



Trade Agreements and Data Governance in the Digital Economy: The Case of Mercosur

→ August 2026

ADC



Trade Agreements and Data Governance in the Digital Economy: The Case of Mercosur

Asociación por los Derechos Civiles · August 2026 · adc.org.ar

Research and Writing: Gabriela Szlak, Celia Lerman and Luciano Gutman, as independent consultants, in collaboration with Alejandro Segarra and Valeria Milanes, Co-Executive Directors of ADC.

Coordination: Marianela Milanes, ADC Project Manager.

Layout and Design: Alternativa Laboral Trans (ALT) Cooperativa.

We would like to thank Anastasia Dozo, Marcelo Elizondo, Luis García Balcarce, and Pablo Palazzi for their critical review of this text. The opinions and conclusions expressed in this work are the sole responsibility of the authors and do not necessarily represent the views of the aforementioned individuals.

Language translation and stylistic editing support were provided by Google Gemini (AI language model), with all final technical and legal terminology reviewed and verified by the authors.



Trade Agreements and Data Governance in the Digital Economy: The Case of Mercosur is published under a Creative Commons Attribution–NonCommercial–ShareAlike license. To view a copy of this license, please visit: creativecommons.org/licenses/by-nc-sa/4.

Executive summary

In recent years, the Southern Common Market (MERCOSUR, in Spanish) has expanded its integration agenda to incorporate the digital economy and, along with it, the regulation of cross-border data flows. In this context, this paper analyzes how regional instruments and the regulatory and institutional frameworks of the States Parties shape data governance within the trade bloc. For these purposes, data governance is understood as the set of public and private rules, standards, practices, and cooperation mechanisms that structure the collection, processing, movement, and use of data. From this perspective, the paper argues that policy and institutional interoperability constitutes the most appropriate approach to promoting the free flow of data within MERCOSUR—given its nature—while simultaneously ensuring the protection of personal data in a context of marked regulatory heterogeneity.

Section 2 examines the treatment of cross-border data flows in MERCOSUR's main regional instruments, primarily the E-Commerce Agreement, but also the Association Agreement with the European Union and the Free Trade Agreement with Singapore, as well as the regulatory frameworks of the States Parties regarding international transfers of personal data. The analysis shows that the trade bloc has moved toward a model compatible with international standards, seeking to reconcile the free flow of data with the protection of personal data. In particular, none of the States Parties impose general data localization obligations, and Argentina, Brazil, and Uruguay recognize broadly compatible mechanisms to enable international transfers. However, regulatory and institutional asymmetries persist, especially in Bolivia and Paraguay, limiting the consolidation of a fully interoperable regional space. Furthermore, the paper compares MERCOSUR's model with other international frameworks, including the Association of Southeast Asian Nations

(ASEAN), Asia-Pacific Economic Cooperation (APEC), and the Ibero-American Data Protection Network (RIPD), identifying experiences that can contribute to strengthening regional governance.

Section 3 analyzes the main mechanisms used to enable international transfers of personal data—adequacy decisions, standard contractual clauses, binding corporate rules, certifications, seals, and codes of conduct—evaluating their advantages and limitations from the perspective of policy and institutional interoperability. The study argues that these mechanisms not only enable to reconcile the protection of personal data with its free flow, but also serve as tools to align heterogeneous regulatory frameworks without requiring full harmonization. At the same time, it identifies challenges associated with their practical implementation, the institutional capacities of supervisory authorities, and the still limited adoption of various co-regulation mechanisms in the region.

Finally, Section 4 concludes that policy and institutional interoperability constitutes the most appropriate approach to deepening MERCOSUR's digital integration. Unlike models based on regulatory harmonization, interoperability makes it possible to preserve the regulatory specificities of the States Parties while fostering cooperation among authorities, the recognition of common mechanisms for international transfers, and the gradual convergence of national data protection systems. In this sense, strengthening these mechanisms emerges as a necessary condition to consolidate a data governance framework that simultaneously fosters economic integration, the development of the digital economy, and the effective protection of individual rights in the region.



Table of contents

Executive summary	3
01 Introduction	6
1.1. Objective of the Analysis	6
1.2. Contextual Background of the Analysis	7
1.3. Introduction to the Conceptual Framework	8
02 MERCOSUR and Its Regulatory Heterogeneity: Agreements and Asymmetries	11
2.1. MERCOSUR Agreements	11
2.2. Domestic Regulatory Frameworks	13
2.2.1. Argentina	14
2.2.2. Brazil	15
2.2.3. Bolivia	17
2.2.4. Paraguay	17
2.2.5. Uruguay	18
2.2.6. Main Similarities and Differences Among Local Regulatory Frameworks	19
2.3. Other International Regulatory Frameworks	21
03 Policy and Institutional Interoperability and Mechanisms for International Data Transfers	27
3.1. Adequacy Decisions	27
3.2. Standard Contractual Clauses and Binding Corporate Rules	29
3.3. Certifications, Seals, and Codes of Conduct	32
04 Conclusions	35
Notes	40

01 | Introduction

1.1. Objective of the Analysis

The Mercado Común del Sur (MERCOSUR) is a regional integration process originally established by Argentina, Brazil, Paraguay, and Uruguay, and subsequently joined by Bolivia and Venezuela.¹ Since its inception, the trade bloc's mission has been to deepen the integration of its States Parties into international markets through coordinated action among them.

Over the past decade, MERCOSUR has expanded its agenda to incorporate issues related to the digital economy. One of the first milestones of this new paradigm was the creation, in 2017, of the MERCOSUR Digital Agenda Group, aimed at “promoting the development of a Digital MERCOSUR.” Within this framework, the trade bloc has also adopted numerous instruments addressing key issues for the digital economy, such as digital consumer protection,² digital signatures,³ and e-commerce,⁴ among others. Likewise, within the framework of the XXX Ordinary Meeting of the MERCOSUR Digital Agenda Group, the creation of the Data Protection Commission⁵ was agreed upon, which is currently working on various projects on the subject. MERCOSUR has also included provisions on the digital economy and its governance in its trade agreements with extra-regional partners, such as the European Union (“EU”)⁶ and Singapore.⁷

This paper aims to identify how regional instruments and the regulatory and institutional ecosystems of its States Parties shape data governance within the trade bloc. This objective is particularly valuable in a region characterized by marked regulatory and institutional heterogeneity, where countries with laws aligned with

international standards coexist with others undergoing legislative transition, strengthening their institutional capacities, or both. Furthermore, within the broad spectrum of digital economy regulation and data processing, this paper focuses specifically on data governance as it relates to cross-border flows, including personal data.

Given the centrality of information flows in the global data economy, an extensive body of literature exists on the subject. However, research focused on South America that integrates the region's specific regulatory, institutional, economic, trade, and technological dimensions remains scarce. The objective of this paper was developed with a view to generating and synthesizing specific knowledge on data governance in MERCOSUR.

1.2. Contextual Background of the Analysis

In recent years, particularly following the COVID-19 pandemic, various technological developments and shifts in consumer habits have occurred both within the States Parties of MERCOSUR and around the world. These factors, alongside other technological advancements impacting the digital business ecosystem, have contributed to a substantial increase in cross-border data flows, including personal data, and it is reasonable to expect this trend to continue growing in the coming years.

For instance, Koneva et al.⁸ projected that, over the coming years, interactions between users and cloud-based artificial intelligence agents will contribute significantly to the growth of internet traffic. They even estimated that text-based agents could generate traffic volumes comparable to those currently reached by email usage and web browsing. Although this study addresses network traffic in general, it is reasonable to argue that data, and personal data

within it, will constitute a substantial portion of these information flows.

1.3. Introduction to the Conceptual Framework

To analyze MERCOSUR's instruments and the regulatory and institutional ecosystems of its States Parties regarding cross-border data flows, this paper will draw upon policy interoperability and institutional interoperability as analytical tools.

The term interoperability is typically used in a technical context to refer to the ability of distinct networks or systems to interconnect and exchange information.⁹ If we apply this concept to the legal and governance sphere, policy interoperability can be understood as the dialogue between diverse regulatory frameworks. In this sense, Howell and Ifayemi¹⁰ consider that this concept refers to how similar or well-aligned the provisions of regulatory frameworks are. To analyze this, a key metric used is evaluating how easy it is to comply with multiple regulatory frameworks simultaneously, and whether compliance with one framework will facilitate compliance with others. Another way to analyze policy interoperability, according to these authors, is to focus on creating regulatory consistency, with the aim of converging and establishing accountability around best practices among countries, while also enabling stakeholders (e.g., auditors, civil society) to compare, study, and evaluate models across borders. Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)¹¹ appears to advocate for this type of interoperability, as it recognizes that its signatories “(...) may take different legal approaches to protecting personal information (...)”, while also committing them to “(...) encourage the development of mechanisms to promote compatibility among these different regimes.”¹²

Regarding institutional interoperability, Howell and Ifayemi understand it as referring to how aligned the functions or operations of institutions are with one another. A high degree of alignment can enable institutional cooperation or mutual recognition of each other's functions. In this way, institutional interoperability can serve as a complement to policy interoperability.

Weber¹³ distinguishes interoperability from the approach of full harmonization. While the former enables distinct regulatory and institutional frameworks to dialogue with each other, the latter tends to unify them. Full harmonization may not be desirable in all cases, given that differences between jurisdictions reflect national sovereignty. The appropriateness of adopting a harmonization model versus an interoperability model depends largely on the nature of the trade bloc in question. Thus, while in the EU—a supranational community both politically and economically—regulatory harmonization may be appropriate in various areas, in MERCOSUR—a process of economic integration—interoperability presents itself as a better alternative.

The concept of policy interoperability becomes critical when dealing with cross-border data flows. As Palazzi¹⁴ points out, the international transfer of data is inevitable and generally difficult to detect. Therefore, the author notes, regulatory mechanisms are required so that data exported from one country maintains a similar level of protection upon entering another jurisdiction. The mechanisms analyzed in Section 3 of this paper act as enablers of this policy and institutional interoperability, making it possible to address the regulatory heterogeneity within MERCOSUR discussed in Section 2 and to identify how this dynamic shapes data governance within the trade bloc. It should be clarified that, for the purposes of this paper, provisions enabling international data transfers under the concept that doctrine and modern regulations define as derogations are excluded from the analysis. Derogations

usually contemplated by regulations include the data subject's consent, the necessity of the transfer to perform a contract between the subject and the controller, reasons of public interest, or defense against legal claims. Their exclusion from this paper stems from the fact that their application is restrictive in nature and is not as clearly associated with building frameworks of policy and institutional interoperability. As a reference, Recitals 111 and 113 of the EU General Data Protection Regulation (“GDPR”) limit these exceptions to transfers of an isolated and non-repetitive nature.¹⁵ Furthermore, the European Data Protection Board¹⁶ has pointed out that such exceptions must be interpreted in a way that does not contradict the fundamental principle: personal data may not be transferred to a third country unless it offers an adequate level of protection or appropriate safeguards have been established.

Regarding data governance, this paper understands it as the set of public and private rules, standards, practices, and cooperation mechanisms that structure the collection, processing, movement, and use of data. The World Economic Forum,¹⁷ for its part, posits the existence of four pillars supporting global data governance: transfer mechanisms, legal and regulatory cooperation, technical standards, and trade commitments in international treaties. As previously mentioned, among all these pillars, this paper will emphasize transfer mechanisms and the extent to which MERCOSUR's instruments and the regulatory and institutional ecosystems of its State Parties utilize them to facilitate international data flows.



02 | MERCOSUR and Its Regulatory Heterogeneity: Agreements and Asymmetries

This section analyzes the regulation of international data transfers in MERCOSUR, focusing on selected intra-bloc instruments and agreements signed with third countries or regional trade blocs. Within this framework, it primarily examines the relevant provisions of the E-Commerce Agreement¹⁸ and the trade agreements with Singapore¹⁹ and the EU.²⁰ This analysis is complemented by a review of the domestic legal frameworks of the States Parties to identify similarities and differences in their approach to this matter.

Finally, a comparison is offered between MERCOSUR's policy and institutional framework and other regional or international models. Among them, the CPTPP,²¹ the Digital Economy Partnership Agreement (DEPA),²² the Free Trade Agreements between Chile and Argentina²³ and Chile and Uruguay,²⁴ the Reciprocal Trade and Investment Agreement between Argentina and the United States of America,²⁵ Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) and its Additional Protocol,²⁶ and the frameworks of RIPD, ASEAN, and APEC stand out.

2.1. MERCOSUR Agreements

The first instrument analyzed is the MERCOSUR E-Commerce Agreement.²⁷ The Association for Civil Rights (*Asociación por los Derechos Civiles*) has summarized the mission of this Agreement as follows: "to establish a common legal framework for electronic commerce across the jurisdictions of the States Parties, with the

aim of leveraging the economic potential and opportunities provided by electronic commerce”.²⁸ There are two specific commitments undertaken by the States Parties regarding cross-border flows that are derived from this overarching objective: protecting personal data and fostering its free flow.²⁹

Regarding the first commitment, States Parties assume the obligation to ensure an adequate level of protection for personal data originating from other States Parties.³⁰ This safeguard constitutes a fundamental pillar for the free flow of data, given that international transfers should not result in the lack of protection or the infringement of the rights and freedoms of data subjects whose personal information crosses national borders. To achieve this standard, the Agreement recognizes various regulatory mechanisms, such as general or specific regulations, bilateral or multilateral agreements³¹—as well as private-sector tools based on contractual clauses or self-regulation. It should be clarified that Article 2.5 of the Agreement, when dealing with trust and legal certainty in e-commerce, lists codes of conduct and trust seals as examples of “self-regulation.” Therefore, we understand that, in essence, the Agreement refers to co-regulation.³²

Regarding the second commitment, States Parties must permit information transfers within the context of commercial activities conducted by businesses within the trade bloc, subject to compliance with the aforementioned guarantee of adequate protection.³³ However, the Agreement recognizes the possibility for States Parties to establish regulatory requirements linked to international data transfers, and even restrictions on transfers based on public policy considerations, provided that these do not constitute arbitrary discrimination or a disguised trade barrier.³⁴ The prohibition on using data protection regulations as trade barriers can be found in several of the instruments mentioned below, following the standard of the General Agreement on Trade in Services (GATS) of the World Trade Organization.³⁵

The Agreement follows a substantially identical approach regarding data localization obligations: imposing certain restrictions and localization requirements is permitted, provided they do not amount to trade barriers.³⁶ By comparison, the EU GDPR approach establishes much narrower margins for restricting the free movement of data between the member countries of that bloc.³⁷ This distinction partly stems from the previously noted differences between the interoperability approach inherent to MERCOSUR and the full regulatory harmonization characteristic of the EU.

In the realm of extra-regional trade agreements, the Free Trade Agreement with Singapore includes a chapter dedicated to Electronic Commerce,³⁸ which establishes that the signatories will collaborate to promote cross-border information flows and encourage private-sector self-regulation through mechanisms such as codes of conduct, model contracts, guidelines, and compliance mechanisms. As with the MERCOSUR E-Commerce Agreement, we consider that this reference to “self-regulation” can actually be understood as referring to co-regulation. Regarding the MERCOSUR-EU Agreement,³⁹ it does not contain detailed commitments on cross-border data flows.⁴⁰ However, it does include general considerations, such as that global Internet governance must guarantee the free flow of information.⁴¹ Similar to the provisions of the MERCOSUR E-Commerce Agreement, the agreement with the European Union allows signatories to impose restrictions related to the protection of personal data, provided they are not applied in an arbitrary manner or used as a disguised trade barrier.⁴²

2.2. Domestic Regulatory Frameworks

The following section identifies the regulatory status of each MERCOSUR State Party regarding cross-border personal data flows, with a specific focus on restrictions on such transfers, the existence

(or lack thereof) of data localization obligations, and the legal mechanisms recognized by each country to enable them. This information can be summarized in the following table:

Table 1. International transfers of personal data in MERCOSUR States Parties

	List of Adequate Countries	Mechanisms Allowed to Enable International Data Transfers to Non-Adequate Countries	Approved Standard Contractual Clauses	Obligation to Report or Register International Transfers, Even When Using Approved Mechanisms
Argentina	YES	Standard Contractual Clauses and Binding Corporate Rules.	YES (National and RIPD)	NO
Bolivia	NO	N/A (Not Applicable)	NO	NO
Brazil	YES (only to EU and European Economic Area Member States)	Standard contractual clauses, Binding corporate rules, and seals, certifications, and codes of conduct.	YES (Its own)	NO
Paraguay (law pending entry into force)	NO	Standard contractual clauses, Binding corporate rules, and seals, certifications, and codes of conduct.	NO	NO
Uruguay	YES	Standard contractual clauses and Binding corporate rules.	YES (RIPD and Committee 108)	YES (except to adequate countries)

2.2.1. Argentina

In Argentina, the personal data protection framework is based on Article 43 of the National Constitution, which recognizes the *habeas data* guarantee, and is primarily regulated by Personal Data Protection Law No. 25,326, its Regulatory Decree 1558/2001, and the regulations issued by the enforcement authority.⁴³ In addition, both Convention 108 and its Additional Protocol have been approved by the National Congress.⁴⁴

Article 12 of the law prohibits the transfer of personal data to jurisdictions that do not provide adequate levels of protection. The regulatory decree assigns the task of conducting adequacy assessments to the enforcement authority.⁴⁵ The decree also establishes that the necessary safeguards to provide an adequate level of protection may derive from the existence of “self-regulation” systems or standard contractual clauses that provide for the protection of personal data subject to transfer. The enforcement authority has regulated these adequacy scenarios, approving model standard contractual clauses⁴⁶ and guidelines and basic contents for binding corporate rules.⁴⁷ In the event that contractual clauses or corporate rules are used that do not reflect the principles and safeguards of the aforementioned models and guidelines, the data exporter wishing to make use of these instruments must request the approval of the enforcement authority.⁴⁸

2.2.2. Brazil

In Brazil, the personal data protection framework is primarily regulated by the General Personal Data Protection Law (*Lei Geral de Proteção de Dados Pessoais*) No. 13,709 and the regulations issued by the enforcement authority.⁴⁹ The Brazilian framework largely follows the regulatory trend initiated with the adoption of the EU GDPR.

International data transfers and the legal mechanisms that enable them are regulated under Articles 33 through 35 of the law, which include adequacy decisions, standard contractual clauses, ad hoc contractual clauses, binding corporate rules, and seals, certificates, and codes of conduct.

The law empowers the enforcement authority to evaluate the level of personal data protection provided by foreign jurisdictions and, where appropriate, issue adequacy determinations.⁵⁰ It is also

responsible for defining standard contractual clauses and verifying that the other mentioned transfer mechanisms offer sufficient safeguards for personal data protection, in line with the standards set by the law. The authority may delegate these supervisory tasks to certification bodies.

Regarding regulatory developments on cross-border data flows, in 2024 the enforcement authority approved the Regulation on International Data Transfers.⁵¹ This regulation establishes criteria for evaluating the level of data protection in foreign jurisdictions, as well as guidelines, minimum requirements, and procedures for the authority's approval of binding corporate rules and specific contractual clauses.⁵² The regulation also approves a flexible set of standard contractual clauses, adaptable to controller-to-controller, processor-to-processor, and controller-to-processor transfers. Furthermore, the enforcement authority may approve contractual clauses from third countries or international organizations that it considers equivalent to its own standard contractual clauses. It should be clarified that the regulation does not offer further details or guidelines regarding other transfer mechanisms, such as seals, certifications, or codes of conduct. However, it explicitly recognizes that it does not preclude international transfers conducted under those mechanisms.

Likewise, the Regulation provides guidelines for international data transfers, aiming to ensure that such transfers respect the principles, rights, and safeguards guaranteed to data subjects under the framework. In particular, it requires maintaining a level of protection equivalent to that of national legislation when data is located abroad or even when subject to onward transfers; promoting simple, interoperable procedures compatible with international best practices; fostering the free cross-border flow of data with trust, without neglecting the rights of data subjects; reinforcing accountability; implementing effective transparency measures toward data subjects regarding the transfer, while

safeguarding trade and industrial secrets; and adopting best practices, as well as prevention and security measures tailored to the nature of the data, the purpose of the processing, and the risks involved in the operation.

2.2.3. Bolivia

Since 2009, the Political Constitution of Bolivia has recognized the existence of the right to privacy and the *habeas data* remedy. However, to date, the Andean country is the only MERCOSUR Member State that does not have an enacted domestic personal data protection law, meaning that specific regulations on international data transfers do not exist either. It should be clarified that Bolivia has a four-year period from its accession to MERCOSUR as a Member State to adopt the bloc's standards, including the aforementioned Agreement on Electronic Commerce.⁵³

It is worth noting that over the past five years, four personal data protection bills have been introduced in the Chamber of Deputies.⁵⁴ All of these bills provide for legal mechanisms to enable international data transfers, including adequacy decisions, standard contractual clauses, binding corporate rules, codes of conduct, and certifications.

2.2.4. Paraguay

Until 2025, Paraguay maintained a personal data protection framework restricted to credit data processing, governed by Credit Personal Data Protection Law No. 6534. Despite its title, this regulation contained provisions applicable to personal data in general, rather than strictly credit-related data.

On November 27, 2025, the President of Paraguay enacted Personal Data Protection Law No. 7593, aligning the country with the aforementioned regulatory trend initiated by the adoption of

the EU GDPR. Although the law will not enter into force until late 2027, it is pertinent to anticipate how international data transfers will be addressed under the new framework.

The law empowers the enforcement authority⁵⁵ to evaluate the level of personal data protection provided by foreign jurisdictions and, where appropriate, publish official resolutions or lists of those deemed adequate. International transfers to non-adequate jurisdictions are also permitted when the exporter adopts appropriate safeguards—for instance, through specific contractual clauses for a given transfer, standard contractual clauses, binding corporate rules, or seals, certificates, and codes of conduct. Given the recent enactment of the law and the fact that the new supervisory authority is not yet operational, regulations detailing the implementation of these mechanisms in Paraguay have not yet been issued.

2.2.5. Uruguay

In Uruguay, the personal data protection framework is primarily regulated by Personal Data Protection Law No. 18,331, its Regulatory Decree No. 414/009, and the regulations issued by the enforcement authority.⁵⁶ Furthermore, like Argentina, Uruguay has approved both Convention 108 and its Additional Protocol.⁵⁷ Article 23 of the law prohibits international data transfers to jurisdictions that do not provide levels of protection aligned with international or regional standards on the subject.⁵⁸ Uruguay stands out as the only MERCOSUR Member State that has recognized the United States of America as an adequate jurisdiction,⁵⁹ although only regarding organizations certified under the Data Privacy Framework program agreed upon between the United States of America and the EU.⁶⁰ Furthermore, the supervisory authority has specified that, to rely on this adequacy determination, the data exporter must demonstrate that the importer has explicitly declared that the safeguards

established under the program apply to data transferred from Uruguay.⁶¹

The law also empowers the supervisory authority to approve transfers to non-adequate jurisdictions, provided that the personal data exporter registers the transfer with the authority and offers sufficient protection guarantees. To demonstrate the existence of these safeguards, the law explicitly contemplates contractual commitments,⁶² while the regulatory decree incorporates the use of binding corporate rules.⁶³

2.2.6. Main Similarities and Differences Among Local Regulatory Frameworks

As a first point of regulatory convergence among the surveyed countries, none of them expressly establishes general data localization requirements, aligning the region with international standards. In this regard, a recent World Bank report⁶⁴ notes that 75% of countries globally do not impose this type of requirement—a figure that rises to 90% for Latin America and the Caribbean. The study further warns⁶⁵ that local storage obligations have an adverse impact on organizations by increasing operational costs and restricting access to potential markets. Within this framework, although Uruguay does not establish express localization requirements, it does stipulate that international transfers to destinations lacking an adequate level of protection require prior approval from its supervisory authority, even when the exporter utilizes the transfer mechanisms recognized under its legislation.

Argentina, Brazil, and Uruguay permit international data transfers to jurisdictions that offer an adequate level of protection, entrusting their respective supervisory authorities with the competence to evaluate this condition. All three countries agree on recognizing EU and European Economic Area Member States as safe destinations and, in turn, hold EU adequacy status. Likewise, both Argentina and

Uruguay recognize each other as adequate, but to date they have not done so with Brazil. Furthermore, Uruguay is the only one that, to date, permits transfers to the United States of America, although it has done so solely with respect to organizations certified under the previously mentioned Data Privacy Framework. Bolivia and Paraguay, for their part, do not yet possess an operational regulatory framework to declare third countries adequate, nor have they been recognized as adequate by the EU or other MERCOSUR States Parties.

Regarding transfers to jurisdictions lacking an adequate level of protection, the laws of Argentina, Brazil, and Uruguay—along with Paraguay's pending law—all recognize standard contractual clauses and binding corporate rules as valid instruments to enable these data flows. In the case of Uruguay, as previously noted, these regulatory mechanisms must be submitted to the enforcement authority for transfer approval. On the other hand, the legal frameworks of Brazil and Paraguay, being more recent and closely aligned with the EU GDPR, permit more modern and globally adopting regulatory instruments, such as seals, certifications, and codes of conduct. Although Argentina and Uruguay do not explicitly recognize these mechanisms under their domestic laws, “self-regulation” mechanisms are recognized under the MERCOSUR E-Commerce Agreement.⁶⁶ As noted earlier, we consider that the term “self-regulation” within the context of the MERCOSUR E-Commerce Agreement should be understood as a reference to co-regulation, encompassing codes of conduct and trustmarks.

The supervisory authorities of Argentina, Brazil, and Uruguay have each approved at least one model of standard contractual clauses. This places all three countries above the global average, given that the aforementioned World Bank study⁶⁷ found that fewer than 40% of countries possess models of this kind. Argentina and Brazil have developed their own versions, and Argentina and Uruguay have adopted the models drafted by the RIPD.⁶⁸ Brazilian law empowers

its supervisory authority to recognize standard contractual clauses from third countries or international organizations that guarantee an equivalent level of protection. However, to date, this has not occurred. Regarding binding corporate rules, both the Argentine and Brazilian authorities have issued guidelines for their drafting.

2.3. Other International Regulatory Frameworks

Having reviewed the regulation of cross-border personal data flows in MERCOSUR instruments and the domestic laws of its States Parties, it is useful to situate the bloc within a global context, comparing it with other international regulatory frameworks. This analysis broadens the perspective and helps identify elements from other data governance frameworks that could be useful for the objectives of this work.

Certain instruments adopted within the trade bloc have already made relevant contributions to its regulatory framework. For example, the MERCOSUR Agreement on Electronic Commerce⁶⁹ has commitments on cross-border data flows and data localization that are very similar to those found in the CPTPP⁷⁰ or the DEPA.⁷¹ It is worth noting that while the MERCOSUR Agreement only commits States Parties to “recognize” self-regulation⁷² as evidence of adequate protection, under DEPA the signatories go a step further, committing to “encourage” its adoption.

The Free Trade Agreements between Chile and Argentina⁷³ and Chile and Uruguay⁷⁴ also regulate cross-border flows in a manner substantially similar to the MERCOSUR E-Commerce Agreement.⁷⁵ Both agreements allow the imposition of localization requirements and restrictions on international transfers for public policy reasons, provided they do not constitute arbitrary discrimination or a disguised restriction on trade.

Argentina has also entered into a bilateral agreement with the United States of America containing specific provisions on international data transfers. Under the Trade and Investment Framework Agreement between both countries,⁷⁶ Argentina commits to recognizing its counterpart as a jurisdiction that provides adequate levels of protection. However, the instrument does not specify whether such recognition can be structured similarly to the EU and Uruguay precedents, in which adequacy is granted strictly to organizations certified under the Data Privacy Framework program.

It should be noted that Uruguay's recognition of the adequacy of U.S. companies under the Data Privacy Framework does not imply that Uruguayan data subjects enjoy the same guarantees provided under said framework for European Union citizens. Within the framework of the Agreement between Argentina and the United States of America, Argentina also committed to submitting its application to join the Global Cross Border Privacy Rules Forum (Global CBPR) and the Global Cooperation Arrangement for Privacy Enforcement. If accepted, Argentina would become the first MERCOSUR country to participate in these initiatives.⁷⁷ Section 3 will delve further into the Global CBPR as a mechanism to enable international data transfers. It should be clarified that, to date, Argentina has not operationalized these commitments.

Another relevant international instrument, having been ratified by two MERCOSUR States Parties,⁷⁸ is Convention 108 and its Amending Protocol of the Council of Europe.⁷⁹ While the original Convention remains in force, the entry into force of the Amending Protocol requires ratification by 38 signatory States.⁸⁰ Convention 108, like other surveyed instruments, aims to protect personal data in the context of international transfers while simultaneously promoting free movement among signatories. To this end, the Convention establishes that “a Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special

authorisation transborder flows of personal data to the territory of another Party”.⁸¹

Continuing with the survey of international frameworks relevant to the previously analyzed countries, almost all MERCOSUR States Parties (with the exception of Bolivia) are members of the RIPD. The Data Protection Standards for the Ibero-American States approved by this body dedicate a specific chapter to international data transfers. In addition to recognizing adequacy decisions and standard contractual clauses as mechanisms to enable cross-border flows, the chapter contemplates certification mechanisms aligned with the domestic laws of the exporting country.

Regarding other regional blocs, the Association of Southeast Asian Nations (ASEAN) has approved standard contractual clauses,⁸² designed primarily to enable intra-bloc international data transfers. ASEAN's regulatory framework stands out for its approach oriented toward regulatory and institutional interoperability. The implementation guide for these clauses, for example, explicitly accounts for the varying levels of regulatory development in personal data protection among its Member States. Furthermore, it notes that these model clauses may be of particular interest to organizations with cross-border personal data flows to countries whose privacy regimes are grounded in OECD and APEC principles, given that ASEAN's personal data protection framework derives from these standards.

In the same vein, and continuing with approaches based on regulatory and institutional interoperability, it is worth highlighting the joint guides developed by ASEAN and the European Commission,⁸³ on the one hand, and by ASEAN and the RIPD,⁸⁴ on the other, for the joint implementation of the model clauses from each regulatory framework. The guide offers a comparison between the models of each bloc, identifies their main similarities and differences, and provides tools to help organizations operationalize

the provisions of both models. This joint effort represents a significant contribution to regulatory and institutional interoperability approaches. In the future, interoperability guides between other regional blocs could be developed, and a bloc might even recognize another's standard contractual clauses as valid.

It is worth noting that ASEAN does not exclude mechanisms other than contractual clauses. The bloc recognizes that its Member States may adopt, among others, codes of conduct, binding corporate rules, ISO certifications, or APEC's Cross-Border Privacy Rules (CBPR) system.⁸⁵ The CBPR system, along with its counterpart designed for data processors, the Privacy Recognition for Processors (PRP) system, are the main components of APEC's cross-border data flow model. APEC Member States commit to not restrict international data transfers among themselves when specific safeguards are in place, explicitly including the CBPR system.⁸⁶ Both the CBPR system⁸⁷ and the PRP system⁸⁸ operate as certification mechanisms, in which organizations complete a self-assessment questionnaire regarding their personal data processing practices and policies. The questionnaire and all supporting documentation are submitted to an accountability agent for evaluation. Organizations that comply with the requirements of the CBPR or PRP system, as applicable, are certified and listed on an official APEC website.⁸⁹ Accountability agents are nominated and approved by Member States based on recommendations from each system's oversight panel. Each Member State must have at least one accountability agent and a supervisory authority with sufficient powers to intervene in cases involving non-compliance that could not be resolved in the first instance by the corresponding accountability agent. It should be clarified that both systems allow for a supervisory authority to be nominated, in turn, as an accountability agent.

Like the ASEAN framework, APEC's approach is highly oriented toward both regulatory and institutional interoperability. On the

regulatory level, this is evidenced by the fact that the rules applicable to the CBPR and PRP systems clarify that they do not alter domestic legislation nor exempt organizations from complying with their local personal data protection obligations. However, Member States might find it necessary to adjust their internal laws to align with these systems—for instance, by ensuring the presence of a supervisory authority with the required enforcement powers or by accepting CBPR and PRP certifications as valid mechanisms for international data transfers. Meanwhile, institutional interoperability can be found in both the CBPR rules and the Cooperation Arrangement for Cross-Border Privacy Enforcement,⁹⁰ insofar as they establish a common standard of minimum powers that supervisory authorities must possess.

The APEC CBPR and PRP systems have served as inspiration for the initiatives known as Global CBPR and Global PRP. These are initiatives led by certain APEC Member States to promote free cross-border personal data flows, regulatory and institutional interoperability, and effective personal data protection on a global scale. Global CBPR and Global PRP operate in a manner very similar to their APEC counterparts. Both are governed by a Forum composed of Member States and Associate States. Member States commit to not restricting data transfers among themselves when specific safeguards are in place, explicitly including the Global CBPR system.⁹¹ As in the APEC framework, organizations complete a self-assessment questionnaire regarding their data processing practices and policies, and the application is evaluated by an accountability agent approved by the Forum. Organizations that meet the requirements of the Global CBPR or Global PRP systems, as applicable, are certified and listed on an official website.⁹² In terms of compliance, the Global CBPR and Global PRP systems exhibit a greater degree of flexibility than their APEC counterparts. Although having a privacy supervisory authority remains mandatory, Member

States are allowed to assign oversight responsibilities to various entities, both public and private.



03 | Policy and Institutional Interoperability and Mechanisms for International Data Transfers

This Section will be dedicated to the analysis of the different types of mechanisms recognized by the international instruments surveyed in Section 2 for personal data transfers. Below is a brief conceptualization of each mechanism alongside a comparative analysis of the opportunities and challenges they present.

3.1. Adequacy Decisions

Adequacy decisions are a mechanism through which a State determines that another country, regional bloc, or international organization ensures an equivalent level of personal data protection. In most jurisdictions, this declaration allows international data transfers to that recipient jurisdiction to flow freely, without the need for additional requirements or safeguards.

⁹³ Furthermore, certain regulatory frameworks allow adequacy to be granted on a targeted basis rather than universally, limiting its scope to specific sectors or organizations.⁹⁴

It should be clarified that this “adequacy” requirement should not be understood as an obligation for personal data to be processed in the importing country in an identical manner to how it is processed in the country of origin. The Court of Justice of the EU had the opportunity to rule on this point in its judgment in the case popularly known as Schrems I.⁹⁵ The Court determined that the means used by the importing country to ensure protection may differ from those applied by the EU, provided they prove effective in practice to guarantee substantially equivalent levels of protection.

In other words, adequacy is evaluated based on outcomes and practical implementation, rather than the specific means employed.

The depth of analysis required prior to issuing an adequacy decision varies across jurisdictions. The EU GDPR establishes a series of criteria to be considered by the European Commission when evaluating the adequacy level of a jurisdiction, including, among other factors: the rule of law, respect for fundamental rights and freedoms, applicable legislation, public authority access to personal data, rules governing onward data transfers to third countries, the existence of effective administrative and judicial remedies for data subjects, and the presence of an independent supervisory authority with adequate enforcement powers. Unlike other jurisdictions, the EU stands out for having periodic review processes for its adequacy decisions,⁹⁶ allowing the European Commission to repeal, suspend, or modify existing decisions. Brazilian law establishes⁹⁷ evaluation criteria similar to those of the EU. However, it incorporates geopolitical criteria that are not as explicit in European regulation. For instance, when determining the adequacy of another jurisdiction, the supervisory authority must weigh the impact of its decision on diplomatic relations, trade, and international cooperation, as well as the country's reciprocity toward Brazil. On the other hand, the case of Colombia is of particular interest: although its legislation provides for its own procedure to evaluate whether a third country offers an adequate level of protection, it also automatically recognizes jurisdictions that have been declared adequate by the European Commission.⁹⁸

We can conclude that adequacy decisions, by their very nature, stand out as instruments that promote an approach to both policy and institutional interoperability. However, as indicated by the analysis of the regulatory frameworks of the MERCOSUR Member States, intra-bloc adequacy decisions remain limited to date. For example, despite Argentina and Brazil being strategic trade partners and both being recognized as adequate by the EU, to date

they do not recognize each other as adequate. Meanwhile, countries such as Bolivia and Paraguay do not even have active adequacy decisions in place. Approval processes also tend to be lengthier, as demonstrated by the case of Brazil and the EU. Although the Latin American country enacted a personal data protection law in 2018 aligned with the European standard, established its supervisory authority in 2020, and achieved administrative autonomy in 2023, the European Commission's adequacy decision was not fully in place until 2026.

3.2. Standard Contractual Clauses and Binding Corporate Rules

Standard contractual clauses and binding corporate rules are not identical mechanisms. However, they share certain essential characteristics that justify addressing them jointly, at least for the scope of this study. First, both instruments facilitate international data transfers from an organization subject to a country's personal data protection framework to another located in a different country that is not deemed adequate by the former. Second, they are co-regulatory mechanisms. The following section will elaborate further on this concept when referring to other regulatory instruments.

Another shared element between contractual clauses and corporate rules is that the signatories or adopters of these instruments not only assume obligations, but also grant rights and safeguards to third-party beneficiaries. These third parties are the data subjects whose personal data is being transferred. In many cases, provisions are also included in favor of the supervisory authority of the exporting country, such as submission to its oversight or the duty to notify it of security incidents. These prerogatives in favor of data subjects and authorities are essential for contractual clauses and corporate rules to function as enabling mechanisms for cross-border personal data flows. Thus, when the

recipient country's regulations are not sufficiently aligned with those of the exporter, the transferring organization is tasked with ensuring that the recipient assumes the necessary obligations and safeguards so that data subject protection is not diluted as a result of the transfer. In other words, these instruments seek to extraterritorialize the reach of policy and institutional protection, thereby offering interoperability.

Regarding the main differences between standard contractual clauses and binding corporate rules, the latter are specifically designed as a mechanism to enable cross-border flows of personal data within corporate groups;⁹⁹ whereas standard contractual clauses can be used by organizations with no corporate affiliation.¹⁰⁰ Furthermore, as pre-approved models, standard contractual clauses generally do not require authorization from the supervisory authority. Binding corporate rules, on the other hand, are typically subject to a submission and approval process before the authority.¹⁰¹ This is because they are internal instruments tailored to the specific structure, business model, and data processing operations of a given corporate group, which prevents their generic standardization or pre-approval.

Taking this into account, standard contractual clauses and binding corporate rules could promote an approach centered on policy and institutional interoperability. To achieve this, it is essential that both the supervisory authorities responsible for approving these instruments and the organizations implementing them join forces to harmonize the standard contractual clauses and corporate rules approved across different jurisdictions.

Some practical applications would include, for instance, a corporate group adopting a single set of binding corporate rules that simultaneously satisfies the requirements of all jurisdictions from which data is exported; or an importer and exporter negotiating and executing a single contract to enable international transfers to

multiple destinations. There are valuable examples in this regard, such as the recognition of the RIPD model contractual clauses by various Latin American countries,¹⁰² the standard contractual clauses approved by the Consultative Committee of Convention 108,¹⁰³ or the joint guides by ASEAN and the European Commission and by ASEAN and the RIPD, for the joint implementation of the model clauses from each regulatory framework. Ultimately, this approach would reduce the administrative burden on organizations, allowing them to reallocate their resources toward ensuring the substantive and effective protection of transferred personal data.

Beyond the opportunities presented by these mechanisms, it is worth highlighting that they face certain practical limitations. In the case popularly known as *Schrems II*,¹⁰⁴ the Court of Justice of the EU made clear that standard contractual clauses do not function as a blank check to transfer data to any country. Due to their strictly contractual nature, these clauses are not binding on the authorities of importing countries. In its judgment, the Court determined that such clauses are insufficient on their own when the law of the destination country permits state interference with privacy, requiring data exporters to assess on a case-by-case basis whether a given flow of information demands the adoption of supplementary measures or, failing that, the suspension of the transfer. This doctrine was subsequently incorporated into the European Commission's 2021 standard contractual clauses and those of the RIPD, which contain specific provisions to operationalize this assessment of the destination country's legislation and the adoption of additional safeguards.¹⁰⁵

On the other hand, control over the effective compliance with the safeguards and commitments assumed in favor of data subjects is often limited. This deficiency is exacerbated when the exporter is a small or medium-sized organization and its counterpart is a large-scale technology company. In these scenarios, the disparity in

resources and specialized knowledge regarding data processing generates a profound information asymmetry. As a consequence, any actual oversight by the exporter becomes illusory, shifting the entire oversight burden onto the competent supervisory authority. This dynamic is particularly concerning in our region,¹⁰⁶ where regulatory bodies often lack the necessary technical and budgetary resources to tackle such a task.

3.3. Certifications, Seals, and Codes of Conduct

Most jurisdictions that recognize them as mechanisms to enable international personal transfers, certifications, seals, and codes of conduct—despite their differences in practical application—share the same theoretical foundation: co-regulation. Co-regulation is characterized by Hirsch¹⁰⁷ as a framework in which the public and private sectors play complementary roles in drafting and enforcing regulation. For instance, in the EU, in Brazil, and under APEC's CBPR and PRP systems, entities granting certifications must be previously evaluated and approved by the corresponding supervisory authorities. In the same vein, the Personal Data Protection Standards for the Ibero-American States of the RIDP recognize certifications as valid instruments for international transfers to non-adequate countries, provided that such certifications are recognized by the supervisory authority of the exporting country.¹⁰⁸ This hybrid approach can be understood as an evolution beyond both traditional state regulation and purely private self-regulation.

The traditional approach stems from the premise that the supervisory authority always possesses sufficient information and resources to enact regulations and audit compliance. Beginning in the 1980s, literature reflects a paradigm shift by recognizing that such an authority does not always have access to perfect information.¹⁰⁹ On the contrary, it assumes the existence of an information asymmetry between the regulator and the regulated

entity, which hinders the implementation of efficient regulations. For its part, the self-regulation approach posits that private organizations have incentives to monitor themselves, provided this aligns with customer preferences and thereby yields competitive advantages. At least within the realm of privacy and personal data protection, this latter model faces widespread criticism, as self-imposed standards tend to be low and lack adequate, independent, and transparent enforcement mechanisms.¹¹⁰

Co-regulation addresses the aforementioned challenges by promoting cooperation between the public and private sectors and facilitating information exchange between both spheres. This gives rise to policies and institutions that are more cost-effective for the public treasury, more effective at regulating private sector obligations, and, above all, better equipped to ensure the effective protection of the rights of individuals and data subjects.

Certifications, seals, and codes of conduct, by their very nature, present opportunities to drive policy and institutional interoperability. Currently, the most modern personal data protection regimes—such as those of the EU, Brazil, APEC, the RIPD, and even the MERCOSUR Agreement on Electronic Commerce—recognize these instruments, or some of them, as valid mechanisms to enable cross-border personal data flows to countries lacking an adequate level of protection. However, in practice, these schemes face certain challenges in their adoption. Compared to other regulatory instruments, particularly standard contractual clauses, certifications have a limited level of use. One of the potential causes could be that certifiers operate in closed blocs: on the one hand, those approved under the European ecosystem,¹¹¹ and on the other, the certifying agents of the CBPR and PRP systems, in their APEC and Global versions. Nevertheless, with sufficient momentum from both the public and private sectors, incentives could be aligned so that these blocs become more permeable, thereby allowing certifiers to emerge under more than one regulatory framework.

The promotion of multi-jurisdictional certifiers could enrich the dialogue between different legal and policy frameworks through the establishment of common compliance standards. Certifiers could thus drive audit processes designed to comply with multiple standards simultaneously or, alternatively, modular or tiered certification models where an organization's prior assessments serve as a baseline, allowing auditors to focus solely on the additional requirements of new frameworks.

Unlike standard contractual clauses and binding corporate rules, these mechanisms make it possible to reduce the supervisory burden on competent control authorities, given the presence of independent third parties responsible for auditing certified importers. This scenario can prove highly advantageous for a region in which supervisory authorities face budgetary constraints. This notwithstanding, in practice, certifiers may lack adequate powers and incentives to conduct effective compliance reviews. Furthermore, certifications, seals, and codes of conduct are not exempt from the objections raised in the case popularly known as *Schrems II*,¹¹² even though these mechanisms were not the specific subject of the ruling. The fact that an importer is certified does not eliminate the risk of interference with privacy by authorities in its country. Therefore, exporters relying on these instruments would also be required to assess, on a case-by-case basis, the need to adopt supplementary measures to the certification or, failing that, suspend the transfer.



04 | Conclusions

This study has identified the manner in which MERCOSUR regional instruments and the regulatory and institutional ecosystems of its Member States govern cross-border data flows. From this legal map, several relevant findings emerge that contribute to understanding the current state and challenges of data governance in the region.

First, a marked institutional asymmetry is observed: three of the five countries analyzed—Argentina, Brazil, and Uruguay—possess both a law in force and an operational supervisory authority. On the other hand, Paraguay has an approved regulatory framework that is pending entry into force and lacks an operational authority, while Bolivia lags behind on both counts. Added to this is the fact that, even among the countries that do have operational authorities, significant gaps exist in their powers or in the availability of human, technological, and financial resources. These disparities represent an exceptionally valuable opportunity to address the issue through a policy and institutional interoperability approach.

A positive aspect identified in this study is that none of the surveyed countries imposes data localization requirements explicitly and across the board, although in certain cases Uruguay requires notifying or seeking approval from the supervisory authority to transfer data internationally. This absence of generalized restrictions not only aligns the region with international standards, but also facilitates interoperability. While specific reasons may exist to require localization—such as national defense concerns—broad restrictions act as an obstacle to policy interoperability.

Regarding mechanisms to enable cross-border personal data flows, adequacy decisions are accepted by most of the countries analyzed.

However, Paraguay has not recognized any country as adequate due to the lack of an operational authority, while Bolivia lacks the regulatory framework to do so. Even among jurisdictions with more mature regulatory and institutional frameworks, inconsistencies are detected. Although Argentina and Uruguay recognize each other as adequate, they have not yet done the same with respect to Brazil, despite it being among their primary trading partners, the high alignment of their personal data protection laws, and the fact that the EU considers all three countries adequate. The recognition of the United States of America as an adequate jurisdiction also reveals discrepancies in the region. Uruguay recognized it under this category in 2023, though only regarding organizations certified under the Data Privacy Framework program,¹¹³ whereas Argentina committed to granting it such status in the Reciprocal Trade and Investment Framework Agreement between both countries,¹¹⁴ without specifying whether it will adopt a scheme analogous to the Uruguayan one. Conversely, Brazil has not yet shown significant progress toward an adequacy determination for the North American country. Thus, we can see that adequacy decisions are a mechanism with clear limitations, given that they often depend on geopolitical and diplomatic factors not necessarily linked to the actual level of data protection in the evaluated country.

Standard contractual clauses also enjoy widespread acceptance among MERCOSUR Member States. Argentina, Brazil, and Uruguay possess their own standard clauses or models based on proposals from international bodies. Among these, the RIPD model clauses stand out, having been adopted by Argentina and Uruguay, as well as by non-MERCOSUR member countries such as Ecuador, Peru, and Panama. Brazil's legal framework empowers its supervisory authority to approve clauses drafted by third parties, such as those of the RIPD. A decision to that effect could facilitate cross-border flows within the region. However, these mechanisms face implementation limitations. Key among them are the objections raised by the CJEU in the *Schrems II* ruling¹¹⁵ and the challenges in

monitoring compliance analyzed in Section 3—a critical hurdle for the region given the limited resources typical of local supervisory authorities.

The legal frameworks of Brazil and Paraguay, being more recent and largely aligned with the EU GDPR, expressly permit more modern policy instruments that are seeing growing global adoption, such as seals, certifications, and codes of conduct. While Argentina and Uruguay do not explicitly recognize these mechanisms in their domestic legislation, “self-regulation” mechanisms are indeed recognized in the MERCOSUR Agreement on Electronic Commerce.

¹¹⁶ As noted previously, we consider that the concept of “self-regulation” within the framework of the MERCOSUR Agreement on Electronic Commerce should be understood as a reference to co-regulation, encompassing at least codes of conduct and trust seals. These mechanisms represent a valuable opportunity for the region, as they alleviate the supervisory burden on control authorities by delegating the auditing of personal data importers to independent third parties.

Despite this advantage, seals, certifications, and codes of conduct as mechanisms to enable cross-border flows have a low level of adoption in our region, and even limited adoption in other parts of the world. While the causes are manifold and exceed the scope of this study, it is appropriate to put forward a few preliminary hypotheses. On the one hand, organizations may be reluctant to opt for these mechanisms due to the considerable investment of time and financial resources they require, especially when compared to standard contractual clauses or binding corporate rules. Furthermore, these schemes entail recognizing third-party audit powers, a territory many companies prefer not to venture into. Another decisive factor is limited government promotion, reflected in the absence of approved certification entities and consolidated certification ecosystems across several countries. For example, although Brazilian law explicitly permits these

mechanisms, its implementing regulations on international transfers¹¹⁷ omit regulating or promoting them. In contrast, international normative frameworks—such as those of ASEAN or APEC—promote a broader range of mechanisms enabling international data transfers. Notable among these are APEC's CBPR and PRP systems, along with their global versions. The approach taken by other blocs offers valuable insights for fostering policy and institutional interoperability, both within our region and in relation to other international integration frameworks.

To conclude, it is evident that MERCOSUR, as an area for the free movement of goods, services, and factors of production, must also move toward the free movement of personal data among its Member States. To achieve this, a certain degree of normative and institutional convergence is indispensable, which will take shape as all Member States establish laws in force and operational supervisory authorities. This convergence does not demand adopting the harmonization model of the European experience; rather, it can be grounded in an interoperability perspective tailored to the region. This entails a dimension of policy interoperability that fosters a fluid dialogue between different domestic frameworks, alongside a dimension of institutional interoperability that guarantees cooperation, the consistent application of personal data protection, and respect for data subjects' rights throughout the bloc.

While an intra-bloc adequacy decision emerges as the ultimate goal, achieving it demands sustained work and clear political will. Until that scenario consolidates, it will be essential for Member States to cooperate in the coordinated implementation of other mechanisms that facilitate cross-border flows, both within MERCOSUR and with other markets. Legal scholars have explored various alternatives to achieve this end, such as the cross-recognition by one bloc of the international transfer tools accepted by another.¹¹⁸ Actions of this nature will strengthen data governance within the bloc and

contribute to consolidating the integration process among Member States.



Notes

1. The Bolivarian Republic of Venezuela has been suspended as a MERCOSUR Member State since 2017.
2. MERCOSUR Resolution 37/19 on Consumer Protection and Consumer Protection in Electronic Commerce. Available in Spanish at: https://normas.mercosur.int/simfiles/normativas/73867_RES_037-2019_ES_Protecci%C3%B3n%20Consumidor%20Comercio%20Electr%C3%B3nico.pdf
3. Mutual Recognition Agreement of Digital Signature Certificates. Available in Spanish at: https://normas.mercosur.int/simfiles/normativas/75396_DEC_011-2019_ES_Acuerdo%20Firma%20Digital.pdf.
4. MERCOSUR Agreement on Electronic Commerce. Available in Spanish at: https://normas.mercosur.int/simfiles/normativas/82753_DEC_015-2020_ES_Acuerdo%20Comercio%20Electronico.pdf.
5. MERCOSUR, Digital Agenda Group (GAD). Minutes No. 07/24: XXX Ordinary Meeting of the MERCOSUR Digital Agenda Group. Pro Tempore Presidency of Uruguay (PPTU), September 26, 2024.
6. MERCOSUR -- EU Trade Agreement. Available in Spanish at: <https://www.cancilleria.gob.ar/es/politica-exterior/acuerdos-preferenciales-y-de-libre-comercio/ue-mercosur>.
7. MERCOSUR–Republic of Singapore Free Trade Agreement. Available in Spanish at: <https://www.cancilleria.gob.ar/es/politica-exterior/acuerdos-preferenciales-y-de-libre-comercio/acuerdo-libre-comercio-mercosur-singapur>.
8. Koneva, N., García Navarro, A. L., Sánchez-Macián, A., Hernández, J. A., Zukerman, M., & González de Dios, Ó. (2025). Introducing large language models as the next challenging internet traffic source. Available at: <https://arxiv.org/pdf/2504.10688>.
9. Weber, R. H. (2014). Promoting Interoperability in the Digital Ecosystem. Global Commission on Internet Governance Paper Series, No. 4. Centre for International Governance Innovation (CIGI). Available at: https://www.cigionline.org/static/documents/gcig_paper_no4.pdf.
10. John Howell J. & Ifayemi S., Policy Alignment on AI Transparency. Analyzing Interoperability of Documentation Requirements across Eight Frameworks. Available at: https://partnershiponai.org/wp-content/uploads/2024/09/PAI_Policy-Alignment.pdf
11. The CPTPP is an agreement concluded between Australia, Brunei Darussalam, Canada, Chile, Malaysia, Mexico, Japan, New Zealand, Peru, Singapore, and Vietnam. It is the successor to the Trans-Pacific Partnership (TPP), which failed to materialize after the United States withdrew from negotiations. For more information, see: Lerman, C., Szlak, G., & Mendiberri, L. S. (2022). *Acuerdo sobre comercio electrónico del Mercosur: Desafíos y oportunidades*. Asociación por los Derechos Civiles (ADC), p. 81. Available at: <https://adc.org.ar/wp-content/uploads/2022/09/ADC-Informe-Acuerdo-sobre-comercio-electronico-del-Mercosur.pdf>.

12. Article 14.5 of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership. Available in Spanish at: <https://www.subrei.gob.cl/acuerdos-comerciales/acuerdos-comerciales-vigentes/cptpp>.
13. Weber, R. H. (2014). Promoting Interoperability in the Digital Ecosystem. Global Commission on Internet Governance Paper Series, No. 4. Centre for International Governance Innovation (CIGI). Available at: https://www.cigionline.org/static/documents/gcig_paper_no4.pdf.
14. Palazzi, P. A. (2026). International Personal Data Transfer Agreement. CDYT.
15. Recitals 111 and 113 of Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR). Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679>.
16. European Data Protection Board. (2018). Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679. Available in Spanish at: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_es.pdf.
17. World Economic Forum. (2020). Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows. Available at: https://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20Flows_2020.pdf.
18. MERCOSUR Agreement on Electronic Commerce. Available in Spanish at: https://normas.mercosur.int/simfiles/normativas/82753_DEC_015-2020_ES_Acuerdo%20Comercio%20Electronico.pdf.
19. MERCOSUR–Republic of Singapore Free Trade Agreement. Available in Spanish at: <https://www.cancilleria.gob.ar/es/politica-exterior/acuerdos-preferenciales-y-de-libre-comercio/acuerdo-libre-comercio-mercosur-singapur>.
20. MERCOSUR–EU Trade Agreement. Available in Spanish at: <https://www.cancilleria.gob.ar/es/politica-exterior/acuerdos-preferenciales-y-de-libre-comercio/ue-mercosur>.
21. Available in Spanish at: <https://www.subrei.gob.cl/acuerdos-comerciales/acuerdos-comerciales-vigentes/cptpp>.
22. Available in Spanish at: https://www.subrei.gob.cl/docs/default-source/acuerdos/depa/depa-es.pdf?sfvrsn=4122158b_2.
23. Available in Spanish at: https://www.subrei.gob.cl/docs/default-source/acuerdos/argentina/texto-acuerdo-de-libre-comercio-chile-argentina.pdf?sfvrsn=da8b6d7_2.
24. Available in Spanish at: https://www.subrei.gob.cl/docs/default-source/acuerdos/uruguay/texto-alc-chile-uruguay.pdf?sfvrsn=85b8e4a5_0.
25. Available at: <https://ustr.gov/sites/default/files/files/Press/Releases/2026/US%20Argentina%20ARTI%20English%20Final%20February%202026.pdf>.
26. Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and its Additional Protocol. Approved and ratified by Argentina and Uruguay. Available in Spanish at: <https://www.argentina.gob.ar/normativa/nacional/ley-27483-318245/actualizacion>.

27. MERCOSUR Agreement on Electronic Commerce. Available in Spanish at: https://normas.mercosur.int/simfiles/normativas/82753_DEC_015-2020_ES_Acuerdo%20Comercio%20Electronico.pdf. .
28. Lerman, C., Szlak, G., & Mendiberri, L. S. (2022). MERCOSUR Agreement on Electronic Commerce: Challenges and opportunities. Association for Civil Rights [Asociación por los Derechos Civiles]. Available in Spanish at: <https://adc.org.ar/wp-content/uploads/2022/09/ADC-Informe-Acuerdo-sobre-comercio-electronico-del-Mercosur.pdf>.
29. The existence of these two objectives predates the MERCOSUR Agreement on Electronic Commerce and can be found in various precedents, including the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), Directive 95/46/EC, and the EU GDPR.
30. Article 6.8 of the MERCOSUR Agreement on Electronic Commerce. Available in Spanish at: https://normas.mercosur.int/simfiles/normativas/82753_DEC_015-2020_ES_Acuerdo%20Comercio%20Electronico.pdf.
31. Article 6.7 of the MERCOSUR Agreement on Electronic Commerce. Available in Spanish at: https://normas.mercosur.int/simfiles/normativas/82753_DEC_015-2020_ES_Acuerdo%20Comercio%20Electronico.pdf.
32. For further discussion on co-regulation models as an alternative to self-regulation, see Lerman, C., Szlak, G., & Mendiberri, L. S. (2022). MERCOSUR Agreement on Electronic Commerce: Challenges and opportunities. Association for Civil Rights [Asociación por los Derechos Civiles]. Available in Spanish at: <https://adc.org.ar/wp-content/uploads/2022/09/ADC-Informe-Acuerdo-sobre-comercio-electronico-del-Mercosur.pdf>.
33. Article 7.2 of the MERCOSUR Agreement on Electronic Commerce. Available in Spanish at: https://normas.mercosur.int/simfiles/normativas/82753_DEC_015-2020_ES_Acuerdo%20Comercio%20Electronico.pdf.
34. Articles 7.1 and 7.3 of the MERCOSUR Agreement on Electronic Commerce. Available in Spanish at: https://normas.mercosur.int/simfiles/normativas/82753_DEC_015-2020_ES_Acuerdo%20Comercio%20Electronico.pdf.
35. World Trade Organization (WTO), General Agreement on Trade in Services (GATS), 1994, Article XIV(c)(ii).
36. Article 8 of the MERCOSUR Agreement on Electronic Commerce. Available in Spanish at: https://normas.mercosur.int/simfiles/normativas/82753_DEC_015-2020_ES_Acuerdo%20Comercio%20Electronico.pdf.
37. See, for example, Recitals 10, 13, and 53, and Article 1 of Regulation (EU) 2016/679 of the European Parliament and of the Council ("General Data Protection Regulation"). Available in Spanish at: <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679>.
38. Chapter 12 of the Free Trade Agreement between MERCOSUR and the Republic of Singapore. Available in Spanish at: <https://www.cancilleria.gob.ar/es/politica-exterior/acuerdos-preferenciales-y-de-libre-comercio/acuerdo-libre-comercio-mercosur-singapur>.

39. Trade Agreement between MERCOSUR and the EU. Available in Spanish at: <https://www.cancilleria.gob.ar/es/politica-exterior/acuerdos-preferenciales-y-de-libre-comercio/ue-mercosur>.
40. The absence of detailed clauses on data transfers in European trade agreements reflects an explicit policy of the European Union, according to which the fundamental right to data protection should not be subject to trade negotiations. Regarding this institutional position separating trade disciplines from data protection guarantees, see European Data Protection Supervisor (EDPS), *Position paper on the transfer of personal data in the context of international trade negotiations*, 2018. Available at: https://www.edps.europa.eu/sites/default/files/publication/18-01-17_annex_2017-1120_en.pdf.
41. Article 8.10.2 of the Trade Agreement between MERCOSUR and the EU. Available in Spanish at: <https://www.cancilleria.gob.ar/es/politica-exterior/acuerdos-preferenciales-y-de-libre-comercio/ue-mercosur>.
42. Article 28.2 of the Trade Agreement between MERCOSUR and the EU. Available in Spanish at: <https://www.cancilleria.gob.ar/es/politica-exterior/acuerdos-preferenciales-y-de-libre-comercio/ue-mercosur>.
43. Currently, the Argentine enforcement authority is the Access to Public Information Agency [Agencia de Acceso a la Información Pública]. Prior to the entry into force of Decree No. 899/2017, this function was performed by the National Directorate for Personal Data Protection [Dirección Nacional de Protección de Datos Personales].
44. Law No. 27,483 (Official Gazette Jan. 18, 2019), approving Convention 108 of the Council of Europe, and Law No. 27,699 (Official Gazette Dec. 12, 2022), approving the Amending Protocol (Convention 108+).
45. AAIP Resolution No. 34/2019 establishes the jurisdictions that Argentina currently considers to provide adequate levels of personal data protection. Available in Spanish at: <https://www.boletinoficial.gob.ar/detalleAviso/primera/202373/20190226>.
46. To date, the supervisory authority has developed its own standard contractual clauses models for international transfers from controller to processor and from controller to controller, and has also approved the standard contractual clauses of the Ibero-American Data Protection Network (*Red Iberoamericana de Protección de Datos*). Models from the supervisory authority available in Spanish at <https://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/norma.htm>. Models from the Ibero-American Data Protection Network Available in Spanish at: <https://www.boletinoficial.gob.ar/detalleAviso/primera/296189/20231018>.
47. Regarding the RIPD standard contractual clauses, the possibility of making modifications to secondary aspects—provided their essence is not altered—stems from their implementation guide.
48. Available in Spanish at: <https://servicios.infoleg.gob.ar/infolegInternet/anexos/315000-319999/317228/norma.htm>.
49. The Brazilian supervisory authority is the National Data Protection Authority (Agência Nacional de Proteção de Dados - ANPD).

50. To date, the supervisory authority has only recognized the Member States of the EU and the European Economic Area as adequate. ANPD Resolution 32/26 available at: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/resolucao-no-32-decisao-de-adequacao-uniao-europeia-em-lingua-inglesa.pdf/@display-file/file>.
51. National Data Protection Authority (ANPD). (2024). Regulation on International Data Transfers (Approved by Resolution CD/ANPD No. 19 of August 23, 2024). Government of Brazil. Available in Spanish at: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/regulamento-de-tid-versao-em-lingua-espanhola.pdf>.
52. Distinct from the standard contractual clauses approved by the supervisory authority.
53. The transition period expires on August 7, 2028 (four years after its entry into force on August 7, 2024), pursuant to Article 13 of the Protocol of Accession of the Plurinational State of Bolivia to MERCOSUR. Available at: <https://www.mercosur.int/documento/protocolo-adhesion-bolivia-mercosur>.
54. Accessed in Spanish at: <https://diputados.gob.bo/proyectos-de-ley-archivados/>.
55. To date, the National Personal Data Agency (Agencia Nacional de Datos Personales), the enforcement authority under the new law, is not operational.
56. The supervisory authority is the Personal Data Regulatory and Control Unit (Unidad Reguladora y de Control de Datos Personales - URCDP).
57. Law No. 19,030 (Dec. 27, 2012), approving Convention 108 of the Council of Europe, and Law No. 19,948 (Apr. 16, 2021), approving the Amending Protocol (Convention 108+).
58. URCDP Resolutions No. 23/021 and No. 63/023 establish the jurisdictions that, to date, Uruguay considers as providing adequate levels of personal data protection. Available in Spanish at: <https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-23021> and <https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-63023>.
59. URCDP Resolution No. 63/023. Available in Spanish at: <https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-63023>
60. It should be noted that although Uruguay recognized adequacy for US companies certified under the EU-U.S. Data Privacy Framework, this does not imply that Uruguayan data subjects enjoy the same guarantees provided in that framework for European Union citizens.
61. URCDP Resolution No. 70/023. Available in Spanish at: <https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-70023>.
62. To date, the supervisory authority has approved the standard contractual clauses of the Ibero-American Data Protection Network (URCDP Resolution No. 50/022, available in Spanish at: <https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-50022>) and of the Consultative Committee of Convention 108 (URCDP Resolution No. 8/026, available in Spanish at: <https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-8026-sobre-clausulas-contractuales>).

63. Article 35 of Regulatory Decree 414/009 refers to these binding corporate rules as “codes of conduct.”
64. World Bank. (2024). Global Regulations, Institutional Development, and Market Authorities Perspective Toolkit (GRIDMAP): Data Markets Module Annexes. Available in Spanish at: <https://documents1.worldbank.org/curated/en/099082225093533728/pdf/P179766-b965d4b5-d8d9-4e11-9c67-5adadb951061.pdf>.
65. World Bank. (2024). Global Regulations, Institutional Development, and Market Authorities Perspective Toolkit (GRIDMAP): Data Markets Module Annexes. Available in Spanish at: <https://documents1.worldbank.org/curated/en/099082225093533728/pdf/P179766-b965d4b5-d8d9-4e11-9c67-5adadb951061.pdf>.
66. MERCOSUR E-Commerce Agreement. Available in Spanish at: https://normas.mercosur.int/simfiles/normativas/82753_DEC_015-2020_ES_Acuerdo%20Comercio%20Electronico.pdf.
67. World Bank. (2024). Global Regulations, Institutional Development, and Market Authorities Perspective Toolkit (GRIDMAP): Data Markets Module Annexes. Available in Spanish at: <https://documents1.worldbank.org/curated/en/099082225093533728/pdf/P179766-b965d4b5-d8d9-4e11-9c67-5adadb951061.pdf>.
68. The adoption of the RIPD model clauses extends beyond the regional bloc, having been approved by the supervisory authorities of non-MERCOSUR member countries such as Peru, Ecuador, and Panama.
69. MERCOSUR E-Commerce Agreement. Available in Spanish at: https://normas.mercosur.int/simfiles/normativas/82753_DEC_015-2020_ES_Acuerdo%20Comercio%20Electronico.pdf.
70. Available in Spanish at: <https://www.subrei.gob.cl/acuerdos-comerciales/acuerdos-comerciales-vigentes/cptpp>. To date, no MERCOSUR State Party is a party to the Treaty, but Argentina is in the accession process.
71. Available at: https://www.subrei.gob.cl/docs/default-source/acuerdos/depa/depa-es.pdf?sfvrsn=4122158b_2.
72. As previously noted, we consider that the concept of “self-regulation” within the framework of the MERCOSUR E-Commerce Agreement should be understood as a reference to co-regulation, incorporating at least codes of conduct and trustmarks.
73. Available at: https://www.subrei.gob.cl/docs/default-source/acuerdos/argentina/texto-acuerdo-de-libre-comercio-chile-argentina.pdf?sfvrsn=da8b6d7_2.
74. Available in Spanish at: https://www.subrei.gob.cl/docs/default-source/acuerdos/uruguay/texto-alc-chile-uruguay.pdf?sfvrsn=85b8e4a5_0.
75. MERCOSUR E-Commerce Agreement. Available in Spanish at: https://normas.mercosur.int/simfiles/normativas/82753_DEC_015-2020_ES_Acuerdo%20Comercio%20Electronico.pdf.
76. Available in Spanish at: <https://ustr.gov/sites/default/files/files/Press/Releases/2026/US%20Argentina%20ARTI%20English%20Final%20February%202026.pdf>.
77. Although it would not be the first Latin American country, as Mexico is a member of these spaces.

78. Uruguay ratified Convention 108 in 2013, and Argentina in 2019. The Additional Protocol, on the other hand, was ratified by Uruguay in 2021, and Argentina did so in 2023.
79. Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and its Additional Protocol. Approved and ratified by Argentina and Uruguay. Available at: <https://www.argentina.gob.ar/normativa/nacional/ley-27483-318245/actualizacion>.
80. To date, 34 States have ratified the Additional Protocol. Further information at: <https://www.coe.int/en-GB/web/conventions/full-list?module=signatures-by-treaty&treaty=223>.
81. Article 12 of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and its Additional Protocol. Approved and ratified by Argentina and Uruguay. Available in Spanish at: <https://www.argentina.gob.ar/normativa/nacional/ley-27483-318245/actualizacion>.
82. Association of Southeast Asian Nations. (2021). ASEAN Standard Contractual Clauses for Cross-Border Data Flows. Available in Spanish at: https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf.
83. Association of Southeast Asian Nations & European Commission. (2024). Joint Guide to ASEAN Standard Contractual Clauses and EU Standard Contractual Clauses. Available in Spanish at: <https://asean.org/wp-content/uploads/2024/02/Joint-Guide-to-ASEAN-Model-Contractual-Clauses-and-EU-Standard-Contractual-Clauses.pdf>.
84. Association of Southeast Asian Nations & Red Iberoamericana de Protección de Datos. *Joint Guide to ASEAN Model Contractual Clauses and RIPD Model Contractual Clauses*, 2025. Available in English at: <https://asean.org/book/joint-guide-to-asean-mccs-and-ripd-mccs/>.
85. Association of Southeast Asian Nations. (2021). *ASEAN Model Contractual Clauses for Cross-Border Data Flows*. Available in English at: https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf.
86. Asia-Pacific Economic Cooperation. (2015). APEC privacy framework. Available in Spanish at: [https://www.apec.org/docs/default-source/Publications/2017/8/APEC-Privacy-Framework-\(2015\)/217_ECSG_2015-APEC-Privacy-Framework.pdf](https://www.apec.org/docs/default-source/Publications/2017/8/APEC-Privacy-Framework-(2015)/217_ECSG_2015-APEC-Privacy-Framework.pdf).
87. Asia-Pacific Economic Cooperation. (2019). APEC Cross-Border Privacy Rules System: Policies, rules, and guidelines. Available in Spanish at: <https://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-updated-1709-2019.pdf>.
88. Asia-Pacific Economic Cooperation. (2020). APEC Privacy Recognition for Processors System: Policies, rules, and guidelines. Available in Spanish at: <https://cbprs.org/wp-content/uploads/2020/08/PRP-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-1.pdf>.
89. Available in Spanish at: <https://cbprs.org/compliance-directory/>.
90. Asia-Pacific Economic Cooperation. (2019). APEC Cross-Border Privacy Enforcement Arrangement (CPEA). Available in Spanish at: https://www.apec.org/docs/default-source/groups/ecsg/cbpr/cpea-2019.pdf?sfvrsn=f1643e20_1.

91. Global CBPR Forum. (2023). Global cross-border privacy rules (CBPR) framework. Available in Spanish at: <https://www.globalcbpr.org/wp-content/uploads/Global-CBPR-Framework-2023.pdf>.
92. Available in Spanish at: <https://www.globalcbpr.org/privacy-certifications/directory/>.
93. In some legislations, such as under the EU GDPR, there is an obligation to inform data subjects of international transfers, even when made to countries considered adequate.
94. For instance, Canada, the EU, and Argentina only grant adequate protection status to private sector organizations. Similarly, the EU and Uruguay only recognize U.S. entities that are certified under the Data Privacy Framework program.
95. Court of Justice of the EU. (2015). Maximillian Schrems v. Data Protection Commissioner (Case C-362/14). Available in Spanish at: <https://infocuria.curia.europa.eu/tabs/document?source=document&docid=169195&doclang=ES>.
96. See, for example, the review processes for the adequacy decisions of 11 countries completed in 2024: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_161.
97. National Data Protection Authority (ANPD). (2024). Regulation on International Data Transfers (Approved by Resolution CD/ANPD No. 19 of August 23, 2024). Government of Brazil. Available in Spanish at: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/regulamento-de-tid-versao-em-lingua-espanhola.pdf>.
98. Circular 005 of August 10, 2017 of the Superintendency of Industry and Commerce of Colombia. Available in Spanish at: <https://www.sic.gov.co/sites/default/files/files/Boletin-juridico/2017/circular005del10Ago2017.pdf>.
99. See, for example, Article 25 of the Regulation on International Data Transfers (Approved by Resolution CD/ANPD No. 19 of August 23, 2024): “Global corporate rules are intended for international data transfers between organizations of the same group or conglomerate of companies, having a binding nature in relation to the members of the group that subscribe to them.” Available in Spanish at: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/regulamento-de-tid-versao-em-lingua-espanhola.pdf>.
100. Although nothing prevents organizations within the same corporate group from relying on standard contractual clauses. This is relevant for jurisdictions where binding corporate rules are not recognized by regulation.
101. This is the case, for example, in the legal frameworks applicable in Argentina, Brazil, and the EU.
102. To date, the RIPD Model Contractual Clauses have been officially adopted by the data protection authorities of Argentina, Ecuador, Panama, Peru, and Uruguay.
103. Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108 Committee). *Model Contractual Clauses for the Transfer of Personal Data in the Framework of Convention 108+*, T-PD(2024)03. Available at: <https://rm.coe.int/es-t-pd-2024-3-mcc-compiled-es-/4880291e4d>.

104. Court of Justice of the EU. (2020). Maximillian Schrems v. Data Protection Commissioner (Case C-311/18). Available in Spanish at: <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:62018CJ0311>.
105. In the 2021 European model, this requirement is explicitly incorporated into Clause 14 (Local laws and practices affecting compliance with the Clauses), whereas in the RIPD models, it is included in Clause 4, which regulates the obligations regarding the assessment of local laws and public sector interference in the importing country.
106. From the World Bank report cited earlier in this work, it emerges that supervisory authorities in Latin America and the Caribbean declare the highest degree of dissatisfaction regarding their budget. For further information: World Bank. (2024). Global Regulations, Institutional Development, and Market Authorities Perspective Toolkit (GRIDMAP): Data Markets Module Annexes. Available in Spanish at: <https://documents1.worldbank.org/curated/en/099082225093533728/pdf/P179766-b965d4b5-d8d9-4e11-9c67-5adadb951061.pdf>.
107. Hirsch, D. D. (2011). The law and policy of online privacy: Regulation, self-regulation, or co-regulation? *Seattle University Law Review*, 34(2), 439. Available at: <https://digitalcommons.law.seattleu.edu/cgi/viewcontent.cgi?article=2003&context=sulr>.
108. Ibero-American Data Protection Network (RIPD), *Data Protection Standards for the Ibero-American States* (2026). Available at: <https://www.redipd.org/documento/estandares-iberoamericanos-2026.pdf>.
109. This paradigm shift takes place primarily in the regulation of monopolies and public utilities. See, for example, Baron, D. P., & Myerson, R. B. (1982). Regulating a Monopolist with Unknown Costs. *Econometrica*, 50(4), 911–930. Available at: <https://www.jstor.org/stable/1912769?seq=1>.
110. For further information on criticisms of self-regulatory models, see Lerman, C., Szlak, G., & Mendiberri, L. S. (2022). MERCOSUR E-Commerce Agreement: Challenges and Opportunities. Association for Civil Rights (ADC). Available in Spanish at: <https://adc.org.ar/wp-content/uploads/2022/09/ADC-Informe-Acuerdo-sobre-comercio-electronico-del-Mercosur.pdf>.
111. List available at: https://www.edpb.europa.eu/our-work-tools/accountability-tools/certification-mechanisms-seals-and-marks_en.
112. Court of Justice of the EU. (2020). Maximillian Schrems v. Data Protection Commissioner (Case C-311/18). Available in Spanish at: <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:62018CJ0311>.
113. URCDP Resolution No. 63/023. Available in Spanish at: <https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-63023>.
114. Available in Spanish at: <https://ustr.gov/sites/default/files/files/Press/Releases/2026/US%20Argentina%20ARTI%20English%20Final%20February%202026.pdf>.
115. Court of Justice of the EU. (2020). Maximillian Schrems v. Data Protection Commissioner (Case C-311/18). Available in Spanish at: <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:62018CJ0311>.
116. MERCOSUR E-Commerce Agreement. Available in Spanish at: https://normas.mercosur.int/simfiles/normativas/82753_DEC_015-2020_ES_Acuerdo%20Comercio%20Electronico.pdf.

117. National Data Protection Authority (ANPD). (2024). Regulation on International Data Transfers (Approved by Resolution CD/ANPD No. 19 of August 23, 2024). Government of Brazil. Available in Spanish at: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/regulamento-de-tid-versao-em-lingua-espanhola.pdf>.
118. Belli, L., Brian Nougreres, A., Mendoza Iserte, J., Palazzi, P. A., & Remolina Angarita, N. (2022). Towards a Latin American Adequacy Model for International Transfers of Personal Data. In *Protección de datos: doctrina y jurisprudencia*, Vol. 4, pp. 22–25.



<https://adc.org.ar/>