UNIO - *EU Law Journal*. Vol. 10, No. 1, May 2024, pp. 70-91.

School of Law – University of Minho

Is it worthwhile for Latin American countries to obtain adequate level of personal data protection from the European approach, or is it better to promote the use of contractual clauses to export such information?

Nelson Remolina Angarita*

ABSTRACT: The international transfer of personal data between countries with diverse legal cultures is set to continue growing as social and economic relationships expand alongside the increasing number of internet users and the widespread adoption of information and communication technologies worldwide. This paper proposes to re-evaluate the emphasis on the "adequate level of data protection" as a strategy to ensure the minimum standards for the proper handling of personal data when exported to other countries. Instead, it suggests that standard data protection clauses might be a more effective approach to achieve this objective. Ensuring an adequate level of data protection is essential for all countries. However, this does not necessarily mean that such a level can only be attained by adhering to processes established by foreign organisations or local authorities from other nations. The absence of a formal certification of an adequate level does not imply that a country lacks the effective mechanisms to ensure proper personal data treatment. The lengthy duration and high uncertainty associated with the adequacy processes are inconvenient for entities that need to legally export personal data to other countries. Therefore, standard data protection clauses are presented as a practical and sensible tool to achieve this goal. It is highly likely that the use of these clauses will eventually replace the need to rely on the "adequate level of data protection" framework.

KEYWORDS: Transfers of personal data to third countries – personal data – cross-border processing – adequate level of protection – standard data protection clauses.

* Associate Professor of the School of Law of the University of The Andes (Bogotá, Colombia).Founder (2001) and director of the GECTI - *Study Group on the Internet, E-Commerce, Telecommunications and Informatics*.

1. Introduction

The export and import of personal information must not become a scenario that reduces the level of protection afforded to the data subject in the country from which personal data is exported. Facing the international concern of states when the data of their citizens circulates across their borders, it has been established as a rule that data should not be sent to countries that do not guarantee an adequate level of protection.

As is well known, regulations on international data transfer or "*cross-border data flow*" seek to guarantee that the level of protection of the personal data of citizens of a country does not decrease or disappear when these must be exported or transferred to another country or countries.

At the end of December 2022, the Organisation for Economic Co-operation and Development (OECD) issued the Declaration on a Trusted, Sustainable and Inclusive Digital Future[1] in which are highlighted, among others, "*[t]he outcomes of the OECD Horizontal Project on Data Governance for Growth and Well-being (Going Digital phase III), which recognise the importance of data as a driver of the global economy (…)*".

This organisation has committed to working towards, among other things, a) "*[a]dvancing a human-centric and rights-oriented digital transformation that includes promoting the enjoyment of human rights, both offline and online, strong protections for personal data, laws and regulation fit for the digital age, and trustworthy, secure, responsible and sustainable use of emerging digital technologies and artificial intelligence.*", and b) "*[s]ecuring the welfare of consumers by empowering them to make informed decisions in the digital environment and by protecting them from misleading, manipulative, deceptive, fraudulent, unlawful, and unfair commercial practices, and unsafe and unsecure goods and services*".[2]

The Global Privacy Assembly (GPA), for its part, adopted the resolution "*Achieving global data protection standards: Principles to ensure high levels of data protection and privacy worldwide*" in October 2023, through which it insists on a decades-old idea: to have global standards regarding data protection and privacy. To this end, it promoted in the declaration some principles, rights and other elements as important to achieve high standards of protection of the aforementioned rights. In this regard, the GPA has decided the following:[3]

> Advocate for, promulgate and promote the principles, rights and other elements set out in this resolution, to ensure they can be effectively implemented and applied in all contexts, particularly in the processing of data with new and emerging technologies and innovations;
>
> Call on law and policy makers to consult data protection and privacy authorities as trusted expert advisers when enacting and amending data protection, privacy and related laws.

In that document, the GPA emphasised the «*importance of providing for the protection of personal data across borders with a range of transfer mechanisms, such as adequacy, model clauses,*

[1] See OECD, Declaration on a Trusted, Sustainable and Inclusive Digital Future, December 2022, OECD/LEGAL/0488. The declaration was the result of the meeting that took place on the island of Gran Canaria (Spain) on 14 and15 December 2022. The official text can be consulted at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0488.

[2] See OECD, Declaration on a Trusted, Sustainable and Inclusive Digital Future, December 2022.

[3] GPA, 45th Closed Session of the Global Privacy Assembly, October 2023: Achieving global data protection standards: Principles to ensure high levels of data protection and privacy worldwide. Available at: https://globalprivacyassembly.org/document-archive/adopted-resolutions/.

certifications and administrative arrangements, to ensure that protection "travels" with the data» and noted the "*benefits of building on commonalities, complementarities and elements of convergence in order to foster future interoperability between existing regulatory approaches and mechanisms enabling safe, trustworthy cross border data flows*".[4]

The transfer of information between countries with different legal cultures is a reality that tends to continue growing as social and economic relations increase along with the growth of Internet users and the massive immersion of ICT in the world.[5] We live in a globalised and technologically interconnected society where the Internet has significantly facilitated the possibilities of information exchange.[6]

This text proposes to rethink whether it is worth continuing to insist on an adequate level of data protection as a strategy to achieve a minimum of due processing of personal data when they are exported to other countries or if, on the contrary, it is better to resort to contractual clauses to achieve said objective.

2. On cyberspace and personal data

Personal data circulates daily in "*cyberspace*". However, the regulation on data processing emerged in a scenario where cyberspace was not yet being discussed. In other words, the current socio-technological reality was not the same as when the first regulations on personal data protection were issued.

In addition to the above, information (and personal data) is a key and essential piece of cyberspace. Although there are different meanings of cyberspace, we consider it relevant to keep in mind that it is made up of the following elements:[7]

A technological infrastructure (technological resources) made up of countless equipment (servers, computers, mobile phones, tablets, among others) that are in many parts of the world.

A worldwide communications platform (global communications network), information and interconnected networks (Internet) of global reach called "*global information infrastructure*".[8]

Millions of people and organisations of various nationalities, domiciled in countries with dissimilar legal systems, who, from anywhere in the world, make use of technology, communications and information to interact with other people or use the services available on the Internet.

Huge amounts of information (including personal data) constantly circulating locally and cross-border.

---

[4] GPA, 45th Closed Session of the Global Privacy Assembly, October 2023: Achieving global data protection standards: Principles to ensure high levels of data protection and privacy worldwide.

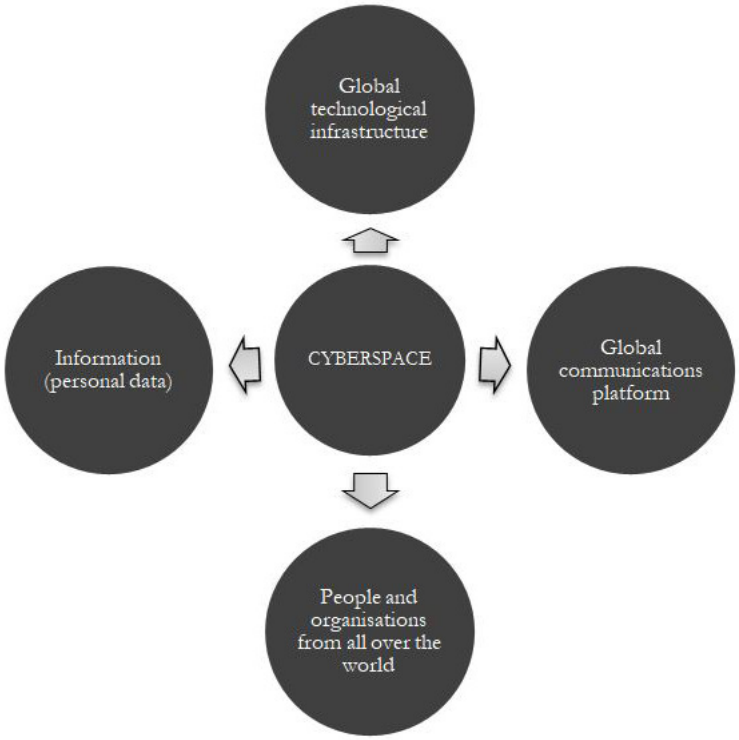
[5] In 1980 the OECD recognised that data flows "have greatly increased in recent years and are bound to continue to grow as a result of the introduction of new computer and communication technology" (from OECD, Council Recommendation on guidelines on the protection of privacy and transborder flows of personal data, 1980).

[6] Cécile De Terwangne, "Is a global data protection regulatory model possible?", in *Reinventing Data Protection?*, ed. Serge Gutwirth *et al.* (Netherlands: Springer, 2009), 175, 177. This author defines our society as "the globalized and networked society".

[7] On some characteristics of cyberspace and the challenges it generates for the Law, see David R. Johnson and David Post, "Law and Borders – The Rise of Law in Cyberspace", *Stanford Law Review*, vol. 48, no. 5 (1996): 1367.

[8] Reidenberg refers to it as «the global information infrastructure ("GII")», [Joel R. Reidenberg, "Governing networks and rule-making in cyberspace", *Emory Law Journal*, vol. 45 (1996): 911, 912].

The above can be graphed as follows:



Graph no. 1. Elements of Cyberspace.
Author's elaboration.

Little by little, we are witnessing the migration from the physical and border world to a technological "*cyberspace*" without geographical borders. We live on a planet divided into territories whose majority of activities are governed by national regulations and authorities with territorial (not cross-border) jurisdiction.[9] At the same time, we are witnessing a process of erosion and disintegration of territorial borders and the emergence of a space of enormous magnitude where the number of people interacting in cyberspace progressively increases.

The world is, among others, a large territory delimited by physical borders, within which live people subject to local (territorial) legal regulations and authorities of the same nature. Both are part of the national legal framework binding on the subjects within a certain space. In this context, the scope of application of the rules, the authorities, their legal competence, the effects of their decisions and the dispute resolution mechanisms were created by the regulators of a territory to be applied in that territory.[10] In the case of certain cross-border issues efforts have been made to respond to them through the rules of international law. That has been, roughly speaking, the legal scenario in which we have lived for several centuries.

Applying the above to the arena of the right to due processing of personal data, we find the following scenario. Several countries have general and local regulations that are mandatory for the processing carried out in each of their territories. The scope of application is normally defined in local regulations on PPD (Processing of

[9] It can be stated that the legal world is currently an amalgam of: (i) local regulators with a field of action defined by a territory; (ii) regulation based on territorial bases; and (iii) dispute resolution normally carried out by judges or authorities with jurisdiction delimited by a territory.
[10] In this sense, see Reidenberg, "Governing networks and rule-making in cyberspace", 914.

Personal Data). To enforce such regulations, they created national data protection authorities with territorial jurisdiction.

We currently do not have an international legal instrument on PPD binding on all countries in the world. There is only one binding international regional agreement, with few exceptions, on European countries. The point to be determined is whether these national and international rules and institutions are sufficient, relevant, and efficient to respond to the challenges that are evident every day in a world called "*cyberspace*", where activities can involve people from diverse legal systems and/or geopolitical areas of the world. In cyberspace, geographical limits are not barriers to interaction, and activities can occur without physical-territorial contact.

Cyberspace has been characterised as a global scenario not delimited by geographic borders[11] where activities occur within the technological architecture of the Internet which, as we saw, is in full bloom of growth from the perspective of the number of users. There is no defined physical space (like our house or the territory of our country) but rather an artificial or virtual and indeterminate field where people interact. In the words of the quoted professor, "*people 'connect' to these virtual spaces and act in them*".[12] Many of these actions in the virtual world have legal implications and consequences in the real world.

Although Internet activities are, in part, intended to be cross-border, this does not mean that the physical borders that delimit the geographical limits of states have disappeared. These borders continue to exist, although in practice technology allows many activities to be carried out without local authorities being able to prevent it or try to control it as they do, for example, in the case of immigration of people or in customs controls of goods moving from one country to another.

It is cross-border to the extent that any activity on the Internet can involve the use of a technological network whose components are distributed in physical locations established in many parts of the world. It is also cross-border because it means that a subject from any part of the world carries out activities that affect subjects located in other countries in the world. On the Internet, what happens in one country (for example, the country of the international collector) can affect people located in other countries (such as the data owner located in a different country than the collector).

3. International transfer in the European General Data Protection Regulation

On 25 January 2012, a proposal for a Regulation[13] was presented to update Directive 95/46/EC, which was conceived at a time when the use of the Internet was not massive nor was its penetration rate high in the world.[14] The process culminated

[11] See Michael Guilden, "Jurisdiction and the Internet: the "real world" meets cyberspace", *ILSA Journal of International & Comparative Law*, vol. 7, no. 1 (2000): 149, 150.

[12] Lawrence Lessig, *El código y otras leyes del ciberespacio*, trans. E. Alberola (Madrid: Grupo Santillana de Ediciones S.A., 2001), 35.

[13] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM/2012/011 final - 2012/0011 (COD)), 2012. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52012PC0011.

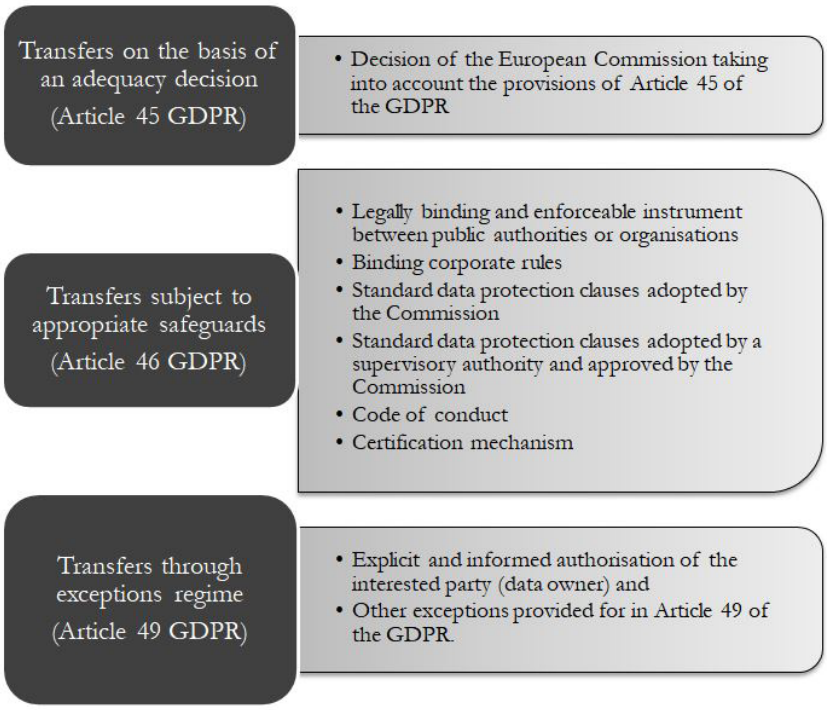
[14] According to the Internet World Stats and the International Telecommunication Union (ITU), the Internet penetration rate in 1995 was 0.4% of the world population. The Court of Justice of the European Union (CJEU), for its part, stated at the time that "Chapter IV of Directive 95/46 contains no provision concerning use of the internet. In particular, it does not lay down criteria for deciding

with the issuing of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

The recitals of the European Union General Data Protection Regulation (hereinafter, GDPR) summarise the general ideas of the European approach to international transfers to the extent that, on the one hand, they highlight that "*[f]lows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation*", but, on the other hand, they are emphatic in emphasising that "*when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation*".

The international transfer of data was regulated in Chapter V (Transfers of personal data to third countries or international organisations), which, among others, establishes the following aspects: a) general principle for transfers (Article 44); b) transfers on the basis of an adequacy decision (Article 45); c) transfers subject to appropriate safeguards (Article 46); d) binding corporate rules (Article 47); e) transfers or disclosures not authorised by Union law (Article 48); f) derogations for specific situations (Article 49); and g) international cooperation for the protection of personal data (Article 50).

The main alternatives offered by the GDPR to transfer personal data are summarised below:



Graph no. 2. Main alternatives offered by the European General Data Protection Regulation (GDPR) to transfer personal data.

Author's elaboration.

whether operations carried out by hosting providers should be deemed to occur in the place of establishment of the service or at its business address or in the place where the computer or computers constituting the service's infrastructure are located" (Judgment CJEU *Göta hovrätt - Switzerland and Bodil Lindqvist*, 6 November 2003, Case C-101/01, ECLI:EU:C:2003:596, recital 67).

As a rule, the regulation establishes that transfers to a third country or international organisation can only be made if the controller and the person in charge of the treatment comply with the conditions established by the regulation, including those relating to subsequent transfers of personal data from the third country or international organisation to another third country or other international organisation. The above aims to maintain the principle of continuity in protecting data owners so that the protection offered by European regulation and its institutions is not diminished or undermined.[15]

Transfers based on the adequacy decision do not require any authorisation when the data is sent to a third country, a territory or one or more specific sectors of that third country, or international organisation that according to the Commission has an adequate level of protection.[16] The regulation establishes the elements that the Commission must keep in mind to classify a country with an adequate level.[17]

If the destination of the transfers does not have an adequate level, the data may be exported if adequate guarantees are granted, such as the following: "*a) a legally binding and enforceable instrument between public authorities or bodies; b) binding corporate rules;*[18] *c) standard data protection clauses adopted by the Commission; d) standard data protection clauses adopted by a supervisory authority and approved by the Commission; e) an approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or f) an approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights*".[19]

Regarding international data transfers, it should be noted that the responsibility of the data exporter to observe all the obligations included in the regulation, but the responsibility is also established in the case of onward transfers, that is, when data transferred to one country is then sent from that country to another country (or countries). In any case, international cooperation[20] with the authorities of other

[15] See Article 44 GDPR.

[16] See Article 45(1) GDPR.

[17] According to Article 45(2) GDPR these are the elements: "a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred; b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data".

[18] Article 47 GDPR establishes the requirements that the Binding Corporate Standards must meet.

[19] Article 46(2) GDPR.

[20] See Article 50 GDPR: "a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data; b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms; c) engage relevant

countries is considered necessary to guarantee compliance with data protection regulations and respect for individual rights.

The GDPR indicates the requirements that must be considered when the transfer occurs in any of these hypotheses: a) with an adequacy decision; b) through appropriate guarantees, c) with binding corporate rules and d) through a regime of exceptions.

The transfer made to international organisations, countries, a part of the country or a processing sector (group of companies or companies in the same sector) that have been the subject of a decision of the European Commission is free and does not require additional authorisations certifying that they have an adequate level of protection.[21] Regarding this level, Article 45 indicates the criteria that must be met to determine it (i.e., the existence of the rule of law, general or sectoral legislation, jurisdictional resources, the existence and effective functioning of control authorities, and the international commitments the country assumes.). At this point, the possibility of geographical and sectoral application of the adequate level within a country is novel.

In the event that the country does not have an adequate level of protection or an unfavourable decision on said level has been made by the Commission, the transfer can only be carried out if appropriate guarantees are offered through a legally binding document. In Article 46(2), the following are stated as appropriate guarantees: a) binding corporate rules; b) standard data protection clauses adopted by the Commission or by the supervisory authority and c) contractual clauses between the person responsible or in charge of processing and the recipients of the data, previously authorised by the data protection authority of the country of origin of the data.

Binding corporate rules are conceived as a tool that allows international transfer within a group of companies with headquarters outside the European Union (EU). Article 47 GDPR establishes that supervisory authorities must consider the following aspects to approve binding corporate rules. First of all, that they "*apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees, who will ensure compliance*". Secondly, that they "*expressly confer enforceable rights on data subjects*", and finally, that they fulfil the requirements laid down in the paragraph.

Finally, if there is no adequacy decision or appropriate guarantees for the international transfer, it may be carried out exceptionally in the cases provided for in Article 49 GDPR, within which it is highlighted that the owner of the data "*has consented to the proposed transfer, after having been informed of the possible risks due to the absence of an adequacy decision and appropriate safeguards*".

4. Contracts as an alternative to export personal data

Contracts represent an exceptional legal alternative to facilitate the international circulation of personal data. It favours both companies from countries not classified

stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data; d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries".

[21] See Article 45(1) GDPR: "A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation".

with an adequate level of protection that wish to "*import*" personal data from Member States of the European Community and companies from said community that wish to "*export*" such information to third countries in the above circumstances. Academics[22] have recommended the use of contractual clauses for international transfers as, among others, an accountability tool (proven responsibility). Specifically, it is suggested to *articulate* accountability *tools in a contract adjusted to the particularities of each transfer.*

In 2018, for example, through the *Guía GECTI para la implementación del principio de responsabilidad demostrada -accountability- en las transferencias internacionales de datos personales. Recomendaciones para los países latinoamericanos*[23] it was noted that contracts represent a legal alternative to demonstrate the implementation of accountability measures in international data transfers. Although there are contract models in this matter, the contract must be consistent with the peculiarities and needs of each organisation and the regulations of each country. Likewise, it is relevant that the data exporter tries to establish whether the data recipient in another country is a serious and responsible company or organisation (not a data haven) that will comply with contractual obligations.

When drafting the contract, it was suggested that several aspects be considered:

"*- The legal nature of the data that will be exported to another country. Depending on the nature of the data (sensitive, minor, private, semi-private, public), agree on special protection measures. Remember, for example, that the processing of sensitive data requires enhanced responsibility, that is, greater security measures, greater restrictions on access, use and circulation.*

- The security measures that the recipient (importer) of the data exported to another country must comply with.

- The amount of data to be exported.

- What are the rights that the recipient of the information or importer must guarantee to the owner of the data?

- What are the principles of personal data processing that the importer or recipient of the data must observe or guarantee?

- Who will be able to access the exported information?

- The mechanisms so that the owner of the data can exercise their rights in a simple and expeditious manner before the recipient of the exported data.

- The purposes for which the data is transferred. It is very important to clarify what the recipient of the transferred data can and cannot do.

- What will be the time limit during which the recipient of the transferred data will be able to process it?

- The data protection law that will govern the contract. It will be the law of the country of the exporter of the data or that of the importer of the data. If you want to guarantee the principle of "continuity of data protection" that we refer to in this document, it is recommended that the contract be governed by the data protection law of the country from which it will be exported.

- The possibility or not of making subsequent transfers to other countries. Make clear whether data initially transferred to one country (A) can later be transferred from that country (A) to another country (B). If so, establish the conditions that must be observed for this purpose.

- What to do to recover the transferred data and guarantee the rights of its owners when the

[22] See Nelson Remolina Angarita, Álvarez Zuluaga, Luisa Fernanda, *Guía GECTI para la implementación del principio de responsabilidad demostrada -accountability- en las transferencias internacionales de datos personales: Recomendaciones para los países latinoamericanos* (Bogotá: University of the Andes, Faculty of Law, GETCI, 2018). Available at: https://habeasdatacolombia.uniandes.edu.co/?p=2817.

[23] The text of the GECTI guide is available at: https://habeasdatacolombia.uniandes.edu.co/?p=2817.

export recipient breaches the contract?
- Who will respond to the data protection authority or the data owners for any improper processing of the exported information and for any damages caused?
- What will be the liability (joint or solidary) of the exporter and importer of the data towards the owner of the data for possible violations of their rights or damages caused?
- What will be done with the data once the contract ends?"[24]

This academic guide was taken into account by the Superintendency of Industry and Commerce – Colombian data protection authority – to issue in 2019 the *Guía para la implementación del principio de responsabilidad demostrada en las transferencias internacionales de datos personales.*[25]

4.1 The contractual clauses of the Ibero-American Data Protection Network (IDPN)

Recently, the Ibero-American countries members of the Ibero-American Data Protection Network (IDPN) approved the *Guía de implementación de las cláusulas contractuales modelo para la transferencia internacional de datos personales (TIDP)*. The text was written by the Argentine expert and Professor Pablo Palazzi. Additionally, it had the support and observations of the members of the IDPN and third parties who, within the preparation process, presented their opinions or suggestions. The Guide of MCCs[26] is accompanied by an annex containing two models for international transfer, namely:

Model agreement for international transfer of personal data between controller and controller.

Model agreement for international transfer of personal data between controller and processor.

When drafting them, the international precedents on international transfers of personal data (ITPD) were taken into account, especially those that give carte blanche to the use of contracts as an alternative to legitimise the sending of personal data from one country to another country (or countries). Additionally, the guidelines on contractual clauses in Europe were considered.[27] Obviously, reference was made to the provisions of the IDPN 2017 Standards and the local regulations of some IDPN countries[28] that expressly or tacitly refer to the ITPD and contractual clauses.

---

[24] See Nelson Angarita, Álvarez Zuluaga, Luisa Fernanda, *Guía GECTI para la implementación del principio de responsabilidad demostrada -accountability- en las transferencias internacionales de datos personales: Recomendaciones para los países latinoamericanos*. This excerpt was freely translated.

[25] The text of the guide is available at: https://www.sic.gov.co/sites/default/files/files/pdf/Gu%C3%ADa%20%20SIC%20para%20la%20implementaci%C3%B3n%20del%20principio%20de%20responsabilidad%20demostrada%20en%20las%20transferencias%20internacionales(1).pdf.

[26] The text of the guide and the annex (Model contractual clauses) are available at: https://www.redipd.org/es/documentos/guias.

[27] The following texts were taken into account, among others: (1) Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021D0914; (2) Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021D0914.

[28] Argentina, Brazil, Cabo Verde, Colombia, Ecuador, Mexico, Nicaragua, Panama, Peru, Democratic Republic of São Tomé and Príncipe, Dominican Republic and Uruguay.

For the IDPN, the objective of the model contractual clauses (MCCs) is "*to ensure and facilitate compliance with the requirements provided for by the data protection law of the country of the data exporter for the transfer of personal data to a third country that has not been recognised with an adequate level of protection. The idea is that the protection initially granted to personal data continues to be present regardless of where this data is located. That is why subsequent transfers are also regulated with precautions to avoid a decrease in the level of protection. Intervention is given to the owners through a universal contract law concept called third party beneficiary. And access by public authorities in the importer's jurisdiction to data that may affect the owner's rights is regulated.*"[29]

The Guide incorporates in the glossary the following definitions, which are useful to understand the drafting of the MCCs:

"P*rocessor: service provider who, as a natural or legal person or public authority, outside the organisation of the controller, processes personal data in the name and on behalf of the controller.*

Data exporter: private natural or legal person, public authority, services, organisation or service provider located in the territory of a state that carries out international transfers of personal data, in accordance with the provisions of these standards.

Data importer: private natural or legal person, public authority, service, body or service provider located in a third country that receives personal data from a data exporter through an international transfer of personal data.

Controller:[30] *private natural or legal person, public authority, services or body that, alone or jointly with others, determines the purposes, means, scope and other issues related to the processing of personal data.*

Sub-processor: when a processor uses another processor to carry out certain processing activities on behalf of the controller.

Third party beneficiaries: owner whose personal data is the subject of an international transfer under this agreement. The owner is a third party beneficiary of the rights provided in his favour in the MCCs and therefore can exercise the rights that the MCCs recognise, even if he has not signed the model contract between the parties.

Onward transfer: transfer of data by the data importer to a third party located outside the jurisdiction of the data exporter that meets the guarantees established in the MCCs."[31]

According to IDPN, MCCs are a "*ready to use*" and "*ready to execute*" instrument[32] in an easy, simple and immediate way. The IDPN points out that "*MCCs are the most accessible and used legal mechanism today for ITPD to non-suitable jurisdictions. It is estimated that around 80 to 90% of companies that implement ITPD mechanisms use MCCs as a solution*".[33]

The following are some advantages and benefits of using MCCs:

Overcome possible limitations to the ITPD when the exporting country and the destination country have different levels of data protection. Common data protection standards are created through contractual means.

Regulatory harmonisation of sensible levels of protection of personal data between exporters and importers of this type of information is promoted.

A contractual balance is achieved between the parties by having model clauses

[29] See IDPN, *Guía de implementación de las cláusulas contractuales modelo para la transferencia internacional de datos personales (TIDP)*, 16. This excerpt was freely translated.

[30] In other words, in charge of.

[31] See IDPN, *Guía de implementación de las cláusulas contractuales modelo para la transferencia internacional de datos personales (TIDP)*, 25-26. This excerpt was freely translated.

[32] See IDPN, *Guía de implementación de las cláusulas contractuales modelo para la transferencia internacional de datos personales (TIDP)*, 17.

[33] See IDPN, *Guía de implementación de las cláusulas contractuales modelo para la transferencia internacional de datos personales (TIDP)*, 18.

prepared by third parties who are experts in the processing of personal data and not by the strong part of the contract.

Trust is generated between the parties and data owners by using a contract model pre-approved by experts and data authorities.

Transfer costs are reduced because it is not necessary for companies to go to their internal or external advisors to prepare or draft the contract (elimination of professional fee costs).

This is good news for those who want to export data to countries that do not have an adequate level of protection, because the process of granting the "*adequate level*" has proven to be very delayed, cumbersome and very formalistic[34] because it focuses on comparing regulations and not on verifying whether they are fulfilled in practice.

5. From the adequate level of personal data protection towards the contractual clauses for data transfers?

The expression "*adequate level of protection*" (ALP) emerged in Europe when establishing rules for transferring personal data from there to third countries. Being classified by Europe as a country with this degree of protection is neither simple nor expeditious. It typically requires countries to issue appropriate regulations and make institutional changes. In fact, it can be stated that Article 25 of Directive 95/46, from 1995, was the trigger of the need for many countries to regulate the processing of personal data and adopt the European approach to be recipients of data coming from Europe.

The reason for the import of the European model in many countries is very simple: for Europe, the "*adequate level of protection*" is that derived from regulations such as, at the time, Directive 95/46/EC or the current GDPR. This phenomenon is referred to and explained by Palazzi under the heading of "*expansion of the European model to non-European countries*" citing authors such as Colin Bennett and Joel Reidenberg who *respectively have referred to the "external* impact of the European Data Protection Directive" and to the "*globalization of privacy solutions*".[35]

In addition to having a legal framework on the subject, it is necessary for the interested country to initiate a procedure before the European Commission[36] so that it is formally classified as a country with an "*adequate level*". This process, according to some experiences, takes a little more than two years. In fact, the European authorities

[34] Establishing the appropriate level is not only a formal matter of comparing the texts of local regulations with those of the country to which the data will be exported, but also of evaluating the actual protection mechanisms (administrative, judicial) that the owner has to protect adequately their data in another state, as well as verifying the existence of independent, technical and efficient data protection authorities. In other words, the actual level of protection that a country offers in practice should be established. In the case of protection authorities, for example, the number of citizen complaints received should be considered, as well as the actions initiated to respond to said complaints along with the orders or sanctions issued to protect rights and punish violators of the data processing regulation.

[35] Pablo A. Palazzi, *La transmision internacional de datos personales y la proteccion de la privacidad. Argentina, América Latina, Estados Unidos y La Unión Europea* (Buenos Aires: Ad-Hoc, 2002), 39-41.

[36] According to the official website of the European Commission, it is the "executive body of the EU and represents the interests of Europe as a whole." Its main functions are: "to set objectives and priorities for action; propose legislation to Parliament and Council; manage and implement EU policies and its budget; ensuring that European law is applied (jointly with the Court of Justice) and representing the EU outside Europe (negotiating trade agreements between the EU and other countries, etc.)." See: https://commission.europa.eu/index_en.

recognise that "*the Commission is unlikely to adopt adequacy findings (…) for more than a limited number of countries in the short or even medium term*".[37]

The then Working Party on the protection of individuals concerning the processing of personal data (also known as the Working Party of Article 29 of Directive 95/46/EC) – today the European Data Protection Board (EDPB)[38] – adopted two documents in 1997[39] and 1998[40] that established the possible ways of evaluating the level of protection of third countries. They stated that an adequate level of protection depends on several factors of a regulatory nature and of an "*instrumental and institutional*" nature (procedural and application requirements). The first, roughly speaking, is the result of a mixture of rights held by the data owner and obligations for those who process personal information or who exercise control over said processing.

The second includes, on the one hand, the existence of judicial and non-judicial mechanisms and procedures that guarantee the effectiveness of the rules, sanction non-compliance and grant the affected person a right of reparation against the improper processing of their information. Additionally, the existence of an independent authority is considered necessary that not only controls, monitors and sanctions those who possess personal data, but also receives complaints from citizens and initiates the pertinent investigations with a view to becoming a guarantor of the protection of their data.

There it was specified that any analysis to establish the adequate level of protection must focus on two basic elements: the content of the applicable standards and the means to guarantee their effective application. Both elements are crucial because the rules are of little use if they are not met, which is why we agree that "*data protection rules only contribute to the protection of individuals if they are followed in practice*".[41]

Based on a small comparative analysis[42] of the opinions and decisions of the EC on "*adequate level*" that it has issued since 1999, in the cases of Switzerland,[43]

[37] See recital 4 of Decision 2001/497/EC.

[38] The EDPB is composed of the representatives of the national data protection authorities of the EU/EEA countries and of the European Data Protection Supervisor. Its main tasks are: "providing general guidance on key concepts of the GDPR and the Law Enforcement Directive, advising the European Commission on issues related to the protection of personal data and new proposed legislation in the European Union, and adopting binding decisions in disputes between national supervisory authorities" (see: https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en). More information on the EDPB available at: https://www.edpb.europa.eu/edpb_en.

[39] European Commission, Working Party on the Protection of Individuals with Regard to the Processing of Personal Data – First orientations on Transfers of Personal Data to Third Countries – Possible Ways Forward in Assessing Adequacy, XV D/5020/97-EN final WP4, Brussels, 1997.

[40] European Commission, Working Party on the Protection of Individuals with Regard to the Processing of Personal Data – Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, DG XV D/5025/98 WP12, Brussels, 1998.

[41] See European Commission, First orientations on Transfers of Personal Data to Third Countries – Possible Ways Forward in Assessing Adequacy, 5 and European Commission, Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, 5.

[42] By 2024, several countries have obtained the adequate level. For the purposes of our analysis, we only considered eight. Details about the four countries not analysed can be consulted in the respective decision issued in each case by the European Commission: Canada – Commission Decision 2002/2/EC of 20 December 2001 on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act; Israel – Commission Decision 2011/61/EU of 31 January 2011; Andorra – Commission Decision 2010/625/EU of 19 October 2010; and New Zealand – Commission Decision 2013/65/UE of 19 December 2012.

[43] See European Commission, Commission Decision of 26 July 2000 pursuant to Directive 95/46/

Hungary,[44] Argentina,[45]Guernsey,[46] Isle of Man,[47] Jersey,[48] Faroe Islands[49] and Uruguay[50] the following can be established:

> 100% of the "*third countries*" analysed have a general rule on protecting personal data that incorporates the basic principles mentioned. Additionally, they have sectoral provisions for the processing of some personal data in particular. 75% of the countries have acquired international commitments regarding data protection, particularly by signing Convention 108 of 1981. 42.85%, for their part, have a constitutional norm that refers to the topic under study.

It is important to note that an "*adequate level of protection of personal data*" does not mean establishing whether one country has the same protection system. In this sense, the Court of Justice, by ruling of October 6, 2015 in case C-362/14, *Maximillian Schrems v. Data Protection Commissioner*[51] (*Schrems*), specified that it is not required that the country to be evaluated or certified has an identical level of protection and that the important thing is to demonstrate that the means used by the third country in question to protect personal data are effective in guaranteeing an adequate level of protection.[52]

In line with the above, in the United States adequate level decision of 10 July 2023, the European Commission noted that the "*standard therefore does not require a point-to-point replication of Union rules. Rather, the test is whether, through the substance of privacy rights and their effective implementation, supervision and enforcement, the foreign system delivers the required level of protection.*"[53]

EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland (Decision 2000/518/EC).

[44] Working Party on the protection of individuals with regard to the processing of personal data, Opinion 6/99 concerning the level of personal data protection in Hungary, 5070/EN/99/final WP 24, adopted on 7 September 1999.

[45] See European Commission, Commission Decision of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina (Decision 2003/490/EC).

[46] See European Commission, Commission Decision of 21 November 2003 on the adequate protection of personal data in Guernsey (Decision 2003/821/EC).

[47] See European Commission, Commission Decision of 28 April 2004 on the adequate protection of personal data in the Isle of Man (Decision 2004/411/EC).

[48] European Commission, Commission Decision of 8 May 2008 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Jersey (Decision 2008/393/EC).

[49] European Commission, Commission Decision of 5 March 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection provided by the Faeroese Act on processing of personal data (Decision 2010/146/EU).

[50] Cf. European Commission, Commission Decision of 21 August 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the Eastern Republic of Uruguay with regard to automated processing of personal data (Decision 2012/484/EU).

[51] Judgment *Schrems*, recital 73.

[52] Judgment *Schrems*, recital 74.

[53] European Commission, Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework. Available at: https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf.

5.1. *Guaranteeing an adequate level of protection does not require that a level of protection identical to that of the European Union be guaranteed, nor that the rules of the Union be reproduced to the letter: Court of Justice of the European Union, the European Commission and the European Data Protection Board*

As specified in Article 45(2) of Regulation (EU) 2016/679,[54] the adoption of an adequacy decision must be based on an analysis of the legal system of the third country. The assessment should determine whether the third country in question guarantees an adequate level of protection or essentially equivalent to that offered in the EU.[55] It is important to note that according to the CJEU, **an identical level of protection is not required**.[56] For said Court, the "*...word 'adequate' (…) admittedly signifies that* ***a third country cannot be required to ensure a level of protection identical to that guaranteed in the EU legal order***"[57] (our bold). On this point, in the *Schrems* case, said court specified that the means existing in another country "*must nevertheless prove, in practice, effective in order to ensure protection essentially equivalent to that guaranteed within the European Union*".[58]

In other words, the legal mechanisms of other countries (such as Colombia) may be different from those applied in the EU, provided that, in practice, they are effective in guaranteeing an adequate level of protection.[59] According to the European Commission, the "*adequacy standard therefore* ***does not require a point-to-point replication of Union rules***. *Rather, the test lies in* ***whether****, through the substance of privacy rights and their effective implementation, supervision and enforcement,* ***the foreign system as a whole delivers the required level of protection***"[60] (our bold).

All of the above was reiterated by the EDPB in the document entitled, "*Adequacy Referential (WP254rev.01)*".[61] In essence, this document updates the initial guidelines taking into account the new legislation[62] and recent case law of the CJEU.[63] Regarding the concept and objective of the adequate level, it is highlighted that: «while the "level of protection" in the third country must be "*essentially equivalent*" to that guaranteed in the EU, "*the means to which that third country has recourse,*

[54] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679.

[55] Recital 104 of Regulation (EU) 2016/679.

[56] Judgment *Schrems*, recital 73.

[57] Judgment *Schrems*, recital 73.

[58] Judgment *Schrems*, recital 74.

[59] Judgment *Schrems*, recital 74.

[60] European Commission, Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, recital 3. The official text can be consulted at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019D0419&from=SV.

[61] EDPB, "Adequacy Referential (WP254rev.01)", available at: https://ec.europa.eu/newsroom/article29/items/614108.

[62] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).

[63] Judgment *Schrems*.

in this connection, for the purpose of such a level of protection may differ from those employed within the [EU]". Therefore, the objective is not to mirror point by point the European legislation, but to establish the essential – core requirements of that legislation».[64]

The EDPB emphasises that "*[a]dequacy can be achieved through a combination of rights for the data subjects and obligations on those who process data, or who exercise control over such processing and supervision by independent bodies. However, data protection rules are only effective if they are enforceable and followed in practice. It is therefore necessary to consider not only the content of rules applicable to personal data transferred to a third country or an international organisation, but also the system in place to ensure the effectiveness of such rules. Efficient enforcement mechanisms are of paramount importance to the effectiveness of data protection rules*".[65] Both the content of the applicable standards and the means to guarantee their effective application are crucial because the standards are of little use if they are not met. In this sense, we agree that "*data protection rules only contribute to the protection of individuals if they are followed in practice*".[66]

5.2. *On the difficulty of obtaining an "adequate level": Will the use of contractual clauses eliminate the need for the "adequate level" figure?*

It is not easy for a country to obtain the "*adequate level*." Although it is not possible to generalise about the adequate level process because everything depends on the particularities of each country, as an example, let the experience of the Republic of Colombia be noted.

For the purposes of cross-border circulation of data, the Superintendency of Industry and Commerce (SIC) of the Republic of Colombia has established since August 2017 that the following countries have an adequate level of data protection:[67] Germany; Australia, Austria; Belgium; Bulgaria; Cyprus; Costa Rica; Croatia; Denmark; Slovakia; Slovenia; Estonia; Spain; United States of America; Finland; France; Greece; Hungary; Ireland; Iceland; Italy; Japan; Latvia; Lithuania; Luxembourg; Malt; Mexico; Norway; Netherlands; Peru; Poland; Portugal; United Kingdom; Czech Republic; Republic of Korea; Romania; Serbia; Sweden; and countries that have been declared with the adequate level of protection by the European Commission (Switzerland; Canada; Argentina, Guernsey, Isle of Man, Jersey, Faroe Islands, Andorra, Israel, Uruguay, New Zealand and Japan).

Notwithstanding the above, the SIC, in its role as personal data protection authority, has initiated several processes to obtain an adequate level of data protection. For now, Colombia has been recognised by the Dubai International Financial Centre as a country that offers an adequate level of personal data protection.[68]

This was the conclusion of 6 October 2022 of the Dubai International Financial Centre Authority (DIFC) Office of the Commissioner of Data Protection: «It is for these reasons that the DIFC Office of the Commissioner of Data Protection ("the Commissioner") should grant adequacy recognition to Colombia. The current risk

[64] EDPB, "Adequacy Referential(WP254rev.01)", 3.
[65] EDPB, "Adequacy Referential (WP254rev.01)", 3.
[66] European Commission, First orientations on Transfers of Personal Data to Third Countries – Possible Ways Forward in Assessing Adequacy, 5, and European Commission, Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, 5.
[67] See SIC, External circulars 5 and 8 of 2017 and 2 of 2018.
[68] See SIC, *Colombia es reconocida por su nivel adecuado de protección de datos por el Centro Financiero de Dubái*, 18 October 2022, available at: https://www.sic.gov.co/slider/colombia-es-reconocida-por-su-nivel-adecuado-de-proteccion-de-datos-por-el-centro-financiero-de-dubai.

assessment regarding Colombia's laws and regulations, as well as the cultural and environmental approach to privacy and redress, align with the DIFC DP Law 2020 such that transfers to Colombia will receive the same or substantially equivalent protection when exported thereto».[69]

Dubai International Financial Centre (DIFC) is the leading global financial centre in the Middle East, Africa, and South Asia (MEASA) region. DIFC has a close to 20-year track record of facilitating trade and investment flows across MEASA. The region comprises 72 countries with a combined population of around 3 billion people and a nominal GDP of approximately USD8 trillion. The Centre connects the fast-growing markets of the MEASA region with the economies of Asia, Europe, and the Americas through Dubai.[70]

For the purposes of international data transfer, Article 26 of the Data Protection Law 2020 (DIFC Law no. 5 of 2020)[71] provides the following:

26. Transfers out of the DIFC: adequate level of protection

"*Processing of Personal Data that involves the transfer of Personal Data from the DIFC to a Third Country or to an International Organisation may take place only if:*

an adequate level of protection for that Personal Data is ensured by Applicable Law, as set out in Articles 26(2) and (3), including with respect to onward transfers of Personal Data; or [if] it takes place in accordance with Article 27."

According to the second part of the Article 26, to determine whether a third country has an adequate level of data protection, the following must be considered:

"*For the purposes of Article 26(1), the Commissioner may determine from time to time that a Third Country, a territory or one (1) or more specified sectors within a Third Country, or an International Organisation ensures an adequate level of data protection, taking into account factors including:*

the rule of law, the general respect for individual's rights and the ability of individuals to enforce their rights via administrative or judicial redress;

the access of a public authority to Personal Data;

the existence of effective data protection law, including rules on the onward transfer of Personal Data to a Third Country or International Organisation;

the existence and functioning of one (1) or more independent, competent data protection or similar supervisory authorities with adequate enforcement powers; and

international commitments and conventions binding on such Third Country or International Organisation and its membership of any multilateral or regional organisations."

As one can see, for the purposes of establishing whether a country has an adequate level of data protection, the DIFC regulation takes into account equivalent factors that are required in paragraphs a), b) and c) of Article 45 of Regulation (EU) 2016/679 (General Data Protection Regulation).

Additionally, since 2019, it has initiated conversations or submitted requests to other organisations or countries for this purpose. In all cases, essentially, the same information considered by the Dubai DIFC was provided.

---

[69] Dubai International Financial Centre Authority ("DIFC" or "DIFCA"), Commissioner of Data Protection, Assessment of Colombia's Data Protection Regime as Substantially Equivalent, 2022. The official text can be consulted at: https://www.difc.ae/application/files/5716/6505/3669/Third_Country_or_Jurisdiction_Adequacy_Assessment_-_Colombia__Final__Executed_6_Oct.pdf.

[70] Cf. https://www.difc.ae/who-we-are.

[71] The text of the law is available at: https://edge.sitecorecloud.io/dubaiintern0078-difcexperie96c5-production-3253/media/project/difcexperiences/difc/difcwebsite/documents/laws–regulations/data_protection_law_final.pdf.

Organisation or country to which Colombia has requested adequate level	Process start date	Decision
European Commission	15 October 2019 preliminary conversations began (Official Letter 19-236409 from the Delegate Superintendent for Data Protection of the SIC)	Pending. More than 4 years have passed as of 31/XII/2023
United Kingdom	April 2021	Pending. More than 2.5 years have passed as of 31/XII/2023
Argentina	31 August 2021 (Official Letter 21-348053 from the Delegate Superintendent for Data Protection of the SIC)	Pending. More than 2 years have passed as of 31/XII/2023
Uruguay	31 August 2021 (Official Letter 21-348062 from the Delegate Superintendent for Data Protection of the SIC)	Pending. More than 2 years have passed as of 31/XII/2023

Graph no. 3. List of requests made by Colombia to obtain an adequate level of protection of personal data.

Indeed, the time that an adequate level processes take and the levels of uncertainty that they generate are not convenient for those who need to legally export personal data to other countries. Therefore, MCCs are an expeditious and sensible tool to achieve this goal. Most likely, using the clauses will displace the need to resort to the figure of "*adequate level of protection of personal data*".

5.3. *Is it useful to continue insisting on the figure of the "adequate level" of data protection?*

We propose some small initial reflections to rethink the need to maintain the figure of "*adequate level*" of data protection within the context or scenario of the cross-border circulation of that type of information. At the same time, we highlight some benefits of the MCCs to expeditiously export information to other countries.

It is important that all countries ensure an adequate level of data protection. But this does not mean that this level is only acquired by complying with the processes established by foreign organisations or local authorities of other countries. In practice, there may be countries that have adequate levels of data protection and that are not part of the countries certified by foreign authorities or organisations. In other words, lacking a formal certification of an adequate level does not mean that the country does not have an adequate and effective level to guarantee the proper processing of personal data.

Adequate level certification processes involve evaluating and qualifying a country by international organisations or authorities from other countries. This means that these processes are impregnated with public policy or geopolitics, which

makes the adequacy decision not fullyobjective. These processes may be influenced by national or regional interests and foreign policy objectives that impact geopolitical dynamics that are usually accompanied by the interaction of geographical, economic, political factors and strategic alliances resulting from diplomacy and negotiations to influence the international scene.

Geopolitical and geoeconomic relations between States are built on bases of inequality to the extent that they are carried out by powerful countries and others that are not. The economy and security of some countries depends on other countries that become their main commercial "*partners*" or "*strategic allies*". If a powerful country is the main economic partner, the weaker country may be subject to significant economic or strategic pressures. The will of the weak country is not free but is an act of convenience or submission. Threats of trade sanctions or manipulation of trade agreements can impact economic independence and decision-making capacity.

This means that there is no full objectivity or freedom to make adequacy decisions on the part of "*non-powerful*" countries or those that have "*dependence*" on other states or the need to maintain "*strategic alliances*". To that extent, the figure of the "*adequate level*" generates "*political and economic pressure*". Therefore, within the framework of an adequacy process, it is very complex for a weak country to deny the decision of adequacy to the powerful countries with which it has commercial relations or economic dependence. In this case, 100% of the decision was not due to creating sensible conditions to guarantee an adequate level of protection for people's data.

Adequate level certification processes depend, among others, on political factors and government management. Some states have not resorted to this figure due to, among other reasons, a lack of awareness, lack of political interest (or priority on the political agenda) and ignorance about its legal, political, economic and social relevance. It is also difficult to objectively demonstrate and measure with figures what are the specific benefits that countries certified with an adequate level of data protection have obtained.

Some states or authorities to which adequate level requests are made also do not know how to properly manage them. When faced with certification requests, "*silence*" often reigns and time passes without responding. Sometimes, some states have to insist, beg or "*lobby*" to schedule a work meeting or to prevent the process from freezing or paralysing.

The regulatory and institutional adjustments involved in obtaining the "*adequate level*" take a long time and it cannot be guaranteed that they will be carried out. Think, for example, of issuing new data processing regulations or creating independent authorities to protect the rights of people regarding the processing of their personal data. That does not depend solely on the will of a government but on the decision of the congress or parliament.

Achieving an adequate level of data protection is a complex and time-consuming process that is not commensurate with the urgent needs to circulate personal data across borders. In the case of Europe, it is noted that in approximately 28 years[72] the European Commission has so far recognised 13 countries with an "*adequate level of data protection*": Andorra, Argentina, Faroe Islands, Guernsey, Israel, Isle of Man,

[72] That is, from 24 October 1995 (date on which Directive 95/46 was issued) to January 2024. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281, 23/11/1995 P. 0031 – 0050.

Japan, Jersey, New Zealand, the Republic of Korea, Switzerland, the United Kingdom under the GDPR and the Legal Examiners Directive (LED) and Uruguay.[73] This recognition has also been given to trade organisations in Canada[74] and the United States. In the latter case, it only covers those that participate in the EU-US Data Privacy Framework.[75]

Regarding the 11 adaptations conferred under the rules of Directive 95/46, the European Commission in January 2024[76] ratified that the following countries maintain an adequate level of data protection: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, and Uruguay.

The adequacy process before the European Commission is not expeditious. Said Commission recognised in 2001 "*that the Commission is unlikely to adopt adequacy findings (…) or more than a limited number of countries in the short or even medium term*".[77] According to some experiences,[78] it takes a little more than two (2) years when a decision is made, but in other cases, such as Colombia, it has been more than four years without any official statement from the Commission, although several work meetings have been held and documents submitted to respond to the questions of said Commission.

---

[73] See https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[74] In the case of Canada, the Commission decided the following: «For the purposes of Article 25(2) of Directive 95/46/EC, Canada is considered as providing an adequate level of protection for personal data transferred from the Community to recipients subject to the Personal Information Protection and Electronic Documents Act ("the Canadian Act")». Article 1 of Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act.

[75] Regarding the United States, the Commission decided the following: "For the purpose of Article 45 of Regulation (EU) 2016/679, the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in the United States that are included in the 'Data Privacy Framework List', maintained and made publicly available by the U.S. Department of Commerce, in accordance with Section I.3 of Annex I". (Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework), https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf.

[76] European Commission, Report from the Commission to the European Parliament and the Council on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC, Brussels, 15 January 2024, https://commission.europa.eu/system/files/2024-01/JUST_template_comingsoon_Report%20on%20the%20first%20review%20of%20the%20functioning.pdf. Also read the following press release dated 14 January 2024: , "Commission finds that EU personal data flows can continue with 11 third countries and territories", Press release, 15 January 2024, Brussels, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_161.

[77] In effect, recital 4 of Decision 2001/497/EC states the following: "Article 26(2) of Directive 95/46/EC, which provides flexibility for an organisation wishing to transfer data to third countries, and Article 26(4), which provides for standard contractual clauses, are essential for maintaining the necessary flow of personal data between the Community and third countries without unnecessary burdens for economic operators. Those Articles are particularly important in view of the fact that the Commission is unlikely to adopt adequacy findings under Article 25(6) for more than a limited number of countries in the short or even medium term." See European Commission, Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC, 2001/497/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32001D0497.

[78] In a recent case such as that of Jersey, the process before the European authorities began with a request in February 2006 and culminated with the adequacy decision in May 2008.

MCCs are an increasingly used tool to facilitate international data transfers. As they are contracts with previously established homogeneous content, they are more efficient to accelerate the export of personal data processes.

The use of MCCs can help reduce uncertainty by providing a standardised set of contractual clauses approved by local data protection authorities to ensure that they include the minimum requirements to ensure proper processing of personal data in destination countries of data exports.

Neither the "*adequate level*" nor MCCs are perfect tools. They are mechanisms designed for certain objectives, but their fulfilment will depend on external factors or third parties such as, among others, the human will to properly comply with what the laws or contracts require.

However, the preference for using MCCs rather than relying on uncertain, complex and time-consuming government processes to obtain the "*adequate level*" should not be lost sight of. This is due, among other factors, to the following:

Greater agility and efficiency in the use of MCCs with respect to the bureaucratic procedures that citizens usually undergo when dealing with public authorities.

MCCs can be more flexible and adaptable to the needs of organisations regarding international transfers of personal data.

In summary, although the figure of the "*adequate level*" is an important strategy in the scenario of international transfers of personal data, its dynamics, adoption process and processing do not adjust to the dynamics and urgency of response to cross-border circulation of personal data. MCCs should be considered as a possible replacement for the "*adequate level of data protection*" institution. Although both institutions can coexist, and the preference for one or the other will depend on various factors, obtaining the appropriate level has proven to be cumbersome, delayed and uncertain.

In theory, it seems that the "*adequate level*" is the best option, but it is necessary to measure its real effectiveness and evaluate whether it is worth carrying out a complex, slow and uncertain procedure. The current dynamics of human rights protection should be rethought to achieve more expeditious, simple, practical, sensible and effective tools in the face of the socio-technological reality of the 21st century.

6. Conclusions

The expression "*adequate level of data protection*" (ALDP) emerged in Europe when establishing rules for transferring personal data from there to third countries. Being classified by Europe as a country with this degree of protection is neither simple nor expeditious. It typically requires countries to issue appropriate regulations and make institutional changes.

The time that adequate level processes take and the levels of uncertainty that they generate are not convenient for those who need to legally export personal data to other countries. Therefore, MCCs are an expeditious and sensible tool to achieve this goal. Most likely, the use of the clauses will displace the need to resort to the figure of "*adequate level of protection of personal data*".

Contracts represent an exceptional legal alternative to facilitate the international circulation of personal data. The contract seeks to establish minimum conditions to guarantee the proper processing of the data that is going to be exported from one country to another. The use of contractual clauses for international transfers has been recommended as, among others, an accountability tool (proven responsibility).

MCCs are an increasingly used tool to facilitate international data transfers. As they are contracts with previously established homogeneous content, they are more efficient to accelerate the export processes of personal data. The use of MCCs can help reduce uncertainty by providing a standardised set of contractual clauses approved by local data protection authorities to ensure that they include the minimum requirements to ensure proper processing of personal data in destination countries of data exports.

Neither the "*adequate level*" nor MCCs are perfect, but they are mechanisms designed for certain objectives, but their fulfilment will depend on external factors or third parties such as, among others, the human or corporate will to properly comply with what the laws or contracts require.

We should reflect and evaluate whether it is convenient or necessary to maintain the figure of "*adequate level*" of data protection within the context or scenario of the cross-border circulation of that type of information. While it is important that all countries guarantee an adequate level of data protection, this does not mean that this level is only acquired by complying with the processes established by foreign organisations or local authorities in other countries. Lacking a formal certification of an adequate level does not mean that the country does not have an adequate and effective level to guarantee the proper processing of personal data.

Adequate level certification processes involve evaluating and qualifying a country by international organisations or authorities from other countries. This means that these processes are impregnated with public policy or geopolitics, which makes the adequacy decision not 100% objective. These processes may be influenced by national or regional interests and foreign policy objectives that impact geopolitical dynamics that are usually accompanied by the interaction of geographical, economic, political factors and strategic alliances resulting from diplomacy and negotiations to influence global and international scene.