# Accountability Guide on Cross-border Transfers of Personal Data

## Recommendations for Latin American Countries

Nelson Remolina Angarita
Luisa Fernanda Álvarez Zuluaga

Universidad de los Andes
Colombia

GECTI

Observatorio Ciro Angarita Barón
sobre la protección de datos personales

February 2019



© Los Andes University
Law School
Street 1 n.º 18A-10, RGC Building, 2nd Floor
Phone Number: 339 49 49
https://derecho.uniandes.edu.co

The original version of this guide was written in Spanish and published in June 2018

ISBN *e-book*: 978-958-774-837-6

Suggested Citation: Remolina Angarita, Nelson. Alvarez Zuluaga, Luisa Fernanda. (2019). Accountability Guide on Cross-border Transfers of Personal Data. Los Andes University (Bogotá, Colombia). School of Law. GECTI, 1-52

Contact: Nelson Remolina Angarita
nremolin@uniandes.edu.co
Luisa Fernanda Alvarez Zuluaga
lf.alvarez10@uniandes.edu.co

Editorial design and layout: Karina Betancur Olmos

Los Andes University | Supervised by the Ministry of Education
Recognition as University: Decree 1297 of 30 May 1964
Recogniced as a legal person: Resolution 28 of 23 February 1949, Ministry of Justice.
High Quality Accreditation, 10 years: Resolution 582 of 9 January 2015, Ministry of Education.

# Contenido

# Who are we?

The Group of Studies in Internet, e-Commerce, Telecommunications and Informatics (GECTI by its initials in Spanish) was created on 5 October 2001 at Los Andes University School of Law (Bogotá, Colombia). It seeks to create a network between the University and society in order to procure reflections and actions in the subject matter of Internet, society of information, and converging topics.

The GECTI's mission[1] is to make an independent academic contribution on different aspects regarding cyberspace, digital economy, and today's socio-technological reality; as well as conducting research, consultancies, writing publications and academic programs of the highest academic levels specialized in Law and Technology.

On the other hand, the Observatory Ciro Angarita Barón on Data Protection in Colombia[2], was funded on 17 January 2008 at Los Andes University School of Law (Bogotá, Colombia) as an academic space of reflection on the protection of the rights of people when their data is collected, stored, or used by third parties.

1 The GECTI's webpage is: https://gecti.uniandes.edu.co.

2 The Observatory's webpage is: https://habeasdatacolombia.uniandes.edu.co.

# Introduction

The processing of personal data has been characterized by its internationalism due to the fact that its recollection, usage, and circulation is usually cross-border. For instance, the digital economy, International Commerce, e-Commerce, amongst other activities require the international circulation of personal data. In addition to the free-circulation of goods, people, and money, the exportation and importation of personal data is the most important asset for the functioning of the global market and the success of various businesses nowadays.

The principle of accountability has become of extreme importance in the processing of personal data. Its real and correct implementation not only benefits the data subjects by guaranteeing the protection of their rights, but also benefits organizations that can maximize the use of data, while increasing their level of competitivity and consolidating a good institutional reputation.

It is crucial to have organizational commitment, including senior management support, in order to anticipate problems and adopt the necessary measures to target them. This will further help organizations exploit data within a competitive, innovative and human rights' friendly environment.

We want this Guide to be a useful reference in the consolidation of the adequate processing of data during cross-border transfers regardless of whether it involves organizations from the public or the private sector.

# Objective of the Guide

The objective of this Guide is to give some recommendations to those who transfer personal data to other countries. As such, we give some orientations on how the cross-border circulation of personal data should be made in order to respect the rights of the data subjects and at the same time protect the interests of the data controller.

Although the Guide is meant to be used in Latin American countries as it seeks to develop aspects that have not been expressly included in the Colombian Accountability Guide, which is the only one in Latin America, this document is also useful for those processing and transferring personal data in non-Latin American countries.

We hope this document is considered by organizations and governmental authorities in the future elaboration of Accountability Guides, mainly in Latin American countries. However, this Guide is in no way a legal concept nor does it constitute a legal consultancy. Adopting the recommendations written in this Guidelines, entails tailoring the measures to meet the specific data handling practices of the implementing organization that intends to use them.

# I. Background and Importance

## • The Processing of Personal Data as a Global Matter and a Daily Activity in Cyberspace

We live in a geographically fractional but technologically merged planet, in which information is the main asset circulating through a global hyperconnected infrastructure known as cyberspace[3]. Consequently, the processing[4] of personal data is characterized by a cross-border and global approach.

As it is widely known, the use of databases is a day-to-day activity crucial to the State, enterprises, and individuals, since information is required to make and implement decisions of diverse nature. Likewise, personal data represents, in certain cases, a company's main asset, such as when the company's object is to analyze, sell, rent, or transfer data. In other cases, personal data is used to make decisions regarding a target population. Additionally, it is also used to create public, economic, risk-managing, or marketing policies, amongst others.

3 Although it is said that cyberspace is an artificial scenario created by technological means, it is important to remember that in cyberspace real people, with different nationalities and domiciles, are constantly interacting with each other. As such, their communications and activities trespass a country's physical territory.

4 For all the matters concerning this document, the words "process" and "processing" must be understood as any operation or set of operations applied to personal data, such as the recollection; registration; organization; conservation; elaboration or modification; extraction; consultation; usage; communication; diffusion; or any other activity that facilitates the access, comparison, interconnection, blockage, suppression, or destruction of data.

Moreover, the Information and Communication Technology (ICT), has contributed to the "datafication" of the contemporary society. It has also contributed to the consolidation of personal data as the building block, and thus, the currency of the digital economy; henceforth, being considered the equivalent to gold in the 21st century.

The processing of personal data is one of the topics that has drawn the most attention from both regulators and organizations. Initially, it was not widely regulated. However, in the last decade there has been a boom of general laws and specific laws for different economic sectors regarding the processing of personal data. Additionally, there has been some efforts to revise and update the first regulatory initiatives in said topic. Furthermore, multiple conferences on data protection have been held across the globe; thus, demonstrating the indisputable social and economic relevance of the processing of personal data.

The right to the protection of personal data has evolved since its first regulatory manifestations in the 1970s and the documents published in its aftermath. With time, other factors were added to the initial motives behind the regulation of personal data; which is why the challenges faced today in the protection of this right are different from those initially foreseen. Existing regulation on the right to the protection of personal data, considers the interests of the data subject, while recognizing the necessity of data recollection in the realization of various legal and legitimate activities. In other words, existing regulation does not antagonize the processing of personal data, but the eventual abuse of its processing which might lead to threats or violations of the Human Rights of data subjects.

Various countries have general and sectoral regulations, as well as jurisprudence, on personal data processing. Although there has been numerous international harmonization attempts on the main aspects of this topic, every country issues its own laws, which may partially follow international documents, while at the same time reflecting

a country's social, political, cultural, and legal particularities. Moreover, each legal system has diverse legal remedies (constitutional, administrative, judicial, amongst others) to protect the right to the lawful processing of personal data. It would be pretentious to cover in detail everything that has to do with data processing from a comparative law perspective; which is why this Guidelines will mostly mention important international harmonization attempts of the right to the protection of personal data that have taken place since the 1980s[5].

The recollection, storage, usage, circulation, and other activities regarding personal data, have been subject to international harmonization with the objective of achieving a legal consensus on the most important aspects[6]. In this sense, different international organizations, specialized networks, and groups and authorities, have published documents containing the rules that must be observed in the processing of personal data. In these documents, various principles are found evoking the most relevant elements that must be materialized in order to avoid the threat or violation of the rights of data subjects due to unlawful recollection, storage, usage, or circulation of said data.

In Table n.º 1, we summarize the main documents on the processing of personal data, issued by different organizations.

5 With regards to the international panorama on data protection, read Remolina Angarita, Nelson: Data protection: panorama nacional e internacional, in I*nternet, comercio electrónico y telecomunicaciones* pp. 99-172, Bogotá: Legis 2002.

6 The joint declaration between the EU and the US on e-Commerce, was emphatical in saying that the role of governments is to create a legal frame that promotes a competitive environment in which e-Commerce can flourish while at the same time ensuring the protection of public interests such as the right to intimacy, intellectual property rights, fraud prevention, consumer protection, and national security.

Table n.º 1. Main international organizations that have published documents on the processing of personal data

| Organization | Main Documents |
|---|---|
| Iberoamerican Data Protection Network (IDPN) | Standards for Data Protection for the Ibero-American States (2017) |
| European Union (EU) | 1. 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); 2. Additional Protocols to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (2001 and 2018); 3. EU Charter of Fundamental Rights (2000); 4. Convention 108 of the Council for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) |
| Organization of American States (OAS) | OAS Principles on Privacy and Personal Data Protection with Annotations (2015) |
| Organization for Economic Cooperation and Development (OECD) | Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013, 1980) |
| International Conference on Data Protection & Privacy Commissioners (ICDPPC) | International Standards on the Protection of Privacy with regards to the Processing of Personal Data- the Madrid Resolution- (2009) |
| Asia-Pacific Economic Cooperation (APEC) | APEC Privacy Framework (2015)<br>APEC Cross Border Privacy Rules (CBPR)<br>APEC Cross Border Privacy Enforcement Arrangement (CPEA) |
| United Nations (UN) | Resolution 45/95 of 14 December 1990. Guidelines for the regulation of computerized data files |

## • Constitutional Relevance of Data Protection in Latin American Countries

The protection of personal data is a matter of constitutional relevance in the Latin American scenario[7]. This is corroborated by a report done by Nelson Remolina Angarita[8] titled "Latin America and Protection of Personal Data: Facts and Figures (1985-2014)", in which the current status of personal data regulation in the following 20 countries is shown: Argentina, Bolivia, Brazil, Chile, Colombia, Costa Rica, Cuba, Dominican Republic, Ecuador, El Salvador, Guatemala, Haiti, Honduras, Mexico, Nicaragua, Panama, Paraguay, Peru, Uruguay, and Venezuela.

With regards to the Constitutions of the aforementioned countries, the following was concluded:

– 75% of Latin American countries incorporate in their Constitution, explicit references to aspects related to the protection of personal data

– 100% of the Constitutional texts studied consecrate the right to access of the data subject. This is understood as the right to know which information data controllers possess. 92.85% explicitly mention personal data or personal information.

– 85.71% establish the right of the data subject to request rectification or correction of erroneous information, while 64.28% confer data subjects the constitutional right to solicit suppression, elimination, destruction, or cancellation of their data.

7 Regarding Habeas Data in Latin America, read Puccinelli, Oscar. 1999. El habeas data in Indoiberoamérica, Bogotá: Temis.

8 Cfr. Remolina, Nelson. Latin America and Protection of Personal Data: Facts and Figures (1985-2014) (March 20, 2014). Available in SSRN: https://ssrn.com/abstract=241209 or in http://dx.doi.org/10.2139/ssrn.241209. The text was originally published by the Ciro Angarita Baron Observatory on the protection of Personal Data in Colombia.

- 64.28% consider the updating of data as a right the data subject is entitled to.
- 57.14% establish habeas data and 7.14% the protective action (amparo) and privacy protection action.
- 50% consecrate the right to know the purpose of the data processing and 21.42% the right of knowing the use that the controller is granting to the data collected
- 28.57% establish the demanding of the confidentiality of personal data as a Constitutional Right.
- 14.28% de of the Constitutions analyzed, expressly grant constitutional rank to the protection of personal data.
- Panama (2004), Ecuador (2008), Mexico (2009) and Chile (2018), explicitly consecrate the right to the protection of personal information and the protection of personal data.
- Dominican Republic (2010) is the only country that contains a plexus of constitutional principles (quality, legality, loyalty, security, and purpose) that must govern the processing of personal data.
- The constitutions of Panama and Ecuador demand personal data to be recollected with the consent of the data subject.

Chile's Senate approved a draft of constitutional reforms, in which the protection of personal data is guaranteed, and the processing of said information will have to follow the standards indicated by a subsequent law[9]. On August 14 (2018), Brazilian President signed the new General Data Privacy Law (Lei Geral de Proteção de Dados

9 Cfr. Republic of Chile. Law Number 21.096 estipulates the right to data protection. The official text is available in: https://www.leychile.cl/Navegar?idNorma=1119730.

Pessoais or "LGPD") making Brazil the latest Latin American country to implement comprehensive data privacy regulation.

Regarding the laws issued by said countries, it was concluded that 100% of them have sectoral laws on different topics, such as clinical history and population census, and 50% have general laws on data protection.

Since the right of protecting personal data is a constitutional right, it requires data to be processed with special care and diligence, which is why the data controller is bestowed with a high degree of legal responsibility in this matter.

## • Good Governance in Personal Data, Digital Corporate Responsibility, and Legal Responsibility of the High Ranks in an Organization

The strategic and economic importance of information systems, especially those containing personal data, is indisputable. As a matter of fact, a wide variety of business models are based in the use of personal data. In this sense, an article published in the *Harvard Business Review* establishes that the new patterns of innovation and the new elements of value generation are found in the processing of data[10].

10 Cfr. Parmar, R., Mackenzie, I., Cohn, D. y Gann, D. (2014) The new patterns of innovation. Harvard Business Review. January-February. Available in: https://hbr.org/2014/01/the-new-patterns-of-innovation Cited by Jeimy Cano (2014) in Presiones emergentes sobre la privacidad de la información, at http://insecurityit. blogspot.com.co/2014/05/presiones-emergentes-sobre-la.html.

Moreover, it has also been affirmed that corporations that correctly process personal data will be leaders in tomorrow's digital economy[11]. As a result, the "due processing of personal data, that goes hand in hand with digital corporate responsibility, will become a de facto rule for companies in this century that aspire to be relevant players in their respective business sectors"[12].

The aforementioned, has raised awareness on the necessity to design and implement adequate strategies of good governance and managing of data. As a result, companies are aiming at 1. creating institutional policies that can be followed in present and future data managing scenarios; 2. achieving verifiable results with regards to the processing of information; and 3. protecting and maximizing the smart and adequate use of the processed data.

Managers, Board Members, and other high ranked officials within an implementing organization, not only have a social and ethical responsibility in data processing matters, but also, according to each country's regulation, might have a relevant legal responsibility. In Colombia, for instance, the legal representative, the liquidator, and the board members, who according to the Statutes have administrative functions, "should act in good faith, loyalty, and with the diligence of a good businessman"[13]. Furthermore, all of them have joint and unlimited liability for damages caused with fraud or fault to the company, its stakeholders, or third parties[14]. Additionally, there's a legal presumption of responsibility over managers or directives in the case of "breach

11 Cfr. Accenture (2016). Guarding and growing personal data value Organizations that demonstrate responsibility in the way they handle personal data today will lead the digital economy of tomorrow. January. In https://www.accenture.com/us-en/insight-guarding-growing-personal-data-value.aspx.

12 Cfr. Cano Martínez, Jeimy. 2016. ¿Eres una empresa digitalmente responsable? January 20. In https://www.linkedin.com/pulse/eres-una-empresa-digitalmente-responsable-jeimy-cano-ph-d-cfe.

13 Republic of Colombia. Law 222 1995, article 23

14 Íbidem, article 24.

or extra limitation of their established functions, in violation of the law or of the Corporation's Statutes". This shows that a high degree of professionalism, ethics, and diligence must be observed and demonstrated by an organization's directives in everything related to data processing.

Digital responsibility and good governance with regards to personal data, is something that must not only be observed when processing data within a delimited territory but also when transferring this data overseas. This topic, will concern us in the following sections of the present document.

## • "Data Havens" in the Processing of Personal Data and "Internet of Corporations"

A great number of countries lack regulation on the processing of personal data. This ultimately means that in these territories there is no certainty on how to protect the rights of data subjects with regards to the processing of personal data or, worse, that there is no protection of their rights at all. In the Explanatory Report[15] of the Convention 108 of the Council of Europe[16] of 28 January 1981, the States recognized the existence of countries with no laws on data protection or with low levels of protection, known as "Data Havens" where the protection of the rights of data subjects is weak or nonexistent.

Palazzi comments that the purpose of Article 25 of Directive 95/46/CE is to "avoid the creation of data havens, in other words, jurisdictions where the lack of data protection

15 The text can be found in: http://conventions.coe.int/Treaty/EN/Reports/ HTML/108.htm.

16 The official version of the Convention is published in http://conventions.coe.int/Treaty/EN/Treaties/ Html/108.htm Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg, 28.I.19

laws, make the countries appealing places to conduct processing of personal data in violation of privacy laws from different jurisdictions"[17]. However, when talking about Data Havens, we are not only referring to countries that lack data protection regulation, since it also covers other subject matters, such as cybercrimes. For instance, for the United Nations, "Data Havens" are "States where reducing or preventing the misuse of computer networks is not a priority, or where no effective procedural laws have been developed"[18].

When referring to data processing in cross-border transfers, a series of rules have been established in order to avoid personal data from entering Data Havens. From documents analyzed, in order for cross border data transfers to take place, the data controller must verify that the overseas recipient can guarantee an adequate level of protection of the personal data. In this context, a recipient with an adequate level of protection is domiciled in a jurisdiction where a superior, equal, or similar level of protection as that of the exporting country, is found.

Although the term "Data Havens" is commonly used to refer to countries, it can also be used to refer to corporations that do not have acceptable safeguards to ensure an adequate level of protection for personal data. It can also be used to refer to corporations that are only interested in making a profit out of their client's data; hence, failing to guarantee the correct processing of said information or the protection of their customers' constitutional rights.

17 Cfr. Palazzi, Pablo. 2003. Comercio electrónico, transferencia internacional de datos personales y armonización de leyes en un mundo globalizado. In *Derecho de internet & telecomunicaciones*, edited by the GECTI. Bogotá: Legis, p. 299.

18 Cfr. United Nations. 2000. Crimes related to computer networks. Document A/CONF.187/10 background paper for the workshop on crimes related to the computer network. IN the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders; Viena: UN, p. 3.

It is important to clarify that the risks for corporations and individuals during the processing of personal data, not only surge in Data Havens, but also in countries with adequate levels of protection. This is due to the fact that data processing related activities, are characterized by its extraterritoriality. As such, data controllers (corporations, individuals, or public entities) and data subjects (citizens) can easily lose control over the data being transferred and might end up being subjected to different laws and decisions from authorities and enterprises alike in a wide number of jurisdictions with different levels of protection.

It is important to highlight that certain corporations have even more power than governmental authorities in the countries where they operate. These corporations, through legal agreements and binding corporate rules, regulate the rights of trillions of people who are constantly using the Internet. As a consequence, this phenomenon, known by the term "Internet of Corporations", describes what has happened with the regulation of the Internet over the past years.

The "Internet of Corporations" has set the path for the Internet and its user, due to the fact that Corporations have hyper regulated the Internet through legal notes and terms and conditions. Consequently, when referring to the "Internet of Corporations"[19], we are talking about rules that entrepreneurs have created to provide services and conduct business through the Internet. In other words, the term comprises the guidelines that an entrepreneur considers reasonable in order to make a profit out of the Internet, which is why we could also denominate this phenomenon as "corporation laws". As a result, corporations have established rules that govern the

19 Regarding the Internet of Corporations, read Remolina Angarita, Nelson. (2016) "Internet de las empresas" ["Internet of Corporations" -IoC-]: una explicación de lo que pasa en internet y del futuro de la protección de los derechos humanos en el ciberespacio (part 1). Universidad de los Andes. Published in: https:// habeasdatacolombia.uniandes.edu.co/?p=2222.

destiny of millions of people located all across the globe which is why they have more incidence and cross-border application than any local law.

## • Cross-border Transfers of Personal Data

The cross-border transfer of personal data, is one of the main reasons behind the regulation related to the processing of personal data. In 23 September 1980, the Organization for Economic Cooperation and Development (OECD) issued some guidelines for the Protection of Data in which cross-border transfers and the protection of people's privacy were the main reasons that motivated the drafting[20].

The guidelines declare the necessity to protect the right to privacy[21] in order to facilitate the cross-border transfer of personal data with the sole purpose of boosting social and economic development[22] as well as the development of businesses. The document also explicitly recognizes that "Member countries have a common interest in promoting and protecting the fundamental values of privacy, individual liberties and the global free flow of information"[23].

20 Cfr. Organization for Economic Cooperation and Development (OECD). 1980. Guidelines for the Protection of Privacy and Transborder Flows of Personal Data.

21 In the acknowledgments of the guidelines, it is established that "the disparities in legislation may create obstacles to the free flow of information between countries"; which is why the OECD requires Member-States to "avoid the creation of unjustified obstacles to the development of economic and social relations among them"

22 Cfr. In the acknowledgment of the guidelines it is indicated that "cross border circulation of personal data contributes to economic and social development"".

23 See the acknowledgement section of the OECD Guidelines, 1980, ob. c

It is necessary to highlight that there are various expressions used when referring to international transfers and transmissions. For instance, several international documents contain the following terms:

> "Transborder flow of personal data" (OCDE, 1980); "transborder flow of personal data" (Convention 108 of 1981); "Transfer of data to third countries" (Directive 95/46); "Transfer of personal data to a recipient that is subject to the jurisdiction of a State or organization that is not Party to the Convention" (2001 Additional Protocol to the Convention 108 - 2001); "Transborder data flows" (UN Resolution 45/95 of 1990); "Transference to another person or international organization" (APEC 2004, 2015); "International Data Transference" (APEC, 2013), "international personal data transfers" (Madrid Resolution 2009); "Trans-border flow of data" (OAS, 2015); "personal data transfer to third countries and international organizations" (EU Regulation 2016/679); "international data for personal matters" (IDPN 2017).

Regardless of the term used to refer to international data transfers, they are all referring to the sending of personal data from the data controller located in one country to a data controller in another country. In other words, personal data is exported from one country to enterprises or organizations located in a different territory or jurisdiction; thus, basically being a process of export of personal data.

Nonetheless, according to the regulation of each country, the terms used to refer to this phenomenon vary. When the export is from one data controller to another one, it is called transference. On the contrary, when the personal data is sent from a data controller to a data processor, it is called transmission of personal data.

## • Cross-border Transmissions of Personal Data

The transmission of personal data occurs when the controller sends personal data to the processor. This can be done nationally or internationally. The former takes place when the remission of the data is done within the boundaries of the same country. The latter, on the contrary, occurs when the data is sent outside the initial territory.

With regards to Latin American countries, in Colombia, the term "transmission" was not foreseen in Law 1581 of 2012. In Mexico, it was designated differently, as "remission"[24]. By using the term "remission", the regulator wanted to differentiate between the sending of data to a party acting on behalf of the controller in the handling of personal data and the delivery of the data to a party acting on its own behalf. In other words, in a transmission, the data processing is still under the scope of the Controller, who, for practical reasons, delivers the data to the processor in order for the latter to provide the services related to the processing of data under the controller's mandate.

The international data transmissions contract is an agreement through which the controller and processor establish the obligations and conditions in which the processing of personal data on behalf of the Controller will take place. In Colombia, article 24 of Decree 1377 of 2013 - incorporated in Decree 1074 of 2015- establishes that international transmissions "do not have to be notified to the data subject and as such, their consent is not necessary whenever there's a data transmissions contract" between the controller and the processor.

The aforementioned contract is stipulated in article 25 of Decree 1377 of 2013, and from a careful reading of said article the following conclusions can be reached: First

24 In the Federal Personal Data Law, "remission" is defined as "the communication of personal data between the controller and the processor, within and outside of the national territory (Article 2 # IX)

of all, the data must be processed under the supervision and instructions of the controller[25]. As such, the contract must define the scope and purposes of the data processing and the obligations of the processor with respect to the data subject and the controller. Second of all, the obligations set in the Controller's Data Treatment Policy must be enforced by the processor. In other words, said policies are part of the contract. Thirdly, the purpose of the processing must be authorized by the data subject or by the country's law. For this, the controller must ensure that he has the required consent if applied or the legal authorization to execute said processing. Lastly, the contract must contain the following obligations since they are legal mandates:

> (…)The following obligations are mandatory for the Processor: 1. To process the data on behalf of the Controller and in conformity with the principles of personal data processing found in the law; 2. Safeguard the security of databases where personal data is found; and 3. Maintain the confidentiality with regards to the data processed.

## • The Risks Private and Public Enterprises, Organizations, and Entities face when participating in Cross-border Transfers of Personal Data

The transfer of data not only poses a risk regarding the protection of the rights of data subjects, but also poses a risk for the interests and assets of organizations transferring

25 This is also established in Consideration 15 of Decision 2010/87/CE in the following terms: "The data importer should process the transferred personal data only on behalf of the data exporter and in accordance with his instructions and the obligations contained in the clauses. In particular the data importer should not disclose the personal data to a third party without the prior written consent of the data exporter. The data exporter should instruct the data importer throughout the duration of the data-processing services to process the data in accordance with his instructions, the applicable data protection laws and the obligations contained in the clauses."

the data. In this section, we will underline the main risks for private and public organizations when doing cross border data transfers.

Eventually, a public or private organization, enterprise, or entity can:

- Be catalogued as a "Data Haven" for exporting data without respecting the rights of the data subjects.
- Lose control of the data. If personal data is valuable for Corporations, the minimum requirement is to safeguard it and use it within the limits of a loyal, respectful, and legal scenario.
- Face reputational damage for transferring data to "Data Havens", or to other organizations who are not committed to protecting personal data or are reckless in its processing.
- Grant unauthorized access to data
- Incur in improper use of personal data
- Accidentally manipulate or destroy data
- Forward data, indefinitely or definitely, from countries with an adequate level of protection to countries that do not fulfill the minimum standards of protection or that are catalogued as "Data Havens".

## • The Risks Data Subjects Face when their Data is Part of a Cross-border Transfer

Cross-border transfers pose an even greater challenge when it comes to guaranteeing the maximum observance to the right to data protection because the data subjects face legal and political risks.

With the cross-border transfer of personal data, the following usually occurs:

- The data is sent to countries or organizations that in practice are Data Havens because the protection is weak or nonexistent
- Data protection laws are not thoroughly enforced in the country where the data exporter is located
- Data subjects are submitted to a foreign jurisdiction
- There is an absence of legal and constitutional remedies that can ensure the full enforceability of the fundamental right to personal data protection.
- The exporter can lose control of the data and the location of the data can therefore become unknown.
- Data subjects are forced to abide decisions made by other governments, authorities, or enterprises located in a country different to their own.
- Foreign organizations may not recognize laws and personal data authorities of a determined country.
- Additional obligations are imposed to data subjects who wish to request the protection of their rights in other countries.

## • Purposes of the Rules on Cross-border Transfers of Personal Data

Regulation on cross-border transfer of personal data[26] or "International Transfer of Data"[27], guarantees that the level of protection of the personal data of a country's

26 "International Transfer" or "International Movement of Data" are other expressions used to refer to Cross Border Data Transfers.

citizens do not diminish when data is exported or transferred to other countries. This is known as the principle of continuity, which is based on the idea that "Cross-border transfers cannot affect the protection of the data subjects with regards to the processing of their data"[28].

Consequently, international documents, like the ones cited above, demand that in order to do a cross-border data transfer, the controller must ensure that there are certain "comparable guarantees", an "adequate level of protection", "equivalent protection", or other similar expressions. These requirements, are stipulated in each jurisdiction; which is why it is not possible to generalize. In the case of the Colombian regulation, for instance, it is forbidden to "transfer personal data of any type to countries that do not have an adequate level of protection"[29]. The Colombian regulation emphasizes the necessity of having absolute clarity on the standards that must be considered in order to establish if a country has said level of protection, which "in any case cannot be inferior"[30] to the one established by Law 1581 of 2012. As it can be observed, for the Colombian case, data cannot be sent to a country that has an inferior protection level than the one established by the aforementioned law.

The export and import of personal data cannot be transformed into a scenario that reduces the level of protection that is conferred to the data subject in the country where the exported data came from. Additionally, it cannot be a factor of risk for the controllers, to whom information is a relevant asset, considering that personal data is the building block of the digital economy. As a result, cross-border transfers cannot

27 Garriga Domínguez, Ana. 2004. *Tratamiento de datos personales y derechos fundamentales*, Madrid: Dykinson, p. 177.

28 De Frutos, José Manuel. 2008. "Globalización de la privacidad: hacia unos estándares comunes. Conferencia realizada en el VI Encuentro Iberoamericano de Protección de Datos, May 27-30 2008, Cartagena, Colombia.

29 Republic of Colombia, Law 1581 of 2012, article 26

30 Republic of Colombia, Law 1581 of 2012, article 26

create scenarios that facilitate the violation of the rights of the data subjects nor decrease the guarantees or legal protection they have in the exporting country.

## • The Principle of Accountability

The term "accountability" comes originally from the Anglo-Saxons[31] and regardless of the different meanings that can be given to the term, it is widely understood that in data protection, said expression refers to the way in which an organization must demonstrate compliance with data protection regulations in a useful, pertinent and efficient way.

To guarantee the effective and practical application of what is enshrined in data protection laws is a permanent challenge to any organization. The principle of accountability is especially important to achieve said purpose. This principle demands controllers and processors alike to implement appropriate, effective and verifiable measures that can allow them to prove the correct compliance to data protection laws. For such purpose, the Privacy Management Program (PMP) constitutes an operative mechanism that helps ensure that the organization takes all the necessary steps towards guaranteeing the due processing of personal data.

The principle of accountability can be as useful as laws are. Therefore, the awaited results of the application of said principle would depend on the commitment the organization has with the compliance of data protection regulations. Even more, it depends on whether or not the organization adopted proactive measures that generate an aggregated value while at the same time guaranteeing an adequate treatment of

31 Working Group of the 29. Opinion 3/2010 on the Principle of Accountability, p.8

personal data. Consequently, the challenge organizations have with regards to the principle of accountability goes beyond the expedition of documents, because they have to be able to demonstrate the real and effective compliance with regulations in the performance of their duties and functions.

There is not a unique or standardized formula to implement the principle of accountability in organizations, since it must come hand in hand with measures adjusted to the specificities of each organization. In order to do so, for its correct implementation, organizations must consider the availability of resources, the nature of the data that they process in their systems, and the risks that both the data subject and the controller face in the processing of said data.

The principle of accountability has been incorporated in the main documents on data protection of the following organizations: Iberoamerican Data Protection Network (IDPN), the European Union (EU), the Organization of American States (OAS), the Organization for Economic Cooperation and Development (OECD), the International Conference on Data Protection & Privacy Commissioners (ICDPPC), the Asia-Pacific Economic Cooperation (APEC), and the United Nations (UN).

From the documents mentioned above, it can be concluded that the ones drafted in the 1980s made reference to accountability without having to demonstrate it (it was some kind of non-demonstrated Accountability). With the passing of time, some of these documents were modified to complement its content and include the obligation of proving that the mechanisms adopted as useful, adequate, and efficient.

The IDPN and the OECD list what should be done to materialize the application of the principle of accountability in the daily practice of organizations. The IDPN especially suggests mechanisms that the controller should adopt to comply with the principle of accountability. In table n.º 2, we will summarize some of these aspects.

Table n.º 2. Incorporation of the principle of Accountability in main international documents

| Principle of Accountability | IDPN 2017 | EU 2016 | OAS 2015 | OECD 2013 | ICDPPC 2009 | APEC 2015 | UN 1999 |
|---|---|---|---|---|---|---|---|
| Is it expressly included in the document? | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | X |
| Does it expressly mention its applicability to both public and private actors? | ✓ | ✓ | | ✓ | ✓ | | |
| Does it order the implementation of mechanisms to demonstrate the compliance of regulation regarding the processing of personal data? | ✓ | ✓ | ✓ | ✓ | ✓ | | |
| Does it enunciate tools to comply with the principle of accountability? | ✓ | X | X | ✓ | X | X | |
| Does it order the allocation of resources to the instrumentation of programs and policies for data processing? | ✓ | | | | | | |
| Does it suggest the implementation of systems of administration of risks associated with data processing? | ✓ | | | ✓ | | | |
| Does it order the elaboration of binding policies and data management programs within the controller's organization? | ✓ | | | ✓ | | | |
| Does it include the need to conduct training and updating programs on data processing? | ✓ | | | | | | |
| Does it suggest the periodic revision of policies and security programs to determine required modifications in data processing? | ✓ | | | ✓ | | | |
| Does it propose the establishment of a system of internal and external supervision, including audits, to prove the compliance with data processing policies? | ✓ | | | | | | |
| Does it suggest the establishment of procedures for feedback and queries presented by the data subjects? | ✓ | | | ✓ | | | |
| Does it order the permanent revision and evaluation of mechanisms incorporated to comply with the principle of accountability? | ✓ | | | | | | |

The principle of accountability has also been included in regulations in Latin America. In Colombia, Decree 1413 of 2017[32] expressly refers to accountability and Privacy Management Programs. On the one hand, it forces "operators of public digital services" to adopt "adequate, effective, and verifiable measures that demonstrate compliance with the processing of personal data regulation"[33]. On the other hand, it requests operators to "create and implement a Privacy Management Program (PMP) as an effective operative mechanism to guarantee the due treatment of personal data"[34]. Additionally, it stipulates that the PMP must satisfy the requirements found in the "Instructions of the Superintendence of Industry and Commerce, in particular, the guide for the implementation of the principle of accountability published by the aforementioned entity"[35].

## • Necessity of Having an Accountability Guide for Cross-border Transfers of Personal Data

There are various reasons as to why cross-border transfer or cross-border circulation of personal data should be developed in detail in accountability guides. Firstly, cross-border transfers, along with the protection of privacy, are two of the main reasons that propelled the creation of regulation on the processing of personal data. Secondly, the digital responsibility of corporations, the legal responsibility of Board

32 Colombia. Decree 1413 of 25 August 2017, "Through which the Title 17 is added to the Part 2 Book 2 of the Technology of information and communication Reglementary Decree, Decree 1078 of 2015, to partially regulate Chapter IV of Title III of the Law 1437 of 2011 and article 45 of the Law 1753 of 2015, establishing general guidelines for the use and operation of public digital services"

33 Cfr. Article 2.2.17.6.3 of Decree 1413 of 2017

34 Cfr. ídem

35 Cfr. ídem

Members, and the correct and ethical behavior that must be observed along with the respect for Human Rights are reasons enough to include recommendations on cross-border transfers in accountability guides. Lastly, data protection officials have also created the necessity to develop this topic in accountability guides. In Colombia's case, through the External Circular Letter 5 of 10 August 2017, the Superintendence of Industry and Commerce (SIC) - Colombia's data protection authority- ordered the following:

> Notwithstanding the fact that the transfer of personal data is done in countries with an adequate level of protection, data controllers, based on the principle of accountability, must be able to demonstrate that they have implemented appropriate and effective measures to guarantee an adequate treatment of the data they transferred to another country and to guarantee the databases' safety when carrying on said transfer[36].

As it can be observed, for the cross-border transfer of data, it is not enough that the receiving country is catalogued by the SIC as a country with an adequate level of protection, but the data controller must demonstrate that it has taken the necessary measures to pursue the following objectives:

1. To guarantee the adequate treatment of the personal data transferred to the other country.

2. To confer security to the "databases at the moment of performing said transfer".

The SIC Guide of 28 May 2015 on Accountability, does not establish anything on cross-border transfers - *it just mentions crossborder transmissions of personal data,*

36 Cfr. #3.2 External Circular Letter 5 of 2017 of the Superintendence of Industry and Commerce.

*which are substantially different*-. As it was already mentioned, personal data can be exported to another country through transference, transmission, or recollection. When referring to international transmissions, the responsible for the treatment of said data is still the controller even when the data processor is located or domiciled in another country.

Data controllers must adopt precise, useful and verifiable measures before transferring the data of Colombians to other countries. This is necessary due to the following reasons:

1. The international transfer of data in accordance with the principle of accountability is a novel question; thus, still widely unknown especially in Latin America, since it was adopted from other jurisdictions without really developing the concept.

2. The principle of accountability is a measure imported from other legal systems and not widely known in Colombia, regardless of the existence of the Guide drafted by the SIC. In practice, a wide number of controllers do not know what to concretely do to comply with said principle. Some have the resources to hire another company with knowledge in accountability, but most lack the resources to do so. As it can be seen, the real implementation of the principle of accountability will depend, in most cases, in the resources each corporation has, which will directly affect the effective protection of the rights of the data subjects

3. Establishing guidelines regarding accountability in cross-border transfers will reduce costs to corporations- since they will at least know what to do- and can establish minimum standards to try to guarantee certain level of protection of the rights of the subjects whose data is being transferred to other countries.

We will now present our suggestions to implement the principle of accountability in the cross-border or international transfer of personal data.

# II. Recommendations to Implement the Principle of Accountability in Cross-border or International Transfer of Personal Data

## • Verify if the Controller has the Legal Entitlement to Transfer or Transmit Personal Data to Another Country

Before exporting data, ask yourself the following: Is your corporation legally entitled to export or send personal data to another country? It is essential to have full legal certainty about this before proceeding.

If the organization is not entitled by law to transfer data, the corporation is then exposed to administrative or criminal investigations. In Colombia's Law 1273 of 2009 there are several criminal offenses related to the treatment of personal data such as the unauthorized access to systems of information, the destruction or manipulation of data, the impersonation in websites to collect personal data, and the violation of privacy. The law stipulates the following: who "without being entitled to it, in its name or acting on behalf of someone else, obtains, compiles, subtracts, offers, sells, exchanges, sends, acquires, intercepts, divulges, modifies, or employs personal codes or personal data contained in databases, archives, or similar means" is punished with a four to eight-year sentence and a fine of 100 to 10000 minimum wages.

As it can be seen, various acts regarding the treatment of personal data generate criminal responsibility. This means that data controllers and processors must be careful and diligent in order to avoid incurring in a punishable offense. It is important to highlight that if the offense is committed by "…the responsible of the administration or

control of said data" the punishment for the offense will increase up to three quarters of the initial one. Additionally, said person can be "disqualified up to three years from practicing any profession related to systems of processed information in computer equipment".

## • Determine the Adequate Mechanism that must be used for the International Transfer or Transmission of Personal Data

The data controller must bear in mind that, depending on the country, there are various legal mechanisms that can be used in order to transfer data without violating the rights of the data subjects or laws and regulations, which are the following:

- Transfers based on the authorization of the data subject;
- Transfers based on a decision of adequacy;
- Transfers based on a declaration of conformity;
- Transfers based on a *sui generis* agreement (Such as the EU-US Privacy Shield).
- Transfers stipulated in contract clauses;
- Transfers established on binding corporate rules;
- Transfers based on other types of adequate guarantees (codes of conduct, mechanisms of certification).

It is important to highlight that not all jurisdictions recognize all the alternatives mentioned above to transfer personal data. Guidelines about the legal mechanisms for cross-border transfers, can be found in the following international documents:

1. 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), 2. The Iberoamerican Data Protection Network (IDPN) Standards for Data Protection for the Ibero-American States (2017).

## • Establish how to Prove the Compliance with the Principle of Accountability to Transfer Personal Data

The controller must not only comply with the principle of accountability, but must also demonstrate what was done in order to guarantee the compliance. Although there are various means for providing evidence, data protection regulation imposes certain burdens of proof that must be considered by the controller. As such, the most practical way to transfer data is through contracts or documents that can be presented as proof of compliance to data protection obligations.

## • Take into Account the Objectives for Cross-border Data Transfer

It is not enough to be legitimated to export data, since data can only be transferred to fulfill certain purposes or objectives that are listed in each legislation.

## • Guarantee the Fulfillment of Desired Objectives through Accountability Measures

In Colombia's case, the measures implemented in order to guarantee compliance with the principle of accountability must be adequate and pertinent with regards to the objectives established in External Circular Letter 5 of 2017 of the SIC, which are the following:

1. Guarantee the adequate treatment of personal data being transferred to another country.

2. Confer security to the "databases when effectuating said transfer".

The adequate treatment of personal data, supposes two things. Firstly, that the country where the receiving party is found has legislation where the rights of the data subjects are respected and protected. Secondly, that the legislation in the receiving country complies with the parameters established in the legislation of the exporting country for the processing of personal data.

## • Create Strategies to Protect the Interests of the Organization

Before transferring data, the Controller must evaluate the concrete risks the organization will face by merely transferring personal data to another country. Furthermore, mechanisms to mitigate said risks such as contractual and technological tools, must be articulated in a proactive plan.

- ## Adopt Measures to not Defraud the Trust of the Customers or the Data Subjects on the Organization

The principle of accountability has generated a lot of expectations and promises. However, it can be a failure if efforts are not made to implement it in practice. For instance, if an organization's main asset is data, the organization must protect the rights of the data subjects, in order to avoid losing their trust. If it is a public organization, it is a constitutional obligation, to respect and protect the rights of people.

- ## Provide onward Transfers of Personal Data

Rules must be established for the forwarding of personal data from the initial receiving country to another. If this is not regulated or controlled, personal data might end up in countries or organizations considered "Data Havens".

- ## Include Privacy by Design and by Default in International Transfers of Personal Data

Privacy by Design and by Default has been traditionally considered another proactive measure. However, in certain cases it has not been catalogued as a measure but as a principle in the processing of personal data. Said measure is mentioned in this guide because it can be applied in an analogous way to various questions related to transfers and transmissions of personal data.

Privacy by Design (PbD) was defined and developed in the 1990s by Ann Cavoukian, who considers that "privacy assurance must ideally become an organization's default mode of operation"[37]. The following principles applied to international transfers are consistent with the principle of accountability:

– *Proactive not Reactive; Preventative not Remedial*. According to this principle, proactive rather than reactive measures must be adopted to protect personal data. According to Cavoukian, PbD "does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after"[38].

When it comes to international transfers, measures should be adopted in a preventive manner and not adopted as repair measures after an incident or problem has occurred.

– *Privacy as the Default Setting:* This principle is based on the fact that "the default rules!"[39], which is why data protection should be part of the predetermined configuration of the system. As such, corporations must ensure that "personal data are automatically protected in any given IT system or business practice"[40].

Taking into consideration the aforementioned, in processes of international circulation of data, strategies to ensure an adequate processing of personal data should be implemented from the beginning.

37 Cfr. Cavoukian, Ann (2011). Privacy by Design. The 7 Foundational Principles. Available in https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

38 Cfr. ídem.

39 Cfr. ídem.

40 Cfr. ídem.

– *Privacy Embedded into Design*: Privacy and the correct treatment of data should be part of the design and architecture of IT systems and the practices of organizations. With this, "privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality"[41].

– *Full Functionality - Positive-Sum, not Zero-Sum*: This principle seeks to emphasize that businesses and activities conducted by organizations should not be incompatible but should seek a breakeven point. According to Cavoukian, "Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum 'win-win' manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made"[42].

– *End-to-End Security- Full Lifecycle Protection*: If PbD is embedded into the system since the beginning, this guarantees security throughout the entire lifecycle of the data involved in the transfer and processing.

It is important to keep in mind that data security is not only beneficial to the data subjects, but to the controllers who consider data as an asset to their organization and good reputation as well.

– *Visibility and Transparency- Keep it Open*: This principle seeks to assure that stated promises and objectives regarding privacy and the processing of personal data are fulfilled and verifiable in practice.

– *Respect for User Privacy - Keep it User Friendly*: "Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering

41 Cfr. ídem.

42 Cfr. ídem.

> such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric"[43].

In Colombia's regulation, Decree 1413 of 2017[44] not only defines Privacy by Design as "the protection of information that demands the incorporation of specificities in the design of technologies, processes, business practices, and physical infrastructure to guarantee the protection of the privacy of data"[45] but it is considered a principle whose scope is the following:

> […] since before the recollection of information and during its lifecycle, preventive measures of diverse nature (technological, organizational, human, and procedural) shall be adopted in order to avoid violations of privacy rights or of the confidentiality of information. Additionally, they should be adopted in order to avoid security breaches and unrightful processing of personal data. Privacy and security shall be a predetermined part of the design, the architecture and the configuration of IT systems[46].

This Decree obliges operators to apply good practices and principles developed internationally with regards to "Privacy by Design (PbD)" and "Privacy Impact Assessment (PIA)", signaling that:

> The protection of data cannot be solely guaranteed through the compliance with a country's legal regulation, but should also be a mode of operation of an organization.

43 Cfr. ídem

44 Colombia. Decree 1413 of 25 August 2017, "Through which the Title 17 is added to the Part 2 Book 2 of the Technology of information and communication Reglementary Decree, Decree 1078 of 2015, to partially regulate Chapter IV of Title III of the Law 1437 of 2011 and article 45 of the Law 1753 of 2015, establishing general guidelines for the use and operation of public digital services"

45 Cfr. Article 2.2.17.1.3. #17 of Decree 1413 of 2017 (Colombia)

46 Cfr. Article 2.2.17.1.5. #6 of Decree 1413 of 2017 (Colombia)

> It should be applied to systems of information, models, business practices, physical design, infrastructure, and interoperability, in order to guarantee the privacy of the data subject with regards to the recollection, usage, storage, divulgation, and disposition of data messages in digital services[47].

In order to comply with the aforementioned, data controllers should take into consideration the following recommendations:

1. Conduct and update impact evaluations on the processing of personal data and on the Privacy Management Program whenever there are changes that generate new privacy risks.
2. Incorporate practices and development processes destined to safeguard personal data throughout the lifecycle of the system, program or service.
3. Maintain the adequate practices and processes with regards to privacy management during the data's lifecycle in order to guarantee that IT systems comply with the requirements, policies, and privacy preferences of data subjects.
4. Use the necessary means to guarantee the safety, confidentiality, and integrity of personal data throughout its lifecycle- starting with its original recollection and through its usage, storage, diffusion, and safe disposal.
5. Guarantee that the infrastructure, IT systems, and business practices are subject to independent verification on behalf of any interested party, including clients, users, and affiliated organizations[48].

47 Cfr. Article 2.2.17.6.5 of Decree 1413 of 2017 (Colombia)

48 Cfr. Article 2.2.17.6.5 of Decree 1413 of 2017 (Colombia).

## • Replicate Proactive Measures Adapted in the Processing of Personal Data to International Transfers

Internationally, the implementation of proactive measures related to data protection is of extreme importance in order to improve compliance with regulation and to consolidate and strengthen the due processing of personal data. The following are examples of measures that can be adopted:

– *Designate a Privacy Officer or a Data Protection Office (DPO)*: This person is the one in charge of verifying that the organization complies with all the legal requirements imposed by the data protection authority with regards to cross-border transfer of personal data. Furthermore, the DPO is in charge of conducting evaluation and monitoring plans with regards to exported data.

– *Conduct privacy impact assessments:* These are useful when the processing of personal data has a high impact or high risks, such as when the data involves sensitive information or data from minors.

– *Specialized training and education*: Organizations should conduct periodical activities directed to educating and training employees who are in charge of exporting personal data overseas. This can help ensure that employees count with enough specialized preparation in order to perform international transfers or transmissions in accordance with the law.

– *Implement monitoring and evaluation programs*: Depending on the case, the data controller should conduct monitoring or auditing visits to the overseas recipient, in order to verify compliance with its obligations with respect to security, due usage, and confidentiality of the data.

– *Adhere to self-regulation agreements.*

– *Have contingency plans*: It is necessary to set from the beginning the guidelines or actions that must be followed by employees in case of an unexpected privacy or security situation or breach related to the data exported to an overseas recipient. For instance, a question a controller might ask when designing said guidelines or action plan is: what to do in case of an informatic attack that compromises the security and confidentiality of data transferred or transmitted to another country?

## • Include Accountability Tools in a Contract Tailormade for the Particularities of each Transfer

Contracts represent a legal alternative to demonstrating the implementation of measurements that prove compliance with the principle of accountability in cross-border data transfers. Although there are model contracts[49], it is crucial that the contract is consistent with the peculiarities and necessities of each organization. Likewise, the data exporter should establish if the recipient of the data in the other country is a corporation or an organization and whether or not it is a "Data Haven", in order to consider the possibilities of compliance with contractual obligations.

49 The European Commission adopted Decisions 2001/497/EC, 2004/915/EC and 2010/78/EC through which it endorses certain standard contractual clauses for the transfer of personal data. Decisions 2001/497/EC and 2004/915/EC suggests contract models when the administration of personal data passes from one operator to another one found in a different country, while Decision 2010/78/EC has a contractual scheme for those cases where the administration of information is still under the responsibility and custody of the Controller who contracts a third party located in another country to processes it under its mandate.

When drafting the contract, organizations should take into consideration the following:

- The personal information exported to the other country and whether there is sensitive, minors, private, semi private, or public information or data involved. According to this, special measures of protection shall be implemented. For instance, in the treatment of sensitive data, a greater responsibility is demanded, which means higher security measurements and restrictions about its access, usage, and circulation must be in place.
- The security measures that must be implemented by the overseas recipient of the exported data
- The quantity of the data being exported
- The rights that the controller and the recipient must guarantee to the data subject
- The principles of data processing that the overseas recipient must observe and comply with
- Who has access to the exported information
- The mechanisms the data subject has in order to exercise its rights in a simple and expedite manner
- The purpose of the cross-border transfer. It is very important to include the allowed and prohibited usage of the data on behalf of the overseas recipient.
- Define the time limit during which the overseas recipient can process the data.
- The data protection regulation that will govern the contract. It can be the law of the exporting country or of the importing country. If the principle of continuity in data protection wants to be guaranteed, it is better for the contract to be governed by the law of the country where the data exporter is domiciled or located.

- The prohibition of performing onward transfers to other countries. It is important to clarify if the data initially transferred to Country A, can then be transferred from this country to Country B. In case this is allowed, conditions that must be observed for this transfer shall be established.
- How to recover the data transferred in order to guarantee the rights of the data subjects when the overseas recipient does not comply with what was stipulated in the contract.
- Who is accountable for the eventual wrongful treatment of the exported personal data and the compensation for damages caused
- Whether or not the importer and exporter will have joint or several liability for the eventual violation of the rights and damages caused by this.
- How would the data be treated once the contract is terminated.

## • Articulate the former Recommendations with the Accountability Guide of the Data Protection Authority of the Exporter's Country

Lastly, it is important to highlight that all the suggestions contained in the present guide are directed to implementing the principle of accountability in the cross-border circulation of personal data, whether it is through international transfers or transmissions. As such, this is a complimentary guide to the general guides that authorities have issued on the matter.

In Colombia's case, for instance, the SIC issued on 28 May 2015, the *Guide for the implementation of the Principle of Accountability*, which mainly replicates, the Canadian

guide of accountability, titled *Getting Accountability Right with a Privacy Management Program*[50], issued in 2012 by the Office of the Privacy Commissioner of Canada. Another Guide that can be used as a reference can be Hong Kong's, titled "Implementing and Demonstrating Accountability[51], prepared by Nymity for the Office of the Privacy Commissioner for Personal Data, Hong Kong.

50 This Guide can be found in https://www.priv.gc.ca/media/2102/gl_acc_201204_e.pdf.

51 This Guide can be found in https://www.pcpd.org.hk/privacyconference2014/files/9_booklet_ guide.pdf.

# Glossary

Some of the following definitions are replicated from international documents whereas others are subtracted from what is contained in Colombia's legislation. It is plausible that this might or might not match the ones signaled in other countries' regulations.

Authorization: Previous, express and informed consent of the data subject in order to carry out the processing of personal data[52].

Personal Data: Any information linked or associated with determined or determinable natural person[53].

Data Processor: Natural or legal person, public or private, that through itself or in association with others processes personal data on behalf of the data controller[54].

Exporter: Person or organization that sends personal data from one country to another.

Internet of Corporations: Rules that corporations have created in order to conduct businesses or provide services through the Internet. It refers to the guidelines that businesses consider reasonable and desirable under their business model in order to gain revenue in the digital economy. An example of these rules are the legal notes or the terms and conditions on a Webpage or APP, and on the remaining Internet services.

52 Cfr. Art. 3 lit. a Law 1581 2012.

53 Cfr. literal C Ibídem

54 Cfr. Literal d Ibídem

Importer: Person or organization that receives the exported data.

Data Havens: Countries or corporations where the protection of data subjects is weak or non-existent.

International Recollection of Personal Data: Activity through which a corporation or organization domiciled in one country recollects data from people located in another country. The data is directly recollected from the data subject with the use of technologies or tools such as webpages, apps, or cookies.

Data Controller: Natural or legal person, public or private, that by itself or in association with others, makes decisions regarding databases and the processing of said data[55].

Data subject: natural person whose personal data is being processed[56].

International Data Transfer: The data transfer that occurs when the data controller, located in Colombia, sends information or personal data to a receiver, who is also a data controller and is located outside the country[57].

International Data Transmission: Treatment of personal data which implies sending said data outside of Colombia's territory in order for the data processor to process the data on behalf of the controller[58].

Processing: Any operation or series of operations on personal data, such as its recollection, storage, use, circulation, and suppression[59].

55 Cfr. lit e Ibídem

56 Cfr. literal f Ibídem

57 Cfr. Art. 2.2.2.25.1.3 #4 Decree 1074 2015 (Decree 1377 2013, article 3)

58 Cfr. numeral 5 ibídem

59 Cfr. literal g article 3 Law 1581 2012.

# References


Accenture. 2016. Guarding and growing personal data value Organizations that demonstrate responsibility in the way they handle personal data today will lead the digital economy of tomorrow. Enero. En https://www.accenture.com/us-en/insight-guarding-growing-personal-data-value.aspx.

Cano Martínez, Jeimy. 2016. ¿Eres una empresa digitalmente responsable? Enero 20. En https://www.linkedin.com/pulse/eres-una-empresa-digitalmente-responsable-jeimy-cano-ph-d-cfe.

Cano Martínez, Jeimy. 2014. Presiones emergentes sobre la privacidad de la información, en http://insecurityit.blogspot.com.co/2014/05/presiones-emergentes-sobre-la.html.

Montezuna, Alberto. 2017. Colombian draft regulation introduces accountability principle to data transfers, en https://iapp.org/news/a/colombian-draft-regulation-introduces-accountability-principle-to-data-transfers.

Palazzi, Pablo. 2003. Comercio electrónico, transferencia internacional de datos personales y armonización de leyes en un mundo globalizado. En *Derecho de internet & telecomunicaciones*, editado por el GECTI. Bogotá: Legis.

Parmar, R., Mackenzie, I., Cohn, D. y Gann, D. (2014) The new patterns of innovation. *Harvard Business Review*. January-February. Disponible en https://hbr.org/2014/01/the-new-patterns-of-innovation.

Puccinelli, Oscar. 1999. *El* habeas data *en Indoiberoamérica*, primera edición, Bogotá: Temis.

Remolina Angarita, Nelson. (2016) "Internet de las empresas" ["Internet of Corporations" -IoC-]: una explicación de lo que pasa en internet y del futuro de la protección de los derechos humanos en el ciberespacio (parte 1). Universidad de los Andes. Publicado en https://habeasdatacolombia.uniandes.edu.co/?p=2222.

Remolina Angarita, Nelson. 2015. Recolección internacional de datos: un reto del mundo post-internet. BOE – *Boletín Oficial del Estado*. Madrid, abril del 2015. ISBN 978-84-340- 2196-9.

Remolina Angarita, Nelson. 2013. *Tratamiento de datos personales: aproximación internacional y comentarios a la ley 1581 de 2012*. Bogotá, Legis, 2013. ISBN 978-958-767-086-8.

Remolina Angarita, Nelson. 2012. Aproximación constitucional de la protección de datos personales en Latinoamérica. *Revista Internacional de Protección de Datos Personales* –RIPDP–. Red Académica Internacional de Protección de Datos Personales (1):1-13.

Remolina Angarita, Nelson. 2010. ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?, 16 *International Law, Revista Colombiana de Derecho Internacional*, 489-524 (2010).

Remolina Angarita, Nelson. 2010. Cláusulas contractuales y transferencia internacional de datos personales, en *Obligaciones y contratos en el derecho contemporáneo*, 357-419, Jorge Oviedo-Albán (ed.), Bogotá, Biblioteca Jurídica Diké y Universidad de La Sabana.

# About the Authors

## Nelson Remolina Angarita

PhD -Summa Cum Laude- in Legal Sciences from the Pontifical Xaverian University (Bogotá). Master of Laws, The London School of Economics and Political Sciences (London). Specialist in Commercial Law and Lawyer from Los Andes University (Bogotá). Former Director of the Group of Studies in Internet, e-Commerce, Telecommunications and Informatics (GECTI) of Los Andes University and of the Observatory Ciro Angarita Barón on Personal Data Protection. Winner of the Personal Data Investigation Award of 2014, conferred by the Spanish Agency of Data Protection to original papers on the protection of data in Iberoamerican countries. He is currently Colombia's Deputy Superintendent for Data Protection.

Author of various books and articles on the processing of personal data. His Doctoral Thesis was centered on the study of the international transfer and recollection of personal data.

## Luisa Fernanda Álvarez Zuluaga

Lawyer from Los Andes University (Bogotá) and Member of the Group of Studies in Internet, e-Commerce, Telecommunications and Informatics (GECTI). Counts with experience in international research on the principle of accountability, Privacy Management Proggrams, and Accountability Guides.

Universidad de los Andes
Colombia

GECTI

Observatorio Ciro Angarita Barón
sobre la protección de datos personales

https://gecti.uniandes.edu.co
https://habeasdatacolombia.uniandes.edu.co