processing of personal data to the competent Supervisory Authority and the Data Subjects, and to demonstrate full compliance with the applicable law and the obligations set forth in the MCCs.

7. Practical issues in the implementation and execution of MCCs

7.1. General aspects

Given the multiplicity of existing laws in Ibero-America, this Guide is based on the Standards approved at the XV Meeting of this Network, which took place in Santiago de Chile, Chile, on June 22, 2017. The joint efforts with the IAJC of the OAS for the modernization of the privacy principles elaborated by the aforementioned organization, as well as the GDPR and the modernized Convention 108, have also been considered.

The definitions of the MCC are taken from the Standards. The same can be said of the substantive obligations arising from the MCC. Similarly, the contractual model clauses approved by the EU have been consulted, as well as the models proposed by New Zealand authorities.

SANTIAGO DE CHILE.
CHILE, ON JUNE 22, 2017
XV MEETING
RED IBEROAMERICANA DE PROTECCION DE DATOS

30. A study conducted estimates that about 85% use MCCs as IPDT mechanisms. See Nigel Cory, Ellysse Dick, Daniel Castro, The Role and Value of Standard Contractual Clauses in EU-US Digital Trade, ITIF, December 17, 2020. Available at: https://itif.org/publications/2020/12/17/role-and-value-standard-contractual-clauses-eu-us-digital-trade . In the same sense: Laura Bradford, Mateo Aboy, Kathleen Liddell, Standard contractual clauses for cross-border transfers of health data after Schrems II, published in the Journal of Law and the Biosciences, Volume 8, Issue 1, January-June 2021, https://doi.org/10.1093/jlb/lsab007.

The sources on which the clauses of the MCC are based are indicated below:

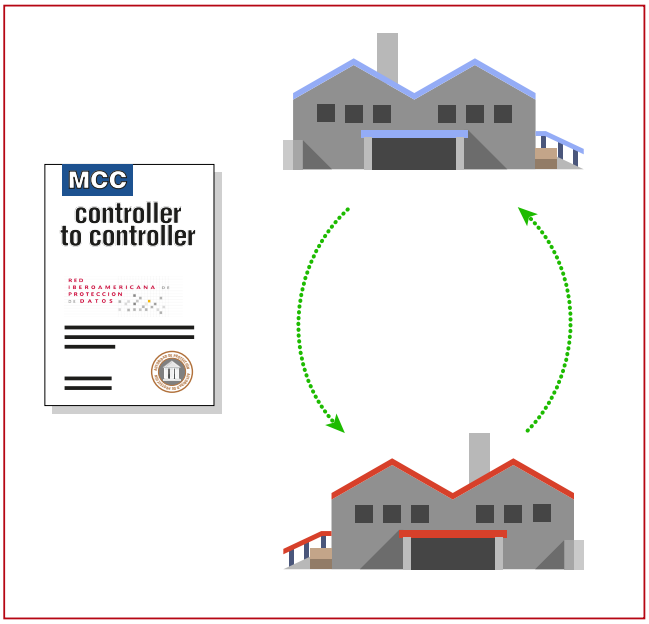
Clause	Source
Clause 1.4 - MCC Definitions	Art. 2 of the Standards. The definition of anonymization is based on Art. 4.3.b of the Standards. The definitions of Data Importer, Onward Transfer, Applicable Law, and Third Party Beneficiary are not in the Standards. It was prepared based on the content of the model clauses.
Clause 6.1 - Principle of responsibility	Article 20 of the Standards
Clause 6.2 - Principle of purpose limitation	Article 17 of the Standards
Clause 6.3 - Principle of Transparency	Article 19 of the Standards
Clause 6.6 y 6.7 Principles of security and confidentiality	Articles 21, 22, and 23 of the Standards
Clause 6.9 - Onward Transfers	Clause 8.7 of the EU's MCC
Clause 7 – Rights of the Data Subject	Articles 24 to 28 of the Standards
Right to compensation	Article 44 of the Standards
Clause on access by public authorities	New Zealand Contractual model Clause
Clause 6.1. of the Controller-Processor model	Article 34 of the Standards

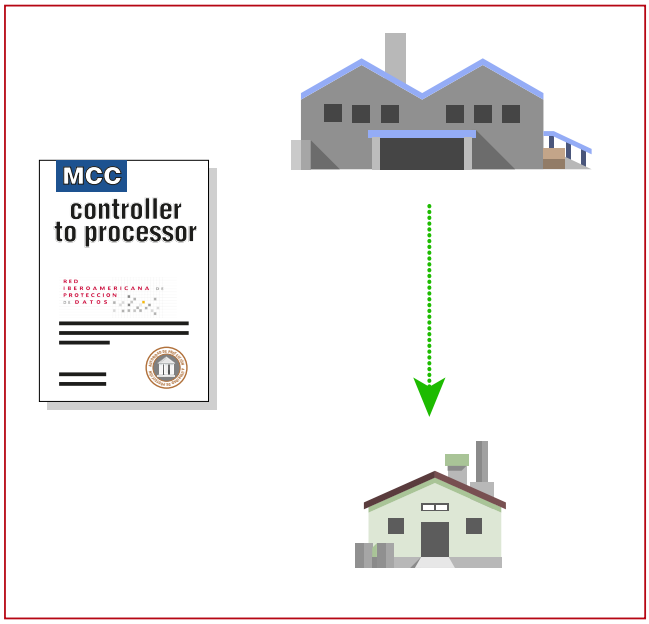
Consequently, as a recommended first step for the adoption of the MCC, we suggest comparing the requirements set forth in the Standards with the regulations of each Member State, since, in the event that the latter establishes additional requirements, supplementary provisions must be included in the MCCs

7.2. MCC Characteristics. Method of use.

The two MCC models included in the Annex to this Guide are characterized by the following:

• The MCC of the Annex contains two models for the different IPDT assumptions: i) Controller to Controller and ii) Controller to Processor.





• The first page or cover is included to enter the information of the parties and the contract and their addresses. The idea is that, in principle, it is not necessary to modify the text of the MCCs at all.

• The MCCs have several annexes to identify the new parties joining the contract after the initial signature of the Data Importer and Exporter (Annex A), the personal data involved in the transfers and their purposes (Annex B), the security measures (Annex C), the list of assistant processors in the case of the second model (Annex D), and the additional legal documentation that the parties wish to include, such as privacy notices or privacy policies (Annex E).

• With regard to Annex A, each new Party joining the MCC must sign an Annex separately and indicate the type of activity that it will carry out in relation to the IPDT.

• With regard to Annex B, the information applicable to each transfer or category of transfers must be clearly identified.

• With regard to Annex C, the security measures must be specified accurately. General information is not allowed.

• With regard to Annex D, the assistant processors must be mentioned in the event that it they had been listed in advance.

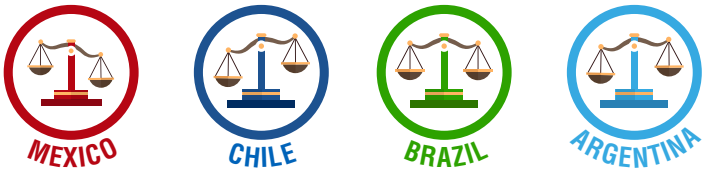
It is also important to point out that, for the use of MCCs, the transfer requirements must be previously verified in the specific case, as well as the characteristics of the entities or persons who carry them out, since the MCC could eventually incorporate additional elements depending on the said assumptions and the applicable regulatory requirements in each of the countries where said processing takes place.

7.3. Position of the parties. Incorporation of new parties and use of the MCCs with other agreements. Modifications

Although we usually speak of standard contractual clauses or MCC, the term refers to a complete contract model that can be used as is, or modified in secondary aspects, provided that their essence, which is the protection of Data Subjects' rights, is not altered, in accordance with applicable regulations. These MCCs can be then used as an annex to a contract that the parties are going to sign or that they have signed, but they shall execute said models effectively for them to be valid and to take effect.

The Parties may include said standard contractual clauses in a broader contract, at their discretion, as well as add other clauses or additional guarantees, provided that they do not, directly or indirectly, contradict, alter, or modify the standard contractual clauses or affect the fundamental rights of the Data Subjects.

7.4. Law applicable to IPDTs



The implementation of MCCs takes place when an entity needs to transfer data to another entity located in another country that has not been recognized as a country with an adequate level of protection by the country of origin. Standard contractual clauses may be used in relation to such transfers insofar as the Data Importer is located in a third country other than the Data Exporter.

In a normal situation, each party would be subject to the laws of their respective country when processing transferred personal data. However, in the event of an IPDT through a MCC, the applicable law (defined in the MCC as "Applicable Law") is that of the country or jurisdiction of the Data Exporter.

The export of personal information cannot become a scenario that reduces the level of protection conferred on the data Subject in the country from which the personal data are exported. The IPDT must not facilitate or allow the violation of the rights of the Data Subjects or the reduction of the guarantees available to the Data Subjects in the exporting country[31]. This is based on the logic that the data is collected and processed under the Data Exporter's law and when it is transferred abroad to a country that has been recognized as having an adequate level, it is necessary to preserve the level of protection of that personal data in the country of origin.

31. IDPN, Recommendations for the processing of personal data through cloud computing services, p. 15.

7.5. Compliance with general regulations on personal data protection

1° LOCAL LEGISLATION

LOCAL DATA PROTECTION AUTHORITY

MODEL CONTRACTUAL CLAUSES

In addition to using MCCs to offer adequate guarantees in international personal data transfers, the Data Exporter must comply with the general obligations applicable to it as the Controller or Processor under the current personal data protection law in its jurisdiction.

These responsibilities include the controller's obligation to clearly inform Data Subjects, in its privacy policy, of the international transfers of their personal data to a third country that does not have a recognized adequate level of protection.

In addition, it is important to consider that, in compliance with the duties, principles, and obligations pertaining to personal data protection in the regulatory framework of each country, there may be additional requirements, as in the case of Mexico, where there is an obligation to communicate the privacy notice. Therefore, the requirements that are not considered in the MCC shall be added in the corresponding annexes, in order to comply with the principles of information and transparency on the processing of personal data.

7.6. Onward transfers

If the Importer needs to transfer the Personal Data to another entity after receiving the data from the Exporter, then a subsequent Transfer occurs, and it is necessary to continue protecting the personal data.

Onward Transfers by the Data Importer to a third party in another third country should only be permitted if such third party adheres to the MCCs of similar tenor and if the continuity of the protection is otherwise ensured or in specific situations covered by the MCCs.
It is worth remembering that each time an Onward Transfer occurs in the sense defined above, the involvement of a third party is assumed, who acquires personal data protection responsibilities for being part of the processing. In such a case, the addition to the Contractual model Clauses would be necessary, either by signing a new MCC particularly with the Data Importer or by means of a specific legal instrument.

7.7. Third party beneficiaries

In the MCCs, the Data Subject is a Third Party beneficiary of the model contract signed by the Parties. Should the Data Importer fail to comply with contractual duties, the Data Subject may, in its capacity as a third-party beneficiary, assert a claim against the Data Importer or Exporter for such non-compliance. This is the case because both Parties provide a stipulation in favor of the Data Subject[32].

The Third Party Beneficiary principle is contemplated in most Ibero-American private law codes. Namely, among others, the civil codes of Argentina (Art. 1027 of the National Civil and Commercial Code), Bolivia (Art. 526 to 529 of the Civil Code), Brazil (Art. 436 to 438 of the Civil Code), Chile (Art. Art. 1449 of the Civil Code), Colombia (Art. 1506 of the Civil Code), Costa Rica (Art. 1026 of the Civil Code of Costa Rica), Ecuador (Art. 1465 of the Civil Code), El Salvador (Art. 1320 of the Civil Code), Guatemala (Art. 1531 of the Civil Code), Honduras (Art. 740 of the Commercial Code), Mexico (Art. 1868-1871 of the Federal Civil Code), Nicaragua (Art. 1875 of the Civil Code), Paraguay (Art. 732 of the Civil Code), Peru (Art. 1457-1459 of the Civil Code), and Uruguay (Art. 1256 of the Civil Code).

7.8. Accountability

Art. 20 of the Standards[33] establishes the principle of accountability. The rule provides that the controller shall implement the necessary mechanisms to prove compliance with the principles and obligations set forth in the Standards, as well as to render accounts to the Data Subject and to the Supervisory Authority for processing the personal data in their possession, for which it may use standards, national or international best practices, self-regulatory schemes, certification systems, or any other mechanism that it deems appropriate for such purposes.

Below are some of the mechanisms that a party to the contract may adopt to comply with the principle of accountability:

32. The stipulation or contract in favor of a third party is an agreement by which one subject (known as the promisor) commits to another (known as promissee) to give something to a third party (or beneficiary) or to do or not do something in favor of said third party, who, although alien to this contract, acquires the rights mentioned therein.

33. Article 20 of the Personal Data Protection Standards for Ibero-American States (2017).

a. Allocate resources for the implementation of personal data protection programs and policies.
b. Implement risk management systems associated with the processing of personal data.
c. Develop mandatory and enforceable personal data protection policies and programs within the Importer's organization.
d. Implement a staff training and refresher program on personal data protection obligations.
e. Periodically review personal data security policies and programs to determine the necessary modifications.
f. Establish an internal and/or external supervision and surveillance system, including audits, to verify compliance with personal data protection policies.
g. Establish procedures to receive and respond to queries and complaints from Data Subjects.

The foregoing shall apply when the personal data is processed by a Controller in the name and on behalf of the Processor, and also when carrying out an IPDT. The aforementioned standard then lists a series of mechanisms that both the Controller and the Processor must implement accordingly. This principle of accountability also applies to international personal data transfers.

In the same sense, the MCCs state that the parties must be able to demonstrate compliance with the standard contractual clauses. Most notably, the MCCs require the data importer to keep the corresponding documentation for the processing activities under its responsibility and to inform the Data Exporter in the event that it cannot comply with the clauses for any reason.

7.9. Impossibility of compliance by the Importer

After entering into the MCC, the Data Importer shall inform the Data Exporter if it has a reason to believe that it will not be able to meet the standard contractual clauses. If the Data Exporter receives such a notification or otherwise discovers that the Data Importer can no longer meet the standard contractual clauses, it must determine the appropriate measures to deal with the situation, in consultation with the competent supervisory authority, where appropriate.

Said measures may consist of complementary actions adopted by the Data Exporter and/or the Importer, such as administrative, physical, and technical measures to guarantee security and confidentiality. The Data Exporter may also be required to suspend the transfer if it considers that there are no adequate guarantees or if ordered by the competent Supervisory Authority. This power is expressly provided for in the MCCs.

***

Glossary

Anonymization: the application of measures of any nature aimed at preventing the identification or re-identification of a natural person without disproportionate efforts.

Competent Supervisory Authority: Personal data protection authority in the country of the personal data Exporter or Importer.

Cloud Computing: model for enabling access to a set of IT services (such as networks, servers, storage, applications, and services) in a convenient manner and on-demand, which can be rapidly provisioned and released with administrative efforts and interaction with the service provider.

Consent: manifestation of the free, specific, unequivocal, and informed will of the Data Subject, through which he/she accepts and authorizes the processing of his/her personal data.

Personal information: any information concerning an identified or identifiable natural person, expressed in numerical, alphabetical, graphic, photographic, alphanumeric, acoustic, or any other form. A person is considered identifiable when their identity can be determined directly or indirectly, provided that this does not require disproportionate time or activities.

Sensitive personal data: data related to the intimate aspects of its Data Subject, or whose improper use may give rise to discrimination or entail serious risk against him/her. By way of example, personal data that may reveal aspects such as racial or ethnic origin are considered sensitive; as well as religious, philosophical, and moral beliefs or convictions; union membership; political opinions; data pertaining to health, life, sexual preference or orientation, genetic or biometric data to uniquely identify a natural person.

Automated individual decisions: Decisions that produce legal effects upon the Data Subject or that significantly affect him/her and that are based solely on automated processing aimed at evaluating certain personal aspects of the Data Subject without human intervention, or particularly analyzing or predicting his/her professional performance, economic situation, health status, sexual preferences, reliability, or behavior.

Processor: service provider who, as a natural or legal person or public authority, outside the organization of the Data Controller, processes personal data in the name and on behalf of the Data Controller.

Standards: Personal Data Protection Standards for Ibero-American States approved by the IDPN in 2017.

Data exporter: natural person or legal entity, public authority, service, agency, or service provider within the territory of a State that carries out international personal data transfers in accordance with the provisions of these Standards.

Data importer: private natural or legal person, public authority, service, agency, or service provider within a third country that receives personal data from a Data Exporter through an international personal data transfer.

Applicable Law: this is the personal data protection law of the Data Exporter's jurisdiction.

Administrative, physical, and technical measures: measures aimed at preventing any damage, loss, alteration, destruction, access, and in general, any illicit or unauthorized use of Personal Data, even if accidentally, sufficient enough to guarantee the confidentiality, integrity, and availability of the Personal Data.

Controller: private natural or legal person, public authority, services, or agency that, by itself or jointly with others, determines the purposes, means, scope, and other issues pertaining to personal data processing.

Assistant processor: when a Data Processor turns to another Processor to carry out certain processing activities on behalf of the Data Controller.

Third party beneficiaries: Data Subject whose personal data is subject to an international transfer under this Agreement. The Data Subject is a third party beneficiary of the rights provided in his/her favor in the MCCs and can therefore exercise the rights granted to it by the MCC, even if the model contract between the parties has not been signed.

Data Subject: natural person to whom the personal data concerns.

Onward transfer: Data transferred by the Data Importer to a third party located outside the jurisdiction of the Data Exporter that meets the guarantees set forth in the MCCs.

Processing: any personal data operation or set of operations conducted through physical or automated procedures, related, but not limited to, the collection, access, registration, organization, structuring, adaptation, indexation, modification, extraction, consultation, storage, conservation, elaboration, transfer, dissemination, possession, use, and in general, any use or disposal of personal data.

Breach of personal data security: any damage, loss, alteration, destruction, access, and in general, any illicit or unauthorized use of personal data, even if accidentally.

Acronyms used

APD *Data Protection Authority or Supervisory Authority.*

Standards *Personal Data Protection Standards for Ibero-American States approved by the IDPN in 2017.*

CEN *Cloud Computing*

IAJC *Inter-American Juridical Committee.*

CSC *Contractual model clauses.*

OAS *Organization of American States.*

BCR *Binding corporate rules.*

GDPR *General Data Protection Regulation or GDPR REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.*

IDPN *Ibero-American Data Protection Network.*

PSCEN *Cloud computing service provider.*

PDT *Personal data treatment.*

IPDT *International personal data transfer.*

EU *European Union.*

Documents consulted

Country references *(alphabetical order)*

Argentina

- Law 25.326, Art. 12 Law No. 25.326 on personal data protection, Art. 12 of Regulatory Decree No. 1558/2001
- Provision 60/2016 of the National Directorate for Personal Data Protection. Available at: http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/texact.htm

Brazil

- Art. 33 to 35 of the LGPD.

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

Cape Verde

- Art. 20, Law No. 41/VIII/2013 of September 17 on the Protection of Personal Data. https://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

- Statutory Law 1581 of 2012 (Article 26)
- Decree 1377 of 2013 (Article 25. Personal data transmission contract)
- Decree 255 of 2022 (Binding Corporate Rules)

- Superintendence of Industry and Commerce (2019-2021) Guide for the implementation of the principle of accountability in international personal data transfers. Available at: 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
- Superintendence of Industry and Commerce (2015) Guide for the Implementation of the Principle of Accountability. Available at: https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf

Ecuador

- Art. 55 to 61 of the Organic Law on Personal Data Protection. https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf

Mexico

- Art. 36 and 37 of the Federal Law on the Protection of Personal Data Held by Private Parties (Published in the Official Gazette of the Federation on July 5, 2010, available at the following electronic link: http://dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010, without reforms; consolidated text in portable document format, by the Chamber of Deputies of the Congress of the Union, at the following electronic link: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf.).
- Art. 67 to 76 of the Regulations of the Federal Law on the Protection of Personal Data Held by Private Parties (Published in the Official Gazette of the Federation on December 21, 2011, available at the following electronic link: http://dof.gob.mx/nota_detalle.php?codigo=5226005&fecha=21/12/2011; without reforms; consolidated text in portable document format by the Chamber of Deputies of the Congress on the Union, available at the following link: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf; links last consulted on 06/10/2021).
- Art. 65 to 71 of the General Law on the Protection of Personal Data Held by Obliged Subjects (Published in the Official Gazette of the Federation on January 26, 2017, available at the following electronic link: http://dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017 , without reforms; consolidated text in portable document format by the Chamber of Deputies of the Congress of the Union, at the following link: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf).

• Articles 108 to 118 of the General Guidelines for the Protection of Personal Data for the Public Sector (Published in the Official Gazette of the Federation on January 26, 2018, available at the following electronic links: https://www.dof.gob.mx/nota_detalle.php?codigo=5511540&fecha=26/01/2018 and http://inicio.inai.org.mx/AcuerdosDelPleno/ACT-PUB-19-12-2017.10.pdf, last modified on November 25, 2020, available at the following electronic links: 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).
Note: The specific legal provisions regarding transfers have been incorporated; however, in order to indicate the complete context on the transfer requirements related to personal data protection, the reference should be expanded with additional articles and complementary regulations.

Nicaragua

• Art.14 of Law No. 787, Personal Data Protection Law.
http://legislacion.asamblea.gob.ni/Normaweb.nsf/xpNorma.xsp?documentId=E5D37E9B4827FC06062579ED0076CE1D&action=openDocument

New Zealand

Nueva Zealand Privacy Commissioner, Model contract clauses for sending personal information overseas. Available at: https://www.privacy.org.nz/responsibilities/disclosing-personal-information-outside-new-zealand/

Panama

• Art. 5 and 33, Law No. 81 of March 26, 2019 on the Protection of Personal Data.
• Art. 51 to 53 of Executive Decree No. 285 of May 18, 2021, (available at: https://www.gacetaoficial.gob.pa/pdfTemp/29296_A/GacetaNo_29296a_20210528.pdf).

Peru

• Article 15 of Law No. 29.733. Personal Data Protection Law. Published in July 2011.
https://www.redipd.org/sites/default/files/inline-files/Ley-29733.pdf

Democratic Republic of São Tomé and Príncipe

• Art. 19 and 20, Law 3/2016 of May 2 on the Protection of the Personal Data of Natural Persons
https://www.redipd.org/sites/default/files/2020-03/lei-3-2016-proteccao-de-dados-pessoais.pdf

Dominican Republic

• Art. 80 of Law No. 172-13 of December 13, 2013 on the Protection of Personal Data.
https://indotel.gob.do/media/6200/ley_172_13.pdf

United Kingdom

• Standard Contractual Clauses (MCCs) after the transition period ends, available at: 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/
• UK Standard contractual clauses https://ico.org.uk/media/for-organisations/documents/2620100/uk-sccs-c-p-202107.docx

Uruguay

Art. 23 of Law No. 1.,331 on the Protection of Personal Data
Resolution No. 4/019 of March 12, 2019.
Resolution No. 41/021 of September 8, 2021. Available at: https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/noticias/cambios-regimen-transferencias-internacionales-datos-uruguay

References from some organizations

(alphabetical order)

European Council

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

European Data Protection Board (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. Available at: https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasures-transferstools_en.pdf

MERCOSUR

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

Organization of American States

OAS, Updated Principles on Privacy and the Protection of Personal Data, with Annotations (CJI/RES. 266 (XCVIII-O/21)). http://www.oas.org/es/sla/ddi/proteccion_datos_personales_Trabajos_Actuales_CJI.asp

Ibero-American Data Protection Network

• Ibero-American Data Protection Network -IDPN- (2017). Personal data protection standards for Ibero-American States. Available at: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

• IDPN, Declaration of Cartagena de Indias, May 2004, section III - "International data transfers. European and Ibero-American Perspectives" at: https://www.redipd.org/sites/default/files/inline-files/declaracion_2004_III_encuentro_es.pdf

• IDPN, XVIII Ibero-American Data Protection Meeting, https://www.redipd.org/sites/default/files/2020-12/declaracion-final-xviii-encuentro.pdf

• IDPN, Regulation of the Ibero-American Personal Data Network, https://www.redipd.org/sites/default/files/2019-11/reglamento-ripd.pdf

European Union

• Directive 95/46/CE of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (DO L 281 of 23.11.1995, p.31). Available athttps://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ%3AL%3A1995%3A281%3ATOC

• Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, DO L 119 of 4.5.2016, p. 1. Available at: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC

• IMPLEMENTING DECISION (EU) 2021/914 of June 4, 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. Available at: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32021D0914&from=EN#ntr2-L_2021199ES.01003701-E0002
• Commission Decision 2001/497/CE of June 15, 2001 on standard contractual clauses for the transfer of personal data to third countries, under Commission

• Decision 2010/87/EU of February 5, 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council. Available at: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ%3AL%3A2010%3A039%3ATOC

• IMPLEMENTING DECISION (EU) 2021/914 of June 4, 2021 on standard contractual clauses for the transfer of personal data to third countries, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council. Available at: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32021D0914&from=EN#ntr2-L_2021199ES.01003701-E0002

• Judgment of the Court of Justice of the EU, judgment of July 16, 2020 in case C-311/18, Data Protection Commissioner/Facebook Ireland Ltd and Maximillian Schrems (“Schrems II”), ECLI:EU:C:2020:559.