Assessment of Colombia's Data Protection Regime as Substantially Equivalent by the Dubai International Financial Centre Authority ("DIFC" or "DIFCA") Commissioner of Data Protection

DIFC

Table of Contents

DIFC

Introduction

Articles 26 and 27 of the Data Protection Law, DIFC Law No. 5 of 2020 and Section 5 of the DIFC Data Protection Regulations 2020 (the "DIFC DP Law 2020") address transfers of Personal Data to Third Countries or International Organisations. Article 26(2) specifically states:

> *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.*

Recognition of the equivalence of another jurisdiction's data protection regime, also known as adequacy, is based on an assessment of key data protection concepts and obligations found in local data protection laws to ensure equivalence with the exporting jurisdiction or international organisation's data protection law. As such, the DIFC Office of the Commissioner of Data Protection assesses Colombia's laws and regulations according to the fundamental data protection principles and criteria, including but not limited to:

1. Basic data protection concepts and definitions

2. Grounds for lawful and fair processing for legitimate basis

    a. Legitimate bases for processing
    b. Controller and Processor obligations

3. Existence of Data Protection Principles
    a. purpose limitation
    b. data quality and proportionality
    c. data retention
    d. security and confidentiality
    e. transparency

4. Data Subjects' Rights
    a. right of access, rectification, erasure and objection

5. International / Onward Data Transfer Restrictions

6. Security of Processing and Breach Reporting

7. Accountability
    a. Special categories of data (aka sensitive personal data)
    b. Direct marketing
    c. Automated decision making and profiling

8. Additional content principles for specific types of processing

9. Existence of international commitments and conventions binding on Colombia or its membership of any multilateral or regional organisations.

DIFC

Summary of Colombia's Applicable Laws and Regulations

The two main data protection laws in Colombia are Statutory Law 1266 of 2008 ("**Law 1266**") enacted in 2008 and Statutory Law 1581 of 2012 ("**Law 1581**") enacted in 2012.

Law 1266 regulates the processing of financial data, credit records and commercial information collected in Colombia or abroad. It also defines general terms on habeas data and establishes basic data processing principles, data subject rights, data controller obligations and specific rules for financial data.

Law 1581 is applicable to all data collection and processing in Colombia, except data regulated under Law 1266 and certain other types of data or regulated industries. The law is further applicable in any case where a data processor or controller is required to apply Colombian law under international treaties.

Observation 1: Basic data protection concepts and definitions

Summary of key obligations / changes reflected in Colombia's data protection regime

- **Concepts and definitions:**
- **Breach notification requirements:**
- **Enforcement powers:**
- **Notifications to the Commissioner / Supervisory Authority:**
- **Powers and objectives of the Commissioner:**

1. Data protection laws of Colombia

Law 1266 regulates the processing of personal data related to the fulfilment or non-fulfilment of monetary obligations. It applies to any company or public entity that collects or uses this information. In practice, 90% of the complaints received at the Superintendence of Industry and Commerce are for possible infractions of 1266, referring to cases of people who are reported as delinquent to financial information providers and analysts (such as Experian, TransUnion).

Law 1581, for its part, regulates the processing of other personal data such as contact information, photos and sensitive data, inter alia.

These two laws are not exclusive. Each one regulates different personal data. In practice, it is feasible for an entity to apply both laws. For example, Law 1266 applies to a bank when it reports its clients as delinquent because they did not pay a loan, and Law 1581 applies when the bank uses the contact information of its clients for marketing or advertising purposes.

Both Law 1581 and Law 1266 apply to data processing that is done by any manual, technological means or with known or unknown technologies. They have a technologically neutral scope of application because they were not created to regulate data processing with certain means or technology. Rather, they apply to all cases in which there is processing (i.e., collection, use, analysis, circulation) regardless of the medium or process that is used for said purpose.

Safety measures adopted by those processing personal data must seek to mitigate the following risks: unauthorized access to personal data; loss; destruction (accidental or unauthorized); contamination by computer virus; fraudulent or unauthorized use, consultation, copy, modification, revelation, communication, or diffusion; and adulteration. The "safety principle" was written from a neutral perspective, meaning that no particular technology has to be implemented by the Data Controller or Processor. Hence, they can choose whatever method fits them better to fulfil their objectives.

2. Non-privacy laws which include data protection elements

Additionally, Colombia has other sectoral laws and regulations with privacy features, such as the following:

- Law 1712 of 2014 - Law of Transparency and the Right of Access to National Public Information.

- Law 1480 of 2011 - Consumer Protection Statute.
- Law 1621 of 2013 - Intelligence and Counterintelligence Law (whereby rules were set to strengthen the legal framework that allows the agencies carrying out intelligence and counterintelligence activities to comply with their constitutional and legal mission).
- Law 599 of 2000 (article 269F Breach of Personal Data) - Penal Code
- Law 79 of 1993 - Demographic Census (by which the conduct of Population and Housing Censuses throughout the national territory is regulated).
- The employment and immigration[1] laws **do not create special rules on data processing**, which is why Law 1581 fully applies in the workplace.

3. Regulatory/Supervisory Authorities

According to Law 1266, there are two different authorities on data protection and data privacy matters.

The first of them, which acts as a general authority, is the Superintendence of Industry and Commerce ("**SIC**"). The SIC is the Colombian Data Protection Authority and is linked to the Ministry of Commerce, Industry, and Tourism. The second authority is the Superintendence of Finance ("**SOF**"), which acts as a supervisor of financial institutions, credit bureaus and other entities that manage financial data or credit records and verifies the enforcement of Law 1266.

Nevertheless, under Law 1581, the SIC is the highest authority regarding personal data protection and data privacy. It is empowered to investigate and impose penalties on companies for the inappropriate collection, storage, usage, transfer and elimination of personal data.

Website: Superintendencia de Industria y Comercio (SIC)

SIC guidance can be found here:

https://www.sic.gov.co/centro-de-publicaciones?field_global_topic_tid=7037&field_anos_p_value=All

Superintendent of Industry and Commerce

Decree 1817 of 2015 established the special conditions to designate the Superintendent of Industry and Commerce ("**Superintendent**") to guarantee the professional, impartial, transparent, and independent competence of the DPA. The rules for the Superintendent's designation are the following:

a) The Superintendent is designated by the President of the Republic of Colombia for a fixed period of time equivalent to that of the President (four years). Before designating the Superintendent, the President can solicit the opinion of social and academic organizations, of citizens, and of universities. Likewise, it can interview the candidates.

[1] Decree 1067 of 2015 regulates the Administrative Sector of Foreign Relations. The full text of the decree can be found at: https://www.migracioncolombia.gov.co/jdownloads/Decretos/Decretos%20-%202015/DECRETO%201067%20DEL%2026%20DE%20MAYO%20DE%202015_compressed%20(1).pdf

b) To designate the Superintendent, a public call is done on the website of the Presidency of the Republic, so that those who fulfil the requirements can apply.

c) The requirements to be Superintendent are:

i. have a University degree and a master's degree or a PhD in a discipline related to the duties or functions the Superintendent must perform; and

ii. have at least ten (10) years of professional experience in areas related to the position applied for, acquired in the public or private sector or as a University Professor.

d) The Superintendent is appointed for the presidential term. As soon as the constitutional term for the presidency (4 years) ends, the new President has three months to appoint the new Superintendent.

Deputy Superintendent for the Protection of Personal Data

The Superintendent appoints a Deputy Superintendent for the Protection of Personal Data ("**Deputy Superintendent for Data Protection**"). This is a position of managerial level, which is additionally of free appointment and removal. To be appointed as the Deputy Superintendent for Data Protection, article 2.2.2.4.2 of Decree 1083 of 2012 and the Specific Handbook of Functions of the SIC requires said person to have a professional and postgraduate degree plus 60 months of professional experience in fields related to the functions performed by the Deputy Superintendence.

Law 1581 ratified that the SIC through the Deputy Superintendence for Data Protection "*will exercise supervision to ensure that the processing of personal data respects the principles, rights, guarantees and procedures provided for in this law*"[2]. The SIC also supervises financial personal data as stated in Law 1266, but it does not get involved in the compliance or breach of the monetary obligations. Furthermore, the Constitutional Court stated that the Deputy Superintendence for Data Protection must act autonomously and independently in the exercise of its functions[3].

Regarding the creation of the Deputy Superintendence for Data Protection, certain statements made by the Constitutional Court deserve to be transcribed due to their importance:

The position of the Courts and the SIC is that data processing of data subjects domiciled in Colombia, even if it is done from abroad, is subject to local data protection laws. Therefore, the application of the law extends to companies that are not incorporated in the Colombian territory. Whilst the mechanisms available to ensure the enforceability of the law against these companies are debatable and will vary from territory to territory, the SIC has nonetheless imposed sanctions on companies that have no local presence for violating the data protection regime.

[2] Law 1581 of 2012, Article 19.

[3] Constitutional Court Ruling C-748 of 2011, paragraph 5

For the Constitutional Court, the right of habeas data "*requires effective protection mechanisms in order to be guaranteed. Said mechanisms should not depend on judges, there should be an administrative institution that besides exercising control and surveillance over private and public entities, also ensures the effective observance of data protection, and due to its technical nature, should have the capacity to develop public policy in the subject-matter, without political inherences for the compliance of said decisions*"[4].

[4] Constitutional Court Ruling C-748 of 2011, paragraph 2.18.3.1

Observation 2: Grounds for lawful and fair processing for legitimate purposes

Constitutional Safeguards

According to the Political Constitution, "*Colombia is a social State under the rule of law, organized in the form of a Unitary Republic; decentralized, with autonomy of its territorial units, democratic, participatory, and pluralistic, based on the respect for human dignity, the work and solidarity of the individuals who belong to it, and the prevalence of the general interest*"[5].

One of the essential constitutional goals of the State is to "(…) ***guarantee the effectiveness of the principles, rights, and duties stipulated by the Constitution*** *(…) the authorities of the Republic are established in order to protect all individuals residing in Colombia, in their life, honour, property, beliefs, and* ***other rights and freedoms****, and in order to ensure the fulfilment of the social duties of the State and individuals*"[6]. Note that the constitutional obligation public authorities have of protecting the rights of people, goes beyond the protection of Colombian citizens, since all people who reside in Colombia must be protected, without discrimination.

Furthermore, regarding the **right of habeas data**, the Constitution dictates that "*all individuals have the right to (…) know, update, and rectify information collected about them in databases and in the records of public and private entities. Freedom and other guarantees approved in the Constitution will be respected in the* ***collection, processing, and circulation of data****"[7].* As it can be seen, the rightful processing of personal data is a fundamental constitutional right, and as such it prevails over all regulations, since "*the Constitution provides the norms of regulations. In all cases of incompatibility between the Constitution and the law or other legal regulations, the constitutional provisions will prevail"[8].* To sum up, data protection in Colombia has the highest legal rank and protection since it is a fundamental constitutional right.

Sensitive Personal Data

Under Law 1266, sensitive personal data is defined as data that due to its sensitivity is only relevant to its owner. Under Law 1581, sensitive personal data is any data that affects its owner's intimacy or whose improper use might cause discrimination. Data that reveals any of the below information is considered sensitive data:

- Ethnic or racial origin
- Political orientation
- Religious or philosophic convictions
- Membership in labor unions, human right groups or social organizations

[5] Political Constitution, Article 1
[6] Political Constitution, Article 2
[7] Political Constitution, Article 15
[8] Political Constitution, Article 4

- Membership in any group that promotes any political interest or that promotes the rights of opposition parties
- Information regarding health and sexual life, and
- Biometrics

Sensitive personal data shall only be processed:

- With the data subject's special and specific consent
- If necessary to preserve the data subject's life, or a vital interest and the data subject is physically or legally unable to provide consent
- If used for a legitimate activity and with all necessary security measures, by an NGO, an association or any kind of nonprofit entity, in which case, the entity will need the data subject's consent to provide the sensitive personal data to third parties
- If such data is related to or fundamental to exercising a right in the context of a trial or any judicial procedure, or
- If such data has a historic, statistical or scientific purpose, in which case the data subject's identity may not be disclosed

Children's Data

Children (under 18 years old) are treated differently, as article 7 of Law 1581 prohibits the processing of non-public personal data of minors, as minors are specially protected under constitutional law, more particularly, article 44. However, the Constitutional Court established by means of Ruling C-748 of 2011 that interpretation of this article must not be understood as an absolute prohibition for the processing of personal data of minors, as this would lead to a disregard of minors' fundamental rights. What this article intends, is that the processing of personal data of minors always pursues the respect of minors' rights, and always looks for their superior interests. In other words, this processing is allowed only if minors' interests and rights are respected and granted during the processing.

For this purpose, Decree 1074 of 2015[9] established that children's legal representatives must always grant the previous consent for the processing of their personal data, and that data processors and controllers involved in the processing of personal data of minors must watch for the adequate use of this information, and must comply with Law 1581. Law 1581 is a recent regulation and data controllers continue to adapt to these requirements, however, in practice, minor's consent is granted by their legal representatives. Data controllers in Colombia adhere to this regime.

[9] Decree 1074 of 2015 regulates different matters of the commerce, industry and tourism sectors, including data privacy subjects explained in this document.

Observation 3: Existence of Data Protection Principles

The adequacy assessment evaluated the framework of Colombia with respect to the following data protection principles, inter alia:

a. purpose limitation;

b. data quality and proportionality;

c. data retention;

d. security and confidentiality; and

e. transparency.

After the promulgation of Law 1581, the Constitutional Court further developed through its jurisprudence the fundamental rules that govern everything related to the recollection, storage, use, circulation, access, and any other activity involving personal data. Regarding this, the Court stated that: "*the guarantees established in article 4 are principles which had already been developed by constitutional jurisprudence as guarantees derived from the fundamental right of habeas data and* ***as such, even in the absence of a law, these principles are of mandatory application in the processing of all types of personal data***" [10].

Article 4, titled "principles for the processing of personal data" establishes the following:

> *"In the development, interpretation, and application of the present law, the following principles will be applied in a harmonic and integrated manner:*
>
> *a)* ***Principle of Legality on Data Processing:*** *The Processing to which the present law refers to, is a regulated activity which must be subject to what is established in the law and remaining dispositions that may partially regulate it;*
>
> *b)* ***Principle of Purpose:*** *The Processing must obey a legitimate purpose which must be in accordance with the Constitution and the Law, said purpose must be informed to the Data Subject;*
>
> *c)* ***Principle of Freedom:*** *The Processing must only be done with the prior, expressed, and informed consent of the Data Subject. Personal Data cannot be obtained or divulged without previous authorization, or without legal or judicial mandate that replaces the subject's consent;*
>
> *d)* ***Principle of Accuracy or Quality:*** *The data processed must be truthful, complete, accurate, updated, verifiable, and understandable. The processing of partial, incomplete, fractionated or misleading data is prohibited;*

[10] Constitutional Court, Ruling C-748 of 2011, paragraph 2.4.5.1.

e) ***Principle of Transparency:*** *In the processing, the controller or processor must guarantee the subject's right to obtain, at any time and without restrictions, information regarding all the subject's data collected;*

f) ***Principle of Access and Restricted Circulation:*** *The processing is subject to limitations arising from the nature of personal data, the provisions of this law, and the Constitution. In this sense, the processing can only be with authorization given by the Subject and/or by the persons covered by this law;*

Personal data, except public information, may not be available on the Internet or other means of disclosure or mass communication, unless the access is technically controllable to guarantee restricted knowledge only to the Data Subject or third parties authorized according to the present law;

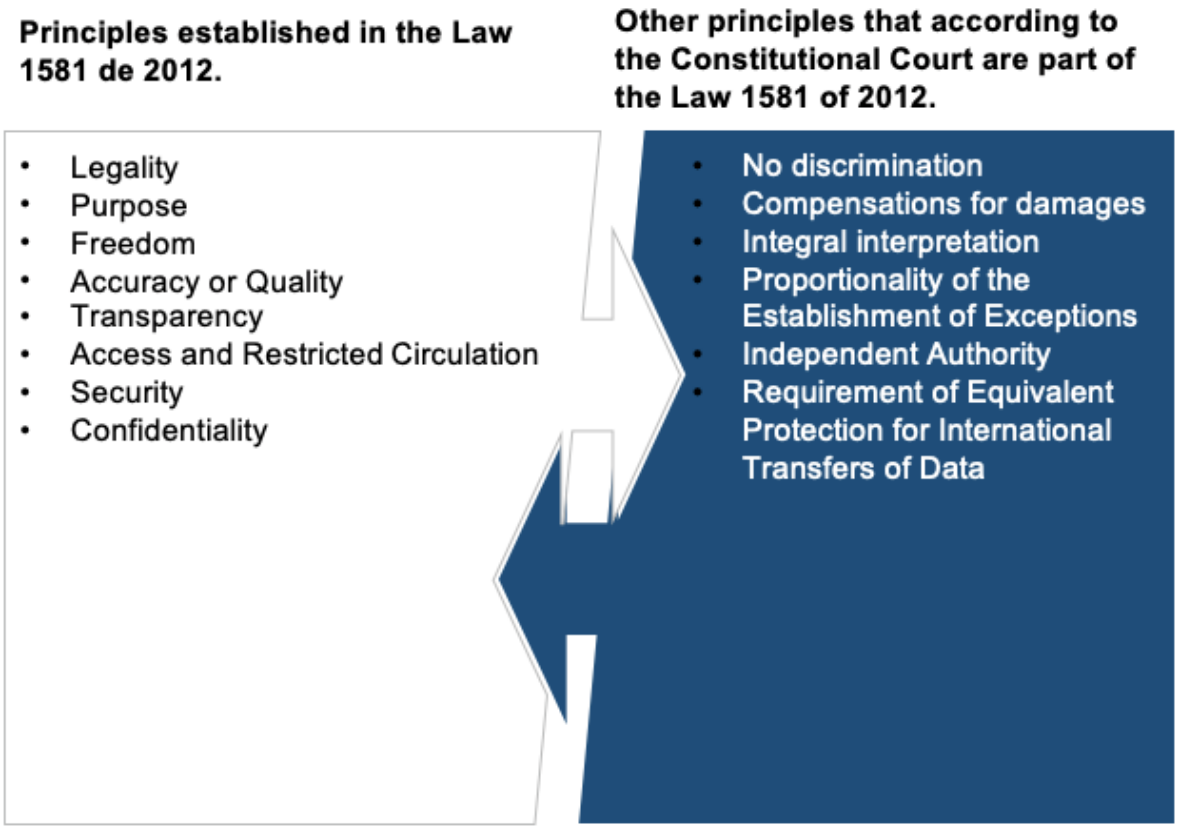
g) ***Safety Principle:*** *The information subject to processing by the Data Controller or Processor covered by this law, must be done with the technical, human, and administrative measures necessary to grant security to the databases, in order to avoid adulteration, loss, consultation, or unauthorized or fraudulent use or access; and*

h) ***Principle of Confidentiality:*** *All persons involved in the processing of personal data that do not have the nature of public, are obliged to ensure the confidentiality of the information, even after ending the processing, in which case the party can only supply or communicate personal data when it is directly involved with the development of authorized activities set forth in the present law and in the terms thereof".*

As the previous article shows, the principles are tools of mandatory compliance and reference in the development or regulation of Law 1581. In the same way, they must be taken into account for the interpretation and application of said Law. In any case, the principles must be applied in a harmonic and integral manner. In other words, the application and interpretation of the law must be done in conformity with the guidelines that emerge from the principles. It is important to note that in each case, all principles must be interpreted as a whole and not in an isolated way.

The Constitutional Court concluded that Article 4 "*defines the axiological context in which the informatic process must take place. According to this general framework, there are certain general parameters that must be respected in order to guarantee that the process of recollection, use and diffusion of personal data is constitutionally legitimate*"[11]. In addition, it concluded that other principles are part of Law 1581 although they are not specifically enshrined in it. The following graphic states all the principles to be met in the processing of personal data:

[11] Constitutional Court, Ruling C-748 of 2011, paragraph 2.6.3



Graph 1. Principles for the Processing of Personal Data - Colombia (See Appendix 3)

Jurisprudential and Regulatory Clarifications on the Principles

This section sets out the scope supported by both the Constitutional Court and the regulator regarding the following principles: (i) legality; (ii) purpose; (iii) freedom or authorization; (iv) accuracy or quality; (v) transparency; (vi) access and restricted circulation; (vii) safety; and (viii) confidentiality.

Other principles are highlighted as well. According to the Constitutional Court, although the following principles are not expressly incorporated into the law, nonetheless it is understood that they are included through an integrated and systematic interpretation of the Constitution and Law 1581:

(i) no discrimination in the processing of personal data;
(ii) compensation for damages caused when wrongfully processing personal data;
(iii) the integral interpretation of the rights involved in the collection, storage, access, circulation and use of the data;
(iv) proportionality in the establishment of exceptions;
(v) independent authority; and
(vi) requirement of equivalent protection for international transfers of data.

Observation 4: Data Subjects' Rights (DSR)

General Rights

The Political Constitution and article 8 of Law 1581 provide the Data Subjects with specific rights with respect to the protection and handling of their personal data, including, amongst others, the right:

(i) to authorize the processing of personal data;
(ii) to revoke the authorization;
(iii) of information regarding the personal data collected and its usage;
(iv) to update the information;
(v) to rectify the information;
(vi) to suppress or cancel the information; and
(vii) to file complaints before the Data Protection Authority.

The rights provided for in article 8 of Law 1581 of 2012 do not have any classification or qualification by law or by the SIC. Its scope and exceptions are those indicated in said article and its regulatory norms (Decree 1377 of 2013). Please refer to Appendix 3 for detailed information on DSR.

Exercise of Rights

In practice, citizens exercise their rights through a consultation or complaint with the Data Controller. If the rights of individuals are not respected, then they can file a complaint with the SIC, which initiates an administrative procedure to investigate and decide whether a contravention has occurred. Please see the following link for further information: https://www.sic.gov.co/tema/proteccion-de-datos-personales/decisiones-administrativas

Further examples of SIC decisions:

Resolución 76920 de 26 de noviembre de 2021 (Tour Vacation)

“People's rights must be respected and guaranteed in accordance with legal mandates and in a timely manner. People do not have to beg or insist that companies respect their human rights. Failure to respect the rights of the data subjects is reprehensible and inadmissible. In no way should it be tolerated as “normal” behaviour because it would be as much as “normalizing” illegality and the violation of human rights".

Resolución 72788 de 11 de noviembre de 2021 (Almacenes Éxito)

The rights of individuals must be respected and guaranteed in accordance with legal mandates and in a timely manner. Responding to a claim extemporaneously is reprehensible and inadmissible. In no way should it be tolerated as "normal" behaviour, because it would be as much as "normalizing" the illegality and violation of the rights of the Data subject. Almacenes Éxito S.A. processes Data of more than 29'957.549 citizens and Éxito Industrias S.A.S. of 941 citizens. The foregoing obliges them to be extremely diligent and to guarantee the real (informal) effectiveness of the rights of the Data subjects.

Resolución 63434 de 30 de septiembre de 2021 (SUMICORP LTDA)

The information that is reported to the financial information centers must be true and of quality -literal a) of article 4 of Law 1266 of 2008-. You cannot report information about which there is no certainty of its veracity because this not only affects the good name of people, but also misleads the users of the information and the public. You cannot play with

people's rights, but they must be guaranteed. Therefore, if the information to be reported is not verifiable, the *Source of Information* must refrain from making the report.

Resolución 56173 de 31 de agosto de 2021 (Colombia Telecomunicaciones)

Failure to respond in a respectful, complete and substantive manner, within the established legal term -15 business days-. A claim, query or request made by a Data subject to the *Source of Information*, the Operator or the User thereof, violates the fundamental right of Hábeas Data of said Data subject, since he is prevented from knowing how his personal information is being used. In the specific case, the Data subject had to request information four (4) times for Colombia Telecomunicaciones to provide a substantive response to his request. People's rights must be guaranteed in a timely and proper manner without the citizen having to beg or insist on companies.

Resolución 47748 del 29 de julio de 2021 (Giros y Finanzas Compañía de Financiamiento S.A.)

There is no legal obligation for individuals to receive data messages, calls or emails for the purposes of advertising, marketing or commercial prospecting. Those who are the object of these commercial conducts can request the suppression of their information at any time from the Data Controller. In this case, the company *Giros y Finanzas Compañía de Financiamiento S.A.* did not duly and timely comply with the legal duty to supress the information of the Data subject. It cannot become a business practice that the Data subject must insist several times so that the respect of their rights is guaranteed. Rights are to be respected and not to delay their fulfilment or deny their effectiveness in practice.

Resolución 27223 del 5 de mayo de 2021 (ALMACENES ÉXITO S.A)

It is imperative - not optional - that Controllers of the Processing of Personal Data duly and timely guarantee the constitutional and legal rights of Data subjects. Responding to a claim extemporaneously is reprehensible and inadmissible. In no way should it be tolerated as "normal" behaviour, because it would be as much as "normalizing" the illegality and violation of the rights of the Data subjects.

Resolución 23194 del 21 de abril de 2021 (COOPERATIVA BELÉN, AHORRO Y CRÉDITO)

Reporting an email address so that people can exercise their rights and not monitor its correct operation is a measure that is not effective or useful because it does not serve the purpose for which it was created, that is, to receive and respond to the requests of the Data subject. It should not be forgotten that the regulation on Data Processing seeks to guarantee a real and effective protection of people's rights and not a formal or symbolic protection.

Resolución 18314 del 31 de marzo de 2021 (BANCO COLPATRIA MULTIBANCA COLPATRIA S.A.)

The Data subjects have the right to request the exclusion or suppression of the information that resides in the Databases of the Controller or Processor of the processing, provided that there is no legal or contractual duty that prevents it -literal a) of the article 17 of Statutory Law 1581 of 2012-. The Data subject does not have to insist that their rights are guaranteed. On the contrary, these must be safeguarded without delay by the Controller or Processor of Processing.

Resolución 2884 del 29 de enero de 2021 (ORIGINAR SOLUCIONES S.A.S.)

Failure to respond or to respond timely to the requests presented by the Data subjects violates their fundamental rights of *habeas data* and petition, preventing them from knowing, updating, or rectifying the information that they have in a database or file.

Resolución 667 del 08 de enero de 2021 (COLOMBIA MÓVIL S.A. E.S.P.)

The Data subject is not obliged to insist that their information be suppressed from a database -literal e) Article 8 Statutory Law 1581 of 2012-, especially when said Data subject does not have a contractual relationship with the Controller. The Data subject should not beg for their rights to be respected. It is imperative - not optional - to respect and guarantee the constitutional and legal rights of people.

In practice individuals can go to the SIC to exercise their data protection rights, which are established in the regulations. For that, data subjects must firstly exercise their rights before the data controller or the data processor. If the data subjects' petition is not solved, data subjects will be able to submit a claim before the SIC.

It is not mandatory to have legal representation for a data subject to exercise his/her privacy rights: a data subject can file a claim before the SIC without counsel. Additionally, there are no costs involved in the proceeding and it is possible to file appeals against the decisions issued by the authority, also without any costs.

It is therefore possible for individuals to exercise rights over their personal data before the SIC as the process is very transparent and straightforward in practice. Moreover, there are unlikely to be potential barriers as, besides being a process free of costs for the parties involved, the SIC tends to be very protectionist of the data subjects' rights in its decisions.

Further information is provided on additional remedies and redress in Observation 7 below.

Observation 5: International Data Transfers

Regarding international transfers, the following applies:

> "*Without prejudice to the transfers of personal data being made to countries that have an adequate level of protection, those Controllers, by virtue of the principle of Accountability, must be able to demonstrate that they have implemented appropriate and effective measures to guarantee the adequate processing of the personal data that they transfer to another country and to grant security to the records at the time of making the transfer*".

At the end of 2019, the SIC published a complimentary document that further developed guidance regarding the principle of Accountability specifically in the international transfers of Personal Data. This guidance was revised and updated in 2021 to improve its content and to account for recent international guidance such as, among others, the Implementing Decision (EU) 2021/914 regarding the standard contractual clauses for the transfer of personal data to third countries.

The specific recommendations embedded in the international transfers guidance are the following:

- Carry out Privacy Impact Assessments (PIA´s) before transferring the data to another country.
- Incorporate privacy, ethics, and security by design and by default.
- Verify that you are empowered to transfer or transmit personal data to another country.
- Establish how the accountability measures to transfer personal data will be demonstrable.
- Ensure compliance with the purposes to be achieved with the accountability measures.
- Consider the subsequent transfers of personal data.
- Replicate proactive measures for the Processing of Personal Data to international transfers of said information.
- Articulate the accountability tools in a contract adjusted to the particularities of each transfer.
- Increase trust and transparency with your clients and third-party data subjects.

Observation 6: Security of Processing and Breach Reporting:

Security

Data controllers are required by law to guarantee that the information under their control is kept under strict security measures. Additionally, they must ensure that such information will not be manipulated or modified without the consent of the data subject. In light of this, they shall construe an information security policy that prevents, amongst others, unauthorized access and the damage or loss of information. Refer to the "Safety Principle" in Observation 3 and to Appendix 3 for more information on the required technical and administrative measures.

Breach notification

There is no obligation in Colombia to report a personal data breach to affected data subjects. However, according to the Incident Management Guidelines published by SIC, data controllers should:

- inform data subjects about the security incident and its possible consequences;
- provide tools for data subjects to mitigate potential or caused damage (e.g., to change username and password, to monitor the billing statement, etc.); and
- adopt a general framework with roles, responsibilities and procedures to handle security incidents.

Notification to the data subject is deemed by the SIC as an advisable practice that will be seen in a favourable light in the event that any investigations are initiated pursuant to a data breach report.

Under Sections 17 and section 18. of Law 1581, both the data controller and the data processor must notify the authority (SIC) in case of a breach of security, security risk, or a risk for data administration. Notification to the SIC must be made within 15 business days from the time the harm was detected.

Law 1581 (articles 17 and 18) requires that any security breach involving personal data must be reported to the SIC, including those related to cyber security. Additionally, there are sector regulations related to the reporting of financial information security breaches.

The SIC has generated 430 security orders regarding cases where citizens file a complaint and 1,417 ex officio that the SIC initiates from the information system it has in the National Registry of Databases. Most of the orders are the product of the ex officio work carried out by the SIC. The proportion is 77/23 (77% are ex officio orders and 23% are orders originating from citizen complaints). Please see:

- Circular 052 of 2007 of the Financial Superintendence.
- Circular 007 of 2018 of the Financial Superintendence.
- Circular 033 of 2020 of the Financial Superintendence.

Also, see Circular 5569 of 2018 from the COMMUNICATIONS REGULATION COMMISSION - CRC-, related to incidents in the Telecommunications sector[12].

Security breach management guidelines can be found at:

https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia_gestion_incidentes_dic21_2020.pdf

All other guidelines are published at:

https://www.sic.gov.co/centro-de-publicaciones?field_global_topic_tid=7037&field_anos_p_value=All

The SIC requests the following information from those who report security breaches:

- Database(s) affected:

- If the database is registered in the National Registry of Databases or not.
- If it is not registered and the subject is obliged, they must register all the information in the database.
- Type of information affected in the incident.

- Record the Incident:

Type of incident

Year / Number of Incidents

2018: 171

2019: 149

2020: 133

2021: 195

Total: 670

During 2021, an average of 16.25 monthly incidents were reported.

[12] Web page: https://www.crcom.gov.co/es

Observation 7: Accountability, Redress and Enforcement

Accountability

The principle of Accountability requires the Data Processor and Controller to implement appropriate, effective, and verifiable measures to prove the correct compliance with data protection regulations. Said measures must be permanently revised and evaluated in order to measure their level of efficiency with regards to the compliance and protection of personal data. A Privacy Management Program (PMP) is an operative mechanism that can be implemented to guarantee the correct processing of personal data.

This principle requires less rhetoric and more actions with regards to the compliance of the Data Controller and Processor's duties. It requires them to implement concrete actions that guarantee the rightful processing of personal data. Said principle is developed in articles 26 and 27 of Decree 1377 of 2013.

Organizations must document and describe the processes used to recollect data in accordance with the purpose of the processing. Likewise, the Processor and Controller must be in capacity to demonstrate the appropriate implementation of security measures (human, technological, organizational, or any other type of measures). In other words, the organizations must prove that what they are doing works and is adjusted to the legal requirements.

There are various factors that must be considered to establish the pertinency and effectiveness of a measure implemented by an organization. First, the nature of the Controller must be determined (whether it is a private or public organization). Next, the size of the company and thus the impact the processing of data will have on society, is also a key point, since the size of the organization will determine the administrative structure of the company, especially with regards to queries and claims. The type of processing (automatic or manual, storage of data, usage, or update, etc.) is relevant to determine the mechanisms that must be adopted by the organization. Finally, the nature of the data (whether there is sensitive information or not) is also relevant. This all goes hand in hand with another requirement imposed by the law: determine the risk and type of risk in order to mitigate it.

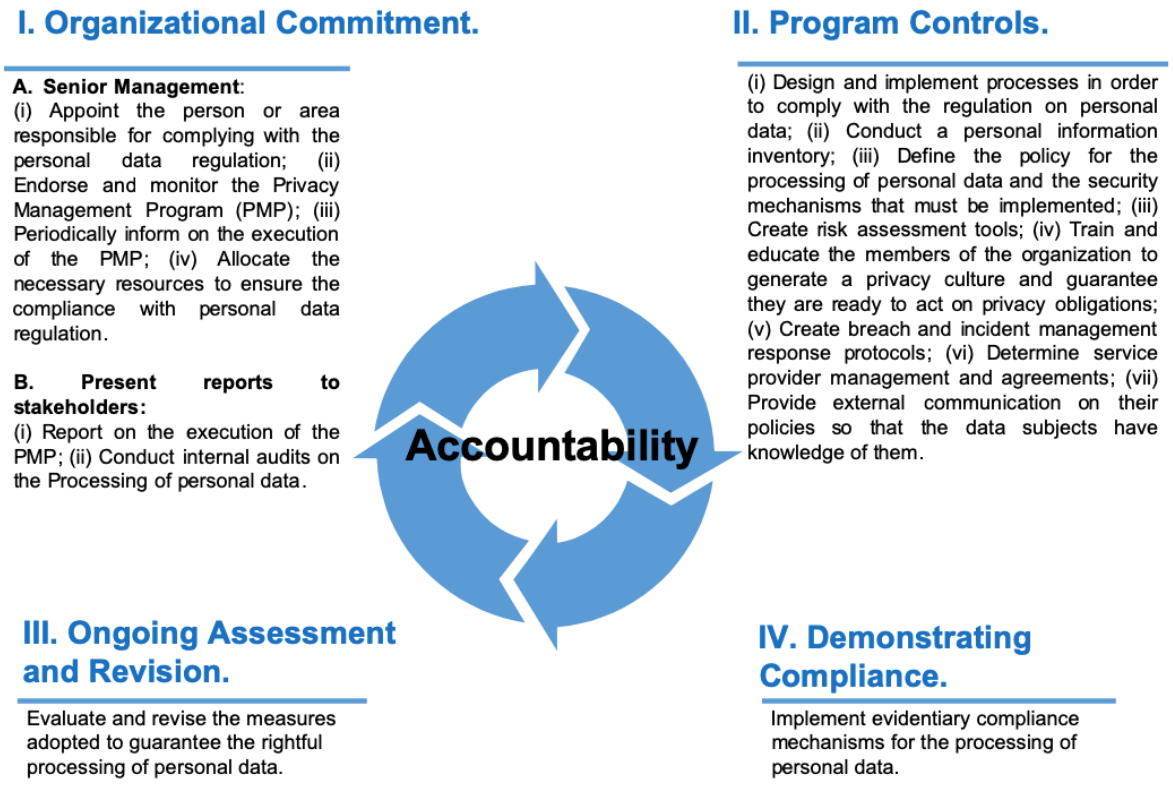
Additionally, in relevant guidelines, the SIC has referred and recommended strategies of Accountability to be implemented in relation to the Processing of Personal Data. For example, this was expressly included in the following guidelines:

- Guide on data processing in the horizontal property (pages 19-20)
- Guide on data processing for e-commerce purposes (Pages 4-6)
- Data processing guidelines for marketing and advertising purposes (Pages 8-10)

The 2021 updated guidance is one of the different actions that the Colombian authority has carried out so that the adequate processing of personal data is guaranteed in practice and human rights are respected.

The Colombian Guide on Accountability

Chapter III of Decree 1377 of 2013 (incorporated in Decree 1074 of 2015) regulates some aspects related to the Principle of Accountability and the SIC. Seeking to provide guidance on comprehensive data management programs the authority issued on the 28 of May of 2015 the "*Guide for the Implementation of the Principle of Accountability*" which, for its part, has the purpose of helping those obliged by Law 1581 to comply with the following fronts:



Graph 2. Structure and Principles from the "*Guide for the Implementation of the Principle of Accountability"* by SIC (2015). (See Appendix 3)

Law 1581 created the National Register of Data Bases ("**NRDB**"). Databases that store personal data and whose automated or manual processing is carried out by a natural or legal person, whether public or private in nature, in the Colombian territory or abroad, shall be registered in the NRDB. Database registration is also required if Colombian law applies to the data controller or data processor under an International Law or Treaty. Registration is mandatory for data controllers that are either of the following:

- Companies or nonprofit entities that have total assets valued above 100,000 Tax Value Units (TVU), meaning COP 3.800.400.000 million (USD 950.100)
- Legal persons of public nature

Decree 866 states that each data controller shall register each one of its databases, independently and must distinguish between manual and automatized databases.

Law 527 of 1999 regulates e-commerce and electronic marketing, but there is no specific regulation regarding data privacy on electronic marketing. In any case, the data subject's consent is required for marketing, whether electronic or not and the processing of any personal data for this purpose shall be in accordance with Law 1581.

In Colombia, Decree 1377 establishes the obligation for data controllers to develop a privacy policy that governs personal data processing and ensures regulatory compliance.

There is no requirement to appoint a formal data protection officer in Colombia. However, companies are required to appoint either a specific person, or a designated group within the company to be in charge of personal data matters, specifically the handling of data subject rights requests.

Redress through the SIC

As noted above, in practice, individuals can go to the SIC to exercise their data protection rights, which are established in the regulations. If the data subjects' petition is not resolved between him and the controller or processor, data subjects will be able to submit a claim before the SIC. This claim will initiate an administrative proceeding that can eventually end in a fine imposed on the data processor or the data controller. In this sense, it is not possible to get compensation through a claim submitted before the SIC for data protection rights.

It is not mandatory to have legal representation for a data subject to exercise his/her privacy rights: a data subject can file a claim before the SIC without counsel. Additionally, there are no costs involved in the proceeding and it is possible to file appeals against the decisions issued by the authority, also without any costs. Foreign lawyers must be admitted to practice law in Colombia in order to represent clients. Foreign citizens would be required to hire local representation, or foreign representation admitted to practice in Colombia.

Additionally, the Criminal Procedure Code (Law 906 of 2004) in Article 269F states that:

> *Violation of personal data. Whoever, without being empowered to do so, for their own benefit or that of a third party, obtains, compiles, subtracts, offers, sells, exchanges, sends, buys, intercepts, discloses, modifies, or uses personal codes, personal data contained in files, archives, databases, or similar means, may incur in a prison penalty of forty-eight (48) to ninety-six (96) months and a fine of 100 to 1000 legal monthly minimum wages in force.*[13]

Judicial Redress

Every citizen is entitled to pursue protection before any Colombian judge, via constitutional action. Any judge may order a private or public entity to modify, rectify, secure or delete personal data if it is kept under conditions that violate constitutional rights. Constitutional actions can take up

to ten days to be resolved and an order issued and failure to comply may result in imprisonment of the legal representative of the violating entity.

The Criminal Code of Colombia sets out in section 269F that anyone who, without authorization, seeking personal or third-party gain, obtains, compiles, subtracts, offers, sells, interchanges, sends, purchases, intercepts, divulges, modifies or employs personal codes or data contained in databases or similar platforms, will be punishable by 48 to 96 months of prison, and a fine of approximately USD 26,700 to USD 267,000.

Enforcement

The SIC can impose:

- fines of up to 2,000 minimum statutory monthly wages (i.e., COP 1.8 billion (approx. €398,000));
- an order to temporarily close the data controller's establishment (for up to six months), or to permanently close the establishment; or
- a suspension of activities related to the processing of personal data for up to six months in the event of material breaches of the obligations of data controllers, ending any activities that are related to the processing or decommissioning the activities related to the processing.

Refer to Observation 4 and Appendix 1 for more information on SIC decisions and enforcement action.

Observation 8: Additional content principles for specific types of processing (including sharing for the purposes of law enforcement)

Public entities must comply with the Constitution, Law 1581 and Law 1712 of 2014. Given the above, any public authority that wishes to Process personal data can do so as long as it bears in mind:

- Its legal and constitutional powers.
- The nature, scope, context and purposes of data processing, as well as the risks of varying likelihood and severity that the processing may imply for citizens' rights and freedoms.
- Law 1266 (Financial Habeas Data), Law 1581 (General Regime for the Protection of Personal Data), and Law 1712 of 2014.
- The guiding principles in the protection of personal data, in particular, the principles of purpose limitation, data minimization, integrity and confidentiality and lawfulness, avoiding possible mass access to personal data.
- The following constitutional Rulings: C-1011 of 2008 and C-748 of 2011, respectively.

For the processing of personal data that a public entity has access to or possesses, the following aspects must be considered at a minimum:

(I) The necessity and relevance of the data collected by the public entity to fulfil its constitutional and legal functions.

(II) A risk management system associated with the processing of reserved personal data - sensitive, private, semi-private- by public authorities.

Bringing a claim against public authorities

Law 1952 of 2019 is one of the most recent laws enacted by the Congress of Colombia regarding the materialization of article 92. This law regulates the General Disciplinary Code, whose purpose is to establish the mechanism by which the State regulates the behaviour of its officers. According to article 26 of Law 1952, any of the conduct set out in the said law that led to a breach of duties, exceeding the limits of his/her functions, without being covered by any of the grounds for exclusion of liability provided for in the same law, constitutes a disciplinary offence. One of the most serious misconducts involves infringing fundamental rights, such as the right to privacy.

Notwithstanding the above, in Colombia there are different procedures and mechanisms that could be initiated before each entity to submit complaints or judicial claims, to comply with what article 92 has established. Under Articles 66 and 67 of the Code of Criminal Procedure, citizens may contact the Attorney General's Office to initiate administrative investigations against public officers for endangering fundamental rights. However, article 8 of Law 1581 has also set the possibility of submitting a complaint before the SIC, in order to analyse whether the data protection regime was infringed. Individuals may submit complaints without submitting evidence about being surveilled.

The Constitution also contains the rights to a fair trial, due process and judicial guarantees (Article 29) and the right of redress against public authorities (Article 92). Article 92 states:

"*Any individual or corporation may request from the competent authority the application of criminal or disciplinary sanctions derived from the conduct of public authorities.*"

Therefore, people have judicial mechanisms such as filing a criminal claim or a constitutional claim against a public officer or an authority but also they have the option of filing a complaint against the authority in charge of sanctioning the officer, which is the Attorney General's Office (Procuraduría General de la Nación) or before the entity to which the officer is linked.

Intelligence and Counterintelligence Law (Law 1621 of 2013)

Law 1621 of 2013 regulates national security and intelligence agencies interception of data. This law regulates intelligence and counterintelligence activities, including "*monitoring the electromagnetic spectrum*".

Law 1621 contains purposes for which the powers under the law can be used (Article 4). These are:

- To ensure the achievement of the essential purposes of the State, the validity of the democratic regime, territorial integrity, sovereignty, security and defence of the Nation.
- To protect the democratic institutions of the Republic, as well as the rights of people residing in Colombia and of Colombian citizens at all times and in any place - in particular the rights to life and personal integrity - against threats such as terrorism, crime. organized crime, drug trafficking, kidnapping, trafficking in arms, ammunition, explosives and other related materials, money laundering, and other similar threats.

- To protect the natural resources and economic interests of the Nation.

In addition, the law also mandates that:

- The intelligence function will be limited by the principle of legal reserve that guarantees the protection of the rights to honour, good name, personal and family privacy, and due process.
- No case will intelligence and counterintelligence information be collected, processed or disseminated for reasons of gender, race, national or family origin, language, religion, political or philosophical opinion, membership of a union, social or human rights organization, or for promote the interests of any political party or movement or affect the rights and guarantees of opposition political parties.

Furthermore, those who authorise and those who carry out intelligence and counterintelligence activities, in addition to verifying the relationship between the activity and the purposes set out in article 4 of this law, have to strictly evaluate and observe the following principles at all times:

- Principle of necessity. Intelligence and counterintelligence activity must be necessary to achieve the desired constitutional ends; In other words, it may be used as long as there are no other less harmful activities that allow such ends to be achieved.
- Principle of suitability. The intelligence and counterintelligence activity must make use of means that are adequate to achieve the purposes defined in article 4; in other words, the appropriate means must be used for the fulfilment of such ends and not others.
- Proportionality principle. The intelligence and counterintelligence activity must be proportional to the aims sought and its benefits must exceed the restrictions imposed on other constitutional principles and values. In particular, the means and methods used must not be disproportionate to the ends to be achieved.

The law permits the intelligence agencies to intercept private mobile or fixed telephone conversations, as well as private data communications. These must be subject to the limitations set out in Article 15 of the Constitution, as well as the Code of Criminal Procedure. Such interception can only be carried out in the framework of judicial procedures.

There is a distinction under Colombian law in the legal meaning and protections conferred on ‘interception’ vs ‘monitoring’ activities under the Intelligence Law (Law 1621).

- Interception of data under Article 17 of Law 1621 is subject to protections and oversight requirements under Article 15 (right to privacy) of the Constitution and the Criminal Procedure Code
- Monitoring under Law 1621 is treated differently. Communications being monitored by the government does not constitute the interception of communications and is not afforded the same protections and oversight. Under article [17] the information collected during monitoring, which does not serve to fulfil Article 4, must be destroyed and may not be stored in the databases of intelligence and counterintelligence.

<u>Authorisation under Law 1621</u>

The Law sets out that intelligence and counterintelligence activities must be authorized by the [order of operations], taking into account the purposes set out in Article 4. The level of

authorisation needed for each activity will increase, taking into account its nature, possible impact and the impact on fundamental rights. Each agency will define for themselves who the head or deputy head of the unit, section or agency in charge of authorization is, taking into account the Constitution and the Law.

The authorisation of interception must be taken into account when such data that is collected is presented for use in a criminal procedure, and evidence will only be admissible where appropriate warrants and protections must have been adhered to. The reasoning is therefore that requirements on the use of intercepted data in judicial proceedings provides the safeguards for the use of such data.

There are no specific requirements in Law 1621 that need to be fulfilled before data can be *monitored* (rather than *intercepted*).

Any official that carries out intelligence and counterintelligence activities that violate their duties or obligations will be guilty of misconduct. “Due obedience” cannot be used as a defence when the misconduct involves a violation of human rights or an infringement of International Humanitarian Law and International Human Rights Law.

Public Prosecutors

Article 235 of the Colombian Criminal Procedure Code (Law 906 of 2004 as amended by article 52 of Law 1453 of 2011) permits public prosecutors (i.e., public officials of the Attorney-General’s office) to order the interception of any form of private communication over any telecommunications network to search for evidence or locate a person in relation to any crime that is under investigation.

Interception orders from a public prosecutor must be sent to the Telecommunications, Network and Service Providers (the bodies responsible for the operation of telecommunications networks and services, as defined in resolution 3067 of 2011 of the Colombian Communications Regulation Commission, “**TNSPs**“) in writing. The confidentiality of all intercepted communications must be ensured throughout the process.

Observation 9: Existence of international commitments and conventions binding on Colombia or its membership of any multilateral or regional organisations

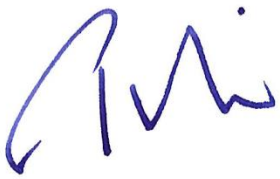
While Colombia has not signed Council of Europe's Convention 108+, the SIC is a Member of the Global Privacy Assembly.

Conclusion

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 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.

It is recommended that this decision is reviewed and where appropriate reconfirmed on an annual basis. The Commissioner has the right to repeal, amend or suspend its adequacy decision regarding Colombia at any time. This decision shall be reviewed annually.

Dated: 6 October 2022



Jacques Visser

DIFC Commissioner of Data Protection

Appendix 1: Enforcement Action

Data Protection Enforcement

The SIC has undertaken the enforcement action in Colombia in the form of investigations, ex-officio or upon request of a party, as well as thematic reviews for supervision purposes. Enforcement decisions have been issued by the SIC since 2014 and 87 such resolutions were issued in 2021. Entities subject to these decisions include firms incorporated in Colombia, as well as international firms, including Big Tech, with a presence in Colombia. Amongst others, the enforcement decisions include:

- Imposing fines
- Issuing warnings or admonishments or recommendations to Data Controllers, including warnings of closing webpages for violation of data protection laws
- Identifying contraventions of the Colombian DP Law and bringing such claims to the attention of the Colombian Courts
- Issuing directions to Controllers or Processors
- Ordering security measures to be adopted
- Conducting investigations

DIFC

Appendix 2: Acknowledgement of Requirement to Comply with Article 28 of the DIFC DP Law 2020

Article 28 of the DIFC DP Law 2020 states the following:

Data sharing

(1) Subject to any other obligations under this Law and, in particular, a Controller's or Processor's obligations under Part 2 regarding accountability, transparency and compliance with general data protection principles or Part 4 regarding transfers out of the DIFC, where a Controller or Processor receives a request from any public authority over the person or any part of its Group ("a Requesting Authority") for the disclosure and transfer of any Personal Data, it should:

> (a) exercise reasonable caution and diligence to determine the validity and proportionality of the request, including to ensure that any disclosure of Personal Data in such circumstances is made solely for the purpose of meeting the objectives identified in the request from the Requesting Authority;
>
> (b) assess the impact of the proposed transfer in light of the potential risks to the rights of any affected Data Subject and, where appropriate, implement measures to minimise such risks, including by redacting or minimising the Personal Data transferred to the extent possible or utilising appropriate technical or other measures to safeguard the transfer; and
>
> (c) where reasonably practicable, obtain appropriate written and binding assurances from the Requesting Authority that it will respect the rights of Data Subjects and comply with the general data protection principles set out in Part 2 in relation to the Processing of Personal Data by the Requesting Authority.

(2) A Controller or, as applicable, its Processor(s) or any Sub-processor(s), having provided (where possible under Applicable Law) reasonable notice to the Controller, may disclose or transfer Personal Data to the Requesting Authority where it has taken reasonable steps to satisfy itself that:

> (a) a request by a Requesting Authority referred to in Article 28(1) is valid and proportionate; and
>
> (b) the Requesting Authority will respect the rights of Data Subjects in the Processing of any Personal Data transferred to it by the Controller pursuant to a request under Article 28(1).

(3) A Controller or Processor may consult with the Commissioner in relation to any matter under this Article 28.

Colombia SIC acknowledges that DIFC entities are required to substantially comply with Article 28 of the DIFC DP Law 2020.

Appendix 3: Colombia's System for Personal Data Protection

The document compiled by Superintendence of Industry and Commerce and the Deputy Superintendence for Personal Data Protection of the Republic of Colombia, titled "Colombia's System for Personal Data Protection" may be provided at the discretion of SIC.