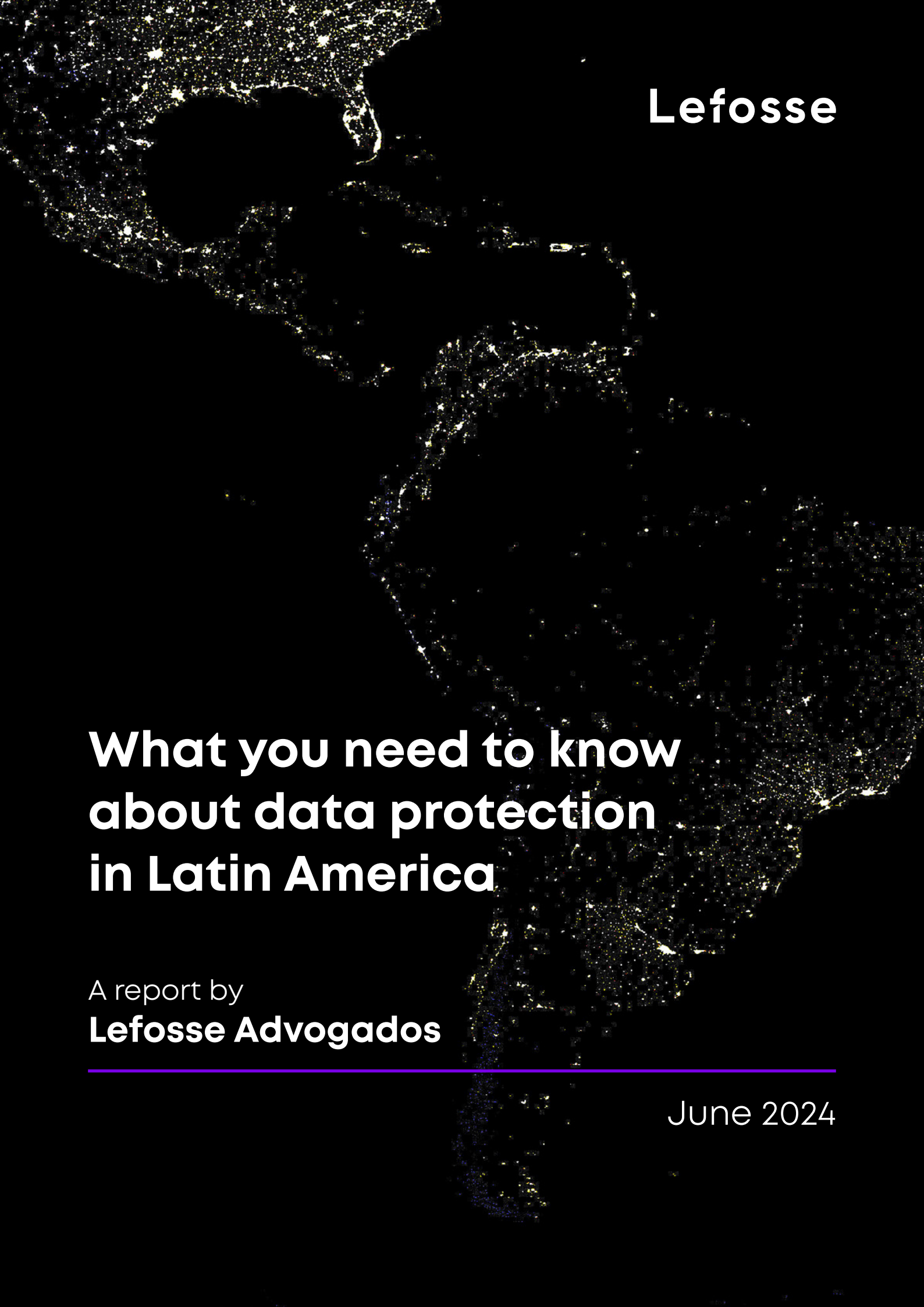


Lefosse

What you need to know about data protection in Latin America

A report by
Lefosse Advogados

June 2024

Coordination

Lefosse Advogados | Paulo Lilla and Carla Segala

Authors

Argentina
Marval O'Farrel Mairal | Diego Fernández

Bolivia
Aguilar Castillo Love | José Carlos Bernal

Brazil
Lefosse Advogados | Paulo Lilla and Carla Segala

Chile
Barros & Errázuriz | Andrés Rodríguez

Colombia
Brigard Urrutia | Juan Nicolás Laverde and Sergio Michelsen

Ecuador
Pérez Bustamonte & Ponce | Francisco Pérez Gangotena

Mexico
Galicia Abogados | Manuel Galicia R., Irma Ross N. and Jorge Armendáriz A.

Paraguay
Ferrere | Montserrat Puente

Peru
Rodrigo, Elias & Medrano Abogados | Francisco Baldeón

Uruguay
Ferrere | Martin Pesce

Contents

Preface

The data protection landscape in Latin America is characterized by significant regulatory complexity that requires proper treatment, in-depth study, application, supplementation, and integration of legal rules, especially for companies operating in multiple jurisdictions (*a common scenario in an increasingly digital economy*). In this regard, a constant challenge for lawyers who work in this legal field is to be able to handle various legislations and to comply with the specific obligations of each locality.

Beyond the above-described aspects, the practice and application of law in Latin America demands an analysis and comprehension of the region's economic, political, social, and cultural elements. This region is characterized by both unifying and diverging forces, adding to its complexity. While the various Latin American legal systems share a common foundation, the development of national legal frameworks has been infused with distinctive characteristics. In a sector that is moving towards increasing uniformity from a global perspective, these characteristics must be articulated and harmonized to streamline business operations and enhance the effective protection of personal data subjects.

Aware of this scenario, Lefosse Advogados, along with its partners in Latin America (Marval O'Farrell Mairal, Aguilar Castillo Love, Barros & Errázuriz, Brigard Urrutia, Perez Bustamante & Ponce, Galicia Abogados, and Ferrere, Rodrigo Elias & Medrano Abogados), initiated the commendable project of creating an informative guide titled 'What You Need to Know About Data Protection in Latin America?'. This valuable and thorough guide provides an overview of the Personal Data Protection laws in Argentina, Bolivia, Brazil, Chile, Colombia, Ecuador, Mexico, Paraguay, Peru, and Uruguay.

In this guide, you will find a series of questions and answers pertaining to the data protection legislation (*lato sensu*) of each country. This includes aspects such as territorial and material scope, the definition of personal data and its categories, references to regulatory authorities, and the obligations and requirements for compliance (principles, legal bases for processing, database registration, data processing agreements, confidentiality, and information security, among other topics). Additionally, the guide addresses the necessity of appointing a Data Protection Officer, the rights of personal data subjects, the requirements for information security, the mandatory reporting in case of a personal data-related information security incident, the procedures for international personal data transfer, and the penalties and liabilities for data protection violations.

With this information, it will be possible to gain an initial understanding of the adjustments necessary to operate within each jurisdiction and/or to negotiate contracts with

parties established in any of the countries under review. For in-house attorneys, the guide is invaluable. It allows for a swift compliance check to ensure that a company's operations meet the minimum standards required in each country, or to identify which aspects need to be considered and questioned during an expansion, merger, or acquisition process.

With appropriate regulatory knowledge and advisory, conducting personal data processing operations in Latin America is set to generate a differential in the market. Therefore, it is possible, advisable, and necessary to overcome local challenges and establish a corporate framework that meets legislative requirements and integrates good international practices. Progressing in this direction is a duty for the economic players in the region, particularly as Europe continues to reinforce its leadership in this area and the United States has started its legislative journey. As of 2024, various Latin American countries are reviewing their laws to align with new demands, while others are crafting their specific regulations. Consequently, the document in question is capable of mirroring the regional reality and offering the fundamental elements to initiate the deepening of discussions based on specific needs.

Congratulations to Lefosse Advogados and its partners in Latin America for the initiative, effort, and dedication in the preparation and dissemination of this document. Your contribution is invaluable and timely for those who work daily in the region.

PhD. Humberto De Jesús Ortiz Rodríguez

Legal & Privacy Senior Manager for Latin America and DPO at Whirlpool Corporation

Attorney / PhD. In Political Science / Legal & Business Counselor / Compliance & Data Protection International Executive

Introduction

The world is once again witnessing a rapid digital transformation driven by innovation and emerging new technologies that rely on processing massive amounts of data, including personal data. A prime example is the increasingly advanced and sophisticated Artificial Intelligence systems, sparking a significant digital economy revolution.

In response to the evolving digital landscape, jurisdictions worldwide are enacting or revising privacy and data protection laws. These measures aim to safeguard fundamental rights and empower individuals to manage their personal data processing in an increasingly digital and data-centric economy. Many of these regulations stem from the so-called "Brussels Effect," heavily influenced by the European Union's General Data Protection Regulation (GDPR), which has become the global benchmark for data protection legislation.

In Latin America, the approach to personal data protection laws and regulations is not uniform, as each country implements its own rules without regional harmonization or standardization. Countries such as Argentina and Chile have longstanding data protection laws, whereas others have more recently enacted legislation. Some of these newer laws, including Brazil's General Data Protection Law (LGPD), draw inspiration from the GDPR model, once more reflecting its influence on global data protection frameworks.

The complex network of different laws and regulations across Latin American countries increases the complexity and challenges for lawyers and Data Protection Officers of multinational corporations with regional operations. These variations also raise the transaction costs for international businesses, as significant transactions, such as mergers, acquisitions, and global joint ventures, must rely upon different criteria for managing personal data, including criteria for international transfers of personal data.

This guide, which received contributions from various Latin American law firms with expertise in data protection, seeks to provide an extensive overview of data protection laws and regulations in Latin America. It is designed to simplify the topic for lawyers and data protection professionals from globally operating organizations, supporting their comprehension and practice.

In this inaugural edition, we have selected the following countries to include in the guide: Argentina, Bolivia, Brazil, Chile, Colombia, Ecuador, Mexico, Paraguay, Peru, and Uruguay. We hope that the following issues incorporate additional jurisdictions, enriching the document and broadening its reach considering the vast diversity that features Latin America.

Executive Summary

Jurisdiction	Does the currently local legislation							
	Have extraterritorial effects?	**Establish a supervisory authority?**	**Require the appointment of a DPO?**	**Provide legal basis for processing personal data?**	**Provide data subject's rights?**	**Require the notification of data breaches?**	**Provide security requirements for personal data processing?**	**Provide rules for international transfers of personal data?**
Argentina*	Yes	Yes	No	Yes. Consent is the main legal basis.	Yes	No	Yes	Yes. Requires appropriate level of protection or adoption of safeguards.
Bolivia**	No	No	No	Yes. Consent is the main legal basis.	Yes	No	No, but there are industry-specific regulations or security standards.	No
Brazil	Yes	Yes	Yes	Yes	Yes	Yes. Data subjects and authority.	Yes, as a general obligation. No regulations providing security standards have been published.	Yes. Requires appropriate level of protection or adoption of safeguards.
Chile*	Yes	No	No. Except for specific sectorial regulations.	Yes	Yes	No. Except for specific sectorial regulations.	Yes, as a general obligation.	No. Except for specific sectorial regulations.
Colombia	Yes	No	Yes	Yes. Consent is the main legal basis.	Yes	Yes. Authority.	Yes, as a general obligation.	Yes
Ecuador	Yes	Yes. In the process of being created.	Yes, in specific situations.	Yes	Yes	Yes. Data subjects and authority.	Yes	Yes. Requires appropriate level of protection or adoption of safeguards.
Mexico	Yes	Yes	Yes	Yes. Consent is the main legal basis.	Yes	Yes. Data subjects.	Yes	Yes
Paraguay***	Yes	Yes	No	Yes. Consent is the main legal basis.	Yes	Yes. Not yet regulated.	Yes, as a general obligation.	Yes, but further regulation is required to clarify the criteria.
Peru	Yes	Yes	No	Yes. Consent is the main legal basis.	Yes	Yes. Data subjects.	Yes	Yes
Uruguay	Yes	Yes	Yes, for entities that fulfill some requirements.	Yes. Consent is the main legal basis.	Yes	Yes. Data subjects and authority.	Yes	Yes

* There is a Bill of Law that may modify some of the provisions.

** There is no comprehensive law regulating personal data protection, but there are provisions on the matter in some laws and regulations.

*** Answers based on Paraguayan Law 6534/2020, related solely to personal credit data/financial information.

Argentina

Marval O'Farrel Mairal

Diego Fernández*

Contact:

* dfer@marval.com

Lefosse

1 Legislation: local laws applicable to data protection

In Argentina, the protection of personal data is governed by Section 43 of the Argentine National Constitution, the Data Protection Law No. 25,326 ("**Argentine Data Protection Law**"), its Regulatory Decree No. 1558/2001 ("**Argentine Regulatory Decree**"), the Convention 108 for the Protection of Individuals with respect to Automatic Processing of Personal Data (approved by Law No. 27,483) and its Amending Protocol (approved by Argentine Law No. 27,699), also known as "**Convention 108+**" (collectively, the "**Argentine Data Protection Regime**").

The Argentine Data Protection Law is currently under review. A bill, drafted by the Argentine Data Protection Authority (as defined below), was filed with Congress in June 2023 by the Executive Branch (the "**Argentine Bill of Law on Data Protection**"). This bill is aligned in many aspects with GDPR.

2 Jurisdiction: territorial applicability

The Argentine Data Protection Law does not provide a clear distinction as to whether it is applicable exclusively to data controllers located in Argentina or if it also applies to data controllers that, despite being located abroad, process personal data from data subjects protected by the Argentine Data Protection Law.

However, the Argentine Data Protection Authority has confirmed that both the Argentine Data Protection Law and Convention 108+ apply to the processing of personal data by foreign data controllers and/or processors of personal data related to subjects protected under the Data Protection Law.

In any event, the Argentine Bill of Law on Data Protection regulates the extraterritorial application of the Argentine Data Protection Law.

3 Scope: information protected under data protection legislation

The Argentine Data Protection Law protects personal data, which refers to any information related to identified or identifiable individuals or legal entities that have a legal domicile, office, or branch in Argentina.

However, the Argentine Bill of Law on Data Protection aims to eliminate legal entities as personal data subjects.

4 Definition of sensitive or special category data

The Argentine Data Protection Law defines "sensitive data" as any personal data revealing racial or ethnic origin, political affiliation, religious, moral, or philosophical convictions, union activity, or information related to health or sexual orientation.

Additionally, biometric data may be considered sensitive data if it could lead to potential discrimination against the data subject. Genetic data is also deemed sensitive data if it unequivocally identifies an individual, reveals information about the individual's health or physiology, or when its processing could result in potential discrimination against the data subject.

When processing sensitive data, the data controller should:

(i) obtain the data subjects' consent to do so;

(ii) adopt technical and organizational measures to ensure the security and confidentiality of the data;

(iii) limit the processing of sensitive data to that strictly necessary to comply with the purposes for which it was collected;

(iv) limit access to sensitive data on a need-to-know basis.

The Argentine Bill of Law on Data Protection introduces a new definition of sensitive data, including the current categories of sensitive data listed in the Argentine Data Protection Law as reference, and defining it as "any information that may give place to discrimination", including biometric data, genetic data, and data that may reveal a person's gender identity.

5 Supervisory authority

The Agency of Access to Public Information acts as the controlling authority of the Argentine Data Protection Law ("**Argentine Data Protection Authority**"). The Argentine Data Protection Authority is responsible for overseeing the integral protection of personal data to ensure individuals' rights to honor, privacy, and access to their personal data. The authority was created by Argentine Law No. 27,275 and functions as an autonomous entity operating within the President's Chief of Staff Office.

6 Obligations and requirements for compliance

When carrying out data processing activities, organizations should comply with the following obligations and requirements:

(i) **Compliance with the Data Protection Law's guiding principles.** The Argentine Data Protection Law states that any processing of personal data shall abide by the following guiding principles:

- **Purpose limitation.** Personal data should be collected for specific, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- **Data minimization.** Personal data must be adequate, relevant, and not excessive in relation to the scope and purpose for which it is collected.
- **Storage limitation.** Personal data must be deleted and/or destroyed, even without the express request of the data subjects, once it is no longer necessary for the purpose for which it was collected (except as otherwise stated in applicable sectorial regulations, such as tax, labor, or corporate regulations).
- **Lawfulness, fairness, and transparency.** Personal data must be processed lawfully, fairly, and in a transparent manner in relation to the data subjects.
- **Accuracy.** Personal data must be accurate and, when necessary, regularly updated. If the data controller becomes aware of any inaccuracies or incompleteness in personal data, it must promptly delete, correct, or complete such data.

(ii) **Database registration.** The Argentine Data Protection Law mandates the registration of databases containing personal data with the Argentine Data Protection Authority. Data controllers must first register themselves before registering a database.

(iii) **Legal basis for the processing of personal data.** The Argentine Data Protection Law requires explicit, informed, and written or equivalent consent from data subjects for the processing of personal data, except when exceptions to consent apply.

(iv) **Duty of information.** Prior to personal data collection, organizations should inform data subjects about: (i) the purpose of processing; (ii) the categories of third parties to whom the personal data may be disclosed; (iii) the existence of the database and the identity and address of the data controller; (iv) whether it is man-

datory or optional to provide personal data; (v) the consequences of failing to provide personal data or providing inaccurate personal data; (vi) their rights, together with information on how, or by what means, they may exercise them; and (vii) the possibility of filing claims before the Argentine Data Protection Authority.

(v) **Assignment of personal data.** The Argentine Data Protection Law allows data controllers to transfer personal data to another controller only if: (i) the processing serves purposes directly related to the legitimate interests of the parties involved; (ii) they obtain prior consent from the data subjects; and (iii) they inform the data subjects about the identity of the recipient.

(vi) **Data processing agreements.** The Argentine Data Protection Law requires data controllers to execute data processing agreements with data processors. These agreements must state that: (i) personal data processed cannot be used or applied for purposes different to those set forth in the services agreement; (ii) personal data cannot be transferred to third parties, even for its storage; (iii) once the data processing services have been rendered, the processed personal data must be destroyed unless there is an express authorization from the controller; and (iv) the data processor also complies with the duties concerning the security and confidentiality of the processed personal data.

(vii) **Confidentiality and security of personal data.** Data controllers and data processors must implement technical and organizational measures to ensure the protection and confidentiality of personal data, preventing unauthorized access, loss, or tampering with such data. Additionally, anyone processing personal data is bound by a duty of confidentiality.

Additionally, the Argentine Bill of Law on Data Protection presents new requirements and obligations regarding the processing of personal data, such as: (i) the obligation for data controllers to report security incidents; (ii) the obligation, under certain circumstances, to carry out data privacy impact assessments; (iii) the obligation to appoint a representative in Argentina when the data controller or data processor is not present in the country; and (iv) the obligation to appoint a data protection officer ("DPO") in certain cases.

7 Data Protection Officer (DPO)

In Argentina, the appointment of a DPO is not mandatory, although it is recommended by the Data Protection Authority for public entities. However, the Argentine Bill of Law on Data Protection mentions that under certain conditions, the nomination of a DPO

is compulsory, while being voluntary in other scenarios. This draft delineates the role, qualifications, and tasks for a DPO. There are also particular circumstances, especially where special security standards apply, that may require appointing an officer for data security, although this is not a general requirement.

8 Data subjects' rights

The Argentine Data Protection Law provides the following rights for data subjects:

(i) **Right to information.** Data subjects must be clearly informed on: (i) the purpose for which their personal data will be processed and any possible recipients; (ii) the existence of any databases and those responsible for them; (iii) whether providing their personal data is mandatory or voluntary; (iv) the consequences of providing the personal data and of failing to do so; (v) the data subjects' right to access, rectify, and suppress their own personal data; and (vi) the possibility of filing claims before the Argentine Data Protection Authority.

(ii) **Right of access.** Data subjects have the right to access any database containing their personal data and request information about it. This right can be exercised at intervals of no less than six months, and data controllers must respond within 10 calendar days of receiving the request.

(iii) **Right to rectification, update, and deletion.** Data subjects can request the rectification, update, or deletion of their personal data from databases. Data controllers must respond within 5 working days of receiving the request. However, data deletion may not occur if it would prejudice the rights or legitimate interests of third parties or when there's a legal obligation to retain the data.

(iv) **Right to withdraw consent.** Data subjects have the right to withdraw their consent for the processing of personal at any time, with no retroactive effect.

(v) **Right to object to marketing.** In marketing communications, data subjects should have the option to remove or block all or part of their personal data from the respective database.

(vi) **Right to file a complaint.** In the event data controllers do not satisfactorily comply with a data access request or a request for update, rectification, or deletion, data subjects have the right to initiate a court action and to give notice of such failure to the Argentine Data Protection Authority.

Additionally, the Argentine Bill of Law on Data Protection provides new rights to the data subject, such as the right to object to the processing of personal data (not limited to marketing), the right to data portability, and the right to not be subjected to decisions based solely or partially on automated processed data if such decision could negatively affect the data subject.

9 Security requirements

The Argentine Data Protection Law states that the data controller, data processor, and the user of a database containing personal data must adopt the necessary technical and organizational measures to ensure the protection and confidentiality of the data, and to prevent any adulteration, loss, or unauthorized access or processing.

In this regard, the Argentine Data Protection Authority issued Resolution No. 47/2018 that provides a set of recommended security measures for the processing and conservation of personal data, both in the digital and physical world and in line with international security standards, such as NIST, PCI-DDS, CIS CONTROLS and ISO/27002.

The abovementioned Resolution includes recommendations regarding: (i) data collection; (ii) access control to personal data; (iii) modification control; (iv) backup and recovery; (v) vulnerability management; (vi) information destruction; (vii) security incidents; and (viii) development environments.

Some of these recommendations also include additional guidelines regarding the processing of sensitive personal data.

10 Data breach notification

The Argentine Data Protection Law does not impose an express obligation to notify data breaches to the Argentine Data Protection Authority nor to the data subjects.

Meanwhile, although not yet enforceable, Convention 108+ provides that data controllers must notify security incidents that may seriously affect the fundamental rights and freedoms of data subjects, without delay, at least to the supervisory authority.

Additionally, Resolution No. 47/2018 recommends having a procedure to manage security incidents, to issue an incident report, and to report security incidents to the Argentine Data Protection Authority.

Please note that general civil principles of law or other sectoral regulations may mandate or recommend notifying a security incident.

Lastly, the Bill of Law on Data Protection introduces the obligation for data controllers

to report security incidents to the data protection authority and, under certain circumstances, to data subjects.

11 International data transfers

Under the Argentine Data Protection Law, transferring personal data to countries or international organizations that do not provide an appropriate level of protection according to the Argentine Data Protection Authority's criteria is prohibited. However, transferring personal data to countries deemed non-adequate is allowed if: (i) the data subject consents to the transfer; or (ii) an adequate level of protection arises from contractual clauses (international data transfer agreements), or systems of self-regulation (as binding corporate rules).

Resolution No. 60 – E/2016, issued by the Argentine Data Protection Authority, provides that personal data can be transferred with no further safeguards to Member States of the European Union and the European Economic Area, Switzerland, Guernsey and Jersey, the Isle of Man, the Faeroe Islands, Canada (only the private sector), New Zealand, Andorra, Uruguay, Israel (specifically for data undergoing automated processing), UK, and Northern Ireland. Moreover, this resolution introduces two sets of standard model clauses for data transfer agreements.

Additionally, Resolution No. 159/2018 approved a set of guidelines for binding corporate rules, providing a framework for multinational companies to use as a self-regulating mechanism to legitimize international data transfers within their corporate groups.

The Argentine Bill of Law on Data Protection modifies the rules for transferring personal data abroad. It specifies that consent may only be an exception for international data transfers, not a regular practice, especially for transfers that occur frequently or involve a large number of data subjects. Additionally, the bill now explicitly recognizes onward transfers (i.e., subsequent transfer of personal data from one entity to another).

12 Penalties

Penalties for non-compliance with personal data protection regulations are limited to: (i) warnings; (ii) fines from ARS 1,000 to ARS 100,000 (equivalent to approximately USD 1.20 to USD 122 at currently exchange rate); (iii) suspensions; (iv) closure; or (v) cancellation of the file, registry, or database.

Infringements are graded as moderate, severe, or very severe:

(i) **Moderate:** for moderate infringements, the sanction to be applied will be up to 2 warnings and/or a fine of ARS 1,000 to ARS 80,000 (equivalent to approximately USD 1.20 to USD 98 at today's exchange rate).

(ii) **Severe:** for severe infringements, the sanction to be applied will be up to 4 warnings, suspension from 1 to 30 days and/or a fine of ARS 80,001 to ARS 90,000 (equivalent to approximately USD 98 to USD 110 at today's exchange rate).

(iii) **Very severe:** for very severe infringements, the sanction to be applied will be up to 6 warnings, suspension of 31 to 365 days, closure, or cancellation of the database and/or a fine of ARS 90,001 to ARS 100,000 (equivalent to approximately USD 110 to USD 123 at today's exchange rate).

Resolution No. 244/2022 limits the fines applicable to several infringements included in the same administrative procedure to: (i) ARS 3,000,000 (equivalent to approximately USD 3,686 at today's exchange rate) in the case of moderate infringements; (ii) ARS 10,000,000 (equivalent to approximately USD 12,286 at today's exchange rate) in the case of severe infringements; and (iii) ARS 15,000,000 (equivalent to approximately USD 18,429 at today's exchange rate) in the case of very severe infringements.

The Argentine Data Protection Authority maintains a public registry of individuals and legal entities that have been sanctioned as a result of a violation of the Argentine Data Protection Law.

In addition to the sanctions that may be imposed by the Argentine Data Protection Authority, there may be claims for damages by data subjects based on the general principles of civil liability provided in the Argentine Civil and Commercial Code, including through class actions.

The Argentine Bill of Law on Data Protection modifies the current sanction regime and provides that the Argentine Data Protection Authority may impose fines from 5 to 1,000,000 adjustable units, or from 2% to 4% of the preceding financial year total worldwide annual turnover. The initial value of the adjustable unit will be ARS 10,000 (equivalent to approximately USD 12 at today's exchange rate) and will be updated annually according to the INDEC Customer Price Index.

Bolivia

Aguilar Castillo Love

José Carlos Bernal*

Contact:

* jbr@aguilarcastillolove.com

Lefosse

1 Legislation: local laws applicable to data protection

Data protection has limited regulation in Bolivia.

The Bolivian Constitution mentions data protection from a procedural angle, focusing on individual's right to access and to modify their personal information in databases. However, it lacks comprehensive data protection regulations. The current Bolivian legislation only recognizes general legal principles safeguarding privacy, dignity, and honor.

Telecommunications Law No. 164 ("**Law 164**") mentions data protection in a single article (article 56), which primarily applies to the telecommunications sector and the obligation to protect the data of their customers.

There are currently two bills in progress dealing with the protection of personal data. Initially, Bill No. 349/2020-2021 for personal data protection was presented to Congress on October 19, 2021. On March 31, 2023, the Government Agency in charge of Information and Communication Technologies ("**AGETIC**") filed a new data protection bill with the Bolivian Senate.

Both bills propose the incorporation of an Agency for the Protection of Personal Data ("**APP**") as the national regulatory authority.

2 Jurisdiction: territorial applicability

Existing legislation and constitutional provisions do not explicitly address the extraterritorial application of these laws.

3 Scope: information protected under data protection legislation

Legal principles indirectly related to data protection revolve around safeguarding information to uphold privacy, dignity, and personal honor. Existing legislation concerning privacy rights may also be invoked in cases of data breaches.

4 Definition of sensitive or special category data

Current data protection laws in Bolivia do not provide specific categories or differentiated handling for various types of personal data.

5 Supervisory authority

There is no specific national authority for supervising the processing of personal data

or enforcing data protection obligations. Existing authorities such as AGETIC and the Telecommunications Authority have other mandates.

6 Obligations and requirements for compliance

The obligations of organizations handling personal data are not extensively defined in a comprehensive data protection law. However, some general principles and obligations related to data protection can be derived from the existing legal framework, including Law 164 and general privacy principles, including the following:

- **obtaining written consent;**
- **allowing data subjects to access, modify or erase their personal data;**
- **implementing basic data security.**

Companies may have their own internal policies that further detail their data protection practices and obligations.

7 Data Protection Officer (DPO)

The formal designation of a Data Protection Officer is not expressly mandated for Bolivian companies.

However, companies operating in specifically regulated industries may be required to appoint personnel to comply with IT security. For example, pursuant to Article 7, Section 2, Chapter II, Title VII, Book 3 of the Financial Services Recompilation of Norms, financial entities must designate a "Responsible of Information Security". This appointee is in charge of overseeing functional and operational autonomy of the entities from a technological and informational standpoint and is in charge of the enforcement of information security protocols. While this operator is not considered a Data Protection Officer, some of the assignments of the position may overlap with those of a DPO.

8 Data subjects' rights

Individuals have certain rights regarding their personal data, including the right to access, modify, update, revoke, and raise objections regarding the use of their data.

While consent for data collection can be retracted, such a retraction does not retro-

actively affect prior data processing. If an entity declines to address a data subject's request, this person may file claims in Bolivian courts to seek compliance. Should the court reject such a plea, the individual retains the option to pursue constitutional claims to redress the matter.

9 Security requirements

Despite the absence of specific information security requirements in Bolivian data protection laws, organizations handling personal data are generally expected to implement reasonable security measures to safeguard the data they collect.

It is important to note that organizations should align their data protection practices with any industry-specific regulations or standards that may apply to their operations. Companies operating in the financial sector for example (banks, brokers, funds etc.) must comply with specific information security standards, required by industry regulations and subject to supervision of the Financial Authority ("**ASFI**" for its acronym in Spanish). Companies in other sectors are not subject to the same regulations.

10 Data breach notification

There are no specific requirements in case of a data breach or other security incidents involving personal data.

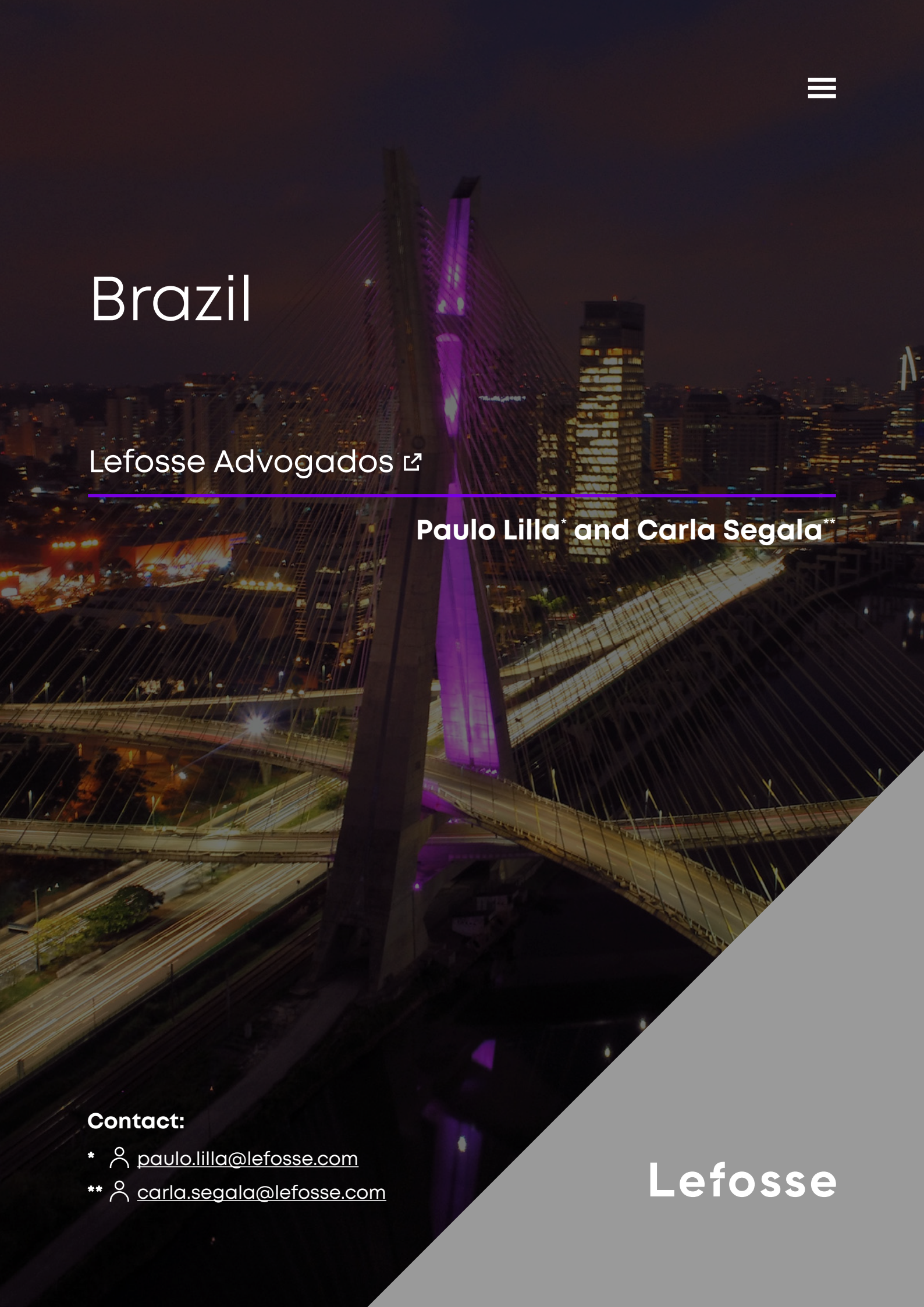
For individuals who can identify a breach's perpetrator, legal recourse relies on general and constitutional provisions within the existing legal framework. This allows them to seek cessation of the breach and claim monetary compensation for damages, including potential harm to reputation or honor.

11 International data transfers

Bolivia does not have comprehensive data protection laws that specifically address the rules for transferring personal data outside of the country.

12 Penalties

Should an individual's privacy be infringed due to a security breach, he/she would have the option to seek financial compensation for damages.



Brazil

Lefosse Advogados

Paulo Lilla* and Carla Segala**

Contact:

* paulo.lilla@lefosse.com

** carla.segala@lefosse.com

Lefosse

1 Legislation: local laws applicable to data protection

In Brazil, privacy and data protection are recognized by the Federal Constitution as fundamental rights of individuals. It also grants the federal government the exclusive jurisdiction to legislate on personal data protection matters.

Data protection is regulated by Law No. 13,709/2018 (Brazilian General Data Protection Law, in Portuguese, *Lei Geral de Proteção de Dados Pessoais* – "**LGPD**"), which was enacted in August 2018 and came into effect on September 18, 2020. The LGPD was designed to establish a comprehensive legal framework for data protection and privacy in Brazil. It is applicable to public and private entities and covers any sort of personal data processing, either online or offline.

There are also several sectorial laws dealing with privacy and data protection matters, such as Law No. 12,965/2014 ("**Marco Civil da Internet**" or "**MCI**") and its Regulatory Decree (Decree No. 8,771/2016), Law No. 8,078/1990 ("**Consumer Defense Code**"), Law No. 12,414/2011 ("**Good Payers Register Law**") and its Regulatory Decree (Decree No. 9,936/2019), among others.

2 Jurisdiction: territorial applicability

The LGPD has extraterritorial effects, which means that it may be applicable to entities processing personal data outside Brazil, as long as: (i) the data has been collected in Brazil; (ii) the processing activity is aimed at offering goods or services to individuals located in Brazil, or (iii) the activity involves the processing of data of individuals located in the Brazilian territory.

3 Scope: information protected under data protection legislation

The LGPD protects personal data, which is defined as any information regarding an identified or identifiable natural person.

4 Definition of sensitive or special category data

The LGPD defines "sensitive data" as any personal data concerning racial or ethnic origin, religious belief, political opinion, trade union or religious, philosophical, or political organization membership, data concerning health or sex life, genetic or biometric data, when related to a natural person.

Sensitive personal data is afforded greater protection under the LGPD.

5 Supervisory authority

Law No. 13,853/2019 amended the LGPD to create the National Data Protection Authority (in Portuguese, *Autoridade Nacional de Proteção de Dados* – "**ANPD**"). The ANPD is responsible for issuing regulations, ensuring compliance with data protection rules in Brazil, preparing guidelines on the provisions of the LGPD, and imposing administrative sanctions in cases of violation of the Law.

6 Obligations and requirements for compliance

When carrying out data processing activities, organizations should comply with the following obligations and requirements:

(i) **Data protection principles.** The LGPD provides 10 (ten) principles that must be complied with by controllers and processors when processing personal data, as follows:

- **Purpose limitation.** Processing must be carried out for legitimate, specific, and explicit purposes of which the data subject is informed, with no possibility of subsequent processing that is incompatible with these purposes.
- **Adequacy.** Processing must be compatible with the purposes informed to the data subject, in accordance with the context of the processing.
- **Necessity (equivalent to data minimization).** Processing must be limited to the minimum necessary to achieve its purposes, covering personal data that is relevant, proportional, and non-excessive in relation to the purposes of the processing.
- **Free access.** Data subjects must be afforded facilitated and free of charge consultation about the processing of their personal data.
- **Quality of the data.** Data subjects are entitled to accuracy, clarity, relevancy, and updating of the data, in accordance with the need and for achieving the purpose of the processing.
- **Transparency.** Data subjects must be provided with clear, precise and easily accessible information about the processing of their personal data and the respective processing agents (i.e., controllers and processors), subject to commercial and industrial secrecy.
- **Security.** Processing agents must implement technical and administrative measures able to protect personal data from unauthorized access and acciden-

tal or unlawful situations of destruction, loss, alteration, communication, or dissemination.

- **Prevention.** Processing agents must adopt measures to prevent the occurrence of damages arising out of the processing of personal data.
- **Non-discrimination.** Prohibition of personal data processing for unlawful or abusive discriminatory purposes.
- **Accountability.** Processing agents must adopt measures which are efficient and capable of proving compliance with the rules of personal data protection, including the effectiveness of such measures.

(ii) **Legal basis for the processing of personal data.** The processing can only be carried out:

- with the consent from the data subject;
- for compliance with a legal or regulatory obligation by the controller;
- by the public administration, for the processing and shared use of data necessary for the execution of public policies provided in laws or regulations, or based on contracts, agreements or similar instruments;
- for carrying out studies by research entities, ensuring, whenever possible, the anonymization of personal data;
- when necessary for the execution of a contract or preliminary procedures related to a contract of which the data subject is a party;
- for the regular exercise of rights in judicial, administrative or arbitration proceedings;
- for the protection of life or physical safety of the data subject or a third party;
- to protect the health, exclusively in a procedure carried out by health professionals, health services or sanitary authorities;
- when necessary to fulfil the legitimate interests of the controller or a third party, except when the data subject's fundamental rights and freedoms which require personal data protection prevail; or
- for the protection of credit.

Some of the legal bases above, such as legitimate interest and protection of credit, are not applicable in the processing of sensitive personal data.

(iii) **Duty of information.** The data subject has the right to facilitated access to information concerning the processing of her/his data, which must be made available in a clear, adequate, and ostensible manner. At least the following information must be provided:

- the specific purpose of the processing;
- the type and duration of the processing, being observed commercial and industrial secrecy;
- identification of the controller;
- the controller's contact information;
- information regarding the shared use of data by the controller and the purpose;
- responsibilities of the agents that will carry out the processing; and
- the data subject's rights, with explicit mention of the rights provided for by the LGPD.

7 Data Protection Officer (DPO)

The LGPD provides that the controller must appoint a Data Protection Officer ("DPO") to be in charge of processing personal data. A DPO is defined by the LGPD as the person appointed by the controller and processor to act as a channel of communication between the controller, the data subjects and the ANPD.

As per the LGPD, the activities carried out by the DPO consist of:

- accepting complaints and communications from data subjects, providing explanations and adopting measures;
- receiving communications from the ANPD and adopting measures;
- orienting entity's employees and contractors regarding practices to be taken in relation to personal data protection; and
- carrying out other duties as determined by the controller or set forth in complementary rules.

8 Data subjects' rights

The LGPD provides for the following rights for data subjects:

- confirmation of the existence of data processing;
- access to data;
- correction of incomplete, inaccurate, or outdated data;
- anonymization, blocking, or elimination of unnecessary or excessive data or of data processed in non-compliance with the provisions of the LGPD;
- portability of the data to other service providers or suppliers of products, by the means of an express request, subject to commercial and industrial secrecy;
- elimination of the personal data processed with the consent of the data subjects;
- information on the public and private entities with which the controller has shared data;
- information on the possibility of not providing consent and on the consequences of such denial;
- revocation of the consent;
- review of decisions based on the processing of personal data carried out exclusively by automated means;
- right to file a complaint against the controller with the ANPD; and
- right to object the processing when the processing is not grounded on the consent from data subject, whenever the processing is not compliant with the LGPD.

9 Security requirements

Both controllers and processors must adopt security, technical and administrative measures able to protect personal data from unauthorized accesses and accidental or unlawful situations of destruction, loss, alteration, communication, or any type of improper or unlawful processing.

The LGPD sets out that the ANPD may provide minimum security technical standards, considering the nature of the processed information, the specific characteristics of the processing and the current state of technology.

10 Data breach notification

The controller must report to the ANPD and to the affected data subjects the occurrence of a security incident that may pose a risk or significant harm to data subjects. According to Resolution No. 15/2024 issued by the ANPD, the initial report of security incidents must be made within 3 business days of becoming aware that the incident affected personal data.

11 International data transfers

The LGPD provides that international transfer of personal data is permitted solely in the following cases:

- **to countries or international organizations that provide an adequate level of protection of personal data provided for by the LGPD;**
- **when the controller provides and demonstrates guarantees of compliance with the principles and rights of the data subject and data protection rules established in the LGPD, in the form of:**
  - specific contractual sections for a given transfer;
  - Standard Contractual Clauses ('SCCs');
  - Binding Corporate Rules ('BCRs'); and
  - seals, certificates, and codes of conduct regularly issued;

- when the transfer is required for international legal cooperation between government intelligence, investigations, and police bodies, in accordance with international law instruments;
- when the transfer is required for the protection of the life or physical integrity of the data subject or any third party;
- when the ANPD authorizes the transfer;
- when the transfer results in a commitment undertaken under an international cooperation agreement;
- when the transfer is required for the enforcement of a public policy or legal attribution of the public utility;
- when the data subject has provided specific and highlighted consent for such transfer, with prior information on the international nature of the operation, clearly distinguishing it from any other purposes;
- when necessary to comply with a legal or regulatory obligation by the controller;
- when necessary for the execution of a contract or preliminary procedures related to a contract to which the data subject is a party; or
- to allow the regular exercise of rights in judicial, administrative, or arbitration proceedings.

Chile

Barros & Errázuriz

Andrés Rodríguez*

Contact:

* arodriguez@bye.cl

Lefosse

1 Legislation: local laws applicable to data protection

The main data protection-related laws in Chile are the following:

- **Article 19 No. 4 of the Chilean Constitution.** Guarantees individuals the right to the protection of private life and the processing of personal data as a constitutional right.

- **Law No. 19.628 on the Protection of Private Life (hereinafter referred to as the "DPL").** This law sets forth the obligations that every individual or entity processing personal data must fulfill, along with the sanctions in case of non-compliance.

- **Article 15 bis of Law No.19.496 on Protection of Consumer Rights.** In December 2021, amendments were made to the Protection of Consumer Rights Law, granting specific administrative interpretation and oversight powers regarding personal data matters in supplier-consumer relationships to the National Consumer Service Authority (hereinafter referred to as "**Sernac**").

- **Sernac's interpretative guide.** Using its interpretative authority, Sernac published an interpretative guide regarding what should be considered as an abusive clause related to personal data processing when engaging in a supplier-consumer relationship. This guide complements the obligations outlined in the DPL, elevating the compliance standards that companies acting as data controllers must adhere to when processing personal data of their customers.

- **Data protection Bill (hereinafter referred to as the "Chilean Bill").** Currently, there is a bill of law in its final stages in Congress that aims to amend the DPL and assimilate data privacy standards to the European General Data Protection Regulation (GDPR).

2 Jurisdiction: territorial applicability

The DPL governs the processing of personal data carried out by data controllers and processors operating within Chile. In addition, the DPL protects individuals residing in Chile. Therefore, if data processing is carried out because of offering goods or services to Chilean citizens, the DPL will be applicable, even if the controller is located abroad.

The Consumer Protection Law applies to relationships between suppliers and consumers at the national level.

Lastly, if the Chilean Bill is approved without modifications, it would apply to all data controllers who have an establishment in Chile; to those whose data processing operations are aimed at offering goods and/or services to data subjects located in Chile; or data controllers who are subject to Chilean law through a contract or international agreement.

3 Scope: information protected under data protection legislation

The DPL and the Chilean Bill safeguard personal data, which includes all or any information related to an identified or identifiable natural person.

It should be noted that Article 15 bis of Law No. 19.496, concerning the Protection of Consumer Rights, stipulates that Sernac's supervisory powers extend only to the processing of personal data of consumers.

4 Definition of sensitive or special category data

The DPL distinguishes between personal data and sensitive data.

Sensitive data is the personal data that refers to the physical or moral characteristics of individuals, or to facts or circumstances of their private or intimate life, such as personal habits, racial origin, political ideologies and opinions, religious beliefs or convictions, physical or mental health conditions, and sexual life.

According to the DPL, sensitive data cannot be processed, except when authorized by law, with the consent of the data subject, or when the data is necessary for the determination or provision of health benefits corresponding to the data subjects.

Regarding the Chilean Bill, it also distinguishes between personal data and sensitive personal data (those that pertain to the physical or moral characteristics of individuals or to facts or circumstances of their private life or intimacy, such as those revealing ethnic or racial origin, political, trade union or guild affiliation, socio-economic status, ideological or philosophical beliefs, religious beliefs, health data, human biological profile, biometric data, and information related to the sexual life, sexual orientation, and gender identity of a natural person). It provides specific lawful grounds for their processing and mandates the need for a prior impact assessment before commencing processing operations.

5 Supervisory authority

There is no national or regional authority directly responsible for supervising the processing of personal data and enforcing data protection laws in Chile. However, the Chilean Bill aims to establish a national authority for these purposes.

Currently, because protection of private life is guaranteed by the Chilean Constitution, data subjects can file a "protection appeal" (*recurso de protección*) with the Appeal Court to safeguard their constitutional rights.

Also, under DPL, data subjects have the right to file a claim with civil courts if a data controller does not comply with or refuses to act on the request of the data subject for the exercise of their data subjects' rights.

On the other hand, due to the modification of the Protection of Consumers Rights Law in 2021, Sernac has the authority to supervise and audit companies that process consumers' personal data. However, Sernac does not have the authority to impose sanctions.

6 Obligations and requirements for compliance

Organizations that handle personal data have the following obligations that they must comply with:

- **Lawful processing.** Count with a legal basis for processing personal data, which may be the data subject's express consent or a legal obligation/ authorization.

  Notwithstanding, under certain circumstances described in the DPL, the processing of personal data (excluding sensitive data) does not require the data subject's authorization, such as: (i) when it is collected from publicly available sources; (ii) when it is included in listings that identifies a group of people with certain categories; (iii) when it is necessary for commercial communications or the sale of goods and services; (iv) when it is made by private entities for its own exclusive use; and (v) when the processing is carried out by public bodies.

- **Inform data subjects.** Duly inform data subject of the processing purposes, the possibility for the data to be transferred to third parties and the potential recipients of such data, if applicable.

- **Data minimization.** Only collect and process personal data that is necessary for the specified purpose.
- **Accuracy.** Ensure the accuracy of the personal data and keep the data up to date.
- **Data security.** Implement appropriate measures to protect personal data from unauthorized access, disclosure, alteration, or destruction.
- **Data subject's rights.** Pronounce to any data subject's rights request within 2 business days.

7 Data Protection Officer (DPO)

The DPL does not mandate the appointment of a Data Protection Officer by organizations that handle personal data.

However, according to bank specific regulations[1], financial institutions are obligated to have an Information Security Officer in their organizational structure.

On the other hand, the Chilean Bill, aiming at modernizing the DPL to the currently standards of data protection legislations, introduces the establishment of a national registry managed by the future authority. This registry will publish a list of data controllers who adopt an infringement prevention model (hereinafter referred to as "**National Compliance Registry**"). As part of the actions outlined in this prevention model, the appointment of a DPO is specified.

In summary, if the Chilean Bill is approved without modifications, appointing a DPO will not be mandatory, but it will become a minimum requirement to be listed on the National Compliance Registry.

[1] Chapter 20-10, Compilation of Regulations from the Financial Market Commission, https://www.cmfchile.cl/portal/principal/613/articles-29310_doc_pdf.pdf

8 Data subjects' rights

The DPL ensures the following rights for data subjects:

- **Access.** Data subjects have the right to obtain confirmation from the data controller as to whether their personal data is being processed and, if so, to be informed about what data is processed, the purposes of the processing, and the recipients to whom the personal data have been or will be disclosed.
- **Rectification.** Data subjects can request the correction of inaccurate or incomplete personal data held by the data controller.
- **Erasure.** Data subjects have the right to request the deletion of their personal data.
- **Objection.** Data subjects can object to the processing of their personal data, especially when the processing is for direct marketing, market research or opinion survey purposes.
- **Restriction.** Data subjects can request the controller to temporarily suspend the processing, in cases where (i) the data subject has voluntarily provided his/her data and it is used for communications, or (ii) the accuracy of personal data cannot be confirmed, and erasure is not applicable.

The portability right is not recognized in the DPL, but it is set to be regulated in the proposed Chilean Bill.

9 Security requirements

The DPL sets out a general security requirement, stipulating that data controllers must exercise due diligence and take proper care of personal data. Additionally, it mandates that all individuals involved in the processing of personal data must be obligated to maintain confidentiality.

Sernac's interpretation guide sets forth that data controller suppliers must implement comprehensive security measures. These measures should encompass technical, organizational, and workforce training aspects to ensure the safeguarding of the confidenti-

ality, integrity, and availability of consumers' personal data to prevent the transmission, loss, and unauthorized access to such data.

10 Data breach notification

There are no express requirements in case of a data breach or other security incidents involving personal data under Chilean data protection laws.

However, industry-specific regulations impose these obligations, such as the Chapter 20-8 on the Operational Incident Reporting; Chapter 20-9 on Business Continuity Management; and Chapter 20-10 on the Information Security and Cybersecurity Management of the Updated Compilation of Regulations of the Financial Market Commission and the Fintech Law (Law No. 21.521), which establishes that institutions under the supervision of the Financial Market Commission and the ones participating in the open finance system are mandated to promptly inform the Financial Market Commission of any data security breaches.

11 International data transfers

In accordance with Chilean data protection legislation, there are no distinct regulations governing the cross-border transfer of personal data.

To transfer personal data to another jurisdiction, it is necessary to comply with the general processing requirements established under the DPL, i.e., having a legal basis for the transfer and informing the data subject of the intended transfer.

However, in the financial industry, there are specific regulations governing the outsourcing of data processing services. As outlined in Chapter 20-7 of the Updated Compilation of Regulations of the Financial Market Commission, entities that outsource data processing services abroad must maintain records of the contracted company's financial stability, certifications, project details, and execute an agreement. Additionally, if a financial institution conducts significant activities abroad, it must meet the following conditions:

- **maintain a contingency Data Processing Center in Chile with a recovery time compatible with the criticality of the service.**
- **report specific measures if their operational risk rating falls below a certain level.**

- monitor the outsourced service's security, business continuity, and processing center operations, regardless of the provider's own monitoring.

12 Penalties

The sanctions provided in the DPL are as follows:

- **Compensation for damages.** In the event of a breach of the law and misuse of personal data, data subjects may request civil courts to compel the controller to compensate them for damages. The amount of compensation will be determined by the judge, who will consider the processed personal data and the breach.

- **Fine of up to 50 UTM (3,600 USD approx.).** If the data controller fails to respond or provides an evasive response to requests from data subjects exercising their rights, the data subject may seek recourse in civil courts. The judge may impose a fine of up to 50 UTM on the data controller, in addition to requiring them to compensate the data subject if deemed appropriate.

The Chilean Bill introduces fines of up to 20,000 UTM (1,536,270 USD) for violations of the law, in addition to holding data controllers liable for damages resulting from legal breaches. In the event of recidivism, the fine could be up to three times the amount assigned to the initial infringement.

Colombia

Brigard Urrutia

Juan Nicolás Laverde* and Sergio Michelsen**

Contact:

* jlaverde@bu.com.co

** smichelsen@bu.com.co

Lefosse

1 Legislation: local laws applicable to data protection

The legal framework for General Data Protection in Colombia is established by Law 1581 of 2012 and Decree 1074 of 2015 (collectively referred to as the "**CGDP**").

2 Jurisdiction: territorial applicability

The CGDP applies to (i) entities based in Colombia, (ii) data processing operations carried out within Colombia, and (iii) data processing operations carried out by foreign entities subject to Colombia law due to international standards and treaties. However, as of now, there is no specific treaty subject to this provision.

3 Scope: information protected under data protection legislation

The CGDP applies to the collection, storage, use, transfer, transmission, suppression, and overall processing of personal data. Under the CGDP, personal data refers to any information that can be associated with or linked to a specific individual, in a manner that allows for his/her identification.

4 Definition of sensitive or special category data

The CGDP defines sensitive data as data that has an intimate relation with the individual, where misuse could lead to discrimination. It provides a non-exhaustive list of examples of sensitive data, including health and medical information, racial or ethnic background, disabilities, sexual preferences, and gender identity. As a general rule, the processing of sensitive data is prohibited unless there is prior express and informed consent from the data subject for a legitimate purpose. Sensitive data is subject to an enhanced level of protection, demanding more stringent security measures.

5 Supervisory authority

The Superintendence of Industry and Commerce ("**SIC**") acts as the data protection supervisory authority in Colombia. The SIC performs both administrative and jurisdictional roles. Its administrative duties encompass the issuance of regulations, investigation of violations, and imposition of penalties for non-compliance with relevant laws. The jurisdictional responsibilities of the SIC (i.e. resolution of controversies between private parties) are limited to consumer protection and unfair competition. In these matters, the SIC has the authority to initiate legal actions, conduct investigations, enforce warranties, and levy fines.

6 Obligations and requirements for compliance

Organizations are subject to the following obligations when handling personal data under the CGDP:

- obtain the prior, free, express, and informed consent of data subjects and retain a copy of this consent;
- process and respond to complaints, petitions, and requests from data subjects concerning their personal data;
- implement and keep technical, human, and organizational measures aimed at ensuring the integrity, confidentiality, and security of personal data;
- implement a data protection policy that informs data subjects of (i) the purposes for processing their data, (ii) how data will be used, (iii) their rights and the mechanisms for exercising them, (iv) the contact details of the designated data protection officer within the entity, and (v) the duration of the database's validity;
- inform the SIC of breaches to security protocols and whenever personal data is at risk;
- appoint a designated individual or department to manage personal data matters, including the implementation of relevant policies and the handling of complaints, petitions, and requests from data subjects, thereby ensuring the protection of data subjects' rights;
- register the databases with the National Database Registry, a requirement exclusive to data controllers. The SIC, which oversees this registry, requires the submission of information about the database, not the database itself.

The legal basis for data processing is consent from data subjects. For consent to be considered valid, it must be prior (obtained before processing), express (indicating clear and unequivocal intention) and informed. To fulfill this last requirement, data subjects must be informed about (i) the name and contact details of the data controller; (ii) their rights and means to exercise them; (iii) where to consult the applicable data protection policy; (iv) that the authorization to process sensitive data is entirely optional; (v)

the specific data that will be collected and processed – especially if sensitive data is involved, and (vi) how the data will be used and for what purposes. This information must be provided at the latest at the time consent is obtained, for instance, through a checkbox during initial onboarding. If consent is incorporated by reference, additional considerations must be addressed to ensure clarity and comprehensibility.

7 Data Protection Officer (DPO)

The CGDP requires appointing a person or department meant to handle personal data matters (i.e., execute relevant policies; address complaints, petitions, and requests from data subjects) and ensure data subjects' rights, which the SIC has characterized as a DPO. Contact data (e.g., email address) of the DPO should be published in the privacy policy.

The CGDP does not specify the qualifications of a DPO, and thus the company is free to appoint the area or individual of its preference (i.e., it does not need to be a local representative). The SIC, however, has recently published non-binding guidelines applicable to DPOs, and according to these guidelines companies must ensure: (i) the DPO's accessibility for stakeholders (i.e., employees, clients, and suppliers), and (ii) the DPO's knowledge about the CGDP and about the sensitivity, complexity, and amount of data processed by the company.

8 Data subjects' rights

The CGDP provides the following data protection rights to data subjects:

- **Right of access:** data subjects are entitled to obtain information about the personal data held and processed about them.
- **Right to rectification:** data subjects have the right to obtain the rectification of any personal data that might be inaccurate or incomplete.
- **Right to erasure or "right to be forgotten":** data subjects can request the deletion of their personal data under conditions similar to those outlined in the GDPR.
- **Right to restriction of processing:** data subjects may request limits on the processing of their personal data under circumstances akin to those specified in the GDPR.

- **Right to request evidence of consent and to withdraw consent:** data subjects have the right to ask for evidence that consent has been granted, as well as to withdraw consent at any time.
- **Right to file claims:** data subjects have the right to file complaints with the SIC when they believe their data protection rights are being violated.

9 Security requirements

There are no specific information security requirements under the CGDP. However, data controllers are imposed a general duty of care towards the personal data in their possession, ensuring its confidentiality, security, integrity, and availability. In line with these responsibilities, data controllers must also ensure that their data processors carry out data processing operations accordingly.

10 Data breach notification

The data controller must notify the SIC about security incidents involving the violation of security codes or risks to the management of personal data that can affect the confidentiality, availability, and integrity of personal data of Colombian residents.

There is no defined statutory threshold, such as the number of affected individuals, type of data, or likelihood of risk, that triggers notification obligations.

Regulations from the SIC set forth that data breaches should be reported within 15 business days after the detection that personal data of Colombian residents was affected.

11 International data transfers

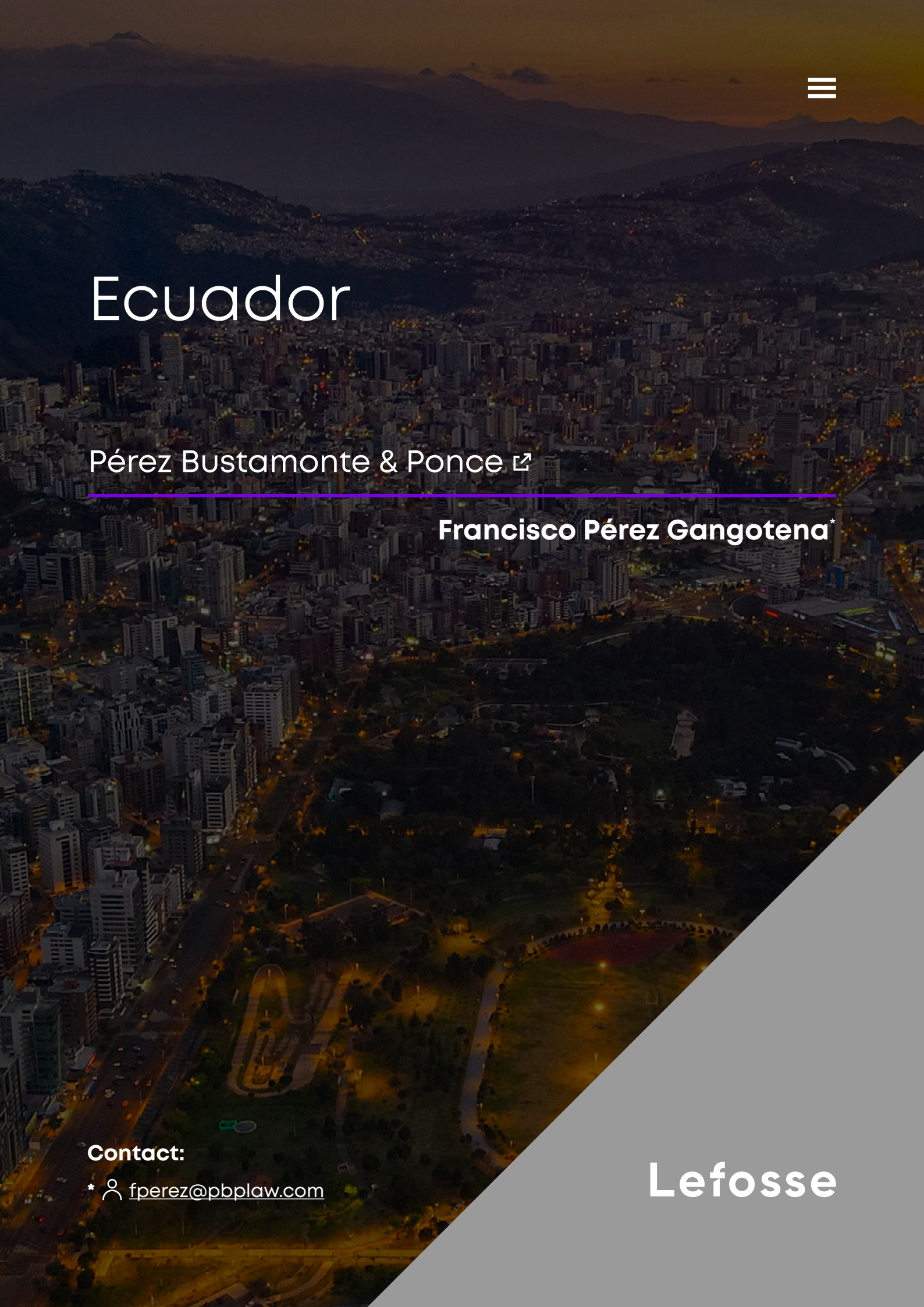
International transfers are permissible under two conditions: (i) obtaining the data subject's prior, express, informed, and unequivocal consent; and (ii) executing a personal data transfer agreement with the data processor, providing for the proper use, confidentiality, security, integrity, and availability of the personal data.

The CGDP prohibits the transfer of personal data to jurisdictions lacking adequate data protection levels, unless the data subject has provided his/her prior, express, and informed consent. A jurisdiction's adequacy for personal data protection is determined by the SIC through a 'declaration of conformity,' similar to the adequacy decisions in the EU or the UK.

The SIC has presented a list of countries it considers to provide adequate levels of protection. Said list includes EU member states, countries recognized by the EU as having an adequate level of data protection, and the following countries: Mexico, the Republic of Korea, Costa Rica, Serbia, Peru, Norway, Iceland, and the US.

12 Penalties

Non-compliance with the CGDP can result in administrative penalties, including: (i) fines of up to 2,000 minimum monthly legal wages (approximately US$575,000); (ii) suspension or temporary cessation of personal data processing operations; and (iii) immediate and permanent cessation of personal data processing operations. The CGDP does not distinguish between data controllers and data processors for purposes of applying penalties. The SIC imposes penalties on a case-by-case basis.



Ecuador

Pérez Bustamonte & Ponce

Francisco Pérez Gangotena*

Contact:

* fperez@pbplaw.com

Lefosse

1 Legislation: local laws applicable to data protection

In Ecuador, the protection of personal data is regulated by the Organic Law on Personal Data Protection ("**Ecuadorian Data Protection Law**") and the regulation to said law ("**Regulation**"), which was issued on November 6, 2023, and became effective on November 13 of the same year.

2 Jurisdiction: territorial applicability

The Ecuadorian Data Protection Law provides for extraterritorial application in the following situations:

- when there is processing of personal data related to data subjects residing in Ecuador by a controller or processor not established in Ecuador, if the processing activities are related to: (i) the offer of goods or services to data subjects, whether they are paid or free; and (ii) the control of data subjects behavior, to the extent that it takes place in Ecuador;
- when the controller or processor of personal data not located in Ecuador is subject to the national law by virtue of a contract or regulations provided by public international laws.

Regarding the territorial scope, Article 2 of the Regulation broadens the application of the Law, as shown in the table below:

Ecuadorian Data Protection Law	Regulation
1. Processing of personal data is carried out in Ecuador.	It expands the first assumption of the Law by providing the following: *"data controllers and processors of personal data of data subjects not residing in Ecuador, when their processing activities are carried out in national territory."*

Ecuadorian Data Protection Law	Regulation
2. When the data controller and/or data processor is domiciled or headquartered in Ecuador.	
3. When the data subject is located in Ecuador, but the controller and/or processor are not established in Ecuador in case the processing activities are related to: **a.** The offer of goods or services to such data subjects. **b.** Control of the behavior of the data subjects	
4. When the controller and/or processor are not established in Ecuador, but are obliged to comply with regulations by: **a.** A contract **b.** Rules of public international law	The Regulation expands the fourth scenario provided by the Law by mentioning the following: *"data controllers and processors of personal data not established in Ecuadorian territory to whom national legislation is applicable by virtue of a contract or current regulations of public international law."* In these cases, a legal representative must be appointed.

3 Scope: information protected under data protection legislation

The Ecuadorian Data Protection Law safeguards all data that directly or indirectly identifies or makes an individual identifiable. This includes personal data such as name, image, genetic data, health information, ethnicity, political affiliations, among others.

4 Definition of sensitive or special category data

The Ecuadorian Data Protection Law sets forth special categories of personal data, such as sensitive data, data of children and adolescents, credit data, health data and data of persons with disabilities.

The Ecuadorian Data Protection Law provides a broad definition of sensitive data, comprising the following information: ethnicity, gender identity, cultural identity, religion, ideology, political affiliation, judicial past, migratory condition, sexual orientation, health, immigration status, sexual orientation, health, biometric data, genetic data, and those whose improper processing may give rise to discrimination or infringe fundamental rights and freedoms.

5 Supervisory authority

The supervisory authority is the Superintendence of Personal Data Protection ("**Ecuadorian Superintendence**"), which was elected on March 28.

6 Obligations and requirements for compliance

To comply with the Ecuadorian Data Protection Law, organizations must observe, at least, the following obligations when handling personal data:

- process personal data in strict accordance with the principles and rights provided in the Ecuadorian Data Protection Law, or in the regulations issued by the Ecuadorian Superintendence;
- apply and implement appropriate administrative, technical, physical, organizational, and legal requirements and tools, to ensure and demonstrate that the processing of personal data is carried out in accordance with the provisions of the Ecuadorian Data Protection Law and its regulations;
- apply and implement verification processes, evaluation, periodic assessment of efficiency and effectiveness of administrative, technical, physical, organizational requirements and tools, and legal provisions implemented;
- implement personal data protection policies related to the processing of personal data;

- use risk analysis and management methodologies adapted to the particularities of the personal data processing activities and the parties involved;
- carry out security adequacy assessments before processing personal data;
- notify the Ecuadorian Superintendence and the data subjects about violations of the implemented security measures for personal data processing, in accordance with procedure provided for this purpose;
- implement personal data protection by design and by default;
- sign confidentiality agreements on the proper handling of personal data with the manager and personnel responsible for processing personal data or those who have access to personal information;
- ensure that the responsible for processing personal data provides sufficient mechanisms to guarantee the right to personal data protection in accordance with the provisions of the Ecuadorian Data Protection Law and its regulations;
- register and keep the National Registry for the Protection of Personal Data updated;
- designate the personal data protection delegate, when required;
- allow and contribute to the performance of audits or inspections by an auditor accredited by the Ecuadorian Superintendence.

Furthermore, organizations must ground a personal data processing activity on one of the following legal bases: consent of the data subject, legal obligation, fulfillment of a court order, public interest, execution of pre-contractual measures at the request of the data subject, compliance with contractual obligations, vital interests, publicly accessible databases, and legitimate interest of the data controller or third party.

7 Data Protection Officer (DPO)

Organizations should appoint a data protection delegate in specific situations, for example:

- when the processing activity is carried out by an entity within the public sector;
- when the processing activities demand a permanent and systematized control, considering factors such as the volume and nature of the processed personal data;
- when there is large-scale processing or special categories of data;
- when the processing does not refer to data related to national security and defense of the State that are not confidential or secret, in accordance with the provisions of the specialized regulations on the subject.

In addition, the Ecuadorian Superintendence may provide new conditions requiring the appointment of the data protection delegate.

Business groups may appoint a single personal data protection delegate, as long as he/she is able to carry out the activities without creating a conflict of interest.

Requirements to be a delegate:

- to be in enjoyment of political rights;
- be of legal age;
- hold a third level degree in Law, Information Systems, Communication, or Technology;
- to prove professional experience of at least five years.

Without prejudice to other aspects defined by the Ecuadorian Superintendence, the following persons may not be personal data protection delegates:

- those who are part of the management bodies (general manager, president, directors) and control of the responsible and in charge;
- partners or shareholders of the data controller and data processor;
- the spouses of the administrators, directors, or commissioners of the company;
- those who have conflicts of interest with the person responsible and in charge, for which the Ecuadorian Superintendence will issue the corresponding regulation establishing the specific cases that would give rise to such conflict of interest.

For the organizations of the public sector, the Ecuadorian Superintendence will define the incompatibilities to be a personal data protection delegate for each case.

8 Data subjects' rights

The Ecuadorian Data Protection Law provides the following rights for data subjects:

- **Right to be informed:** data subjects have the right to receive clear information about how their personal data is processed.
- **Right to access:** data subjects may request access to their personal data held by data controllers.
- **Right to rectification and update:** data subjects may request the correction of inaccurate or incomplete data.
- **Right to deletion:** data subjects may request the deletion of their personal data when it is no longer necessary, consent is withdrawn, or processing is unlawful.
- **Right to object:** data subjects may oppose the processing of their personal data for specific purposes, including direct marketing.

- **Right to portability:** data subjects have the right to receive their personal data in a structured, commonly used format and transmit such data to another controller.
- **Right to suspend processing:** data subjects may request a temporary suspension of the processing of their data under certain circumstances.
- **Right not to be subject to a decision based solely or partially on automated decisions:** data subjects may object to decisions made about them based only on automated processing.
- **Right to consultation:** data subjects may consult with the Ecuadorian Superintendence about their rights and the processing of their personal data.
- **Right to digital education:** data subjects have the right to be educated about digital literacy and data protection to understand and exercise their data protection rights effectively.

9 Security requirements

Security measures must be implemented across the following areas: physical, technological, organizational, administrative, and legal.

The Ecuadorian Data Protection Law generally recommends the following technical measures:

- anonymization, pseudonymization or encryption of personal data;
- measures aimed at maintaining the confidentiality, integrity, and permanent availability of personal data processing systems and services and access to personal data in a rapid response in case of security incidents;
- measures aimed at improving technical, physical, administrative, and legal frameworks (or systems);
- entities responsible for processing personal data can adopt international standards to effectively manage risks, ensuring the protection of rights

and freedoms. They can also implement and manage information security systems or follow codes of conduct that have been recognized and authorized by the Ecuadorian Superintendence.

10 Data breach notification

- **Notification to the authority:** the controller must report a personal data security breach to the Ecuadorian Superintendence and the Telecommunications Regulation and Control Agency as soon as possible, within a period of five (5) days after the controller or processor have become aware of it, unless such breach of security is unlikely to cause a risk to the rights and freedoms of the data subjects. If the notification to the Ecuadorian Superintendence does not occur within the abovementioned term, it must be accompanied by an indication of the reasons for the delay.
- **Notification to the data subject:** the controller must notify without delay the security violation of personal data to the data subject when it entails a risk to his/her fundamental rights and individual freedoms, within a period of three (3) days from the date on which the controller became aware of the risk.

11 International data transfers

As a general principle, personal data can be transferred to countries, organizations, and legal entities that offer adequate levels of protection and adhere to internationally recognized standards, thereby fulfilling the obligation to comply with and guarantee these standards. The Ecuadorian Superintendence will issue a resolution listing which countries provide an adequate level of protection of personal data.

In the event of an international transfer of data to a country, organization, or international economic territory that has not been qualified as having an adequate level of protection, such international transfer may be carried out if the controller or processor of the personal data provides adequate safeguards for the data subject. These safeguards include: (i) ensuring compliance with the principles, rights, and obligations in the processing of personal data to a standard equal to or greater than the existing Ecuadorian regulations; (ii) ensuring effective protection to the rights related to personal data; (iii) the right to seek full redress, where necessary.

In the event that none of the above two options can be applied, controllers or processors of personal data may submit to the Ecuadorian Superintendence binding

corporate rules, specific and applied to the scope of their activity. The Ecuadorian Superintendence will establish the procedures and format for such data transfers or communications by controllers, processors, and supervisory authorities.

For all those cases involving international transfers of personal data not contemplated above, the authorization of the Ecuadorian Superintendence will be required. The authorization may be granted as long as the data controller or data processor complies with one of the following:

- **that by means of a contract between the controller or processor and the recipient, the receiver undertakes, voluntarily and formally, to comply with the regulations and the Ecuadorian Superintendence; and**
- **that by means of a contract between the controller or processor and the recipient, the latter undertakes to comply with the applicable regulations, and that in the country or territory where the recipient is established, it guarantees the exercise of the rights of the data subjects.**

The Ecuadorian Data Protection Law provides exceptional cases where international data transfers may occur in the following events:

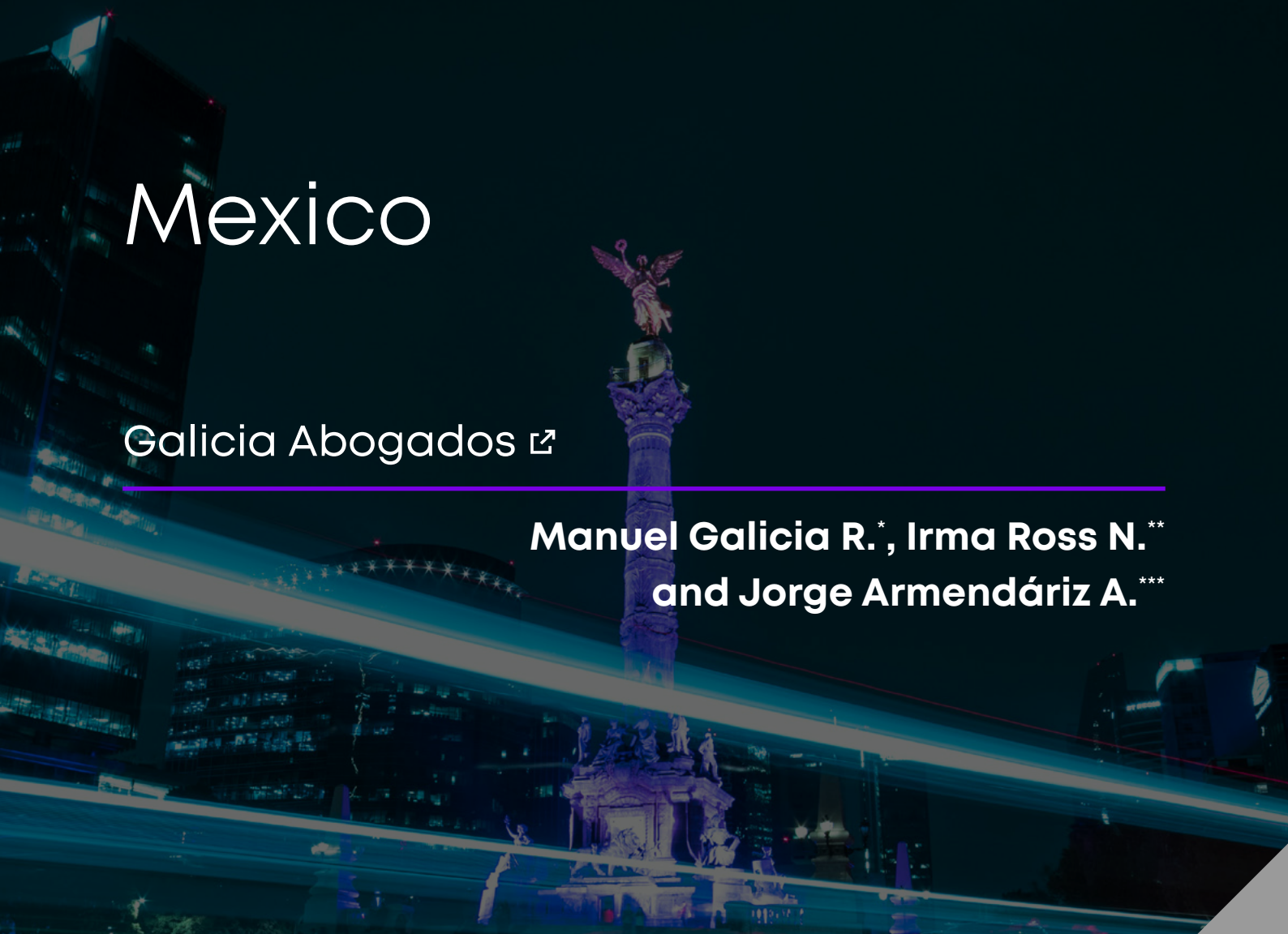
- **for the fulfillment of institutional competencies, in accordance with the applicable regulations;**
- **by explicit consent to the proposed transfer or disclosure, after having been informed of the potential risks;**
- **when the purpose is to comply with a legal or regulatory obligation;**
- **for the execution of a contract or pre-contractual measures between the owner and the controller of the personal data;**
- **in the public interest;**
- **for international judicial collaboration;**
- **for cooperation in the investigation of infractions;**

- for international cooperation between States;
- for transfers of data in banking and stock exchange operations;
- for the formulation, exercise or defense of claims, administrative or jurisdictional actions and appeals;
- to protect the vital interests of the data subject, where the data subject is physically or legally incapable of giving his or her consent.

12 Penalties

The penalties in case of a violation of the rules and obligations provided by the Ecuadorian Data Protection Law vary, with minor offenses incurring fines ranging from 0.1% to 0.7% of the company's annual turnover from the previous fiscal year. For severe offenses, fines will range from 0.7% to 1%. The Ecuadorian Superintendence will determine the specific fine, adhering to the principle of proportionality.

Mexico



Galicia Abogados

Manuel Galicia R.*, Irma Ross N. and Jorge Armendáriz A.*****

Contact:

* mgalicia@galicia.com.mx

** iross@galicia.com.mx

*** jarmendariz@galicia.com.mx

Lefosse

1 Legislation: local laws applicable to data protection

In Mexico, the personal data protection laws have separate regulations for the private and public sectors (together, the "**Data Protection Regulations**"):

- **Private sector:** Federal Law on the Protection of Personal Data held by Private Parties (in Spanish, *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, "**FLPPDPP**").
- **Federal public sector:** General Law on the Protection of Personal Data held by Obligated Parties (in Spanish, *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados* "**GLPPDOP**").

Regarding the public sector, each Mexican federative entity (state), in accordance with its territorial jurisdiction, has its own regulations for the protection of personal data processed by any state, which must be in line with the provisions of the GLPPDOP.

Regarding credit information societies and their processing of personal data, the applicable law is the Law for the Regulation of Credit Information Societies (in Spanish, *Ley Para Regular las Sociedades de Información Crediticia*).

2 Jurisdiction: territorial applicability

When a data controller (as defined hereinafter) not established in Mexico uses means located in the Mexican territory for the processing of personal data, the FLPPDPP is applicable (unless such means are limited to transit purposes that do not involve personal data processing). Therefore, the controller might be required to comply with the obligations set out by the Data Protection Regulations with respect to the processing of personal data. Moreover, the Data Protection Regulations oversee the transfer of personal data by a data processing entity to international entities.

3 Scope: information protected under data protection legislation

The Data Protection Regulations are only applicable to data pertaining to individuals, including employees, customers, representatives, or contractors, which is under the control of an individual or corporation, expressly excluding data from legal entities.

Under the Data Protection Regulations, personal data is any information concerning a specifically identified or identifiable individual (a "**Data Subject**"), including his/her

image and voice pattern. The Data Protection Regulations apply to all processing of personal data, regardless of its form or the medium in which it is held. Moreover, processing is defined as the set of activities that the individual or corporation deciding on the data processing (a "**Data Controller**") may carry out with respect to personal data, ranging from the retrieval or collection, use, disclosure, and storage of personal data by any means, whereas use is defined as covering any action of access, management, exploitation, transfer, or disposal of personal data.

4 Definition of sensitive or special category data

The Data Protection Regulations define Sensitive Personal Data as: "*Personal data that may impact the most intimate sphere of the Data Subject, or which its improper use may give rise to discrimination or entail serious risk to the individual. Specifically, sensitive data is considered to encompass data that can disclose aspects such as racial or ethnic origin, current and future health status, genetic information, religious, philosophical, and moral beliefs, union membership, political opinions, and sexual orientation.*"

5 Supervisory authority

The National Institute for Transparency, Access to Information and Personal Data Protection (in Spanish, *Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*, "**INAI**") is the national authority that supervises the processing of personal data and the corresponding compliance with de Data Protection Regulations. Locally, each Mexican federative state has its own Personal Data Protection Institute for the supervision of personal data processing under state regulations.

6 Obligations and requirements for compliance

Prior to processing personal data, Data Controllers must provide Data Subjects a privacy notice containing, among others: (i) information regarding the processed personal data; (ii) the purposes of processing; (iii) the mechanisms through which Data Subjects may access, rectify, cancel, and oppose or limit the use and disclosure of their personal data (ARCO rights); (iv) any potential transfers of data and the purpose of said transfers; (v) the use of cookies, when applicable; and (vi) the means through which Data Controller will notify any amendments to the privacy notice.

Data Controllers must implement adequate physical, administrative, and technological security measures to ensure the integrity and confidentiality of personal data. When a Data Controller that is not established in Mexico uses means located in the Mexican territory, the FLPPDPP shall apply (unless such means are limited to transit purposes that

do not involve personal data processing). Therefore, the Data Controller might be required to comply with the obligations imposed by the Data Protection Regulations with respect to the processing of personal data and, consequently, the reporting of security breaches. More specifically, the Data Protection Regulations provide the obligation for Data Controllers to immediately report data security breaches that materially affect the property or moral rights of Data Subjects, so that the latter can take appropriate action to defend their rights.

7 Data Protection Officer (DPO)

Data Controllers must appoint a data protection officer or set up a department in charge of the protection of personal data in Mexico. The main responsibilities of the personal data officer or department include the establishment and management of mechanisms for receiving, processing, monitoring, and addressing ARCO Rights (i.e., access, rectification, cancellation, and opposition) requests, and handling complaints or requests submitted by Data Subjects related to the implementation of internal privacy policies.

8 Data subjects' rights

Data Subject's rights in Mexico are described as follows:

- **Access right.** Data Controllers must implement mechanisms that enable Data Subjects to access their personal data, as well as any information regarding the terms and conditions under which the Data Controller processes such personal data.

- **Rectification right.** When a Data Subject identifies that his/her personal data processed by a Data Controller is inaccurate, he/she may request rectification or correction of such personal data. The relevant rectification request must indicate the personal data to be rectified, as well as the correction to be made, supported by the necessary documentation.

- **Cancellation right.** Data Subjects may request the Data Controller to cease the processing of their personal data. Data Controllers must block (prevent the processing or possible access by any person, except for the storage) the personal data for a period of fifteen days and then, if applicable, delete such personal data, as per the regulations to the FLPPDPP.

- **Objection right.** Data Subjects may, at any time, object to the processing of their personal data or request Data Controllers to cease such processing. Data Controllers may implement internal exclusion lists setting forth identified Data Subjects who have objected to the processing of their personal data, the specific matter of such objection and the processing activities to which such Data Subject has objected. Data Controllers must inform Data Subjects when their information has been uploaded to the relevant exclusion list.

9 Security requirements

The Data Protection Regulations set out certain obligations for Data Controllers in relation to security, including maintaining appropriate information security measures and notifying Data Subjects of security breaches. Specifically, Data Controllers must establish and maintain physical, technical, and administrative security measures designed to protect personal data from damage, loss, alteration or destruction, or unlawful use, access, or processing.

- Administrative security measures must include mechanisms aimed at maintaining the security of personal data at any level within the organization as well as training programs for staff members who manage personal data. These actions must be conducive to the identification and correct classification of personal data and the people having access to the said data.

- Physical security measures must include such actions and tools (whether technological or not) that prevent unauthorized access and use of personal data, prevent unauthorized access to mobile devices inside or outside the facilities of the Data Controller and guarantee the elimination of the personal data in a secure manner. Physical security may include, among others, the implementation of alarms and security lighting as well as controls for access to premises.

- Technical security measures must be implemented through technological instruments that ensure safe access to the databases only by authorized users. Technological security measures must guarantee that access to the

relevant databases will be limited to previously identified staff with appropriate clearance.

10 Data breach notification

While official reporting of personal data breaches to the INAI is not covered by the Data Protection Regulations and, thus, not mandatory, the Data Protection Regulations require Data Controllers to communicate such breaches to the affected Data Subjects when the breach causes significant harm to the economic or moral rights of such individuals. Individuals' notification usually takes place after a contention period (i.e., the phase to limit the scope or impact of the identified incident), and before any mitigation procedures are enabled (i.e., the period or phase seeking to minimize the possibility of a breach being repeated).

Harm to economic rights, as described in the INAI's recommendations, occurs when the breach involves personal property, tax information and credit records, income and outcome, bank accounts, insurance, retirement plans, bonds, and financial services. Moral rights, on the other hand, are harmed when the breach relates to feelings, emotions, beliefs, honor, reputation, private life, physical configuration and aspect, opinions of self from others, or when liberty and the physical and psychological integrity of a person is illegitimately impaired.

11 International data transfers

International data transfers are not *per se* prohibited under the Data Protection Regulations. All transfers of personal data, however, are subject to the consent of the relevant Data Subjects, except for limited cases. Data Controllers must inform Data Subjects about data transfers through the relevant privacy notice. Transfers must be limited to the purposes described in the privacy notice and the Data Controller must provide to the data recipient the privacy notice to which Data Subjects consented in connection with the processing of their personal data, for the purposes set forth therein.

All data transfers, domestic and international, must be documented. Data Controllers and data recipients must enter into a data transfer agreement in which the recipient acquires the same data processing obligations as those imposed to the Data Controller by the data protection legal framework. Additionally, the agreement must contain the terms under which Data Subjects consented to the processing of their personal data.

12 Penalties

Regarding the processing of personal data by private parties, penalties include the following, in accordance with the violation to the regulations of the FLPPDPP:

- notice or warning by the authority to the Data Controller to seek its compliance with the corresponding regulations;
- a fine ranging from 100 to 160,000 days of the current minimum salary in Mexico City (from USD 1,200 to USD 1,900,000 approximately);
- a fine ranging from 200 to 320,000 days of the current minimum salary in Mexico City (from USD 2,400 to USD 3,800,000 approximately);
- if the violations persist, an additional fine ranging from 100 to 320,000 days of the current minimum salary in Mexico City will be imposed (from USD 1,200 to USD 3,800,000 approximately). In the case of violations regarding Sensitive Personal Data, the fines may increase to double the established amounts.

When imposing fines to private parties, INAI considers the nature of the data being processed, the intentional nature of the action or omission constituting the violation, and the financial position of the Data Controller.

Regarding the processing of personal data by governmental entities, penalties include public notice or warning, or a fine ranging from 150 to 1,500 units of measurement and update (from USD 900 to USD 9,000 approximately).

When imposing fines to obliged subjects, INAI considers the severity of the violation, the financial position of the Data Controller and the repeated offense (which may carry a fine of up to double the original fine).

Paraguay

Ferrere

Montserrat Puente*

Contact:

* mpuente@ferrere.com

Lefosse

1 Legislation: local laws applicable to data protection

The Paraguayan Constitution (1992) incorporated to the Paraguayan legal system the Habeas Data legal figure (Article 135), which assures everyone the right to judicially request the updating, rectification, or destruction of erroneous personal data or data that illegitimately affects a person's rights that is in official (public) or private publicly accessible records (such as credit information bureaus).

Additionally, since 2020 there is a specific data protection-related law, i.e., Law No. 6534/2020 "On the Protection of Personal Credit Data ("**Law 6534/20**"). Law 6534/20 aims to ensure the security and privacy of individuals' financial information.

There is a bill under study in Congress, specifically focused on the protection of personal data, aiming to provide even stronger safeguards for individuals' privacy rights. The bill follows the framework set by the GDPR. Currently, the different commissions are issuing their comments and suggestions. At the moment, it is not possible to predict when the bill will be voted on by Congress.

2 Jurisdiction: territorial applicability

Law 6534/20 is mandatory for the processing of personal data whenever personal data is either collected or stored in Paraguayan territory.

Because of its public order status, the provisions of Law 6534/20 may not be waived by the data controller, whenever personal data is collected or stored in the Paraguayan territory. Any infringement thereof would initially be prosecuted through an administrative procedure before the data protection pertinent authority.

3 Scope: information protected under data protection legislation

Law 6534/20 protects personal credit data of all persons, regardless of their nationality, residence, or domicile. It also regulates the collection and access to credit information data, as well as the incorporation, organization, operation, rights, obligations, and termination of companies that are dedicated to obtaining and providing credit information (i.e., credit bureaus). Law 6534/20 aims to preserve the fundamental rights, privacy, informational self-determination, freedom, security, and fair treatment of people, in accordance with the Constitution and international instruments which Paraguay is a signatory of.

Law 6534/20 is also applicable to the processing of personal data (Article 2), whenever collected or stored in the Paraguayan territory. Law 6534/20 is applicable regardless of the mechanisms being used for data processing (for example, public or private regis-

tries, information systems, archives, physical, electronic, or digital records or databases through manual, automated, or partially automated data collection mechanisms).

4 Definition of sensitive or special category data

Under Law 6534/20, data is classified into these three categories:

- **Personal Data:** Any type of information referring to legal entities or individuals that can be used for identification by means of an identifier or by one or more characteristic elements of the individual's physical, physiological, genetic, psychological, economic, cultural, or social identity.
- **Sensitive Personal Data:** Refers to any information related to the intimate aspects of an individual's life. This includes data whose improper handling could lead to discrimination or pose a significant risk to the individual. Such data encompasses details that may reveal racial or ethnic origin; religious, philosophical, and moral beliefs; union membership; political opinions; and aspects related to health, sexual preferences or orientation. It also includes genetic and biometric data specifically aimed at uniquely identifying a person.
- **Personal Credit Data:** Encompasses all information related to the credit history of individuals and legal entities, and their credit, commercial, and other activities of a similar nature, which serves to identify the person, their domicile, commercial activity, determine their level of debt, compliance with their obligations and, in general, credit risks at a given time.

5 Supervisory authority

According to Law 6534/20, there are two authorities responsible for supervising the processing of personal data and/or its compliance with said law.

The Secretary of Consumer Defense ("**SEDECO**", by its Spanish acronym) is responsible for supervising the processing of personal data. The responsibilities of the SEDECO under this law and related consumer protection regulations include:

- ensuring compliance with the provisions of the law and other relevant consumer and user protection laws and regulations;
- disseminating consumer rights and responsibilities and carrying out informational and educational activities for consumers;
- promoting market formalization to prevent data subject vulnerability;
- developing, implementing, and promoting consumer education and information programs through mass media and other available means;
- receiving and processing consumer concerns, complaints, and reports, and channeling them through the Central Bank of Paraguay;
- authorizing inspections and investigations related to Law 6534/20;
- requesting reports and opinions form entities regarding consumer and user protection regulations;
- maintaining a National Registry of Complaints, Inspections, and Violators, in coordination with the Central Bank of Paraguay;
- collaborating with local authorities responsible for consumer protection;
- conducting and promoting research in the field of consumer protection;
- seeking, through legal channels, the assistance of law enforcement, or any necessary measures to fulfill its functions;
- exercising other powers and duties as provided for by the SEDECO's organic law, which apply to the scope of consumer and user protection.

The Central Bank of Paraguay ("**BCP**", by its Spanish acronym), through the Banking Superintendency, has the following powers and functions in connection to Law 6534/20:

- register Credit Information Societies;
- regulate, interpret, and enforce the law concerning credit information, as well as approve the operating protocol of Credit Information Bureaus –

companies dedicated to providing credit reference services;

- supervise the mechanisms for storing and using credit information data by Credit Information Bureaus and entities regulated by the BCP;
- impose sanctions on Credit Bureaus.

6 Obligations and requirements for compliance

Under Paraguayan law, all companies that collect personal data, whether on an occasional or regular basis, must comply with the following obligations:

- **Informed Consent.** Companies must obtain informed consent from the data subject. This consent must be explicit and unequivocal, under conditions that leave no doubt about its granting, and must be recorded in writing, electronically, digitally, or through another mechanism. The processing and transfer of personal data are unlawful when the data subject has not provided his/her free, explicit, and conscious consent.
- **Data Deletion.** Organizations must delete personal data within 5 years of the date of collection.
- **Duty of Secrecy.** Those responsible for, or in charge of, the processing of credit data, as well as those involved in any phase of data collection, processing, storage, use, or circulation for credit purposes, are obliged to keep the information confidential unless it needs to be disclosed by competent authority with a court order.
- **Access to Collected Information.** If requested by the data subject, the information must be provided in a clear and understandable manner, free from coding, and, if necessary, accompanied by an explanation in accessible language. Additionally, the information must cover the entirety of the data related to the data subject, even if the request only pertains to a specific aspect of the personal data.

Furthermore, Credit Information Bureaus must comply with the following obligations:

- handle information with ethics, confidentiality, and security;
- protect credit information from loss or alteration;
- report information requested by data subjects without changes;
- rectify data upon request from the source or the data subject;
- redirect complaints to the data sources when the bureau is not responsible for fulfilling the complaint;
- keep the record of positive and negative credit data up to date;
- delete expired information according to the law;
- provide the complete credit history upon the data subject's request within 24 hours from the request, if it is not immediately available;
- do not disclose data on debts that are: (i) overdue and unclaimed for more than 3 years; (ii) canceled immediately upon notification; or (iii) subject to creditor's meeting judgments after 5 years from the judicial resolution.

These obligations are illustrative rather than exhaustive, allowing for the possibility of new obligations to emerge either at the request of the BCP or through the introduction of new regulations.

7 Data Protection Officer (DPO)

Under current legislation in Paraguay, there is no requirement for organizations to appoint a Data Protection Office.

8 Data subjects' rights

Law 6534/20 recognizes the traditional ARCO rights (Access, Rectification, Cancellation and Opposition), plus the right to transparency of information, the right to erasure (right to be forgotten), and the right to data portability.

All individuals subject to a process of collection, processing, or storage of their personal and/or credit data, have the following rights:

- **Right to be informed.** Law 6534/20 grants all persons the right to be informed expressly and clearly about the purpose of the processing of their personal data.
- **Right to access.** Law 6534/20 guarantees to all persons (individuals or legal entities) the right to access the information and data about themselves, about those who are under their parental authority and about people who prove to be under their guardianship or care, as well as their assets, which are in official records or private databases of a public nature or in entities that provide information on economic solvency and financial situation.
- **Right to rectification.** Data subjects have the right to request the data controller the updating, rectification, or elimination of illegal, inaccurate, or incomplete information. Rectification must be carried out without any charge for the data subject and without undue delay.
- **Right to erasure.** Law 6534/20 provides that data subjects have the right to obtain the erasure or aggregation of their personal credit information after 5 years.
- **Right to object/opt-out.** The law provides that data subjects may oppose the processing of their personal data.
- **Right to data portability.** Law 6534/20 entitles data subjects or their representatives to request the controller the portability of their personal data.

9 Security requirements

Law 6534/20 provides that data controllers must ensure the adoption and implementation of technical, organizational, and security measures necessary to safeguard the access and integrity of personal data, in order to avoid its alteration, loss, consultation, commercialization or unauthorized access.

10 Data breach notification

Although Law 6534/20 provides that "*the incomplete, late, or defective notification of a breach of security of personal data or credit information*" is considered a violation of the law, the notification process has not yet been duly regulated.

Resolution No. 3/2023, issued by the BCP, provides that credit bureaus must report within 24 hours, to the Superintendency of Banks, the corrective actions taken when there have been violations to the security codes and risks in the administration of the information of data subjects.

11 International data transfers

Law 6534/20 provides that international data transfers are lawful, provided that the jurisdiction of destiny has adopted protection measures similar to the ones foreseen in local regulation. Nevertheless, the provision of the law is too concise, and further regulation is required.

Until the matter is duly regulated, consent shall suffice, provided that the jurisdiction of destiny has adopted adequate security standards. If future regulation imposes additional conditions or requirements on international data transfer, regulation shall also contemplate an adaptation period. However, it is not possible to foresee when the regulatory agencies will address this matter.

12 Penalties

Law 6534/20 sets out a series of sanctions for those who fail to comply with its provisions. The Supervisory Authorities may impose the following sanctions on those responsible for and entrusted with the processing of personal data:

- **Warnings.**
- **Fines** (up to approx. USD 195,000. Fines are calculated based on the following parameters: (i) nature of the infringement; (ii) seriousness of the riks or damage caused; (iii) benefit or gain, obtained as a consequence of the infringement; (iv) the timely acknowledgment of the infringement; (v) repairing/amending the infringement by the entity's own initiative; (iv) previous conducts of the entity. In the event of a recurrence of the same offense, the initial fine will be doubled and may be raised up to approx.

USD 650,000 for the legal entity that registers an annual turnover of more than G. 6,000,000,000 (Guaraníes six billion) – approx. USD 925,000).

- **Suspension of activities related to data processing.**
- **Disqualification of the offender** from holding positions, offices, or commissions within the financial, credit, and personal data information societies.
- **Temporary closure of operations related to data processing** following suspension if the corrective measures ordered by the supervisory authority have not been adopted.
- **Immediate and definitive closure of operations** involving the processing of sensitive data.

It is important to note that these administrative sanctions are independent of the corrective or precautionary measures that supervisory authorities may issue to protect the public interest and proper management of societies handling personal and credit information.

Sanctions are graded, considering various criteria, such as the nature of the offense, the severity of the danger or harm caused, the benefit obtained as a result of the offense, the timely acknowledgment of the facts, voluntary correction of the offense, and the prior conducts of the offender or the entity, considering sanctions imposed within the last 5 (five) years. Competent authorities will maintain a public register of sanctions for this purpose.

So far, SEDECO has sanctioned several companies, which are users of credit information services, for contravening the prohibition on using personal credit data for labour-related decisions. The penalties imposed to date range from warnings and the obligation to adopt improvement measures, to fines of around USD 8,000.

Finally, violations of Law 6534/20 prescribe within a period of 5 (five) years from the date they were committed. In cases where the offense consists of an ongoing activity, the prescription period begins from the date of the last action.

Peru

Rodrigo, Elias & Medrano Abogados

Francisco Baldeón*

Contact:

* fbaldeon@estudiorodrigo.com

Lefosse

1 Legislation: local laws applicable to data protection

Personal data protection in Peru is mainly regulated by Law No. 2,9733 (the "**Peruvian Data Protection Law**"); its regulations, enacted by Supreme Decree No. 003-2013-JUS (the "**Regulations**"), and the Security Directive passed by the Peruvian Data Protection Authority, enacted by Resolution No. 019-2013-JUS/DGPDP (the "**Peruvian Directive**"). The Regulations will soon be amended, inasmuch as on August 26, 2023, the draft of the new Regulations was published by Ministerial Resolution No. 270-2023-JUS to receive comments from the citizens.

2 Jurisdiction: territorial applicability

Peru's data protection laws are applicable when: (i) the processing of personal data is performed in an establishment located in Peru belonging to the data controller; (ii) the processing of personal data is performed by a data processor on behalf of a data controller established in Peru; or, (iii) if the data controller established outside Peruvian territory makes use of means located in Peru for the processing of the personal data unless the only processing involved is the transit through Peru.

3 Scope: information protected under data protection legislation

Peruvian data protection laws protect personal data, which is defined as any information about an individual that identifies or makes said individual identifiable. It includes all numerical, alphabetical, graphic, photographic, sound, or any other type of information concerning an individual, which identifies or could be used to identify the individual through reasonable means.

4 Definition of sensitive or special category data

The Peruvian Data Protection Law defines sensitive data as personal data consisting of biometric data that by itself can identify the data subject; data referred to racial and ethnic background; income of an individual; political, religious, philosophical, or moral opinions or creed; union membership; and data related to health or sexual orientation.

Likewise, the Regulations of the Peruvian Data Protection Law define sensitive data as data related to physical, mental, and emotional characteristics, facts, or circumstances of emotional or family life, personal habits corresponding to the most intimate sphere of private life, data related to physical or mental health, among others that affect the intimacy of the data subject.

As a rule, the processing of sensitive data requires written consent.

5 Supervisory authority

The Peruvian Data Protection Authority (the "**DPA**") is the body in charge of enforcing data protection laws in Peru. The DPA may impose fines for non-compliance with Peruvian data protection laws.

6 Obligations and requirements for compliance

The Peruvian Data Protection Law provides the following principles that must be observed when processing personal data:

- **Principle of legality:** Data processing must be performed in accordance with the Peruvian Data Protection Law. Data collection carried out by fraudulent, dishonest, or illegal means is forbidden.

- **Principle of consent:** As a rule, data processing requires the data subject´s consent, although there are some exceptions for this requirement, such as the processing of data of public domain, or the processing of data to comply with legal obligations, to perform a contract or to protect data subject's interests. The Regulations provide that the processing of personal data requires the prior, free, informed, explicit, and unequivocal consent of the data subject.

  a) Free: Consent must be given freely, without errors, bad faith, coercion, or any form of willful misconduct that could influence the data subject's decision.

  b) Prior: Consent must be obtained before collecting personal data or, if applicable, before processing the data for a purpose other than the one for which it was originally collected.

  c) Explicit and unequivocal: Consent must be given under conditions that leave no doubt as to its provision. Clicking a digital button will be considered explicit and unequivocal consent, for example.

  d) Informed: The data subject has the right to be informed in detail, simply, expressly, unequivocally and prior to collecting, about the purpose for which his or her personal data will be processed; who will be or who may be the recipients, the existence of the database in which the personal data will be stored, as well as the identity and address of the data controller and, if applicable, the data processor of his/her person-

al data; the mandatory or optional character of his or her answers to the proposed questionnaire, especially concerning sensitive data; the transfer of personal data; the consequences of providing his or her personal data and of his or her refusal to do so; the time during which the personal data will be kept; and the possibility to exercise the A.R.C.O. rights provided by law (as defined below).

If personal data is collected online through electronic communication networks, the duty of information may be satisfied through the publishing of privacy policies, which must be easily accessible and identifiable.

Even if consent is not required (for example, when the data is necessary for the development, entering and compliance with a contractual relationship with the data subject, or when the data is of public domain), the duty of information must still be satisfied.

- **Principle of purpose:** Personal data must be collected for a determined, explicit, and lawful purpose. Data processing must not be extended to any purpose other than the one unequivocally determined at the time of collection, excluding the cases of activities of historical, statistical, or scientific value where a dissociation or anonymization procedure is applied.

- **Principle of proportionality:** Data processing must be adequate, relevant, and not excessive to the purpose for which the data was collected.

- **Principle of quality:** Personal data must be truthful, accurate, and, when possible, updated to ensure it is necessary, relevant, and adequate for the purpose of its collection. It should be securely stored only for the duration necessary to achieve the processing's purpose.

- **Principle of security:** Data controllers and those responsible for the processing must adopt technical, organizational, and legal measures necessary to ensure the security of the personal data they handle. The measures taken must ensure a level of security appropriate to the nature and purpose of the processed personal data.

- **Principle of adequate protection levels:** For cross-border transfers, personal data must be protected at a level sufficient and, at a minimum, comparable to the provisions of the Peruvian Data Protection Law or applicable international standards.

In addition, data controllers must comply with the following obligations when handling personal data:

- **Registration of databases:** Data controllers must register with the DPA their databases containing personal data and report the transfer of personal data abroad to the said authority.
- **Confidentiality:** Data controllers must keep the confidentiality of the personal data they hold.
- **A.R.C.O. rights:** Data subjects have the rights of access, rectification, cancellation, and opposition, which can be exercised with the respective data controller.
- **Data breaches:** According to the Peruvian Directive, data controllers must inform data subjects of data breaches that may affect their rights.

7 Data Protection Officer (DPO)

The Peruvian Data Protection Law does not require the appointment of a DPO for private sector entities.

8 Data subjects' rights

As per Peruvian laws, data subjects have the right:

- To be informed about the data processing and access information processed about themselves.
- To update, include, rectify, or delete incomplete or incorrect data about themselves, as well as when the data is no longer necessary for its collection purpose or the term determined for the data processing has expired.
- To prevent disclosure of their personal data, for legitimate reasons.
- To oppose the processing of their personal data in situations where there is no law requiring the data processing, there are legitimate reasons to op-

pose the processing, or the data was obtained from public sources, without the data subject's consent.

9 Security requirements

Data controllers and those responsible for the processing of personal data must adopt technical, organizational, and legal measures necessary to ensure the safety of the personal data they hold or process. The measures taken must ensure a level of security appropriate to the nature and purpose of the processing and personal data involved. The Peruvian Directive sets forth the security standards for the processing of personal data, providing different standards depending on the features of the database.

The relevant criteria are the: (a) number of data subjects whose data are stored in the database; (b) number of fields of the database (for example, name, address, phone number), (c) existence of sensitive data, and (d) data controller of the database (an individual or entity).

10 Data breach notification

The Peruvian Directive regulates data breach notifications. On this regard, the data controller must inform the data subjects of any incident that significantly affects their property or moral rights as soon as the occurrence of the incident is confirmed. The minimum information required in the notice are: (a) description of the incident; (b) disclosed personal data; (c) recommendations to the data subject; and (d) implemented corrective measures.

The data controller must keep documentation of all breaches, including: (a) date and time of the incident; (b) name of the person that reports the incident; (c) detailed description of the incident; (d) disclosed personal data; (e) name of the persons involved in solving the incident; (f) consequences of the incident; (g) implemented corrective measures; (h) recommendation to the data subject; (i) if the data has been recovered; and, (j) in case of data recovery, name of the person that recovered the data, description and date of the recovered data, and description of the manually recovered data, as the case may be.

The Peruvian laws do not provide specific obligations of notifying the DPA in case of data breaches.

11 International data transfers

The following are the main rules that apply to cross-border transfers:

- The exporter must have obtained the data subject's consent to perform the cross-border transfer of their personal data or rely in an exemption to consent (for example, when the data transfer is necessary for the development, entering and compliance with a contractual relationship with the data subject).
- The data subject must be informed of the cross-border transfer, the purposes of the transfer of his/her data, and the type of activity that will be developed by the recipient. Data subjects must be informed of the recipient's identity and, if such recipient is a data processor (for example, cloud storage providers), of its address.
- Cross-border transfers are permissible when the recipient agrees to fulfil all responsibilities previously held by the data exporter as the data controller, which can be done through contractual means.
- Exporters of personal data must refrain from making cross-border transfers of personal data if the destination country does not provide adequate data protection levels.

If the destination country fails to provide adequate protection levels, the data exporter must ensure that the processing of personal data meets adequate protection levels (for example, through contractual clauses and/or codes of conduct for business groups). This does not apply if, among other cases, (a) the data subject has given his/her prior, informed, express and unequivocal consent to the transfer of data under such circumstances; or, (b) the cross-border transfer of personal data is needed for the performance of a contractual relationship in which the data subject is a party.

Note that no specific list of countries (whitelist) with adequate protection levels has been published by the DPA.

Data controllers must report international transfers of personal data abroad to the DPA.

12 Penalties

The infractions that are typified by Peruvian data protection laws are the following:

Minor infractions:

(i) Processing personal data in breach of the security measures determined in the Peruvian Data Protection Law and its Regulations.

(ii) Collecting personal data that is not necessary, appropriate, or adequate in connection to the specific, explicit, and lawful purposes for which they are obtained.

(iii) Not modifying or rectifying personal data when it is known to be inaccurate or incomplete.

(iv) Not deleting personal data when it is no longer necessary, relevant, or adequate for the purpose for which they were collected or when the time for their processing has expired, except for cases where a dissociation or anonymization procedure has been applied.

(v) Not registering databases or updating them with the Peruvian Data Protection Registry.

(vi) Processing data in contravention of the provisions of the Peruvian Data Protection Law and its Regulations.

Serious infractions:

(i) Failing to comply with, obstructing, or hindering the exercise of data subject´s rights in accordance with the provisions of the Peruvian Data Protection Law.

(ii) Processing personal data without the free, express, unequivocal, prior, and informed consent of the data subject, when such consent is required in accordance with the Peruvian Data Protection Law and its Regulations.

(iii) Processing sensitive data in breach of the security measures set forth in the Peruvian Data Protection Law and its Regulations.

(iv) Collecting sensitive data that is not necessary, appropriate, or adequate in connection to the specific, explicit, and lawful purposes for which they are obtained.

Very serious infractions:

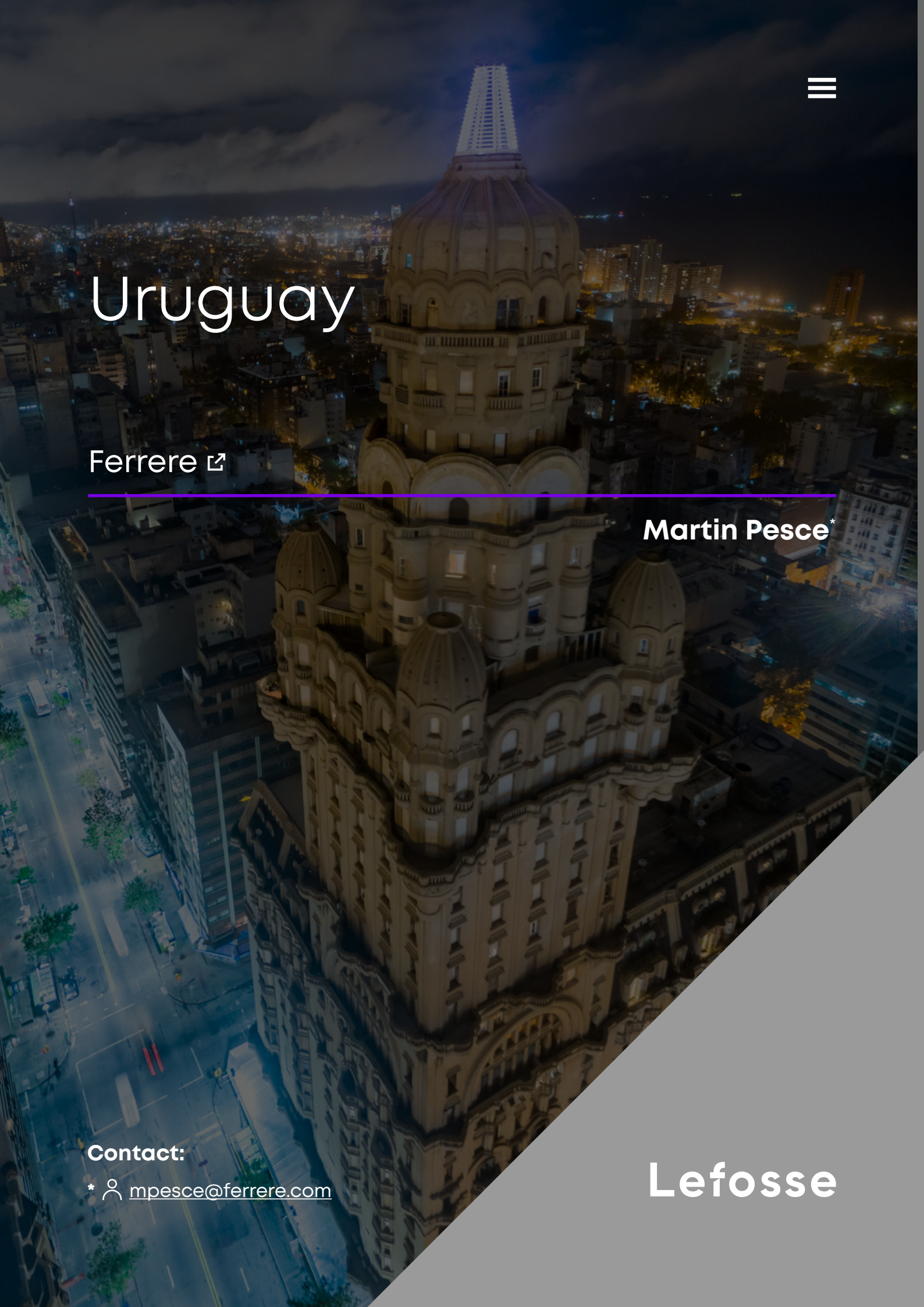
(i) Processing personal data in a manner that violates the obligations set forth in the Data Protection Law and its Regulations, and that either hinders the exercise of other fundamental rights or directly violates them.

(ii) Collecting personal data by fraudulent, unfair, or unlawful means.

(iii) Providing false documents or information to the DPA.

(iv) Failing to stop the improper processing of personal data when required to do so by the DPA due to a sanctioning or trilateral procedure.

(v) Failing to adhere to the corrective measures mandated by the DPA as a result of a trilateral procedure.



Uruguay

Ferrere

Martin Pesce*

Contact:

* mpesce@ferrere.com

Lefosse

1 Legislation: local laws applicable to data protection

Uruguay has the following key data protection laws and regulations:

- Law No. 18,331, "Personal Data Protection Law" ("**PDPL**") and its Regulating Decree No. 414/009.
- Law No. 19,670, "Accountability Act and Balancing of Budget Execution of the Exercise 2017", and its Regulating Decree No. 64/020 (collectively, the "**Uruguayan Data Protection Laws**").

2 Jurisdiction: territorial applicability

Uruguayan Data Protection Laws have an extended scope which includes: (i) organizations located in the Uruguayan jurisdiction; (ii) organizations located outside the jurisdiction offering goods or services to data subjects in the Uruguayan jurisdiction; and (iii) organizations located outside the jurisdiction engaged in monitoring the behavior of data subjects located in the jurisdiction.

The PDPL also applies to processing activities that utilize means located in Uruguay, except when those means are solely used for transit, or when exempted by public international law rules. Under no circumstances may the contracting parties exclude the application of national law when applicable.

3 Scope: information protected under data protection legislation

Uruguayan Data Protection Laws protect any kind of personal information. Under the PDPL, personal data is defined as information of any kind relating to natural persons or legal entities, determined or determinable.

Sensitive data is defined as personal data that reveals racial or ethnic origins, political preferences, religion or moral beliefs, trade unions affiliations, and/or health or sexual information. Sensitive data is specially protected.

4 Definition of sensitive or special category data

As mentioned above, Uruguayan Data Protection Laws provide a different personal data categorization.

Personal data such as sensitive data (as defined previously), genetic data, biometric data, data concerning mental and/or physical health or medical information, data related to commercial or credit activity, is specially protected by PDPL.

5 Supervisory authority

The PDPL created an enforcement authority called "Regulatory and Personal Data Control Unit" ("**URCDP**", for its acronyms in Spanish). It is linked to the E-Government and Information and Knowledge Society Agency ("**AGESIC**", for its acronyms in Spanish).

URCDP has the following competences, among others: (i) fulfill the objectives and provisions of PDPL law; (ii) assist and advise individuals about PDPL queries; (iii) issue rules and regulations applicable to activities covered by PDPL; (iv) conduct a census of the databases covered by PDPL and maintain a registry of such databases; (v) monitor compliance with the legal regime and carry out relevant supervisory and inspection proceedings.

6 Obligations and requirements for compliance

The PDPL provides different principles that must be considered when processing personal data:

- **Legality.** Databases must be registered within the URCDP to be considered lawful.
- **Accuracy.** Personal data must be truthful, accurate, adequate, fair, and not excessive in relation to the purpose for which it was obtained.
- **Purpose limitation.** Personal data should not be used for purposes different from or incompatible with those for which it was obtained. Data must be eliminated when it is no longer necessary or relevant to the purposes for which it was collected.
- **Accountability.** Data controllers and data processors are responsible for complying with the data protection standards. They must adopt appropriate technical and organizational measures, including privacy by design, privacy by default, and perform data protection impact assessments. A Data Protection Officer must be appointed under certain circumstances.

- **Security.** Necessary measures must be taken to guarantee the security and confidentiality of personal data.
- **Prior informed consent.** As a rule, the processing of personal data requires the prior consent of the data subject, which must meet some requirements, such as being prior, express, informed, and unequivocal. Furthermore, when given the option to consent, data subjects must be able to make this choice themselves without any default selections influencing their decision. However, this principle allows exceptions, for example, when the data comes from public sources[2], or derives from a contractual, scientific, or professional relationship and is necessary for its fulfillment or compliance.
- **Confidentially.** Personal data must be used in a confident manner and exclusively for the usual operations of its line of business or activity, and it is prohibited to share it with third parties unless in case of a Court Order or consent from the data subject.

7 Data Protection Officer (DPO)

The appointment of a DPO is mandatory for entities that process sensitive data as their core business or that process a large volume of personal data (more than 35,000 data subjects).

8 Data subjects' rights

Under PDPL, data subjects have the following rights:

- access to their own personal data.
- rectification and/or correction of their own personal data when inaccurate or incomplete.

[2] According to local regulations, public sources refers to data contained in the following sources or documents: (i) official gazette and official publications; (ii) mass media publications (such as coming from the press); (iii) directories, annual reports and similar containing names and addresses, or other personal data obtained with the consent of the data subject, and; (iv) any other register or publication in which the general interest prevails in that the personal data contained therein may be consulted, disseminated or used by third parties.

- erasure of their personal data.
- object to the processing of personal data; and
- withdraw consent.

9 Security requirements

Data controllers and processors must adopt appropriate technical, physical, and/or organizational security controls and assess national and international standards in information security, such as the Cybersecurity Framework prepared by AGESIC, when determining what security measures to adopt. However, there are no specific security controls required by the regulation.

10 Data breach notification

Both data controllers and processors must immediately report a data breach upon learning about it. The report must detail the breach and the measures undertaken to address it. In the case of data controllers, the notification should be addressed to the URCDP within a maximum of 72 hours and to all affected individuals. Although the legislation provides that the notification to data subjects whose rights have been significantly affected must be made immediately, no specific term has been indicated for such notification. In addition, the regulation provides that in case the breach has been known by a data processor, it must immediately notify the data controller.

Within the first 24 hours of a breach being verified, controllers and processors must initiate the necessary procedures to minimize the impact of such incidents.

Once the violation has been solved, the controller must prepare a detailed report of the breach and the measures adopted and communicate it to URCDP.

11 International data transfers

The PDPL prohibits the transfer of any personal data to countries or international organizations that do not offer proper protection in accordance with the standards of international or regional law on this matter.

The prohibition on transferring personal data to countries or organizations that do not meet the standards on this subject does not apply in the cases of: (i) international judi-

cial cooperation, in accordance with the corresponding international instrument; (ii) exchange of medical information, whenever required for the treatment of patients, either for health or public hygiene reasons; (iii) bank or stock exchange transactions, pertaining to the respective transactions and in accordance with the applicable legislation; (iv) agreements within the framework of international treaties agreed upon by Uruguay; (v) international cooperation among intelligence organizations to fight against organized crime, terrorism and drug trade.

International transfers of personal data may also be possible if the transfer: (i) is required to execute pre-contractual measures taken at the interested party's request; (ii) is required for to execute or perform a contract in the interest of the data subject between the controller and a third party; (iii) is required or demanded by law to protect a major public interest; (iv) is required to protect the vital interest of the interested party; (v) takes place from a registry, which is created by virtue of legal or regulatory provisions, to provide information to the public and is open to consultation from the general public or from any person who may prove that they have a legitimate interest, as long as the conditions established by law for the consultation are met for each particular case.

Separately, URCDP may additionally authorize international transfers of personal data to a third country which does not guarantee the proper protection if the data controller offers the necessary guarantees for the protection of private life, essential rights and freedoms of people, as well as guarantees for the exercise of their respective rights. These guarantees may stem from corresponding contractual clauses.

International transfers of personal data within multinational organizations (i.e., between affiliates, subsidiaries, branches, or a parent company) would be permitted if the local entity (data controller) files for the registration of a Code of Conduct (type of binding corporate rules) to govern such transfers with the local data protection authority.

12 Penalties

If provisions of PDPL are violated, URCDP may take the following punitive measures: (i) notice of violation; (ii) warning; (iii) fines amounting to no more than 500,000 Index Units (USD 70,000 approx.); (iv) suspension of the respective database for a five-day period; and (v) closing of the respective database.

Sanctions shall be graded based on severity, recurrence, or repetition of the committed offense.

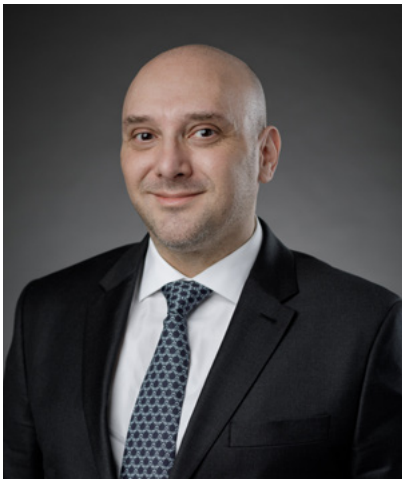
Lefosse

Our Practice

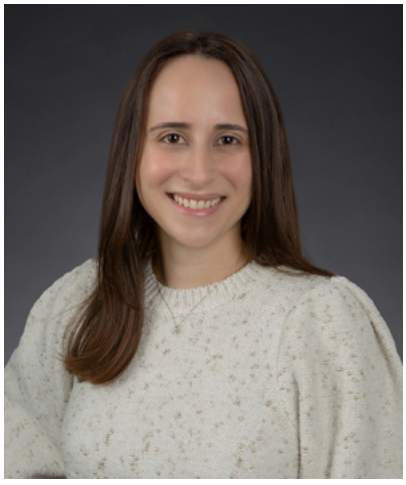
Technology, Data Protection and Intellectual Property

Our practice closely monitors the changes and updates that will impact the market. For further clarification on these or other topics of interest to you, please contact our **Technology, Data Protection and Intellectual Property practice**.

If you have any questions, please contact our partners and lawyers.



Paulo Lilla | Partner
Technology, Data Protection and Intellectual Property
paulo.lilla@lefosse.com



Carla Segala | Senior Associate
Technology, Data Protection and Intellectual Property
carla.segala@lefosse.com

Lefosse

São Paulo

1227 Tabapuã St. – 14th floor
04533-014 Itaim Bibi
São Paulo SP Brazil
+ 55 11 3024-6100

Rio de Janeiro

Praia do Flamengo, 200 – 20th floor
22210-901 Flamengo
Rio de Janeiro RJ Brazil
+ 55 21 3263-5480

Brasília

SCS Quadra 09, Edifício Parque Cidade Corporate
Torre B, 8th floor
70308-200 Asa Sul
Brasília DF Brazil
+ 55 61 3957-1000

lefosse.com

Follow us