



Protection of Personal Data in LATAM

Quick Reference Guide

EY Law
Latin America



The better the question. The better the answer.
The better the world works.



Shape the future
with confidence

Table of Contents

Introduction	2
Argentina	3
Brazil	13
Chile	26
Colombia	38
Costa Rica	48
Ecuador	56
Mexico	64
Panama	72
Paraguay	79
Peru	87
Dominican Republic	94
Uruguay	101
EY Law Latam	109
List of Contacts	109

Introduction

In today's fast-paced world, where technology evolves rapidly and data usage expands exponentially, we are witnessing a profound transformation in our economic, political, and social landscapes globally. Staying informed about these changes and adapting swiftly is essential for success. At EY, we recognize the importance of preparing businesses to tackle these challenges, particularly in the areas of cybersecurity and personal data protection. As new technologies reshape the digital economy, EY Law is excited to present **the fourth edition of the Quick Reference Guide to Personal Data Protection in LATAM**.

Data is undoubtedly the driving force behind the digital economy, enabling organizations to connect with individuals more effectively. However, with this expanded reach comes the critical responsibility of safeguarding fundamental rights, such as privacy and personal data protection.

In this constantly evolving technological environment, organizations must prioritize the protection of their data and information against potential cyber threats, fostering public trust in their ability to handle information securely. Security breaches and non-compliance with personal data protection regulations can severely damage a company's reputation and disrupt business continuity, undermining public confidence in their operations, activities, and services. Therefore, organizations not only have a duty to protect the information they manage but also to ensure its proper use. This emphasis on privacy and personal data protection is increasingly central to the focus of regulatory bodies and society at large.

Our guide aims to provide concise and clear answers to the most frequently asked questions regarding personal data protection in Latin America. It is designed to help businesses navigate the complex legal and regulatory challenges inherent in this dynamic and technological landscape. To support this effort, we have assembled a team of specialized privacy attorneys and cybersecurity experts across the region, offering a coordinated and comprehensive perspective on the subject.

While we acknowledge that there is still much work to be done, data protection laws in the region have made significant strides toward aligning with the highest international standards. As such, our guide offers practical and preliminary guidance on the requirements specific to each jurisdiction, directly addressing common inquiries.

Lastly, we want to emphasize that the information in this guide is accurate as of its publication date. Therefore, we always recommend checking the applicability of relevant regulations at the time you seek advice.

We hope you find this material valuable, and we are always here to support you should you need the assistance of our specialists in this field.

EY LAW | LATAM





Argentina



Matter	Concept	Yes / No / NA	Observations / comments
Regulations	Does the country have a personal data protection law? If so, please name the applicable regulation.	Yes	<p>Personal data protection is regulated by the Personal Data Protection Law No. 25,326, that is the Personal Data Protection Law ("PDPL"). This regulatory framework is supplemented by other standards, such as:</p> <ul style="list-style-type: none"> ▶ The Constitution of the Argentinian Nation in its Section 43, third paragraph. ▶ Decree No. 1,558/2001, and its modifications, regulatory of the Law of Personal Data Protection No. 25,326. ▶ Law No. 27,483: adherence to Agreement to the Protection of People in regard to the Automatic Processing of Personal Data from Strasbourg, France. ▶ Law No. 27,725: Right to Access to Public Information. ▶ Disposition No. E 60/2016. ▶ Resolution No. 159/2018: Guidelines and basic contents of binding corporate standards. ▶ Resolution No. 47/2018: Recommended security measures for the treatment and conservation of private data by informatic and non-informatic means. ▶ Resolution No. 4/2019: Guiding criteria and indicators of good practices in the application of Law No. 25.326, whose annex refers to (i) Systems of video surveillance; (ii) Data dissociation; (iii) Biometric data; and (iv) Consent. ▶ Law No. 26,951: Creation of the "Do not Call" National Registry. ▶ Additional Protocol No. 108+. Ratified by Law No. 27,699. ▶ Disposition No. 2/2023: Recommendations for a reliable Artificial Intelligence. ▶ Law No. 26,548: Genetic Data National Bank. ▶ Resolution No. 161/2023: Creation of the Program for Transparency and Personal Data Protection in the Use of AI. ▶ Resolution No. 198/2023: Approval of Model Contractual Clauses. ▶ Resolution No. 126/2024: Update, systematization, and unification of regulations and the National "Do Not Call" Registry.
Enforcement Authority	Who is the enforcement authority? If applicable, please provide their website link	Yes	<p>Through Decree No. 746/2017, the Agency of Access to Public Information, hereinafter ("AAIP") is established as the enforcement authority. The AAIP is a decentralized body in reach of the Presidency of the Cabinet of Ministers, in the Executive Power.</p> <p>https://www.argentina.gob.ar/aaip</p>
Scope of Application	Which is the regulation's scope of application? I.e., is it a strictly national or cross-border concept?	Yes	PDPL regulations are of public order and apply in all the Argentinian national territory. Argentinian regulations do not foresee the concept of extraterritorial application of the Personal Data Protection Law (LPDP).
Data collection	Which are the mandatory requirements or processes for personal data collection? (For example, data subject consent, information on purpose of data use and ossubject's rights, etc.)	Yes	<p>Personal data processing will be legal when the subject has provided free, express and informed consent, in written or similar matter, according to the circumstances. When collecting personal data, the subjects shall be informed expressly and clearly beforehand:</p> <ol style="list-style-type: none"> 1. Their purpose and who could their recipient or type of recipients be. 2. The existence of a file, registry, data bank, electronic or of any other kind of bank, as well as the controller's identity and address. 3. Mandatory or optional nature of the answers to the proposed questionnaire, especially in regard to the data mentioned in the following section. 4. The consequences of providing, refusing or misstating data. 5. The interested party's possibility of exercising rights of access, rectification and deletion of data.
Legal concept of "personal data"	What are personal data?	Yes	PDPL defines "personal data" as information of any kind that refers to determined or determinable individuals or corporations/entities.

Matter	Concept	Yes / No / NA	Observations / comments
Personal data categories	Are there different personal data categories? Please explain each category, if applicable.	Yes	<p>The Argentine regulation contemplates the following categories of personal data:</p> <ul style="list-style-type: none"> ▶ Sensitive data: These are personal data that reveals racial and ethnic origin, political opinions, religious, philosophical or moral beliefs, union affiliations or health or sexual related information (section 2 PDPL). They can only be collected and processed when there are reasons of general interest authorized by law. They may also be processed for statistical or scientific purposes when their subjects cannot be identified (section 7 PDPL). ▶ Health related Data: The public or private sanitary establishments and the professionals related to health sciences can collect and process personal data related to the mental or physical health of patients that contact, are or were under their treatment, respecting the principles of professional secrecy. ▶ IT Data: These are the personal data subject to electronic or automatic treatment or processing (section 2 PDPL). Furthermore, when personal data processing services are provided on behalf of third parties, such data may not be applied or used for a purpose other than that stated in the service contract, nor may they be transferred to others, even for storage purposes. Once the contractual performance has been fulfilled, the processed personal data must be destroyed, except with the express authorization of the party on whose behalf such services are rendered, when it is reasonably presumed that further orders may be placed, in which case they may be stored under due security conditions for a period of up to two years (section 25 PDPL). ▶ Criminal or misdemeanor data: Data related to criminal or misdemeanor records that can only be treated by the corresponding public authorities (section 7 PDPL). ▶ Credit data: These are not defined by the PDPL, although they are understood to be included within the definition of personal data. Notwithstanding the foregoing, section 26 of the PDPL establishes that, in the provision of credit information services, only personal data of a pecuniary nature relevant to the assessment of the economic solvency and credit of an individual may be processed. Such data must be obtained from publicly available sources, from reports provided by the concerned party, or with their consent. In addition, the provision of credit information services shall not require the prior consent of the data subject for the purposes of the transfer of data, or the subsequent transmission of such data, provided that such data are related to the business or credit activities of the recipients. <p>In addition, although there are no references to other types of sensitive data within the PDPL, it can be mentioned that the AAIP has published different guidelines and recommendations that clarify certain concepts and terms such as "location data". Thus, an AAIP guideline states that there are fundamental principles related to the use of geolocation and tracking tools, whether such tools are used by the public sector, the private sector, or both in collaboration. All information related to an individual's location or movements is considered personal data and is therefore regulated by the PDPL. Therefore, the controller must rely on a legal basis in accordance with section 5 of the PDPL for the collection and processing of this type of information. In addition, "location data" is defined as information collected by a network or service where the user's phone or other device was or is located. Location data may be collected by GPS, cell phone operators, Wi-Fi networks, Bluetooth or a combination of signals.</p>
Situation of the corporations and other legal entities	Does the regulation sufficiently protect the personal data of the corporations or entities?	Yes	The PDPL covers data related to determined or determinable corporations/entities.
Data subject consent	Is the data subject's consent required to collect the data? If so, are there conditions to obtaining the data subject's consent? (For example, prior information that must be provided to the data subject.)	Yes	<p>The granting of consent must be free, express and informed, and given beforehand.</p> <p>When collecting personal data, the subjects shall be informed expressly, clearly and beforehand:</p> <ol style="list-style-type: none"> 1. The purpose for which they will be processed and who may be the recipients or class of recipients. 2. The existence of the file, registry, data bank, electronic or otherwise, and the identity and address of the person responsible for it. 3. The obligatory or optional nature of the answers to the proposed questionnaire, especially with regard to sensitive data. 4. The consequences of providing the data, of the refusal to do so or of their inaccuracy. 5. The possibility of the interested party to exercise its access, rectification or suppression rights of data.

Matter	Concept	Yes / No / NA	Observations / comments
Exceptions to the consent	<p>Are there exceptions to the voluntary consent of a data subject? If so, please list the exceptions.</p>	Yes	<p>It should be noted that consent will not be necessary when:</p> <ol style="list-style-type: none"> 1. Data are obtained from unrestricted public sources. 2. Data are collected for the proper functioning of State Powers or in lieu of a legal obligation. 3. Data are limited to the listing of names, national identification documents, tax or social security identifications, occupation, date of birth and domicile. 4. Data are derived from a contractual, scientific or professional relationship of the subject, and are necessary for its development or compliance. 5. Data are about financial entities operations, and the information received from their clients.
Content and scope of the information to be validated by the data subject	<p>What should be the content of the consent? (For example, data use or destination, international data transfer, etc.)</p>	Yes	<p>See answer in the "data collection" section above (section 6 PDPL).</p>
Transfer of personal data	<p>Are there requirements or restrictions on the transfer of personal data? Are there requirements that apply to the international transfer of data? (Example: model clauses, control authority's authorization, etc.)</p>	Yes	<p>The transference of personal data of any kind to countries or international/supranational bodies that do not provide proper protection levels is forbidden in the PDPL. However, this prohibition does not rule if the data subject has expressly consented the transfer.</p> <p>On the other hand, through Disposition No. 60 - E/2016 published in the Official Gazette on November 18, 2016, the National Directorate of Personal Data Protection (now AAIP) regulated aspects related to the transfer of personal data. According to the PDPL, transfer to countries not considered adequate in regard to personal data protection is forbidden.</p> <p>The Disposition establishes the countries that meet the adequate legislation in regard to personal data protection. States members of the European Union and members of the European Economic Area, Switzerland, Guernsey, Jersey, Isle of Man, Faroe Islands, Canada solely the private sector, New Zealand, Andorra and Uruguay. I.e., the statements of adaptation issued by the European Union have been considered.</p> <p>The Disposition approves two contract models to employ in the international transfer of data to non-adequate countries both for data transference as well as the rendering of services. These models follow in many ways the guidelines in the contractual model clauses the EU established in Decision No. 2001/497/CE and Decision No. 2010/87/UE.</p>
BCR	<p>Do they have binding corporate rules (BCR)?</p>	Yes	<p>Additionally, Resolution No. 198/2023, published on October 19, 2023, approves the model contractual clauses for international data transfers and the Implementation Guide of the Ibero-American Data Protection Network (RIPD). The model contractual clauses for international data transfers were developed by the RIPD as a cost-effective alternative for companies or organizations to avoid negotiating individual agreements.</p> <p>Through Resolution No. 159/2018 the AAIP adopted Binding Corporate Rules in order to be considered in the designing of documents related to self-regulation rules in corporations' part of the same economic group for the international transfer of personal data.</p> <p>Sensitive data is understood as personal data that reveal:</p> <ul style="list-style-type: none"> ▶ Racial and ethnic origin. ▶ Political opinions. ▶ Religious, philosophical or moral beliefs. ▶ Union affiliation. ▶ Health-related or sexual information.
Sensitive data	<p>What is understood by sensitive data? How is sensitive data processed, if applicable?</p>	Yes	<p>Sensitive data can only be collected and be subject to processing due to the general reasons approved by the PDPL in its Section 7.</p>

Matter	Concept	Yes / No / NA	Observations / comments
Database registration or periodic reporting to the control authority	Is it mandatory to register (e.g., with the corresponding enforcement body) a database and/or a database ownership, processing and/or use? Is it mandatory to submit any type of information or report periodically to the enforcement authority?	Yes	<p>Every file, registry, or public or private data bank that provides reports must be inscribed in the Registry of the Agency of Access to Public Information, in accordance with the information requirements set forth in Section 21 of the PDPL. No data user will be able to hold personal data of a different nature to the ones established in the registry. Non-compliance with these requirements will incur in administrative sanctions from the AAIP, expressed in Section 29 of the PDPL.</p> <p>With the release of Resolution AAIP 38/2024, there has been an important update to the model notice of the advertising poster used for collecting digital images, particularly for data controllers and their required database registrations. This notice is vital as it ensures that individuals are informed in advance about how their data will be used, in line with legal requirements. This is especially important for those managing video surveillance databases, which are typically employed for security purposes. By providing clear information to data subjects, organizations can foster trust and transparency in their data handling practices.</p> <p>Pursuant to Section 9 PDPL, the data controller must adopt the technical and organizational measures that:</p> <ol style="list-style-type: none"> 1. Are necessary to guarantee the safety and confidentiality of the personal data, in order to avoid their adulteration, loss, or non-authorized query or processing, and 2. Those that allow the detection of information deviation, whether intentional or not, due to risk from human actions or the technical mean used.
Data security	Are there technical measures to guarantee the security	Sí	<p>Likewise, it is forbidden to record personal data in files, registers or banks that do not meet adequate technical conditions of integrity and security.</p> <p>The PDPL states that the data subject has the following rights:</p> <ul style="list-style-type: none"> ▶ Right to information and its content. ▶ Right of access. ▶ Right to update/rectify ▶ Right of deletion.
Rights of the data subjects	What are the data subjects' rights? (Example: correction, update or deletion). Please list and explain.	Yes	<p>The PDPL also refers to the possibility of filing a complaint before the AAIP in case of lack of response or incomplete information when exercising their rights. Along these lines, section 33 of the PDPL provides for an action for the protection of personal data or Habeas data, which will proceed:</p> <ol style="list-style-type: none"> 1. To become aware of the personal data stored in public or private files, registers or data banks intended to provide reports, and of the purpose thereof. 2. In cases in which it is presumed that the information in question is false, inaccurate or outdated, or the processing of data whose registration is prohibited by law, to demand its rectification, deletion, confidentiality or updating. <p>The actions of the data subjects can be exercised in the following manner:</p> <ul style="list-style-type: none"> ▶ Right to information and its content: Everybody can request information about the existence of files, registries or personal data banks to the AAIP in regard to their purpose and the identity of the responsible parties. ▶ Rights of access of data subjects: The data subject, after verifying their identity, has the right to request and obtain information on their personal data included in public or private data banks destined for reporting. ▶ Right to update, rectify and delete: Everybody has the right to rectify, update, and when applicable, delete or make private the data they own that is included in a data bank. ▶ Action for the protection of personal data or Habeas Data: The legal standing, procedural forms, requirements and other information for the exercise of the referred action are provided for in Chapter VII "Action for the protection of personal data" of the PDPL.
Actions by the data subjects	How can they exercise them?	Yes	

Matter	Concept	Yes / No / NA	Observations / comments
Assignment of personal data	What are the requirements for the assignment of personal data?	Yes	<p>Personal data subject to processing can only be assigned in order to comply with purposes directly related to the legitimate interest of the assignor and the assignee, and with the data subject's previous consent, who must be informed on the purpose on the assignment and provide the assignee or elements allowing so.</p> <p>However, the consent of the data subject is not required when:</p> <ol style="list-style-type: none"> 1. It is provided by law. 2. In the cases provided for in Section 5, paragraph 2 of the PDPL, which lists the cases in which the consent is not required. 3. It is carried out directly between government agencies, to the extent of the fulfillment of their respective competences. 4. The data shared are of a personal nature related to health, and it is necessary for public health or emergency reasons, or for the performance of epidemiological surveys, as long as the identity of the data subjects is preserved by means of adequate dissociation mechanisms. 5. A procedure for disassociating the information has been applied, so that the individuals to whom the information relates are not identifiable. <p>It should be noted that the assignee will be subject to the same legal and regulatory obligations as the assignor and shall answer jointly for their compliance before the corresponding body and the data subject.</p>
Data processing	Can the services be provided through a third party (data processing)? If so, please explain the procedure and exceptions, if applicable.	Yes	<p>When services of personal data processing are rendered on behalf of third parties, these shall not be applied or used for a different purpose than what is stated in the contract, nor assigned to other individuals, not even for retention.</p> <p>As a general rule, the PDPL establishes that personal data must be retained only for the time necessary to fulfill the purposes for which they were collected.</p>
Data retention	Is it mandatory to retain/conserve the data collected or processed for a specific term? If so, what is the term?	No	<p>However, the PDPL provides a specific retention period for certain categories or documents, such as:</p> <ul style="list-style-type: none"> ▶ IT services: once the corresponding contractual obligations have been fulfilled, the processed personal data must be destroyed, except in the case of express authorization given by the person on whose behalf such services are provided, on the grounds that the data may be used for future services, in which case the data may be stored under appropriate security conditions for a maximum period of up to two years (Section 25 PDPL). ▶ Credit information: only personal data relevant to assessing the economic and financial solvency of the parties concerned within the last five years may be archived, recorded or communicated. This period shall be reduced to two years when the debtor settles or otherwise discharges the obligation, and this fact shall be stated in the report. ▶ Personal data recorded for law enforcement purposes: it will be cancelled when it is not considered necessary for the investigations that gave rise to its storage (Section 23 PDPL).
Data elimination	Is there an obligation to eliminate the data collected or processed? If so, under what conditions and for what term?	Yes	<p>The PDPL states that data must be destroyed when they are no longer necessary or relevant for the purposes for which they had been collected. The data must be deleted without the need for any additional request made by the data subject (Section 4, paragraph 7 of the PDPL).</p> <p>It should be noted that, if a third party is contracted to provide IT data processing services, the data must be destroyed when the work is completed, unless otherwise agreed (Section 25, paragraph 2).</p> <p>Also, data must be deleted at the request of the data subject.</p> <p>Where the PDPL provides for specific retention periods for certain categories, such as in the case of credit/financial data and computerized/computerized data, such data must be deleted upon expiration of the respective periods indicated.</p>

Matter	Concept	Yes / No / NA	Observations / comments
Privacy Impact Assessment	Are Privacy Impact Assessments required and/or mandatory?	No	<p>Not stipulated in the PDPL. However, the AAIP along with the Regulatory and Personal Data Control Unit of Uruguay set up an impact assessment guide for the processing of personal data. In order to provide a reference document to companies and public entities about concept, context and methodologies in an impact assessment regarding data protection (EIPD).</p> <p>It should be noted that the referred guide's objective is to act as a tool for responsibly assessing, in accordance with set safety and comprehensive standards, the practices and projects that could affect the rights of the individuals in regard to the processing of their personal data.</p> <p>The Guide also provides some factors that should be assessed to decide whether or not to carry out an EIPD. When one or more of these factors concur, it can be inferred that the project or activity under analysis involves significant risks to the rights of individuals. In such cases, the data controller should conduct a PIDP to comply with the applicable regulations.</p>
Incidents	Is it mandatory to report security incidents or breaches or the related legal provisions?	No	<p>Although there is no local regulatory requirement in force, Argentina enacted the Law No.27,699 in 2022, by which they adhere to the Additional Protocol (Convention No. 108+) amending Convention No. 108.</p> <p>Through Section 7 of the Convention, it is established that the controller must notify, within the first 72 hours after knowing the incident, at least to the competent supervisory authority (AAIP), those data breaches that may seriously interfere with the fundamental rights and freedoms of data subjects.</p> <p>The PDPL provides for different types of sanctions, as identified below.</p>
Sanctions	Are there sanctions for failures to comply with this obligation? If so, please list them along with the corresponding sanction or penalty amounts.	Yes	<p>▶ Administrative sanctions (Section 31): which may consist of:</p> <ul style="list-style-type: none"> - Warning. - Suspension of the file, registry or data bank. - Fine: It can vary depending on the severity of the violation (i.e., minor, serious, and very serious infractions). According to Resolution AAIP 126/2024, fines can range from one thousand (\$1,000) to one hundred thousand Argentinean pesos (\$100,000). - Closure of the file, registry or data bank. - Cancellation of the file, registry or data bank. <p>These penalties will be graduated according to the seriousness and extent of the infringements and the damages derived from the infringement, guaranteeing the principle of due process.</p> <p>Likewise, the AAIP publishes on its official website the list of the main sanctioned companies, which also triggers a reputational damage to be considered, together with the corresponding resolutions of the AAIP containing the details of the sanctioned infringement.</p> <p>▶ Criminal penalties (Section 32): the possibility of applying those penalties included in Sections 117 bis and 157 bis of the National Criminal Code is foreseen. This entails that the criminal courts may order criminal penalties such as imprisonment from 1 month to 3 years depending on the specific infringements related to data protection. Both penalties also include a complementary penalty of disqualification when the offender is a public official.</p> <p>It should be noted that the Argentine Criminal Code contemplates the following crimes related to personal data (without including in its definition the modality through which they are carried out):</p> <ul style="list-style-type: none"> a) Intentional insertion of false information in a personal database. b) Intentional disclosure to a third party of false information in a personal database. c) Knowingly and unlawfully breaking into or violating the confidentiality of data and data security systems, in any way, in a personal database (unauthorized access). d) Disclosure of confidential information in a personal database that must be kept secret by law. <p>▶ Civil penalties: Section 33 and following of the PDPL regulate the Habeas Data action, also referred to in the National Constitution (Section 43, third paragraph of the National Constitution), which allows civil claims for the reparation of damages caused by an infringement of the PDPL.</p>

Matter	Concept	Yes / No / NA	Observations / comments
Legal actions	Are there any legal actions for personal data protection? Who has the right to exercise/request them?	Yes	<p>The legislation establishes that the action for personal data protection or habeas data, which shall proceed:</p> <ol style="list-style-type: none"> 1. To take knowledge of the personal data stored in public or private files, registers or data banks intended to provide reports, and of the purpose thereof. 2. In cases in which it is presumed that the information in question is false, inaccurate or outdated, or the processing of data whose registration is prohibited by this law, in order to demand its rectification, suppression, confidentiality or updating. <p>It should be noted that this action can be requested by the affected party, their guardians or custodians and successors of individuals, directly or collateral up to second degree, by themselves or through a proxy.</p> <p>When the action is requested by a corporation/entity, this shall be filed by its legal representatives, or the proxies assigned.</p>
Personal data protection officer or responsible party.	Is there a Data Protection Officer (DPO) or similar position? If so, is their appointment mandatory? Must they be appointed locally?	No	<p>The law does not establish a requirement to appoint a data protection officer.</p>
Processing Records	Are there any mandatory requirements for maintaining processing records under the applicable laws? Specifically, what information must be included in these records, and are there any particular conditions or circumstances under which data controllers or processors are obliged to keep detailed records of their data processing activities?	Yes	<p>The AAIP shall perform all required actions for the fulfillment of its objectives. In this line, the AAIP has the power to carry out investigations and impose administrative sanctions for violations of the regulations in force, as well as to become a plaintiff in criminal actions brought for violations to the PDPL.</p> <p>Inspections are carried out to:</p> <ol style="list-style-type: none"> 1. Take knowledge of the activities of the responsible for the database, the personal data they administer, the means and the manner in which they do it. 2. Verify that the database manager adopts the necessary technical and organizational measures to ensure the security and confidentiality of personal data. 3. Evaluate the degree of compliance with the provisions of the PDPL. 4. Make observations.
Registro de procesamiento	¿Existen requisitos obligatorios para mantener registros de procesamiento según las leyes aplicables? Específicamente, ¿qué información debe incluirse en estos registros y hay alguna condición o circunstancia particular bajo la cual los controladores o procesadores de datos están obligados a llevar un registro detallado de sus actividades de procesamiento de datos?	Sí	<p>Article 21 of Law 25.326 outlines the mandatory requirements for maintaining records of data processing. Specifically, it states that every file, record, database, or bank of both public and private data intended for reporting must be registered with a register approved by the regulatory body. Data controllers are required to include the following information in their records:</p> <ul style="list-style-type: none"> ► The name and address of the person responsible for the file or database. ► The characteristics and purpose of the file. ► The nature of the personal data contained in each file. ► The methods used for collecting and updating the data. ► The intended use of the data and the individuals or entities to whom it may be transmitted. ► The way information is interrelated within the records. ► The security measures implemented to protect the data, including the categories of individuals with access to the information. ► The duration for which the data will be retained. ► The conditions and procedures by which individuals can access, rectify, or update their data.
Similarities with the GDPR	Per your understanding, do you believe that the regulation contemplates all of the requirements set by similar international regulations (e.g., the GDPR)? What relevant differences did you find?	No	<p>The Argentinian legislation does not consider all requirements set by international regulations. Nevertheless, projects to modify the PDPL have been submitted before National Legislative Branch. In this regard, on June 30, 2023, the National Executive Branch sent to Congress for its treatment Message No. 87/2023, that is, the new Personal Data Protection Bill, which is in line with international standards and presents great similarities with the GDPR.</p>

Matter	Concept	Yes / No / NA	Observations / comments
Other obligations	<p>Are there other additional considerations/requirements or legal obligations on data protection that must be met?</p>	Yes	<p>The National "Do Not Call" Registry is an initiative designed to help individuals who prefer not to receive advertising/marketing calls. Recently, the AAIP renewed the registry system, making registration, inquiries, and complaints more straightforward and accessible. Now, everything can be managed online and free of charge through the website nolname.aaiip.gob.ar.</p> <p>Individuals with fixed or mobile phone lines can easily register their number using their ID card and the transaction number. There is a limit of up to five lines that can be registered. Once registration is confirmed, if the user continues to receive calls from advertising or marketing companies, they can file a complaint at any time of day by completing a form on the website.</p> <p>The administration of this registry is handled by the AAIP, which also manages administrative actions in cases of non-compliance. This registry applies throughout Argentina and guarantees the right not to receive commercial calls, thereby facilitating the exercise of the "right to block" established by Law 25.326. The initiative covers various telephone services, including both fixed and mobile lines, as well as future technologies such as instant messaging.</p> <p>Although no confirmation of registration is sent, users can verify their status at any time. Registered numbers appear immediately on the lists, although companies have up to 30 days to cease calling.</p> <p>If someone wishes to cancel their registration, they can do so at any time through the same website. While registration significantly reduces advertising calls, it does not eliminate all of them, as certain calls, such as those for public service campaigns or emergencies, are exempt. It is also allowed for companies that maintain a contractual relationship with the user to contact them regarding purchased products or services.</p>

A scenic landscape of the Serra Geral mountain range in Brazil, with its distinctive red and green peaks and lush green forests under a blue sky with white clouds.

Brazil



Matter	Concept	Yes / No / NA	Observations / comments
Regulations	Does the country have a personal data protection law? If so, please name the applicable regulation.	Yes	<p>The protection of personal data is regulated in the:</p> <ul style="list-style-type: none"> ▶ Brazilian General Data Protection Law ("LGPD"), Federal Law No. 13,709/2018, with the amends law No. 13,853/2019 and 14,010/2020. ▶ Decree 10,474/2020. <p>In addition, there are some important regulation instruments published by the National Data Protection Authority ("ANPD"), as the Resolutions CD/ANPD No. 1/2021, No. 2/2022, No. 4/2023, No. 15/2024 and No. 19/2024.</p>
Enforcement Authority	Who is the enforcement authority? If applicable, please provide their website link	Yes	<p>Currently the main state authority involved in overseeing personal data protection issues is the National Data Protection Authority ("ANPD"), and its website is https://www.gov.br/anpd/</p>
Scope of Application	Which is the regulation's scope of application? I.e., is it a strictly national or cross-border concept?	Yes	<p>Section 3 of the LGPD provides that the law applies to any processing operation carried out by a natural person or legal entity governed by public or private law, irrespective of the means, of the country in which its headquarter is located or of the country in which the data are located, provided by the processing, purpose of the processing or processed personal data of individuals located or collected in the Brazilian territory.</p> <p>Section 3 of the LGPD: It applies to any processing operation carried out by a natural person or by a legal entity under public or private law, regardless of the means, the country of its head office or the country where the data are located, provided that:</p> <ol style="list-style-type: none"> 1. The processing operation is carried out in the national territory. 2. The purpose of the processing activity is to offer or supply goods or services or to process data from individuals located in the national territory. 3. The personal data processed have been collected in the national territory.

Matter	Concept	Yes / No / NA	Observations / comments
Data collection	<p>Which are the requirements or processes for personal data collection? (For example, data subject consent, information on purpose of data use and subject's rights, etc.)</p>	Yes	<p>Processing of personal data shall be done in good faith and be subject to the following principles (Section 6):</p> <ul style="list-style-type: none"> ▶ Purpose. ▶ Suitability. ▶ Necessity. ▶ Free access. ▶ Quality of the data. ▶ Transparency. ▶ Security. ▶ Prevention. ▶ Nondiscrimination. ▶ Accountability. <p>The processing of personal data of children shall be carried out with the specific and separate consent of at least one of the parents or by the legal guardian. Personal data of children may be collected without the consent whenever the collection is necessary to contact the parents or the legal guardian. (Section 14).</p> <p>In addition, Section 7 of the LGPD: The processing of personal data may only be carried out when at least one of the following authorizing hypotheses is present:</p> <ol style="list-style-type: none"> 1. By means of the data subject consent. 2. For compliance with legal or regulatory obligation by the controller. 3. By the public administration, for the processing and shared use of data necessary for the execution of public policies provided for in laws and regulations or supported by contracts, agreements or similar instruments, in compliance with the provisions of chapter iv of the law. 4. For the performance of studies by research body, guaranteed, whenever possible, the anonymization of personal data. 5. Where necessary for the performance of a contract or preliminary procedures relating to the contract to which the data subject is a party, at the request of the data subject. 6. For the regular exercise of rights in judicial, administrative or arbitral proceedings, the latter pursuant to law No. 9,307 of September 23, 1996 (arbitration law). 7. For the protection of the life or physical safety of the data subject or third party. 8. For the protection of health, in a procedure performed by health professionals or by health entities. 9. For the protection of health, exclusively, in a procedure performed by health professionals, health services or health authority. 10. Where necessary to meet the legitimate interests of the controller or third party, except where the fundamental rights and freedoms of the data subject prevail. 11. For the protection of credit, including as to the provisions of the relevant legislation. <p>Also, Section 11 of the LGPD indicates different authorizing hypotheses for the sensitive data processing, as:</p> <ol style="list-style-type: none"> 1. by means of the data subject or his/her legal guardian consent. 2. Without the consent, in cases where it is essential to: <ul style="list-style-type: none"> a. Compliance with legal or regulatory obligation by the controller. b. Shared processing of data necessary for the execution, by the public administration, of public policies provided for in laws or regulations. c. Conducting studies by research body, guaranteed, whenever possible, the anonymization of sensitive personal data. d. Regular exercise of rights, including in contract and in judicial, administrative and arbitral proceedings, the latter pursuant to law No. 9,307 of September 23, 1996 (arbitration law). e. Protection of the life or physical safety of the data subject or third party. f. Health protection, exclusively, in a procedure performed by health professionals, health services or health authority. g. Guarantee of the prevention of fraud and the security of the data subject, in the processes of identification and authentication of registration in electronic systems, protected the rights mentioned in Section 9 of the law and except in the case where fundamental rights and freedoms of the data subject that require the protection of personal data prevail.
Legal concept of "personal data"	What is personal data?	Yes	According to the LGPD, personal data consists of the information related to an identified or identifiable natural person (Section 5).

Matter	Concept	Yes / No / NA	Observations / comments
Personal data categories	Are there different personal data categories? Please explain each category, if applicable.	Yes	<p>LGPD defines other two categories of data in Section 5:</p> <ul style="list-style-type: none"> ▸ Sensitive data: as data related to racial or ethnic origin, religious belief, political opinion, membership in trade unions or religious, philosophical or political organizations, health or sexual life, genetic or biometric data, when related to a natural person. ▸ Anonymized data: as data relating to a data subject who cannot be identified, considering the use of reasonable technical means available at the time of the processed thereof. Furthermore, according the LGPD Section 12, anonymized data is not considered personal data (except when the anonymization process to which they were submitted is reversed, using exclusively proprietary means, or when, with reasonable efforts, it can be reversed). <p>In addition: Section 14 defines specific procedures to processing of personal data of children and adolescents.</p>
Situation of the corporations and other legal entities.	Does the regulation sufficiently protect the personal data of the corporations or entities?	No	N/A
Data subject consent	Is the data subject's consent required to collect the data? If so, are there conditions to obtaining the data subject's consent? (For example, prior information that must be provided to the data subject).	Yes	<p>The prior consent of the data subject is one of the authorization hypotheses for the processing of personal data provided in Sections 7 and 11 of the LGPD. If the most appropriate legal basis (authorization hypothesis) is consent, it should be collected freely, informed and unequivocal making sure that the data subjects agree to the processing of their personal data for a specific purpose. The consent must be provided in writing or by other means that proves the manifestation of will of the data subject. It also must be referred to defined purposes, and generic authorizations shall be null. (Section 8).</p>

Matter	Concept	Yes / No / NA	Observations / comments
Exceptions to the consent	<p>Are there exceptions to the voluntary consent of a data subject? If so, please list the exceptions.</p>	Yes	<p>The consent requirement is waived for data manifestly made public by the data subject, safeguarding the rights of the data subject and the principles provided in the Law (Section 7, Item 4).</p> <p>In addition, Section 7 of the LGPD brings another 9 authorization hypotheses for the processing of data that dispense with consent:</p> <ol style="list-style-type: none"> 1. For the compliance with legal or regulatory obligation by the controller. 2. By the public administration, for the processing and shared use of data necessary for the execution of public policies provided for in laws and regulations or supported by contracts, agreements or similar instruments, in compliance with the provisions of chapter iv of the law. 3. For the performance of studies by research body, guaranteed, whenever possible, the anonymization of personal data. 4. Where necessary for the performance of a contract or preliminary procedures relating to the contract to which the data subject is a party, at the request of the data subject. 5. For the regular exercise of rights in judicial, administrative or arbitral proceedings, the latter pursuant to Law No. 9,307 of September 23, 1996 (arbitration law). 6. For the protection of the life or physical safety of the data subject or third party. 7. For the protection of health, in a procedure performed by health professionals or by health entities. 8. For the protection of health, exclusively, in a procedure performed by health professionals, health services or health authority. 9. Where necessary to meet the legitimate interests of the controller or third party, except where the fundamental rights and freedoms of the data subject prevail. 10. For the protection of credit, including as to the provisions of the relevant legislation. <p>The hypotheses for the processing of sensitive personal data are more restricted and are in Section 11 of the LGPD: The processing of sensitive personal data may only occur in the following cases:</p> <ol style="list-style-type: none"> 1. When the data subject or his legal guardian consents, in a specific and prominent manner, for specific purposes. 2. Without providing the data subject's consent, in cases where it is indispensable to: <ol style="list-style-type: none"> a. Compliance with legal or regulatory obligation by the controller. b. Shared processing of data necessary for the execution, by the public administration, of public policies provided for in laws or regulations. c. Conducting studies by research body, guaranteed, whenever possible, the anonymization of sensitive personal data. d. Regular exercise of rights, including in contract and in judicial, administrative and arbitral proceedings, the latter pursuant to Law No. 9,307 of September 23, 1996 (arbitration law). e. Protection of the life or physical safety of the data subject or third party. f. Health protection, in a procedure performed by health professionals or by health entities. g. Health protection, exclusively, in a procedure performed by health professionals, health services or health authority. h. Guarantee of the prevention of fraud and the security of the data subject, in the processes of identification and authentication of registration in electronic systems, protected the rights mentioned in section 9 of the law and except in the event that the fundamental rights and freedoms of the data subject that require the protection of personal data prevail.

Matter	Concept	Yes / No / NA	Observations / comments
Content and scope of the information to be validated by the data subject What should be the content of the consent? (For example, data use or destination, international data transfer, etc.)		Yes	<p>According to the Section 5, XII of LGPD, the consent must be provided through a free, informed, and unequivocal expression, by which the data subject agrees to the processing of their personal data for a specific purpose. Also, the LGPD provides the data subject right to access information about the processing of their personal data (Section 9), and in order to ensure that these specificities are met, it is essential to include at least the following information:</p> <ol style="list-style-type: none"> 1. The specific purpose of the processing. 2. The type and duration of the processing, being observed commercial and industrial secrecy. 3. Identification of the controller. 4. The controller's contact information. 5. Information regarding the shared use of data by the controller and the purpose. 6. Responsibilities of the agents that will carry out the processing. 7. The data subject's rights, with explicit mention of the rights (Section 9). <p>Furthermore, the LGPD provides some guidelines regarding consent, such that:</p> <ul style="list-style-type: none"> ▶ Section 7, § 5: The controller who obtained the consent and needs to communicate or share personal data with other controllers must obtain specific consent from the data subject for this purpose, except in cases where consent is not required. ▶ Section 8, caput and §§ 1 and 2: The consent must be provided in writing or by another means that demonstrates the data subject's expression of will. If the consent is provided in writing, it must be in a clause that is distinct from the other contractual clauses, and the burden of proof that consent was obtained in accordance with the LGPD bears to the Controller. ▶ Section 8, § 3: The processing of personal data through a defect in consent is prohibited. ▶ Section 8, § 4: The consent must refer to specific purposes, and generic authorizations for the processing of personal data will be null and void. ▶ Section 8, § 5: Consent can be revoked at any time through an express statement by the data subject, by a free and facilitated procedure, ratifying the treatments carried out under the consent previously expressed while there is no request for elimination. ▶ Section 8, § 6: In case of a change in the purpose, form, and duration of the processing, identification of the controller and/or information about the shared use of the data, the controller must inform the data subject, with a specific highlight of the content of the changes, and the data subject, in cases where their consent is required, may revoke it if they disagree with the change.

Matter	Concept	Yes / No / NA	Observations / comments
Transfer of personal data	<p>Are there requirements or restrictions on the transfer of personal data? Are there requirements that apply to the international transfer of data? (Example: model clauses, Supervisors' authorization, etc.)</p>	Yes	<p>The international transfer of personal data is only allowed according to the provisions set off in Section 33. The international transfer of personal data is only allowed according to the provisions set off in Section 33. International transfer of personal data is only permitted in the following cases:</p> <ol style="list-style-type: none"> 1. For countries or international organizations that provide the degree of protection of personal data appropriate to the provisions of the Law. 2. When the controller offers and proves guarantees of compliance with the principles, rights of the data subject and the data protection regime provided for in the Law, in the form of: <ol style="list-style-type: none"> a. Specific contractual clauses for a given transfer. b. Standard contractual clauses. c. Global corporate standards. d. Regularly issued stamps, certificates and codes of conduct. 3. Where the transfer is necessary for international legal cooperation between public intelligence, investigative and pursuit bodies in accordance with the instruments of international law. 4. Where the transfer is necessary for the protection of the life or physical safety of the data subject or third party. 5. When the national authority authorizes the transfer. 6. When the transfer results in a commitment made in an international cooperation agreement. 7. When the transfer is necessary for the execution of public policy or legal attribution of the public service, being given publicity in accordance with item I of the caput of Section 23 of the Law. 8. When the data subject has provided his specific consent and highlighted the transfer, with prior information on the international character of the operation, clearly distinguishing it from other purposes. 9. When necessary to meet the hypotheses provided for in items II, V and VI of Section 7 of the Law. <p>To regulate each of these possibilities provided by the LGPD, the ANPD published Resolution CD/ANPD No. 19/2024, which reinforces the above provisions and introduces the content of standard contractual clauses, as well as the International Data Transfer Regulation. This regulation highlights important information such as the criteria that will be used in assessing the level of personal data protection of a foreign country or international organization, including standard or specific contractual clauses, transparency measures, provisions on global corporate norms for international data transfer, as well as any approval procedures and amendments to both the clauses and the norms. It is important to emphasize that the standard contractual clauses provided by the ANPD through Annex II of the Resolution must be adopted, and that in the case of using other specific clauses, due to exceptional factual or legal circumstances duly proven by the controller, they must be submitted for ANPD's approval according to the terms of articles 21 to 24 and 29 to 30 of the Resolution.</p>
BCR	<p>Do they have binding corporate rules (BCR)?</p>	Yes	<p>Both the LGPD and Resolution CD/ANPD No. 19/2024 provide for binding corporate rules, which must be approved by ANPD in accordance with Section 35 of the LGPD and Section 28 of the Resolution.</p>

Matter	Concept	Yes / No / NA	Observations / comments
Sensitive data	What is understood by sensitive data? How is sensitive data processed, if applicable?	Yes	<p>The concept of sensitive data is expressed in Section 5 of LGPD. Sensitive personal data are provided for by law as personal data on racial or ethnic origin, religious conviction, political opinion, membership of a trade union or organization of a religious, philosophical or political nature, given regarding health or sexual life, genetic or biometric data, when linked to a natural person; the hypotheses for the processing of sensitive personal data are more restricted and are foreseen in Section 11 of the LGPD. The processing of sensitive personal data may only occur in the following cases:</p> <ol style="list-style-type: none"> 1. When the data subject or his legal guardian consents, in a specific and prominent manner, for specific purposes. 2. without providing the data subject's consent, in cases where it is indispensable to: <ol style="list-style-type: none"> a. Compliance with legal or regulatory obligation by the controller. b. Shared processing of data necessary for the execution, by the public administration, of public policies provided for in laws or regulations. c. Conducting studies by research body, guaranteed, whenever possible, the anonymization of sensitive personal data. d. Regular exercise of rights, including in contract and in judicial, administrative and arbitral proceedings, the latter pursuant to law No. 9,307 of September 23, 1996 (arbitration law). e. Protection of the life or physical safety of the data subject or third party. f. Health protection, exclusively, in a procedure performed by health professionals, health services or health authority. g. Guarantee of the prevention of fraud and the security of the data subject, in the processes of identification and authentication of registration in electronic systems, protected the rights mentioned in Section 9 of the law and except in the case where fundamental rights and freedoms of the data subject that require the protection of personal data prevail.
Database registration or periodic reporting to the corresponding authority	Is it mandatory to register (e.g. with the corresponding enforcement body) a database and/or a database ownership, processing and/or use? Is it mandatory to submit any type of information or report periodically to the enforcement authority?	No	There is no general obligation to make a prior notification to the ANPD about details of regular processing activities.
Data security	Are there technical measures to guarantee the security and confidentiality of personal data? If so, what are they?	Yes	The processing agents shall adopt security, technical and administrative measures that can protect the personal data from unauthorized accesses and accidental or unlawful situations of destruction, loss, modification, communication or any form of inappropriate or unlawful processing. Technical measures may include the anonymization. (Section 46 and 48).
Rights of the data subjects	What are the data subjects' rights? (Example: correction, update or deletion). Please list and explain.	Yes	<p>The rights of the data subjects referred to in the LGPD as all-natural people are ensured the ownership of their personal data and the guarantee of the fundamental rights to freedom, intimacy and privacy, pursuant to the provisions of the LGPD, data subjects are entitled to obtain from the controller, in relation to its personal data processed by such controller, at any time and upon request:</p> <ul style="list-style-type: none"> ▶ Confirmation of the existence of processing. ▶ Access to the data. ▶ Correction of incomplete, inaccurate or outdated data. ▶ Anonymization, blocking or elimination of unnecessary or excessive data or of data processed in noncompliance with the provisions of the LGPD. ▶ Portability of the data to other service providers or suppliers of product, at the express request, and observing the business and industrial secrets, in accordance with the regulation of the controlling body. ▶ Elimination of the personal data processed with the consent of the data subjects. ▶ Information of the public and private entities with which the controller carried out the shared use of data. ▶ Information on the possibility of not providing consent and on the consequences of the denial. ▶ Revocation of the consent. <p>(Section 17 and 18).</p>

Matter	Concept	Yes / No / NA	Observations / comments
Actions by the data subjects	How can they exercise them?	Yes	<p>The rights will be exercised upon express request from the data subject, to the processing agent (Section 18, § 3), and through a petition in relation to their data against the controller before the supervisory authority (Section 18, § 1) upon request to the controller.</p>
Transfer of personal data	What are the requirements for the transfer of personal data?	Yes	<p>The information related to an identified or identifiable a natural person can be transferred prior his/her consent and shall observe the good faith and the principles already mention in data collection. (Section 5)</p> <ul style="list-style-type: none"> ▸ Section 7, § 5 of the LGPD: The controller who obtained the consent referred to in item I of the caput of this section who needs to communicate or share personal data with other controllers shall obtain specific consent from the data subject for this purpose, subject to the possibilities of waiver of consent provided for in the Law. ▸ Section 11, § 3 of the LGPD: The communication or shared use of sensitive personal data between controllers in order to obtain economic advantage may be subject to sealing or regulation by the national authority, after hearing the sectoral bodies of the Public Power, within the scope of its powers. Section 11, § 4 of the LGPD: Communication or shared use between controllers of sensitive personal data related to health is not permitted in order to obtain economic advantage, except in the hypotheses related to the provision of health services, pharmaceutical care and health care, provided that paragraph 5 of this Section is observed, including the auxiliary services of diagnosis and therapy, for the benefit of the interests of data subjects, and to enable: <ul style="list-style-type: none"> a. Data portability of data when requested by the data subject. b. The financial and administrative transactions resulted from the use and provision of the referred services. ▸ Section 27 of the LGPD: The communication or shared use of personal data of a legal entity of public law to a person of private law shall be informed to the national authority and shall depend on the consent of the data subject, except: <ul style="list-style-type: none"> a. In the case of waiver of consent provided for in the Law. b. In cases of shared use of data, in which advertising will be given in accordance with item I of Section 23 of the Law. c. In the exceptions contained in § 1 of Section 26 of the Law. <p>Single paragraph. Information to the national authority dealing with the caput of this section will be regulated.</p> <ul style="list-style-type: none"> ▸ Section 37. The controller and the operator shall keep track of the processing operations of personal data they carry out, especially when based on legitimate interest. ▸ Section 38. The national authority may determine to the controller to draw up an impact report on the protection of personal data, including sensitive data, relating to its data processing operations, in accordance with the regulation, in accordance with trade and industrial secrets. <p>Single paragraph. In accordance with the provisions of the caput of this section, the report should contain, at least, the description of the types of data collected, the methodology used for the collection and assurance of the security of information and the analysis of the controller with respect to measures, safeguards and risk mitigation mechanisms adopted.</p> <ul style="list-style-type: none"> ▸ Section 39. The operator shall carry out the treatment in accordance with the instructions provided by the controller, who shall verify compliance with the instructions and the rules on the subject. ▸ Section 40. The national authority may provide for interoperability standards for portability, free access to data and security, as well as on record storage time, in particular with a view to the need and transparency. <p>Single paragraph. Information to the national authority dealing with the caput of this section will be regulated.</p>
Data processing	Can the services be provided through a third party (data processing)? If so, please explain the procedure and exceptions, if applicable.	Yes	<p>The controller and the processor shall keep records of personal data processing operations carried out by them. Moreover, the national authority may determine that the controller must prepare an impact report on protection of personal data, including sensitive data, referring to its data processing operations, pursuant to regulations, subject to commercial and industrial secrecy. The processor shall carry out the processing according to the instructions provided by the controller, which shall verify the obedience of the own instructions and of the rules governing the subject.</p> <p>(Section 37 and 38).</p>
Data retention	Is it mandatory to retain/conserve the data collected or processed for a specific term? If so, what is the term?	No	<p>Although it is possible to find specific data retention periods on the Brazilian legislation, there is no obligation to retain the data collected or processed under the LGPD.</p>

Matter	Concept	Yes / No / NA	Observations / comments
Data deletion	Is there an obligation to eliminate the data collected or processed? If so, under what conditions and for what terms?	Yes	<p>The personal data shall be eliminated after termination of the processing thereof, within the scope and technical limits of the activities, and the conservation shall be authorized for the purposes mentioned in Section 16. The processing can be considered as finalized in the events mentioned at Section 15.</p> <ul style="list-style-type: none"> ▸ Section 15. Termination of the processing of personal data shall occur in the following events: <ul style="list-style-type: none"> a. Verification that the purpose was reached or that the data are no longer necessary or pertinent to attain the specific purpose sought. b. Lapse of the processing period. c. Communication of the data subjects, including in the exercise of their right to revoke the consent as set forth in paragraph 5 of section 8 of the law, upon protection of the public interest. d. Order of the supervisory authority, in the event of breach of the provisions of the Law. ▸ Section 16. The personal data shall be eliminated after termination of the processing thereof, within the scope and technical limits of the activities, and conservation thereof shall be authorized for the following purposes: <ul style="list-style-type: none"> a. Compliance with a statutory or regulatory obligation by the controller. b. Studies by a research body, guaranteeing, whenever possible, the anonymization of personal data. c. Transfer to third parties, upon compliance with the data processing requirements set forth in the law. d. Exclusive use of the controller, provide the data are anonymized, it being understood that the access thereto by third parties is prohibited.
Privacy impact assessment	Are privacy impact assessments mandatory?	No	<p>The LGPD has as one of its principles a general accountability obligation. This requires the demonstration and adoption of effective measures capable of proving compliance with data protection law and demonstrating the effectiveness of these measures.</p> <p>Moreover, the adoption of these measures is a mitigating factor if sanctions are imposed.</p> <p>The LGPD defines the data protection impact assessment as a documentation of the controller that contains a description of the personal data processing processes that could generate risks to the civil liberties and to the fundamental rights, as well as measures, safeguards and mechanisms to mitigate risks. However, there is no obligation to do the Privacy Impact Assessment, unless when required by the ANPD.</p> <p>The ANPD, may request to the controller to prepare a data protection impact assessment, including of sensitive data, relating to its data processing operations, as provided for by the regulations, with due regard for trade and industrial secrets (Section 38), and to the government agents the publication of personal data protection impact assessment and suggest the adoption of standards and good practices for the processing of personal data by the Government (Section 16 and 32).</p> <p>In addition, Section 10, § 3 - The national authority may request the controller to report on the protection of personal data, where the processing is based on its legitimate interest, in the interests of commercial and industrial secrets.</p> <p>LGPD brings the competence to ANPD edit regulations and procedures on the protection of personal data and privacy, as well as on Privacy Impact Assessments for cases in which the treatment represents a high risk to the guarantee of the general principles of protection of personal data provided in the law. Until now the ANPD does not have an official template about it.</p>

Matter	Concept	Yes / No / NA	Observations / comments
Incidents	Is it mandatory to report security incidents or breaches or the related legal provisions?	Yes	<p>The controller must inform the national authority and the data subject of the occurrence of a security incident that may cause significant risk or damage to the data subjects. The ANPD shall verify the seriousness of the incident and may, if necessary, to safeguard the rights of the data subjects, determine the controller to adopt measures. (Section 48 and 49).</p> <p>Furthermore, the ANPD published Resolution CD/ANPD No. 15/2024, which introduces the Regulation on Security Incident Reporting, indicating that this communication must occur when the incident may entail a significant risk or harm to the data subjects (Section 4), outlining the criteria for determining the existence of this risk, which are:</p> <ul style="list-style-type: none"> ▶ Section 5: The security incident may entail a significant risk or harm to the data subjects when it can significantly affect the interests and fundamental rights of the data subjects and, cumulatively, involve at least one of the following criteria: <ul style="list-style-type: none"> I - sensitive personal data. II - data of children, adolescents, or the elderly. III - financial data. IV - authentication data in systems. V - data protected by legal, judicial, or professional secrecy. VI - large-scale data. <p>Moreover, the communication of a security incident to the ANPD must be made by the controller within three business days, except for the existence of a communication deadline provided for in specific legislation (Section 6), with such period being counted from the controller's knowledge that the incident affected personal data (Section 6, § 1), and must contain the following information (Section 6, § 2):</p> <ul style="list-style-type: none"> I - the description of the nature and category of personal data affected. II - the number of data subjects affected, specifying, when applicable, the number of children, adolescents, or the elderly. III - the technical and security measures used to protect the personal data, adopted before and after the incident, observing commercial and industrial secrets. IV - the risks related to the incident with identification of the possible impacts on the data subjects. V - the reasons for the delay, in case the communication was not made within the stipulated period. VI - the measures that have been or will be taken to reverse or mitigate the effects of the incident on the data subjects. VII - the date of the incident occurrence, when possible to determine it, and its knowledge by the controller. VIII - the data of the officer or the person representing the controller. IX - the identification of the controller and, if applicable, a statement that it is a small-scale processing agent. X - the identification of the operator, when applicable. XI - the description of the incident, including the main cause, if it can be identified. XII - the total number of data subjects whose data are processed in the activities affected by the incident.

Matter	Concept	Yes / No / NA	Observations / comments
Sanctions	Are there sanctions for failures to comply with this obligation? If so, please list them along with the corresponding sanction or penalty amounts.	Yes	<p>Violation of provisions of the LGPD shall lead into administrative responsibilities. The provisions in this section of the LGPD does not replace the imposition of administrative, civil or criminal penalties defined by any specific Brazilian law. The data processing agents, in connection with any infractions of the rules established in the LGPD, shall be subject to the Section 52 administrative penalties.</p> <p>Section 52. Data processing agents, due to violations committed to the rules provided for in the Law, are subject to the following administrative sanctions applicable by the national authority:</p> <ul style="list-style-type: none"> I. Warning, with indication of a deadline for the adoption of corrective measures. II. Simple fine, up to 2% (two percent) of the revenue of the legal entity of private law, group or conglomerate in Brazil in its last fiscal year, excluding taxes, limited in total to R\$ 50,000,000.00 (fifty million reais) per infraction. III. Daily fine, observing the total limit referred to in item II. IV. Publicization of the infringement after properly cleared and confirmed its occurrence. V. Blocking of the personal data referred to in the infringement until its regularization. VI. Deletion of the personal data to which the infringement relates. VII. (vetted). VIII. (vetted). IX. (vetted). X. Partial suspension of the operation of the database referred to in infringement for a maximum period of 6 (six) months, extendable for the same period, until the regularization of the processing activity by the controller; (included in law No. 13,853, 2019). XI. Suspension of the exercise of the activity of processing personal data to which the infringement refers for a maximum period of 6 (six) months, extendable for the same period; (included in law No. 13,853, 2019). XII. Partial or total prohibition of the exercise of activities related to data processing. (included in law No. 13,853, 2019).
Legal actions	Are there any legal actions for personal data protection? Who has the right to exercise/request them?	Yes	<p>The defense of the interests and rights of the data subject may be exercised in court, individually or collectively, in the form of the provisions of the applicable law (LGPD), about the instruments of individual and collective protection. In addition, the personal data relating to the regular exercise of rights by the data subjects cannot be used against them. (Section 21 and 22).</p>
Delegate or Responsible for the protection of personal data	Is there a Data Protection Officer (DPO) or similar position? If so, is their appointment mandatory? Must they be appointed locally?	Yes	<p>In the LGPD the DPO figure is defined as a person appointed by the controller, who acts as a channel of communication between the controller and the data subjects and the supervisory authority. The controller shall indicate a data protection officer. Additionally, the ANPD published Resolution CD/ANPD No. 18/2024 that introduces the Regulation on the DPO role, indicating the requirement for formalization in the appointment of the DPO (Section 3), as well as the disclosure of the identity and information of this DPO (Sections 8 and 9), the characteristics to be observed for the position (Sections 12 to 14), and the activities to be performed (Sections 15 to 17). It is highlighted that the officer may be either a natural person or a legal entity (Section 12) but must be able to communicate with the data subjects and with the ANPD, clearly and precisely, and in Portuguese (Section 13). Furthermore, the officer must act with ethics, integrity, and technical autonomy, avoiding situations that may constitute a conflict of interest (Section 18), and may also hold multiple roles and perform their activities for more than one data processing agent, provided that they can fully meet their responsibilities related to each data processing agent and there is no conflict of interest (Section 19).</p>
Processing Records	Are there any mandatory requirements for maintaining processing records under the applicable laws? Specifically, what information must be included in these records, and are there any particular conditions or circumstances under which data controllers or processors are obliged to keep detailed records of their data processing activities?	Yes	<p>Section 37 of the LGPD stipulates that the controller and the operator must keep a record of the personal data processing operations they carry out, especially when based on legitimate interest. Thus, it is understood that these records must always be maintained, although the law does not specify the details of the information that must be contained in this record.</p>
Research	Can a competent authority officially act and/or investigate breaches of personal data protection?	Yes	<p>In the event of a violation on LGPD, as a result of the processing of personal data by public bodies, the supervisory authority like ANPD, may send a communication with applicable measures to cease the violation (Section 31). In addition, the Resolution CD/ANPD No. 01/2021, provides that the ANPD can act ex officio in monitoring duties (Section 16).</p>

Matter	Concept	Yes / No / NA	Observations / comments
Similarities with the GDPR	Per your understanding, do you believe that the regulation contemplates all of the requirements set by similar international regulations (e.g., Example: GDPR)? What relevant differences did you find?	Yes	Yes, in general, the LGPD is very similar to the GDPR.
Other obligations	Are there other additional considerations/requirements or legal obligations on data protection that must be met?	Yes	The LGPD provides that ANPD will be in charge of defining some important dispositions to ensure the law. In this way, future regulations on privacy and personal data protection may be published by the ANPD.

A scenic landscape of the Andes mountains in Chile. In the foreground, a small stream flows through a rocky, grassy area. The middle ground shows a valley with low hills and a path leading towards the mountains. The background is dominated by a range of high, rugged mountains with snow-capped peaks under a blue sky with scattered clouds.

chile



Matter	Concept	Yes / No / NA	Observations / comments
Regulations	Does the country have a personal data protection law? If so, please name the applicable regulation.	Yes	<p>Personal data protection is regulated mainly in Law No. 19,628, on the protection of privacy ("PDPL"). However, in August 2024, the Data Protection Bill (bulletins No. 11,092-07 and No. 11,144-07) was approved, which is currently in its final approval stages and will replace the text of the existing legislation (the "Bill"). Likewise, Law No. 20,575 established the principle of purpose in relation to the processing of economic, financial, banking, or commercial personal data.</p> <p>Moreover, the Constitution of the Chile Republic, in its Section 19 No. 4, consecrates the right to the protection of privacy and personal data, so this right is constitutionally protected.</p>
Enforcement Authority	Who is the enforcement authority? If applicable, please provide their website link	Yes	<p>Since currently there is no authority specifically in charge of overseeing matters related to personal data protection. The National Consumer Service (SERNAC) was granted legal powers to enforce compliance with the PDPL in the context of consumer relations. The SERNAC website can be found at the following link.</p> <p>However, the Bill includes the creation of the Data Protection Agency, which will be an autonomous public law corporation, technical in nature, decentralized, with legal personality and its own assets.</p> <p>The purpose of the Data Protection Agency will be to ensure the effective protection of the rights that safeguard individuals' privacy and their personal data, in accordance with the provisions set forth in the Bill, as well as to oversee compliance with its regulations.</p> <p>This agency has not yet been created, and therefore does not currently have a website.</p>
Scope of Application	Which is the regulation's scope of application? I.e., is it a strictly national or cross-border concept?	Yes	<p>The scope of the PDPL is territorial and does not extend its application outside the country.</p> <p>The Bill will apply to the processing of personal data conducted under any of the following circumstances:</p> <ol style="list-style-type: none"> When the controller or processor is established or constituted in Chile. When the processor, regardless of its place of establishment or incorporation, performs personal data processing operations on behalf of a controller established or constituted in Chile. When the controller or processor is not established in Chile, but their personal data processing operations are aimed at offering goods or services to individuals located in Chile, regardless of whether payment is required, or monitoring the behavior of individuals in Chile, including their analysis, tracking, profiling, or prediction of behavior. The processing of personal data carried out by a controller who, without being established in Chile, is subject to Chilean legislation due to a contract or international law.
Data collection	Which are the requirements or processes for personal data collection? (For example, data subject consent, information on purpose of data use and subject's rights, etc.)	Yes	<p>According to Section 4 of the PDPL, the processing of personal data, including its collection, must be authorized by the holder in advance, expressly and in writing, or by equivalent electronic means. Likewise, the data subject must be duly informed, regarding the purpose of the storage of his personal data and its possible disclosure to the public.</p> <p>According to Article 12 of the Bill, the processing of personal data concerning the data subject is lawful when the subject grants their consent for it.</p> <p>This consent must be free, informed, and specific regarding its purpose or purposes, and it must be expressed in advance and unequivocally through a verbal statement, written declaration, or an equivalent electronic means, or through an affirmative act that clearly indicates the will of the data subject.</p>
Legal concept of "personal data"	What are personal data	Yes	<p>In its Section 2, the PDPL defines personal data as those related to any information concerning identified or identifiable individuals.</p> <p>The Bill, in Article 2, letter f, defines the concept of personal data as "any information linked to or referred to a natural person who is identified or identifiable. An identifiable person is one whose identity can be determined, directly or indirectly, particularly through one or more identifiers, such as name, identity card number, or analysis of elements specific to that person's physical, physiological, genetic, mental, economic, cultural, or social identity. To determine whether a person is identifiable, all means and objective factors that could reasonably be used for such identification at the time of processing must be considered".</p>

Matter	Concept	Yes / No / NA	Observations / comments
Personal data categories	Are there different personal data categories? Please explain each category, if applicable.	Yes	<p>Personal data categories included in Section No. 2 of PDPL are:</p> <ul style="list-style-type: none"> ▶ Expired data: data that is no longer updated by provision of law, because of the compliance with the condition, or the expiration of its validity term, or should there not be an express rule, because of the change of facts or circumstances that it consigns. ▶ Statistical data: data that in its origin or processing cannot be associated to an identified or identifiable subject. ▶ Sensitive data: personal data that refers to physical or moral characteristics of individuals, or 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. <p>The Bill recognizes the following categories defined in Article 2:</p> <ul style="list-style-type: none"> ▶ Obsolete Data: Data that has lost its relevance due to a legal provision, the fulfillment of a condition, or the expiration of the defined period for its validity. If there is no express regulation, it may also become obsolete due to changes in the facts or circumstances it records. ▶ Statistical Data: Data that, in its origin or through its processing, cannot be associated with an identified or identifiable holder. ▶ Sensitive Personal Data: These are personal data that refer to the physical or moral characteristics of individuals or to facts or circumstances of their private or intimate lives. This category includes data that reveals ethnic or racial origin, political, union, or professional affiliation, socioeconomic status, ideological or philosophical beliefs, religious beliefs, health-related data, biological profiling, biometric data, and information related to sexual life, sexual orientation, and gender identity of a natural person.
Situation of the corporations and other legal entities.	Does the regulation sufficiently protect the personal data of the corporations or entities?	No	The definition of "personal data" offered by PDPL and the Bill, in Section 2, is limited to information concerning natural persons excluding corporations.
Data subject consent	Is the data subject's consent required to collect the data? If so, are there conditions to obtaining the data subject's consent? (For example, prior information that must be provided to the data subject).	Yes	<p>According to Section 4 of the PDPL, previous, explicit, and written consent - or by equivalent electronic means - from the data subject must be obtained. Before giving their consent, the interested party must be informed of the purpose for the data processing, and its possible disclosure to the public.</p> <p>According to Article 12 of the Bill, the processing of personal data concerning the holder is lawful when they grant their consent for such processing.</p> <p>This consent must be free, informed, and specific regarding its purpose or purposes. Additionally, it must be expressed prior to the processing and in an unequivocal manner, through a verbal or written declaration, via an equivalent electronic means, or through an affirmative act that clearly demonstrates the holder's will.</p>

Matter	Concept	Yes / No / NA	Observations / comments
Exceptions to the consent	<p>Are there exceptions to the voluntary consent of a data subject? If so, please list the exceptions.</p>	Yes	<p>The exceptions contemplate in PDPL to the consent given by the data subject, that is, the occasions in which the data controller shall not require the consent of the data subject for the processing of his or her data are:</p> <ol style="list-style-type: none"> 1. When processing is authorized by law. 2. When the information is coming or collected from public access sources, when it is about economic, financial, banking, or commercial matters, contained in listings related to individuals stating their belonging to a group, occupation, educational degrees, address, or date of birth, or when necessary for commercial notifications of direct answer or trade or sale or goods or services. 3. Regarding sensitive personal data, the consent of the subject will not be required when the data is necessary for the determination or granting of health benefits that correspond to their subjects. <p>The Bill contains exceptions to the holder's consent in Article 13, which states that the processing of personal data is lawful without the holder's consent in the following cases:</p> <ol style="list-style-type: none"> 1. When the processing relates to socioeconomic data concerning economic, financial, banking, or commercial obligations and is conducted in accordance with the regulations of Title III of the law, which governs the use of such data. 2. When the processing is necessary for the execution or compliance with a legal obligation or as stipulated by law. 3. When the processing is necessary for the celebration or execution of a contract between the holder and the responsible party or for the execution of pre-contractual measures taken at the holder's request. 4. When the processing is necessary to satisfy the legitimate interests of the controller or a third party, provided that the rights and freedoms of the holder are not affected. In any case, the holder may always demand to be informed about the processing affecting them and the legitimate interest on which the processing is based. 5. When the processing of data is necessary for the formulation, exercise, or defense of a right before the courts or public agencies. <p>The controller must demonstrate the lawfulness of the data processing.</p>
Content and scope of the information to be validated by the data subject.	<p>What should be the content of the consent? (For example, data use or destination, international data transfer, etc.)</p>	Yes	<p>Data subjects must be duly informed regarding the purpose of storing their personal data and possible notification to the public. According to Article 12 of the Bill, the processing of personal data concerning the holder is lawful when they provide their consent for such processing.</p> <p>This consent must be free, informed, and specific regarding its purpose or purposes. It must also be expressed in advance and unequivocally, through a verbal or written declaration, an equivalent electronic means, or through an affirmative act that clearly demonstrates the holder's will.</p>
Transfer of personal data	<p>Are there requirements or restrictions on the transfer of personal data? Are there requirements that apply to the international transfer of data? (Example: model clauses, Supervisors' authorization, etc.)</p>	Yes	<p>Although in PDPL there are no specific dispositions on personal data transfer both national and cross-border transfers are subject to general data processing standards.</p> <p>Therefore, the transfer of personal data will be legitimate, as a general rule, when it is based on the consent expressly given in written form - or equivalent electronic means - by the data subject. It should also be noted that, in its Section 5, the PDPL admits the possibility of automatic data transfer.</p> <p>The Bill regulates the transfer of personal data in Article 15, stating that personal data may be assigned with the consent of the data subject and for the fulfillment of the processing purposes (as well as in other specific circumstances, such as the legitimate interest of the assignor or assignee).</p> <p>If the consent given by the data subject at the time of data collection did not include the possibility of transfer, new consent must be obtained before such transfer occurs, which will be considered a new processing operation for all legal purposes.</p> <p>On the other hand, international transfers are regulated in Article 27 and subsequent articles, which state that these operations will be lawful when certain conditions are met, such as when the recipient is subject to the legal framework of a country that provides adequate levels of protection (this is further regulated by Article 28). Specific circumstances are also included that allow for the transfer of data even when adequate guarantees do not exist, such as when data must be transferred to fulfill obligations arising from treaties or international agreements that have been ratified by the Chilean State and are currently in force, among others.</p>

Matter	Concept	Yes / No / NA	Observations / comments
BCR	Do they have binding corporate rules (BCR)?	No	<p>Not stated in the Law.</p> <p>Article 28 of the Bill, which regulates the rules for determining adequate countries for the international transfer of data, states that international data transfers will be lawful when they are covered by contractual clauses, binding corporate rules (BCR), or other legal instruments signed between the transferring data controller and the receiving data controller or third-party processor, provided that adequate safeguards are established within them.</p> <p>Additionally, the Bill indicates that when the transfer occurs between companies or entities that belong to the same corporate group, as long as all of them operate under the same standards and policies regarding the processing of personal data, the transfers may be covered by binding corporate rules (BCR) previously approved by the Data Protection Agency.</p>
Sensitive data	What is understood by sensitive data? How is sensitive data processed, if applicable?	Yes	<p>Sensitive data, as defined in Section 2 of the PDPL, are those that refer to the individuals' physical or moral characteristics of individuals, or facts or circumstances of their private or intimate life, such as:</p> <ul style="list-style-type: none"> ▶ Personal habits. ▶ Racial origin. ▶ Political opinions and ideologies. ▶ Religious convictions or beliefs. ▶ Physical or psychic wellbeing. ▶ Sex life. <p>Sensitive data processing is only allowed when authorized by law, when there is consent of the subject or are necessary data for the determination or granting of health benefits that correspond to their holders.</p> <p>According to Article 2 of the Bill, sensitive personal data refers to:</p> <ul style="list-style-type: none"> ▶ The physical or moral characteristics of individuals. ▶ Facts or circumstances related to their private life or intimacy. ▶ Information revealing ethnic or racial origin, political, union, or professional affiliation, socioeconomic status, ideological or philosophical convictions, and religious beliefs. ▶ Data related to health, human biological profiling, and biometric data. ▶ Information regarding sexual life, sexual orientation, and gender identity of a natural person. <p>According to Article 16, the processing of sensitive personal data may only occur when the data subject explicitly provides their consent through a written, verbal declaration, or an equivalent technological mean.</p> <p>Certain exceptions to consent are also contemplated, such as when the data has been made public or when it is necessary to safeguard the life, health, or physical or mental integrity of the data subject or another person, among other cases.</p>
Database registration or periodic reporting to the corresponding authority	Is it mandatory to register (e.g., with the corresponding enforcement body) a database and/or a database ownership, processing and/or use? Is it mandatory to submit any type of information or report periodically to the enforcement authority?	No	<p>The PDPL does not establish any registration obligation regarding databases, their ownership, processing, or use, to the extent that they are private.</p> <p>Regarding public bodies, Section 22 of the PDPL established that the Civil Registry and Identification Office must keep record of personal data banks in the hands of public bodies.</p> <p>The Bill does not include obligations for a database registry, nor does it mandate the submission of periodic reports to the authority.</p>

Matter	Concept	Yes / No / NA	Observations / comments
Data security	Are there technical measures to guarantee the security and confidentiality of personal data? If so, what are they?	No	<p>In its Section 11, the PDPL establishes that the data controller must safekeep data with all due diligence. In turn, Section 7 of the PDPL in turn establishes that people that work in personal data processing, whether publicly or privately, are obliged to their secrecy.</p> <p>The obligations of the data controller, as outlined in Article 14 and subsequent articles of the Bill, include:</p> <ul style="list-style-type: none"> ▶ Duty of Secrecy or Confidentiality: The data controller is required to maintain the secrecy or confidentiality of the personal data concerning a data subject, unless the data subject has made it manifestly public. This duty continues even after the relationship with the data subject has ended. ▶ Duty of Protection by Design and by Default: The controller must apply appropriate technical and organizational measures from the design stage and throughout the processing of personal data. The measures should take into account the state of technology, implementation costs, the nature, scope, context, and purposes of data processing, as well as the associated risks. ▶ Duty to Adopt Security Measures: The data controller must implement necessary measures to ensure compliance with the principle of security, considering the current state of technology and application costs, along with the nature, scope, context, and purposes of data processing. This includes the likelihood of risks, and the severity of their effects related to the type of data processed. The measures adopted should ensure the confidentiality, integrity, availability, and resilience of the data processing systems. Furthermore, they should prevent unauthorized alteration, destruction, loss, processing, or access. Such measures may include data pseudonymization and encryption, as well as regular verification, assessment, and evaluation processes to ensure the effectiveness of the technical and organizational measures in safeguarding data processing security.
Rights of the data subjects	What are the data subjects' rights? (Example: correction, update, or deletion). Please list and explain.	Yes	<p>The PDPL expressly recognizes the following data subject rights in Section 12:</p> <ul style="list-style-type: none"> ▶ Right to be informed about data concerning your person, its source and recipient, the purpose of storage and the identification of the persons or agencies to which your data is regularly transmitted. ▶ Right to rectify data, that is, to be modified in case the personal data is erroneous, inaccurate, misleading, or incomplete. ▶ The right to have their data deleted or blocked in the event that their storage lacks legal grounds or when they are out of date; when they have been voluntarily provided or are used for commercial communications and the holder does not wish to continue appearing in the respective registry, either definitively or temporarily. <p>The information, modification or elimination of data shall be completely free. At the subject's request, a copy of the corresponding amended record must also be provided. If new modifications or deletions of data are made, the holder may also obtain, free of charge, a copy of the updated registry, provided that at least 6 months have elapsed since the last time a copy of the registry was requested.</p> <p>The Bill recognizes the following rights of data subjects in Article 4:</p> <ul style="list-style-type: none"> ▶ Right of Access: The right to request and obtain confirmation from the data controller regarding whether the personal data concerning them is being processed, and, if so, to access such data and related information (purposes, categories, etc.). ▶ Right of Rectification: The right to request and obtain from the data controller the rectification of personal data concerning them that is being processed, when such data is inaccurate, outdated, or incomplete. ▶ Right of Erasure: The right to request and obtain from the data controller the deletion of personal data concerning them in certain cases, such as when the data is no longer necessary for the purposes for which it was collected, when the data subject has revoked their consent, when the data has been obtained or processed unlawfully, or when it consists of outdated data, among others. ▶ Right of Opposition: The right to object to the data controller regarding specific or determined processing of their personal data in certain cases, such as when the legal basis for processing is the satisfaction of the legitimate interests of the controller, or if the processing is conducted solely for marketing or direct marketing purposes of goods, products, or services, including profiling, among others. ▶ Right to Block Processing: The right to request the temporary suspension of any operation involving the processing of personal data when a request for rectification, erasure, or opposition is made in accordance with the law. ▶ Right to Data Portability: The right to request and receive a copy of the personal data concerning them that they have provided to the controller, in a structured, commonly used, and machine-readable electronic format that allows interoperability with different systems, and to communicate or transfer this data to another data controller, when the processing is automated and based on the consent of the data subject.

Matter	Concept	Yes / No / NA	Observations / comments
Actions by the data subjects	How can they exercise them?	Yes	<p>With respect to the exercise of the aforementioned rights, the PDPL establishes in its Section 16 that, if the responsible party does not decide on the holder's request within two business days, the holder may appeal before a civil court judge.</p> <p>Likewise, Section 23 of the PDPL states that data controllers must compensate data subjects for the economic and moral damage caused by improper data processing, in addition to deleting, modifying, or blocking the data as requested by the data subject or as ordered by the court if applicable.</p> <p>To do so, the holder must file an action before civil courts.</p> <p>Finally, the right to protection of personal data and privacy is a constitutionally established right, so that constitutional actions, such as the appeal for protection, are also tools to exercise the rights of data subjects, to the extent that they have been violated.</p> <p>The Bill establishes in its Articles 10 and 11 that these rights can be enforced against the data controller, and, if there are multiple controllers, any of them may be approached.</p> <p>The exercise of the rights to rectification, erasure, and opposition will always be free for the data subject. The right of access can also be exercised free of charge at least quarterly.</p> <p>To exercise these rights, the data subject must submit a request to the data controller, which must include certain details, such as their identification, contact method, and the specific data regarding which the right is being asserted. In the case of a rectification request, the subject must indicate the correction to be made and provide supporting documentation.</p> <p>The data controller is required to acknowledge receipt of the request and respond within 30 days (extendable by an additional 30 days). In the event of a total or partial denial of the request, controllers must justify their decision by stating the invoked reason and the evidence that supports it. Additionally, controllers must inform the data subject that they have a period of thirty consecutive days, which can be extended for the same duration, to lodge a complaint with the Data Protection Agency. If, after the 30-day period, the data subject does not receive a response, they may directly appeal to the Data Protection Agency.</p>
Assignment of personal data	What are the requirements for the assignment of personal data?	Yes	<p>The transfer of personal data is governed by the general rules for processing, that is, express written authorization - or equivalent electronic means - of the data subject must be obtained.</p> <p>Likewise, according to Section 5 of PDPL, the data or personal bank controller can establish an automatic transfer procedure, as long as it is stated on record:</p> <ol style="list-style-type: none"> 1. The individualization of the applicant. 2. The reason and purpose of the request. 3. The type of data being transferred. <p>Article 15 of the Bill states that personal data may be transferred with the consent of the data subject and for the fulfillment of the purposes of processing. Personal data may also be assigned/shared when such disclosure is necessary for the performance and execution of a contract in which the data subject is a party; when there is a legitimate interest on the part of the assignor or the assignee; and when provided by law.</p> <p>Regarding public bodies, Article 22 of the Bill indicates that they are authorized to communicate or disclose specific personal data, or all or part of their databases or data sets, to other public bodies, exclusively, as long as the communication or disclosure of data is necessary for the fulfillment of their legal functions and both bodies operate within the scope of their competences. The communication or assignment of data must be carried out for a specific processing purpose, and the receiving public body may not use the data for different purposes.</p> <p>The assignment of data must be documented in writing or through any suitable electronic means. It must specify the parties involved, the data that will be assigned, the intended purposes for processing, and any other agreements or stipulations made by the assignor and the assignee.</p> <p>Once the assignment of the data is completed, the assignee assumes the role of data controller for all legal purposes. The assignor, for its part, also retains its status as data controller regarding the processing operations it continues to carry out.</p> <p>If a data assignment occurs without the necessary consent of the data subject, the assignment will be null and void, and the assignee must delete all received data, without prejudice to any corresponding legal liabilities.</p>

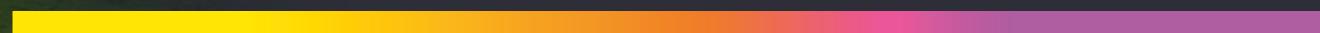
Matter	Concept	Yes / No / NA	Observations / comments
Data processing	Can the services be provided through a third party (data processing)? If so, please explain the procedure and exceptions, if applicable.	Yes	<p>There are no additional requirements under PDPL.</p> <p>Data processing services may be provided on behalf of third parties. According to Section 8 of the PDPL, in the event that data are processed by attorney in fact, the general rules of the same shall apply. In addition, the power of attorney must be granted in writing, leaving a special record of the conditions of the use of the data.</p> <p>According to Article 15 bis of the Bill, the data controller may process data directly or through a third-party processor, who must do so in accordance with the instructions and directives provided by the controller. The processor is prohibited from processing the data for any purpose other than that agreed upon with the controller, as well as from transferring or disclosing the data in cases where the controller has not expressly and specifically authorized it to fulfill the purpose of the tasks.</p> <p>If the processor handles the data for a purpose different from the agreed tasks, or transfers or discloses it without authorization as stipulated in the previous paragraph, they will be considered a data controller for all legal purposes and must personally bear responsibility for any violations committed. Furthermore, they will be jointly liable with the data controller for any damages caused, without prejudice to any contractual liabilities they may have towards the assignor or data controller.</p> <p>Once the directives are completed, the data held by the processor must either be deleted or returned to the data controller, as appropriate.</p>
Data retention	Is it mandatory to retain/conserve the data collected or processed for a specific term? If so, what is the term?	No	<p>The PDPL does not establish a specific term for data retention/conservation.</p> <p>However, its Section 6 establishes that personal data must be eliminated or canceled when there is no legal basis for their storage or once they have expired.</p> <p>The Bill does not specify a particular retention period for personal data; however, the data subject may exercise the right to erasure if the data is no longer necessary in relation to the purposes for which it was collected or if the data is outdated.</p>
Data elimination	Is there an obligation to eliminate the data collected or processed? If so, under what conditions and for what term?	Yes	<p>As expressed in Section 6 of the PDPL, personal data must be eliminated or canceled when there is no legal basis for their storage or once they expire PDPL.</p> <p>The principle of proportionality, as outlined in Article 3 of the Bill, stipulates that personal data processed must be strictly limited to what is necessary, appropriate, and relevant to the intended purposes. Personal data may be retained only for the time necessary to fulfill these purposes, after which it must be erased or anonymized, unless exceptions are provided by law. Retention for a longer period requires legal authorization or the data subject's consent.</p>
Privacy impact assessment	Are privacy impact assessments mandatory?	Yes	<p>The PDPL does not regulate impact assessments.</p> <p>The impact assessment is addressed in Article 15 ter of the Bill, which mandates that when a particular type of data processing is likely to pose a high risk to the rights of data subjects due to its nature, scope, context, technology used, or purposes, the data controller must conduct a personal data protection impact assessment prior to beginning processing operations.</p> <p>The Bill also specifies cases where an impact assessment is mandatory, including when there is large-scale or mass data processing, or the processing of sensitive and specially protected data, particularly in scenarios where exceptions to consent apply.</p>
Incidents	Is it mandatory to report security incidents or breaches or the related legal provisions?	Yes	<p>The PDPL does not provide any obligation to report in case of security breaches.</p> <p>It states just one general obligation regarding data safety, imposed to the party responsible for the data bank in its Section 11: "to take care of them with due diligence, accounting for the damages". This obligation does not state specific safety measures to be applied by the party responsible.</p> <p>Article 14 of the Bill includes the duty to report breaches of security measures that lead to the accidental or unlawful destruction, leak, loss, or alteration of personal data, as well as unauthorized communication or access to such data, whenever there is a reasonable risk to the rights and freedoms of data subjects. The report must be made by the most expedient means possible.</p>

Matter	Concept	Yes / No / NA	Observations / comments
Sanctions	Are there sanctions for failures to comply with this obligation? If so, please list them along with the corresponding sanction or penalty amounts.	No	<p>As a general rule, the PDPL does not establish sanctions nor fines associated to non-compliance with legal obligations. The only existing sanction in the PDPL is the one given in Section 16 which states that in the event that the claim before the courts is accepted due to the lack of pronouncement of the responsible party in the exercise of the rights of the holders, the court may apply a fine of approximately USD 65 to USD 650 (1 to 10 Monthly Tax Units).</p> <p>In accordance with the above, Section 23 of the PDPL states that data controllers must compensate data subjects for the economic and moral damage caused by improper data processing, in addition to deleting, modifying, or blocking the data as requested by the data subject or as ordered by the court if applicable. To do so, the holder must file an action before civil courts.</p> <p>According to Article 34 quatre of the Bill, the deliberate omission of notifying security breaches that may impact the confidentiality, availability, or integrity of personal data constitutes a very serious infraction, which may be sanctioned with a fine of up to 20,000 monthly tax units. Furthermore, failure to notify or record security breaches (without fraud) constitutes a serious infraction under Article 34 and may result in a fine of up to 10,000 monthly tax units.</p>
Legal actions	Are there any legal actions for personal data protection? Who has the right to exercise/request them?	Yes	<p>In accordance with the above, Section 23 of the PDPL states that data controllers must compensate data subjects for the economic and moral damage caused by improper data processing, in addition to deleting, modifying, or blocking the data as requested by the data subject or as ordered by the court if applicable. To do so, the holder must file an action before civil courts.</p> <p>Furthermore, since the protection of personal data and privacy is a constitutionally guaranteed right, there is also the possibility of filing a constitutional protection action, which aims to have the court order all necessary measures to reestablish the violated right and ensure its protection.</p> <p>According to Articles 41 and subsequent provisions of the Bill, several legal actions are available to protect the rights of personal data holders:</p> <ol style="list-style-type: none"> Administrative Procedure for the Protection of Rights: Data holders may file a claim with the Data Protection Agency if the data controller has denied a request submitted per Article 11 (holder rights) or has not responded within the legally established timeframe. Administrative Procedure for Legal Violations: A sanctioning process can be initiated by the Data Protection Agency against data controllers who breach or fail to uphold data processing principles. Judicial Claim Procedure: Interested individuals or legal entities may file a claim for illegality with the Court of Appeals of Santiago or the court in the claimant's place of residence if they believe an administrative act that halts proceedings, or a final decision issued by the Data Protection Agency, is unlawful. The choice of court is at the claimant's discretion.
Personal data protection officer or controller.	Is there a Data Protection Officer (DPO) or similar position? If so, is their appointment mandatory? Must they be appointed locally?	No	<p>The PDPL does not establish a DPO. However, Law No. 20,575, in its Section 4, establishes that in regard to the use of personal data, the controller of economic, financial, banking, and commercial data must set an individual to act as a data protection officer, before whom the subjects can exercise the rights granted by the PDPL.</p> <p>Article 49 of the Bill introduces an infraction prevention model, which data controllers may adopt voluntarily as a compliance program. Among the essential elements of this program is the designation of a Data Protection Officer (DPO).</p> <p>While appointing a DPO is not mandatory, it is a basic requirement for an effective compliance program. The DPOs do not necessarily need to be designated locally but must have adequate independence and sufficient resources to carry out their responsibilities.</p>
Investigations	Can a competent authority officially act and/or investigate breaches of personal data protection?	Yes	<p>The responsibilities of the Data Protection Agency, as outlined in the Bill, include:</p> <ul style="list-style-type: none"> Monitoring Compliance: The agency is empowered to oversee adherence to the law and related data protection regulations. To fulfill this role, it can require data controllers to provide any documents, records, or information deemed necessary to support its supervisory functions. Identifying Infractions: The agency can determine violations and non-compliance by those engaged in data processing activities, specifically concerning the principles and obligations established by law. For this purpose, and with proper justification, it may summon individuals involved in data processing—such as data subjects, legal representatives, managers, advisors, employees, or anyone with relevant knowledge—to give statements. These declarations can also be collected through alternative means that ensure accuracy.

Matter	Concept	Yes / No / NA	Observations / comments
Processing Records	Are there any mandatory requirements for maintaining processing records under the applicable laws? Specifically, what information must be included in these records, and are there any particular conditions or circumstances under which data controllers or processors are obliged to keep detailed records of their data processing activities?	No	The Bill does not mandate the creation of compulsory data processing records.
Similarities with the GDPR	Per your understanding, do you believe that the regulation contemplates all the requirements set by similar international regulations (e.g., Example: GDPR)? What relevant differences did you find?	No	<p>The PDPL dates back to 1999 and, although it has some amendments, it is still far away from the standards commonly incorporated in international regulations, such as GDPR.</p> <p>Despite having theoretically high standards (express written consent is required from the data subjects) the inexistence of other sources of legitimacy, the lack of a competent authority exclusively dedicated to supervising this matter and the absence of fines and administrative procedures to facilitate the exercise of the rights of data subjects, in particular, has meant that compliance with the PDPL is practically non-existent. For example, it does not regulate the same legal basis or principles for data processing, nor does it establish precise obligations to the data controller, there is no authority in charge of the matter, it does not consider sanctions, nor states the right of data portability, among others.</p> <p>The bill that amends the current LDPD incorporates protection standards very similar to those of the GDPR. Some of its novelties compared to the effective law are the creation of an Agency for the Protection of Personal Data, the establishment of fines for non-compliance, the incorporation of new sources of legitimacy (legitimate interest, contractual compliance, tacit consent, etc.), the incorporation of the right of portability, among others.</p>
Other obligations	Are there other additional considerations/requirements or legal obligations on data protection that must be met?	N/A	



colombia



Matter	Concept	Yes / No / NA	Observations / comments
Regulations	<p>Does the country have a personal data protection law? If so, please name the applicable regulation.</p>	Yes	<p>Colombian data protection regulations are as follows:</p> <ul style="list-style-type: none"> ▶ Sections. 15 and 20, Political Constitution of Colombia. ▶ Statutory Law No. 1,266/2008 ("Law 1266"). ▶ Decree No. 2,952/10 ("Dec. 2952"), compiled in Decree No. 1,074 of 2015 ("Dec. 1074"). ▶ Decree No. 1,727/2009 ("Dec. 1727"), compiled in Decree No. 1,074 of 2015 ("Dec. 1074"). ▶ Law No. 1,273 of 2009 ("Law 1,273"). ▶ Statutory Law No. 1581/2012 ("Law 1,581"). ▶ Decree No. 1,377/2013 ("Dec. 1,377"), compiled in Decree No. 1,074 of 2015 ("Dec. 1,074"). ▶ Law No. 1,712/2014 ("Law 1,712"). ▶ Decree No. 886/2014 ("Dec. 886"), compiled in Decree No. 1,074 of 2015 ("Dec. 1,074"). ▶ Decree No. 1,413/2017 ("Dec. 1,413") adds to Decree No. 1,078 of 2015 ("Dec. 1,078"). ▶ Law No. 1,928/2018 ("Law 1,928"). ▶ Decree No. 090 of 2018 ("Dec. 090"). ▶ Decree No. 255/2022 ("Dec. 255") by which Section 7 is added to Chapter 25 of Title 2 of part 2 of Book 2 of Dec. 1,074. ▶ Single legal circular of the Superintendence of Industry and Commerce ("SIC"). <p>On a regular basis, the SIC, as the national authority responsible for ensuring compliance with personal data regulations, publishes guidelines in this field. While these guidelines are not legally binding, they aim to provide guidance to individuals and legal entities on the proper handling of personal data.</p> <p>To date, the SIC has published the following guidelines, which can be consulted at the following link: Publicaciones Superintendencia de Industria y Comercio (sic.gov.co):</p> <ul style="list-style-type: none"> ▶ Guidelines on Personal Data for Public and Private Education (2015). ▶ Guide for the Implementation of the Principle of Accountability (2016). ▶ Guide for Requesting the Declaration of Compliance on International Transfers of Personal Data (2016). ▶ Guide on the Processing of Personal Data for Marketing and Advertising Purposes (2019). ▶ Guide for the Implementation of the Principle of Accountability (2019). ▶ Guide on the Processing of Personal Data for Electronic Commerce Purposes (2019). ▶ Guide on the Processing of Personal Data in Horizontal Property (2020). ▶ Guide on the Processing of Photos as Personal Data (2020). ▶ Guide for Security Incident Management in the Processing of Personal Data (2020). ▶ Guide for the Implementation of the Principle of Demonstrated Responsibility (2021). ▶ Guide on Recommendations for the Processing of Personal Data through Cloud Computing Services (2021). ▶ Guide on Recommendations from the Ibero-American Network of Data Protection (RIPD) for the Processing of Personal Data related to Health in Times of Pandemic (2021). ▶ Guide on the Processing of Personal Data in State Entities (2021). ▶ Guide on Protecting Your Digital Identity and Personal Data: Risks related to the Processing of Personal Data of Children and Adolescents (2021). ▶ Implementation Guide - Model Contractual Clauses for the International Transfer of Personal Data (2022). ▶ Official Guide on Personal Data Protection (2023). <p>Additionally, the SIC, in its role as the highest authority on data privacy matters, issues External Circulars to expand and update legal concepts, aligning with the provisions established in the regulations. In 2024, the SIC has issued three External Circulars:</p> <ul style="list-style-type: none"> ▶ External Circular 001 dated June 26, 2024, clarifying the authority of its Delegation for the protection of personal data concerning Law 2,023 of 2023. This law establishes measures to protect consumers' right to privacy, regulating the channels, hours, and frequency with which they can be contacted for collection activities and sending advertising messages. ▶ External Circular 002 dated August 21, 2024, providing guidelines on the processing of personal data in Artificial Intelligence systems. ▶ External Circular 003 dated August 22, 2024, issuing instructions for corporate administrators regarding the processing of personal data.

Matter	Concept	Yes / No / NA	Observations / comments
Enforcement Authority	Who is the enforcement authority? If applicable, please provide their website link	Yes	SIC is the national authority that protects competition, personal data, legal metrology, and consumer rights and manages the National System of Industrial Property through its administrative and jurisdictional functions. https://www.sic.gov.co/tema/proteccion-de-datos-personales
Scope of Application	Which is the regulation's scope of application? I.e., is it a strictly national or cross-border concept?	Yes	It applies to all personal data processed in the Colombian territory by public and private entities or when the Colombian legislation regarding international treaties and regulations apply to the data controller or data processor not domiciled in the country. Section 2, Law No. 1,581.
Data collection	Which are the requirements or processes for personal data collection? (For example, data subject consent, information on purpose of data use and subject's rights, etc.)	Yes	Generally, the data subject's express and informed consent is required in advance for personal data processing, unless the personal data is publicly available or there is an exception to Section 10 of Law 1581. Section 12 of Law 1581 and Sections 2.2.2.25.2.1. to 2.2.2.25.2.5. of Decree 1,074 establish the data collection regulations and requirements per the Colombian regulations.
Legal concept of "personal data"	What are personal data	Yes	"Personal data" is any information related or that may be related to one or more specific or definable individuals. Section 3, para. c), Law 1,581. Under Law 1,266, the concept of "personal data" is defined as any information related to, or that can be associated with, one or more identified or identifiable natural or legal persons. Personal data can also be categorized as public, private, or semi-private. Public data refers to information available to the public by legal or constitutional mandate. In contrast, private or semi-private data do not serve a public purpose; they are of an intimate nature and its disclosure pertains only to the data subject.
Personal data categories	Are there different personal data categories? Please explain each category, if applicable.	Yes	Regulations establish five different data categories: <ul style="list-style-type: none">▶ Personal data: any information related or that may be related to one or more specific or definable individuals.▶ Financial personal data: any financial, credit, commercial, service and foreign information that refers to the generation, execution and termination of monetary obligations, regardless of the nature of the contract that creates them or their link to one or several specific or definable individuals or corporations.▶ Public data: data qualified as public by the law or the Political Constitution or data that is not private or semi-private per the law. Data contained in public documents, unreserved enforced court rulings and documents related to individuals' civil status is also considered public.▶ Semi-private data: Semi-private data is the data that is not private, reserved, or public, and its disclosure may interest its subject and a certain sector, group of people or society, such as financial and credit data of commercial activities or services.▶ Private data: data that is relevant only to its subject due to its private or reserved nature. It includes sensitive data.▶ Sensitive data: data that affects subject's privacy whose inappropriate use may cause discrimination, such as data on racial or ethnic origin, political orientation, religious or philosophical convictions, membership to unions, social organizations, human rights organizations, or organizations that promote interest in political parties or ensure the rights and guarantees of opposition political parties, health, sexual life, and biometric data. Section 3 paragraph c) and 5, Law No. 1,581 and Section 3, paragraph 2), Dec. 1,377.
Situation of the corporations and other legal entities.	Does the regulation sufficiently protect the personal data of the corporations or entities?	Yes	Personal data regulations only protect the financial, commercial, and monetary obligation compliance information of the corporations per Law No. 1,266.

Matter	Concept	Yes / No / NA	Observations / comments
Data subject consent	Is the data subject's consent required to collect the data? If so, are there conditions to obtaining the data subject's consent? (For example, prior information that must be provided to the data subject).	Yes	<p>It is required to obtain the prior, express and informed consent of the subject through any means that can be consulted later, such as written and verbal means or unambiguous behaviors. Sensitive data can only be collected through written or verbal means.</p> <p>The data controller must inform the data subject about what information will be collected and the purposes for processing that data. When there are substantial changes in the purpose of the processing, the data controller is required to notify the data subject and obtain their consent for the processing of personal data under those new purposes.</p> <p>The SIC has emphasized that the silence of the holder cannot in any case be understood as the granting of authorization through a tacit or unequivocal conduct, and that under no circumstances can the privacy notice be confused with the prior, express and informed consent, since the former has purposes that are substantially different from those of a consent and, therefore, in no way replaces it (cf. Resolution number 59001 of 2020 of the SIC - Radication 19-47344-).</p> <p>Section 3, paragraph a), 4, paragraph c) and 9, Law No. 1581 and Section 5, Dec. 1,377.</p>
Exceptions to the consent	Are there exceptions to the voluntary consent of a data subject? If so, please list the exceptions.	Yes	<p>Subject's consent will not be necessary for the following cases:</p> <ol style="list-style-type: none"> 1. Information required by a public or administrative entity for its legal functions or by court order. 2. Public data. 3. Health emergencies. 4. Data processing authorized by the law for historical, statistical, or scientific purposes. 5. Data related to the Civil Registry. <p>The international transmission of personal data (between a data controller and a data processor) shall not require to be informed to the data subject or to have his consent when there is an agreement between the data controller and the data processor, subject to the terms set forth in Section 2.2.2.25.5.2., of Dec. 1,074.</p> <p>Section 10, Law No. 1,581</p> <p>Section 2.2.2.2.25.5.2., of Dec. 1,074.</p>
Content and scope of the information to be validated by the data subject.	What should be the content of the consent? (For example, data use or destination, international data transfer, etc.)	Yes	<p>The data controller, at the time of requesting the subject's consent shall inform him/her in a clear and express manner the following:</p> <ol style="list-style-type: none"> 1. The processing of his personal data and its purpose. 2. The optional nature to answer the questions asked when they relate to sensitive data or data of children and adolescents. 3. His rights as subject. 4. The name, physical or electronic address and phone number of the data controller. <p>Section 12, Law No. 1,581 of 2012, Section 7, Dec. 1,377, and Section. 2.2.2.25.2.3 and 2.2.2.25.2.4 of Dec. 1,074.</p>

Matter	Concept	Yes / No / NA	Observations / comments
Transfer of personal data	Are there requirements or restrictions on the transfer of personal data? Are there requirements that apply to the international transfer of data? (Example: model clauses, Supervisors' authorization, etc.)	Yes	<p>Section 26 of Law No. 1,581 prohibits the transfer of personal data to countries that do not have the proper data protection level. A country has a proper data protection level when it complies with the standards set by the SIC on this matter, which in no case may be lower than those required by law from receivers per Section 3, paragraph 3.1 of External Circular No. 005 Bogotá D.C.</p> <p>This prohibition shall not apply in the case of:</p> <ol style="list-style-type: none"> 1. Information in respect of which the Data Subject has granted his express and unequivocal consent for the transfer. 2. Exchange of medical data, when so required by the Processing of the Data Subject for reasons of health or public hygiene. 3. Banking or stock exchange transfers, in accordance with applicable legislation. 4. Transfers agreed within the framework of international treaties in which the Republic of Colombia is a party, based on the principle of reciprocity. 5. Transfers necessary for the execution of a contract between the Data Subject and the Data Controller, or for the execution of pre-contractual measures, as long as the authorization of the Data Subject is obtained. 6. Transfers legally required for the safeguarding of public interest, or for the recognition, exercise or defense of a right in a judicial process. <p>In cases not contemplated as an exception, the SIC shall be responsible for issuing a declaration of conformity regarding the international transfer of personal data. For this purpose, the Superintendent is empowered to request information and to take the necessary steps to establish compliance with the requirements for the viability of the operation.</p> <p>The above provisions are applicable to all personal data, including those contemplated in Law No. 1266.</p> <p>Section 26, Law No. 1,581 and Section 3, paragraph 3.1, 3.2 and 3.3), External Circular No. 005 Bogotá D.C4.</p> <p>https://www.sic.gov.co/sites/default/files/normatividad/082017/Circular_Externa_005_de_2017.pdf</p>
BCR	Do they have binding corporate rules (BCR)?	Yes	<p>Section 27 of Law No. 1,581 establishes that the National Government must issue the Binding Corporate Rules for the certification of good practices in personal data protection and transfer to third-party countries.</p> <p>Decree No. 255 establishes the minimum conditions of the Binding Corporate Rules ("BCR"), which may be adopted by business groups that transfer personal data to a controller of the same group, outside the Colombian territory.</p> <p>The NCV correspond to the policies, principles of good governance or codes of good business practices of mandatory compliance assumed by the controller of the processing of personal data that is established in the Colombian territory, to make transfers or a set of transfers of such data to a controller that is located outside the Colombian territory and that is part of the same business group. These rules are materialized through self-regulatory systems that confer rights to the holders of personal information and impose duties and obligations on the head of the business group and each of its members.</p> <p>All the companies of the business group and each of its members will be jointly and severally liable for compliance with the NCV, so the SIC is empowered to require, investigate and sanction the data controller that is established in Colombia, for those violations committed by any of the members of the business group.</p> <p>The SIC is empowered to approve NCVs that:</p> <ol style="list-style-type: none"> 1. Are legally binding and apply to all members that are part of the same business group. 2. Expressly confer to the data subjects the power to exercise the rights provided in the applicable rules. 3. Comply with the requirements set forth in Decree No. 255. <p>The NCVs may only be submitted to the SIC for authorization when they have been approved by the competent corporate body, in accordance with the bylaws of the respective company or the agreements of the business group. Therefore, these rules may only be implemented when they have gone through the corporate process and the SIC has subsequently approved their content and issued the certification of good practices, the latter to be reported on the website of the data controller.</p> <p>The NCV will not be mandatory when the business group applies other data transfer mechanisms established in Colombian legislation, such as the declarations of conformity issued by the SIC.</p> <p>Section 27, Law No. 1,581, and Section. 3, paragraph 4) and 5), 24 and 25, Dec. No. 1,377. Also compiled in Sections. 2.2.25.1.3, 2.2.25.5.1 and 2.2.25.2.2 of Dec. No. 1,074, respectively. Dec. No. 255.</p>

Matter	Concept	Yes / No / NA	Observations / comments
Sensitive data	What is understood by sensitive data? How is sensitive data processed, if applicable?	Yes	<p>Sensitive data is understood as data that affects subject's privacy whose inappropriate use may cause discrimination, such as data on racial or ethnic origin, political orientation, religious or philosophical convictions, union membership, social organizations, human rights organizations, or organizations that promote interest in political parties or ensure the rights and guarantees of opposition political parties, health, sexual life, and biometric data. Sensitive data processing is regulated by Section 6 of Law No. 1,581 and Section 6 of Dec. No. 1,377, also compiled in Section 2.2.2.25.2.3 of Dec. No. 1,074. The Superintendency of Industry and Commerce has also highlighted that security measures must be reinforced for sensitive data. Sections 5 and 6, Law No. 1581 and Section 6, Dec. No. 1,377, as compiled in Article 2.2.2.25.2.3 of Decree 1,074. Arts. 5 y 6, Ley 1.581 y Art. 6, Dec. 1.377, compilado en el art. 2.2.2.25.2.3 del Dec. 1.074.</p>
Database registration or periodic reporting to the corresponding authority	Is it mandatory to register (e.g., with the corresponding enforcement body) a database and/or a database ownership, processing and/or use? Is it mandatory to submit any type of information or report periodically to the enforcement authority?	Yes	<p>Data controller must register and update the databases containing personal data that can be processed with the National Registry of Databases (RNBD in Spanish), managed by the Superintendency of Industry and Commerce, provided that databases belong to corporations or non-profit organizations with total assets greater than 100,000 Tax Units (UVT in Spanish). Public corporations must also register and update these databases.</p> <p>They must provide the information stated in Section 5 of Dec. No. 866. Also compiled in Section 2.2.2.26.2.1 of Dec. No. 1,074.</p> <p>While it is not required to submit periodical reports to the "RDBD", data controllers must update the registered information when it changes. No substantial changes must be updated between January 2 and March 31 of each year. Additionally, data controllers must update the information registered in the RNBD (National Registry of Databases) within the first 10 business days of each month when substantial changes occur in the databases. Substantial changes include those related to the purpose of the database, the data processor, the classification or types of personal data stored in the database, the implemented information security measures, the Information Processing Policy, international transfers and transmissions of personal data, and the channels for addressing data subjects' concerns.</p> <p>They must also update information regarding claims filed by data subjects between July and December of the previous year within the first fifteen (15) business days of February each year. This update should consider what data subjects have reported, and the types of claims predefined in the RNBD. This report must consolidate the claims presented by data controllers to those responsible and/or in charge of data processing. The same obligation applies within the first 15 business days of August each year for claims filed between January and June of that same year.</p> <p>Finally, data controllers must report security incidents within 15 business days of their detection and register new databases within 2 months following their creation.</p> <p>Section 25, Law No. 1,581 and Sections 3, 5, 6 and 14, Dec. No. 866. Also compiled in Sections 2.2.2.26.1.3, 2.2.2.26.1.4 and 2.2.2.26.2.2 of Dec. 1,074, respectively.</p>
Data security	Are there technical measures to guarantee the security and confidentiality of personal data? If so, what are they?	Yes	<p>There are no security measures on this matter stated by the current regulations.</p> <p>However, all public companies and entities must implement technical, human, and administrative measures to secure records and keep information under security measures necessary to avoid its falsification, loss, consultation, use or unauthorized or fraudulent access.</p> <p>Based on the above, if there are no security measures, data controllers must develop personal data "Processing Policies" and ensure data processors comply with them.</p> <p>Processing Policies must be developed according to Section 13 of Dec. No. 1,377.</p> <p>Sections 4, paragraph g), 17, paragraph d), Law No. 1,581 and Sections. 13, 19 and 26, Dec. No. 1,377. Also compiled in Sections 2.2.2.25.3.1, 2.2.2.25.3.7 and 2.2.2.25.6.1 of Dec. No. 1,074, respectively.</p>

Matter	Concept	Yes / No / NA	Observations / comments
Rights of the data subjects	What are the data subjects' rights? (Example: correction, update, or deletion). Please list and explain.	Yes	<p>Data subjects have the following rights:</p> <ol style="list-style-type: none"> 1. Know, update, and correct their personal data in front of data controllers or data processors. 2. Ask for the proof of the consent granted to the data controller, except when the consent is required for data processing. 3. Be informed by the data controller or data processor. 4. File claims for breach of this law and the regulations that modify, complement or add information to it before the Superintendence of Industry and Commerce. 5. Revoke the authorization and/or ask for data deletion when constitutional and legal principles, rights and guarantees are breached during data processing. 6. Freely access their processed personal data. <p>In addition, Section 7 of Law No. 1,581 states that personal data processing of children and adolescents is prohibited, except for public data and when the data processing complies with certain requirements.</p> <p>Sections 7 and 8, Law No. 1581 and Section 12, Dec. No. 1,377. Also compiled in Section 2.2.2.25.2.9, of Dec. No. 1,074.</p>
Actions by the data subjects	How can they exercise them?	Yes	<p>Subjects or successors in title may exercise their data protection rights per Sections 14 and 15 of Law No. 1,581 and Section 20 and 21 of Dec. No. 1,377 by making consultations or filing claims before the data controller and/or data processor. If consultations or claims are disregarded as stated by law, subjects or successors in title may file them with the Superintendence of Industry and Commerce and finally resort to a recourse of protection before a judge of the Republic.</p> <p>Sections 14 and 15, Law No. 1,581 and Sections 20 and 21 Dec. No. 1,377. Also compiled in Sections 2.2.2.25.4.1 and 2.2.2.25.4.2 of Dec. No. 1,074, respectively.</p>
Assignment of personal data	What are the requirements for the assignment of personal data?	N/A	<p>Data protection regulations do not regulate the institute of personal data assignment. They only refer to the national or international transfer of personal data.</p>
Data processing	Can the services be provided through a third party (data processing)? If so, please explain the procedure and exceptions, if applicable.	Yes	<p>Personal data regulations include the figure of "data processor," who can be any public or private individual or corporation that individually or jointly processes the personal data on behalf of the data controller.</p> <p>Although there are no specific regulations for this figure, the duties that they must comply are included in Section 18 of Law No. 1,581.</p> <p>Section 3, paragraph d) and 18, Law No. 1,581. Also included in Section 2.2.2.25.5.1 and 2.2.2.25.5.2 of Dec. No. 1,075.</p>
Data retention	Is it mandatory to retain/conserve the data collected or processed for a specific term? If so, what is the term?	No	<p>This obligation must be fulfilled only when required to comply with a legal or contractual obligation.</p> <p>Section 11 Dec. No. 1,377. Also compiled in Section 2.2.2.25.2.8, of Dec. No. 1,074.</p>
Data elimination	Is there an obligation to eliminate the data collected or processed? If so, under what conditions and for what term?	Yes	<p>Data controllers and data processors may collect, store, use or disclose personal data for as long as is reasonable and necessary according to the purposes of the data processing. Once the purpose of data processing is fulfilled and without precluding the legal regulations that provide otherwise, data controllers and data processors must delete the personal data they have.</p> <p>Section 11 Dec. No. 1,377. Also compiled in Section 2.2.2.25.2.8, of Dec. No. 1,074.</p>
Privacy Impact Assessment	Are privacy impact assessments mandatory?	No	<p>In its Personal Data Processing Guidelines, the Superintendence of Industry and Commerce (SIC) states that, when there is high risk of affecting the right to protect subject's personal data, a Privacy Impact Assessment (PIA) must be conducted to effectively manage risks and internal controls to ensure that data is properly processed per the current regulations. The SIC states that this assessment should include at least:</p> <ol style="list-style-type: none"> 1. A detailed description of personal data processing operations included in the Company's project. 2. An assessment of specific risks to rights and liberties of personal data subjects. <p>The identification and classification of risks and the adoption of mitigation measures are core elements of the proven accountability principle.</p>

Matter	Concept	Yes / No / NA	Observations / comments
Incidents	Is it mandatory to report security incidents or breaches or the related legal provisions?	Yes	<p>It is mandatory for data controllers and data processors, regardless of whether the data controller must register its databases with the National Registry of Databases (RNBD), managed by the Superintendence of Industry and Commerce (SIC).</p> <p>When security codes are breached and there are risks in the management of subjects' data, the Superintendence of Industry and Commerce must be informed within a maximum of 15 business days after knowing the infringement.</p> <p>Section 17, paragraph n) and 18, paragraph), Law No. 1,581.</p>
Sanctions	Are there sanctions for failures to comply with this obligation? If so, please list them along with the corresponding sanction or penalty amounts.	No	<p>There are no sanctions for failure to comply with the obligation of reporting breaches.</p> <p>However, since it is mandatory, it may be understood as a breach of the provisions of the current regulations, leading the SIC to impose sanctions of Sections 22 and 23 of Law No. 1581.</p> <p>Section 22 and 23, Law No. 1,581.</p>
Legal actions	Are there any legal actions for personal data protection? Who has the right to exercise/request them?	Yes	<p>The Political Constitution establishes the figure of Habeas Data in Section 15 and the right to information as a fundamental right in Section 20. Therefore, the recourse of protection may be filed to enforce these rights, or civil actions in the event of damage caused by the improper processing of personal data. Likewise, there are criminal proceedings that protect these rights.</p> <p>Sections 15 and 20, Political Constitution and Sections 16, Law No. 1,266. Also, sections 16, 22, 23 and 24 of Law 1,581.</p>
Personal data protection officer or controller.	Is there a Data Protection Officer (DPO) or similar position? If so, is their appointment mandatory? Must they be appointed locally?	Yes	<p>The SIC, through the Personal Data Protection Office, will monitor and ensure that personal data processing respects the principles, rights, guarantees and procedures included in the personal data processing regulations. The designation of this figure is mandatory.</p> <p>Decree No. 4,886/113, Section 16 establishes the functions of the Office of the Personal Data Protection Superintendent (modified by Section 6 of Decree No. 092/22).</p> <p>Section 19, Law No. 1,581 and Section 16, Decree No. 4,886/113 and 2.2.2.25.3.1 and 2.2.2.25.4.4 of Dec. No. 1,074.</p>
Investigations	Can a competent authority officially act and/or investigate breaches of personal data protection?	Yes	<p>In case of breaching the data protection legislation, the Superintendence of Industry and Commerce may carry out investigations ex officio or at request of the interested party to enforce habeas data rights.</p> <p>When rights are ignored, it may grant access to and provide the data, rectification, update, or deletion.</p> <p>Section 21, Law No. 1,581.</p>
Processing Records	Are there any mandatory requirements for maintaining processing records under the applicable laws? Specifically, what information must be included in these records, and are there any particular conditions or circumstances under which data controllers or processors are obliged to keep detailed records of their data processing activities?	No	<p>There is no specific requirement that obliges data controllers and processors to maintain detailed records of the processing of personal data they handle. However, some controllers (companies and non-profit entities) must register the personal databases they manage when they have total assets exceeding 100,000 Tax Value Units (UVT), as well as public legal entities (see the response to question number 14).</p>
Similarities with the GDPR	Per your understanding, do you believe that the regulation contemplates all the requirements set by similar international regulations (e.g., Example: GDPR)? What relevant differences did you find?	Yes	<p>In principle, the GDPR provisions are complied with. One of the main differences is that, in Colombia, the data controllers that must register personal databases are non-profit organizations and corporations with total assets greater than 100,000 Tax Units (UVT in Spanish) and public corporations.</p>
Other obligations	Are there other additional considerations/requirements or legal obligations on data protection that must be met?	Yes	<p>The national regulations and jurisprudence highlight the proven accountability principle which states that data controllers must be able to always prove the effective and timely actions taken to protect the personal data in their possession and guarantee the proper processing. The Superintendence of Industry and Commerce may use these actions to adjust sanctions during investigations.</p>



Costa Rica



Matter	Concept	Yes / No / NA	Observations / comments
Regulations	Does the country have a personal data protection law? If so, provide the applicable regulation.	Yes	<p>Section 24 of the Political Constitution of Costa Rica states that citizens have the right to have their privacy protected by the State.</p> <p>Specifically, personal data are regulated by the Law on the Protection of Persons from Personal Data Processing No. 8,968, effective since September 5, 2011 (hereinafter "Law 8,968") and the Regulations of the Data Protection Law No. 37,554-JP, effective since March 5, 2013.</p>
Enforcement Authority	Who is the enforcement authority? If applicable, please provide their website link.	Yes	<p>Section 15 of Law 8,969 establishes as the authority in charge the Inhabitants Data Protection Agency (Prodhab in Spanish), which is a maximum decentralized body attached to the Ministry of Justice and Peace.</p> <p>http://www.prodhab.go.cr</p>
Scope of Application	Which is the regulation's scope of application? I.e., is it a strictly national or cross-border concept?	Yes	<p>Law 8,968 and its Regulations are of public order and apply to all automated databases of public or private entities within the Costa Rican territory.</p> <p>(Section 2 of the Law and Section 3 of the Regulations).</p>
Data collection	Which are the mandatory requirements or processes for personal data collection? (For example, data subject consent, information on purpose of data use and subject's rights, etc)	Yes	<p>Law 8,968 has the informative self-determination as a fundamental principle. Therefore, when personal data is required, it is necessary to inform data subjects or their representatives expressly, accurately, or distinctly in advance about its use and physically or digitally obtain their voluntary, express, and informed consent.</p> <p>Data controllers must include in the informed consent document the purposes of data collection, data processing conditions, recipients, persons allowed to consult databases, compulsory, or optional nature of their answers to the questions made during data collection, negative consequences of providing data, possibility to exercise their rights, and identity and address of the database controller.</p> <p>(Sections 4 and 5 of the Law and Sections 4, 5, 12 and 28 of the Regulations)</p>
Legal concept of "personal data"	What is understood by personal data?	Yes	<p>Law 8,968 defines personal data as any data related to an identified or identifiable individual.</p>
Personal data categories	Are there different personal data categories? Please explain each category, if applicable.	Yes	<p>According to Section 9 of Law 8,968, special categories are:</p> <ul style="list-style-type: none"> ▶ Sensitive data: Private information of individuals, such as racial origin, political opinions, religious or spiritual beliefs, socio-economic condition, biomedical or genetic information, sexual life, and orientation, etc. ▶ Restricted-access personal data: Data that, even forming part of public access records, are not of unrestricted access because they are of interest only to their subject or to the Public Administration. ▶ Unrestricted-access personal data: Information contained in public general-access databases according to special laws and collections purposes. <p>*Data related to credit behavior. Data related to credit behavior will be ruled by the regulations of the National Financial System to ensure an acceptable risk rating from financial entities without avoiding full exercise of informative self-determination rights or exceeding legal limits.</p>
Situation of the corporations and other legal entities	Does the regulation sufficiently protect the personal data of the corporations or entities?	No	<p>N/A</p>
Data subject consent	Is the data subject's consent required to collect the data? If so, are there conditions to obtaining the data subject's consent? (For example, prior information that must be provided to the data subject.)	Yes	<p>The regulations prohibit collecting data without the informed consent of subjects or their representatives. When collecting personal data, the written free, specific, informed, unambiguous, and individual consent of data subjects or their representatives, physically or electronically. This consent may be revoked in the same way, without retroactive effect.</p> <p>When the consent is provided online, the data controller must provide the data subject with a procedure to grant consent according to the Law.</p> <p>(Section 5 of Law 8,968 and Sections 4 and 5 of the Regulations).</p>

Matter	Concept	Yes / No / NA	Observations / comments
Exceptions to the consent	Are there exceptions to the voluntary consent of a data subject? If so, please list the exceptions.	Yes	<p>Law 8,968 establishes that data subjects' express consent will not be necessary when:</p> <ol style="list-style-type: none"> 1. There is a reasoned order from a competent judicial authority, or an agreement made by a special investigation commission of Congress. 2. Unrestricted-access personal data obtained from public sources is used. 3. Data should be delivered per legal or constitutional provision. <p>(Section 5.2 of the Law and Section 5 the Regulations).</p>
Content and scope of the information to be validated by the data subject	What should be the content of the consent? (For example, data use or destination, international data transfer, etc.)	Yes	<p>Section 5.1 of the Law states that the informed consent must include the following information:</p> <ol style="list-style-type: none"> 1. Existence of a database of personal nature. 2. Data collection purposes. 3. Information recipients and people allowed to consult it. 4. Compulsory or optional nature of answers to the questions made during data collection. 5. Processing of data requested. 6. Consequences of refusal to provide data. 7. Possibility to exercise related rights. 8. Identity and address of the database controller.
Transfer of personal data	Are there requirements or restrictions on the transfer of personal data? Are there requirements that apply to the international transfer of data? (Example: model clauses, control authority's authorization, etc.)	Yes	<p>Law 8,968 and its Regulations (Section 14 of the Law and Section 40 of the Regulations) establish, generally, that the database controller may only transfer data contained in databases when the right subject has expressly and validly authorized the transfer, which must be made without breaching the principles and rights recognized in this law, unless otherwise provided by law.</p> <p>In addition, Section 43 of the Regulations of the Data Protection Law establishes that, as a legal requirement for data transfer, the database controller, through contract, must verify that the recipient of the information complies with the same obligations it is subject to.</p> <p>The regulations do not establish any applicable requirement on international data transfers.</p>
BCR	Do they have binding corporate rules (BCR)?	Yes	<p>In Costa Rican regulations, BCRs are defined as "Protocols of Action" which work as a self-regulation system for all public and private individuals and corporations that collect, store, and use personal data.</p> <p>According to Section 32 of the Regulations, Protocols of Actions must:</p> <ol style="list-style-type: none"> 1. Prepare privacy manuals and policies mandatory and required internally to the data controller's organization. 2. Implement a personnel training, update, and awareness manual on personal data protection obligations. 3. Establish an internal control procedure to comply with privacy policies. 4. Implement agile, expeditious and free procedures to receive and answer questions and claims made by personal data subjects or their representatives; access, rectify, modify, block, or delete information contained in databases; and revoke consents. 5. Create technical measures and procedures to keep the personal data history during the processing. 6. Develop a mechanism in which the data controller sender informs the data controller recipient about the conditions under which the data subject consented the collection, transfer, and processing of his data. <p>If the database controller assigns personal data, the Protocol of Action should be register with Prodhab. (Section 12 of Law 8,968 and Sections 32 and 41).</p>

Matter	Concept	Yes / No / NA	Observations / comments
Sensitive data	What is understood by sensitive data? How is sensitive data processed, if applicable?	Yes	<p>Paragraph e) of Section 3 of the Law defines sensitive data as private information of individuals, such as:</p> <ul style="list-style-type: none"> ▶ Racial origin. ▶ Political opinions. ▶ Religious or spiritual beliefs. ▶ Socio-economic condition. ▶ Biomedical or genetic information. ▶ Sexual life and orientation. <p>Section 9.1 of the Law establishes that no person shall be obliged to provide sensitive data and prohibits its processing. However, it also establishes the following exceptions:</p> <ol style="list-style-type: none"> 1. When data processing is necessary to safeguard the vital interest of the interested party or any other party if the interested party is physically or legally incapable of giving their consent. 2. When the data processing is legally carried out and duly guaranteed by a foundation, association, or any other entity whose purpose is political, philosophical, religious, or union, provided that it exclusively refers to their members or persons regularly in touch with the foundation, association or entity due to such purposes, provided that the data is not communicated to third parties without interested parties' consent. 3. When the data processed refers to data that the interested party made public voluntarily or are necessary to recognize, exercise or defend the rights in judicial proceedings. 4. When the data processing is necessary for medical prevention or diagnosis, health assistance provision, medical treatments, or health service management, provided that the data processing is carried out by a health officer subject to professional confidentiality, another subject person, or a similar confidential obligation.
Database registration or periodic reporting to the control authority	Is it mandatory to register (e.g. with the corresponding enforcement body) a database and/or a database ownership, treatment and/or use? Is it mandatory to submit any type of information or report periodically to the enforcement authority?	Yes	<p>According to Section 21 of the Law, public or private databases used for distribution, disclosure or trade must be registered with the registry allowed by Prodhab. The registration does not imply the transfer of data to the authority.</p> <p>The database controller must also register any other information requested by Prodhab and the Protocols of Action mentioned in Section 12 and in the BCR Section.</p>
Data security	Are there technical measures to guarantee the security and confidentiality of personal data? If so, what are they?	Yes	<p>Minimum security measures must include, at least, the most appropriate physical and logical security mechanisms per the current technological development to guarantee the protection of the stored information. (Section 10 of Law 8,968)</p> <p>The Regulations (Sections 36 and 37) fully describe the minimum actions required and recommended by Prodhab to guarantee data security:</p> <ol style="list-style-type: none"> 1. Fully describe the type of personal data processed or stored. 2. Create and keep the technological infrastructure inventory up to date, including equipment, computer programs and licenses. 3. Describe the type of system, program, method or process used for data processing or storage and indicate the name and version of the database used (if applicable). 4. Analyze risks, identifying threats and calculating risks that may affect personal data. 5. Establish personal data security measures and identify those implemented effectively. 6. Calculate residual risks based on the difference between existing security measures and those missing but necessary to protect personal data. 7. Prepare a work plan to implement missing security measures, based on the results of the calculation of residual risks. <p>Security measures should be updated at least once a year.</p> <p>If databases that must be registered do not include the actions and the conditions that fully guarantee their security and integrity and of processing centers, equipment, systems and programs, the authority will not register them.</p>

Matter	Concept	Yes / No / NA	Observations / comments
Rights of the data subjects	What are the data subjects' rights? (Example: correction, update or deletion).	Sí	<p>Internal processes must always be established and implemented to ensure the following rights to data subjects:</p> <ul style="list-style-type: none"> ▶ Right of access to information. ▶ Right to rectification. ▶ Right to revoke or cancel the consent to use, process or collect personal information. ▶ Right to delete or cancel the personal information provided. ▶ Right to be forgotten. <p>(Section 7 of the Law and Sections 7, 1, 21, 23 and 25 of the Regulations).</p>
Actions by the data subjects	How can they exercise them?	Yes	<p>Data controllers must provide data subjects with electronic communication means, simplified forms or other relevant means for them to exercise their rights.</p> <p>Any request made by data subjects to exercise their rights will be for free and resolved within five (5) business days from the date after the request was received by the data controller.</p> <p>(Section 7 of the Law and Sections 13 to 20 of the Regulations).</p>
Assignment of personal data	What are the requirements for the assignment of personal data?	Yes	<p>Personal data processed can only be assigned to fulfill the purposes directly related to the legitimate interest of the assignor and the assignee, including the data subject's prior consent. The data subject must be informed about the purpose of the assignment and the identification of the assignee or elements allowing so. On the other hand, the assignee will be subject to the same legal and regulatory obligations as the assignor, who shall jointly comply with such obligations before the controlling body and the data subject.</p>
Data processing	Can the services be provided through a third party (data processing)? If so, please explain the procedure and exceptions, if applicable.	Yes	<p>Section 29 of the Regulations of Law 8,968 defines the contracting or subcontracting of services as a transaction through which the database controller hires a third party (technological intermediary or service provider) to carry out the personal data processing.</p> <p>The data processor has the following obligations:</p> <ol style="list-style-type: none"> 1. Process personal data per the instructions by the data controller. 2. Do not process personal data for purposes other than those instructed by the data controller. 3. Implement security measures and comply with minimum protocols of actions per the Law, these Regulations and other applicable provisions. 4. Observe confidentiality of processed personal data. 5. Do not transfer or disclose personal data, unless otherwise indicated by the data controller. 6. Delete personal data processed once the legal relationship with the data controller is terminated or at the data controller's instruction, provided that there is no legal provision requiring personal data retention. <p>Nevertheless, the law clearly states that the contractor of services is responsible for personal data processing. Therefore, the data controller must verify that the third party complies with the minimum-security measures to ensure the integrity and security of personal data.</p> <p>The data processor's intervention will be strictly limited to the instructions and provisions of the contract signed by the data controller.</p>
Data retention	Is it mandatory to retain/conserve the data collected or processed for a specific term? If so, what is the term?	No	N/A

Matter	Concept	Yes / No / NA	Observations / comments
Data elimination	Is there an obligation to eliminate the data collected or processed? If so, under what conditions and for what term?	Yes	<p>Law 8,968 establishes that the database controller must delete the data irrelevant or unnecessary for the purpose of the data processing. Personal data retention will not exceed ten (10) years from the date of termination of the data processing purpose. If data needs to be retained beyond the stipulated term, it must be disassociated from its subject. However, the regulations establish the following exceptions to change the retention term:</p> <ol style="list-style-type: none"> 1. Special regulations establishing another term. 2. Agreement between the parties to change the term. 3. Continuous relationship between the parties. 4. Public interest to preserve the data. <p>(Section 6 and 30 the Law and Section 11 of the Regulations).</p>
Privacy Impact Assessment	Are Privacy Impact Assessments required and/or mandatory?	Yes	Paragraph d) of Section 36 of the Regulations establishes the mandatory risk analysis to identify threats and calculate risks that could affect personal data registered in the data controller's database.
Incidents	Is it mandatory to report security incidents or breaches or the related legal provisions?	Yes	<p>If database security is breached, the data controller must inform data subjects and the authority about any irregularity (e.g., loss, destruction, misplacement, etc.).</p> <p>It must inform data subjects about this within five business days from the moment when the event occurred so that data subjects take the respective actions. (Section 38 of the Regulations).</p> <p>Below is the minimum information that must be included (Section 29 of the Regulations):</p> <ol style="list-style-type: none"> 1. Nature of the incident. 2. Affected personal data. 3. Corrective actions immediately taken. 4. Means or place to obtain more information.
Sanctions	Are there sanctions for failures to comply with this obligation? If so, please list them along with the corresponding sanction or penalty amounts.	No	<p>However, if data subjects are affected by the incident or breach, the article 28 of the Law 8,968 establishes three types of offenses: minor, serious, and very serious.</p> <p>Below are the sanctions due to the breach of legal provisions:</p> <ul style="list-style-type: none"> ➢ Minor offenses: Sanction between \$1,000 and \$5,000 ➢ Serious offenses: Sanction between \$5,000 and \$20,000 ➢ Very serious offenses: Sanction between \$15,000 and \$30,000 and suspension of file functioning from one to six months.
Legal actions	Are there any legal actions for personal data protection? Who has the right to exercise/request them?	Yes	<p>Any person holding subjective rights or legitimate interest may report to Prodhab (authority) that a public or private database infringes the rules or basic principles of data protection and informative self-determination established by this law.</p> <p>In addition, any person that may be affected by a security incident or breach of the current data protection regulations may civilly report it to the data controller for the damages caused (if the data controller is domiciled in Costa Rica).</p>
Personal data protection officer or responsible party.	Is there a Data Protection Officer (DPO) or similar position? If so, is their appointment mandatory? Must they be appointed locally?	No	N/A
Investigations	Can a competent authority officially act and/or investigate breaches of personal data protection?	Yes	At its own initiative or at the request of either party, Prodhab may initiate a procedure aimed at demonstrating if a database regulated by this law is used per its principles.

Matter	Concept	Yes / No / NA	Observations / comments
Processing Records	Are there any mandatory requirements for maintaining processing records under the applicable laws? Specifically, what information must be included in these records, and are there any particular conditions or circumstances under which data controllers or processors are obliged to keep detailed records of their data processing activities?	No	N/A
Similarities with the GDPR	Per your understanding, do you believe that the regulation contemplates all of the requirements set by similar international regulations (e.g., the GDPR)? What relevant differences did you find?	No	<p>The Costa Rican regulations do not provide all the requirements for international regulations (GDPR). One of the relevant differences is the scope of application of Law 8968 and its Regulations, which leaves data subjects unprotected against the noncompliance of international individuals or corporations such as the case of international data assignments. It does not provide the right of data portability for privacy by design and impact assessments where there is a high risk for rights and liberties of persons, activity registration, risk analysis, record keeping before the competent authority and the figure of the Data Protection Delegate. Finally, the authority does not have the budget or human resources to comply with its obligations; therefore, the control of databases in the country is limited.</p> <p>In 2021, based on situations of public interest on data protection matters, several sectors are drafting and preparing different bills of laws (to be presented at Congress) to reform the data protection legislation in Costa Rica.</p>
Other obligations	Are there other additional considerations/requirements or legal obligations on data protection that must be met?	Yes	Regarding the acceptance of Informed Consent and Privacy Policies in electronic commerce web sites, the Law on Promotion of Competition and Effective Consumer Protection No. 7,472 and its Regulations establish that traders must guarantee that consumers accept these policies freely and unambiguously, not pre-selected.



Dominican Republic



Matter	Concept	Yes / No / NA	Observations / comments
Regulation	Does the country have a personal data protection law? If so, please name the applicable regulation	Yes	Law No. 172-13 whose object is the comprehensive protection of personal data included in files, public records, data banks, or other technical data processing means intended for public or private reports. G. O. No. 10,737 of December 15, 2013.
Enforcement authority	Who is the enforcement authority? If applicable, please provide their website link	Yes	Dominican Telecommunications Institute (INDOTEL from Spanish). https://www.indotel.gob.do
Scope of application	What is the regulation's scope of application? Is it a strictly national or cross-border concept?	Yes	The regulations of the Law are of public order and apply in all the national territory.
Data collection	Which are the mandatory legal requirements or processes for personal data collection? (for example, data subject consent, information on purpose of data use and owner's rights, etc.)	Yes	When personal data is collected it requires the consent of the data subject to be able to process or assign such information once consent has been granted. At least one of the data subjects must be previously, clearly, and expressly informed by explaining: 1. The object for which such information will be used and who may its recipients or type of recipients be. 2. The existence of the file, record, data bank, or any other kind of information safekeeping and the identity and domicile of its controller. 3. The possibility of the interested party to exercise its data access, rectification, and suppression rights.
Legal concept of "personal data"	What is understood by personal data?	NA	Personal data: Any numeric, alphabetic, graphic, photographic, and acoustic information or information of any other kind that refers to identified or identifiable individuals.
"Personal data" categories	Are there different personal data categories? Please explain each category, if applicable.	Yes	<ul style="list-style-type: none"> ▶ Specially protected data: Personal data that reveals racial and ethnical origin, political opinions, religious, philosophical, or moral convictions, union membership, and information about health or sex life. ▶ Personal data: Any numerical, alphabetical, graphical, photographic, acoustic, or any other type of information concerning identified or identifiable individuals. ▶ Personal data related to health: Any information about past, present, and future physical or mental health of an individual.
Situation of the corporations and other legal entities	Does the regulation sufficiently protect the personal data of the corporations or entities?	No	<p>Section 4.4 of Law No. 172-13: The personal data protection regime shall not apply: To the processing of data referring to legal persons, nor to personal data files that are limited to incorporate the data of the natural persons who render their services in those, consisting of their names and surnames, the functions or positions performed, as well as the professional postal or electronic address, telephone and fax number.</p> <p>Keep in mind the following information:</p> <ul style="list-style-type: none"> ▶ Right of information: When personal data that requires the consent of the data subject is collected, to be able to process or assign such data after being granted consent, at least one of the data subjects must be previously informed in an express and clear manner by explaining: <ul style="list-style-type: none"> a) The object for which such information will be used and who may its recipients or type of recipients be. b) The existence of the file, record, data bank, or any other kind of information safekeeping and the identity and domicile of its controller. c) The possibility of the interested party to exercise its data access, rectification, and suppression rights. ▶ Consent of the affected party: Personal data processing and assignment is illegal when the data subject has not granted its free, express, and conscious consent that must be granted in writing or by similar means depending on the circumstances. The consent, provided by other statements, must be express and clear, with previous notice to the data recipient as described in numeral 3 of this Section.
Data subject consent	Is the data subject's consent required to collect the data? If so, are there conditions to obtaining the data subject's consent? (For example, prior information that must be provided to the data subject.)	Yes	

Matter	Concept	Yes / No / NA	Observations / comments
Exceptions to the consent	Are there exceptions to the voluntary consent of a data subject? If so, please list the exceptions.	Yes	<p>According to Section 27 of Law No.172-13, consent shall not be necessary for the collection of data when:</p> <ol style="list-style-type: none"> 1. They are obtained from public access sources. 2. They are collected for the exercise of functions proper to the powers of the State or by virtue of a legal obligation. 3. They are obtained from lists for marketing purposes, whose data are limited to name, identity and electoral card, passport, tax identification and other biographical information. 4. They are derived from a commercial, labor or contractual, scientific or professional relationship with the natural person, and are necessary for its development or fulfillment. 5. It is personal data received from their clients in relation to the operations carried out by financial intermediation entities regulated by the Monetary and Financial Law and economic agents, Credit Information Companies (SIC), and entities that develop credit scoring tools for the evaluation of the risk of debtors of the national financial and commercial system, in accordance with the conditions established in Section 5, numeral 4. 6. So provided by law. 7. It is carried out directly between State agencies, to the extent of the fulfillment of their respective competences. 8. It concerns personal data related to health, and it is necessary for reasons of public health, emergency or for the performance of epidemiological studies, provided that the secrecy of the identity of the data subjects is preserved by means of appropriate dissociation mechanisms. 9. A procedure of dissociation of the information would have been applied, so that the data subjects are not identifiable.
Content and scope of the information to be validated by the data subject	What should be the content of the consent? (For example, data use or destination, international data transfer, etc.)	Yes	<ol style="list-style-type: none"> 1. The object for which such information will be used and who may its recipients or type of recipients be. 2. The existence of the file, record, data bank, or any other kind of information safekeeping and the identity and domicile of its controller. 3. The possibility of the interested party to exercise its data access, rectification, and suppression rights.
Transfer of personal data	Are there requirements or restrictions on the transfer of personal data? Are there requirements that apply to the international transfer of data? (Example: model clauses, control authority's authorization, etc.)	Yes	<p>The transfer of personal data of any kind to countries or international or supra national organisms that requires the consent of the data subject, will only be done when:</p> <ol style="list-style-type: none"> 1. The individual freely, consciously, and voluntarily decides to authorize the transfer of data or when the laws allow it. 2. It is to exchange medical information as required by the affected parties' medical treatment or for an epidemiological investigation, or for public hygiene or health reasons. 3. The transfer is to bank or trading entities and pursuant to any applicable laws. 4. The data transfer has been agreed or stated in the framework of international treaties or conventions and in free trade agreements in which the Dominican Republic is a party. 5. The object of the data transfer is international cooperation between intelligence organisms for the fight against organized crime, terrorism, human trafficking, drug trafficking, and other crimes and offenses. 6. The data transfer is needed for the execution of a contract between the data subject and the data controller or for the execution of precontractual measures. 7. The legally required data transfer is to safeguard the public interest or for the knowledge, exercise, or defense of a right in a judicial process, or the data transfer is requested by a fiscal or customs administration in compliance of its competencies. 8. The data transfer is performed to provide or request international judicial aid. 9. The data transfer is performed at the request of an international organism with legitimate interest from a public record. <p>It should be noted that Section 28 of Law No.172-13 states that the transfer of personal data subject to data processing can only be transferred for the fulfillment of purposes directly related to the legitimate interest of the transferor and the transferee, with the prior consent of at least one of the data subjects.</p>
BCR	Do they have binding corporate rules (BCR)?	N/A	

Matter	Concept	Yes / No / NA	Observations / comments
Sensitive data	What is understood by sensitive data? How is sensitive data processed, if applicable?	Yes	<p>Personal data that reveals:</p> <ul style="list-style-type: none"> ▶ Political opinions. ▶ Religious. ▶ Philosophical, or moral convictions. ▶ Union membership; and ▶ Information about health or sex life.
Database registration or periodic reporting to the control authority	Is it mandatory to register (e.g. with the corresponding enforcement body) a database and/or a database ownership, processing, and/or use? Is it mandatory to submit any type of information or report periodically to the enforcement authority?	N/A	
Data security	Are there technical measures to guarantee the security and confidentiality of personal data? If so, what are they?	Yes	<p>The personal data file controller and, where appropriate, the data processor, shall adopt and implement the technical, organizational, and security measures needed to safeguard personal data and avoid its unauthorized alteration, loss, processing, consult, or access. Consequently:</p> <ol style="list-style-type: none"> 1. It is prohibited to record personal data in files, registries, or data banks that do not meet technical integrity and safety conditions. 2. The data providers, the Credit Information Companies (SIC), and users and subscribers must adopt the technical measures and controls needed to avoid the unauthorized alteration, loss, processing, or access of credit history data handled or kept in databases of the Credit Information Companies (SIC). 3. The Credit Information Companies (SIC) must adopt the appropriate measures to protect its databases against natural risks such as accidental loss or destruction due to accidents and against human risks such as unauthorized access, the hidden use of data, or contamination due to information viruses.
Rights of the data subject	What are the data subject' rights? (Example: correction, update or deletion). Please list and explain.	Yes	<ul style="list-style-type: none"> ▶ Right of consultation for data protection: Every person has the right to a judicial action to know of the existence and access of its personal data kept in public or private registries or data banks and, in the event of discrimination, inaccuracy, or error, to demand the suspension, rectification, and update of such data in accordance with this law. ▶ Right of Access: Every person has the right to access its personal information and data and information about its assets kept in official or private registries, as well as to know the object and use to be given to such information with the limitations established by this law. Personal information and data processing, or the processing of its assets must be performed respecting the principles of quality, legality, loyalty, security, and finality. Every person may request before the competent judicial authority the update, processing opposition, rectification, or destruction of information that illegitimately affects its rights. ▶ Rectification and cancellation rights: Every person has the right to request the rectification, update and, as the case may be, suppression of its personal data that is included in a data bank. ▶ Right to indemnity. Interested parties who, due to the noncompliance of the provisions of this law suffer any damages, have the right to be indemnified as established by common law.

Matter	Concept	Yes / No / NA	Observations / comments
Actions by the data subject	How can they exercise them?	Yes	<ul style="list-style-type: none"> ▶ Section 17.- Habeas data action. Without limiting the mechanisms established for the exercise of rights of interested parties, such parties may file a habeas data judicial action pursuant to the Constitution and the laws that regulate the matter. The habeas data judicial action will acknowledge the existence of personal data stored in public or private files, registries and data banks due to a commercial, work, or contractual relation with a public or private entity or will simply acknowledge personal data that is presumed to be stored in public or private files, registries, or data banks. This action may be filed when inaccuracy, outdated information, or data processing whose registration is prohibited by this law is presumed, to demand its rectification, suppression, or update. ▶ Section 18.- Active legitimation. The personal data protection or habeas data action will be filed by the affected party, its guardians, successors, or its Attorneys-in-Fact. When the judicial action is filed by companies, they will do so by means of their legal representative or Attorneys-in-Fact appointed for such purposes. ▶ Section 19.- Passive legitimation. The judicial action will be filed against public and private data bank controllers and users whose object is to provide reports when they act against the provisions set forth in this law. ▶ Section 20.- Competence. The judge in the domicile of the defendant will have competence for this action and, in the event of plurality of defendants, in the domicile of one of them. ▶ Section 21.- Applicable procedure. The habeas data action will be processed as per the provisions of this law and by the corresponding procedure of an appeal for protection. During the procedure the registry or data banks must record or publish in its reports that the questioned information is submitted to a judicial process or habeas data challenge procedure.
Assignment of personal data	What are the requirements for the assignment of personal data?	Yes	Personal data object of data processing may only be assigned to comply purposes directly related to the legitimate interests of the assignee and assignor with the previous consent of at least one of the data subjects.
Data processing	Can the services be provided through a third party (data processing)? If so, please explain the procedure and exceptions, if applicable.	Yes	By means of communications, consults, interconnections, or transfers. In other words, any operation or set of technical operations or procedures, automated or not, that within a database allow the collection, organization, storage, preparation, selection, extraction, comparison, sharing, communication, transmission, or cancellation of consumer data.
Data retention	Is it mandatory to retain/conserve the data collected or processed for a specific term? If so, what is the term?	Yes	Varies depending on the matter. Law No. 172-13 does not establish an obligation or specific term to withhold/keep data. However, this obligation could arise in a contract or by provisions of any other sectorial law. For example, in tax matters, the taxpayers, controllers and third parties are required to keep in an orderly manner for a period of ten (10) years: accounting books, special books and records, backgrounds, receipts or proofs of payment, or any physical or electronic document regarding the operations and activities of the taxpayer.
Data elimination	Is there an obligation to eliminate the data collected or processed? If so, under what conditions and for what term?	Yes	Partially or fully inaccurate data or data that is incomplete must be suppressed and replaced or, where applicable, completed by the file or database controller when such inaccuracy or incomplete information is known, without limiting the rights of the data subjects established in this law.
Privacy Impact Assessment	Are Privacy Impact Assessments required and/or mandatory?	N/A	
Incidents	Is it mandatory to report security incidents or breaches or the related legal provisions?	N/A	Law No. 172-13 does not establish a specific obligation to report a security incident or any noncompliance of legal provisions. However, data processing controllers are required to keep the information under the security conditions needed to avoid its unauthorized tampering, loss, consult, use, or access.
Sanctions	Are there sanctions for failures to comply with this obligation? If so, please list them along with the corresponding sanction or penalty amounts.	N/A	Must be evaluated depending on the case because Law No.172-13 establishes the Indemnity Right. Interested parties who, because of the noncompliance of the provisions of this law, suffer damages have the right to be indemnified as established by the common law. Specific sanctions established in the Law and its regulations are for Credit Information Companies (SIC).
Legal actions	Are there any legal actions for personal data protection? Who has the right to exercise/request them?	Yes	Every person has the right to a judicial action to know of the existence and access of data recorded in public or private registries or data banks and, in the event of discrimination, inaccuracy, or error, demand the suspension, rectification, and update of such data as provided for in this law.

Matter	Concept	Yes / No / NA	Observations / comments
Personal data protection officer or controller.	Is there a Data Protection Officer (DPO) or similar position? If so, is their appointment mandatory? Must they be appointed locally?	No	
Investigations	Can a competent authority officially act and/or investigate breaches of personal data protection?	Yes	Must be evaluated depending on the case. For example, in the matter of money laundering, personal data may be processed depending on the investigation being performed.
Processing Records	Are there any mandatory requirements for maintaining processing records under the applicable laws? Specifically, what information must be included in these records, and are there any particular conditions or circumstances under which data controllers or processors are obliged to keep detailed records of their data processing activities?		<p>However, the law stipulates regarding data security that the data file controller and, where applicable, the data processing manager must adopt and implement the necessary technical, organizational, and security measures to safeguard personal data and prevent its alteration, loss, unauthorized processing, consultation, or access.</p> <p>Consequently:</p> <ul style="list-style-type: none"> a) It is prohibited to register personal data in files, records, or databases that do not meet technical integrity and security conditions. b) Data contributors, Credit Information Companies (CICs), and users or subscribers must adopt the necessary technical measures and controls to prevent the alteration, loss, processing, or unauthorized access to credit history data that they handle or store in the databases of Credit Information Companies (CICs). c) Credit Information Companies (CICs) must adopt appropriate measures to protect their databases against natural risks, such as accidental loss or destruction due to disasters, and against human risks, such as unauthorized access, covert use of data, or contamination by computer viruses.
Similarities with the GDPR	Per your understanding, do you believe that the regulation contemplates all of the requirements set by similar international regulations (e.g., the GDPR)? What relevant differences did you find?	No	There are relevant differences in the sense that Law No. 172-13 is a law whose main focus is personal data processing by credit entities.
Other obligations	Are there other additional considerations/requirements or legal obligations on data protection that must be met?	Yes	Constitutional and jurisprudential considerations depending on the case.

A scenic landscape of Ecuador featuring a river flowing through a valley, with a snow-capped mountain range in the background under a blue sky with white clouds.

Ecuador



Matter	Concept	Yes / No / NA	Observations / comments
Regulations	Does the country have a personal data protection law? If so, please name the applicable regulation.	Yes	Personal data protection is regulated by the Organic Law of Personal Data Protection ("OLPDP"). These regulations came into effect on May 26, 2021.
Enforcement Authority	Who is the enforcement authority? If applicable, please provide their website link	Yes	The OLPDP mentions a Personal Data Protection Authority ("PDPA") and/or competent judges. Fabrizio Peralta Díaz serves as the first head of the Data Protection Authority (Superintendence of Personal Data Protection).
Scope of Application	Which is the regulation's scope of application? I.e., is it a strictly national or cross-border concept?	Yes	<p>Regardless of the rules established in the international instruments ratified by Ecuador, the legal provisions of the OLPDP Bill provide territorial application when:</p> <ol style="list-style-type: none"> 1. The processing of personal data is carried out within the Ecuadorian national territory. 2. The data controller is domiciled within Ecuadorian national territory. 3. The data controller not domiciled in Ecuador processes data from data subjects that reside in Ecuador when the activities of the processing relate to: <ol style="list-style-type: none"> a. Offer of goods or services to subjects. b. Control of their behavior as long as this takes place in the Ecuadorian national territory. 4. The person responsible or in charge is subject to national legislation by virtue of an agreement or regulations of public international law, despite not being domiciled in Ecuador.
Data collection	Which are the requirements or processes for personal data collection? (For example, data subject consent, information on purpose of data use and subject's rights, etc.)	Yes	<p>Personal data processing will be legitimate and lawful when the following conditions are met:</p> <ol style="list-style-type: none"> 1. By the existence of the consent of the data subject for the processing of his/her personal data. 2. That it is carried out by the data controller expressly and clearly. 3. That it is carried out by the data controller in compliance with a legal obligation or court order. 4. That the processing is based on a public interest. 5. For the execution of pre-contractual measures at the data subject's request 6. To protect vital interests (life, health, integrity). 7. For processing of personal data contained in public databases. 8. To satisfy a legitimate interest of the data controller or a third party, when the interest or rights of the subjects do not prevail. <p>Only data that are strictly necessary for the realization of the purpose may be processed. Likewise, the processing must be transparent to the data subject.</p>
Legal concept of "personal data"	What are personal data	Yes	The OLPDP defines personal data as the information on (directly or indirectly) identified or identifiable individuals.
Personal data categories	Are there different personal data categories? Please explain each category, if applicable.	Yes	<ul style="list-style-type: none"> ▶ Sensitive data: data related to ethnics, gender identity, cultural identity, religion, ideology, political association, criminal record, migration status, sexual orientation, health, biometric data, genetic data, and information whose improper processing may cause discrimination, threatens, or may threaten human rights or the dignity and integrity of people. The Personal Data Protection Authority will determine other categories of sensitive data. ▶ Recordable personal data: Personal data that should be registered in Public Registries per the law. ▶ Genetic data: Unique personal data related to genetic characteristics inherited to or acquired from individuals that provide unique information on physiology or health of a person. This data is generally analyzed based on biological samples. ▶ Biometrical data: Unique personal data obtained from specific technical processing of physical, physiological, or behavioral characteristics of a person which allow or confirm his/her unique identification, such as facial features or fingerprints, etc. ▶ Recordable personal data: Personal data that should be registered in Public Registries per the law. ▶ Credit personal data: Data on individuals' behaviors to analyze their payment and financial capacity.

Matter	Concept	Yes / No / NA	Observations / comments
Situation of the corporations and other legal entities.	Does the regulation sufficiently protect the personal data of the corporations or entities?	No	The OLPPD protects only natural persons, excluding legal persons or corporations.
Data subject consent	Is the data subject's consent required to collect the data? If so, are there conditions to obtaining the data subject's consent? (For example, prior information that must be provided to the data subject).	Yes	Consent must be free, expressed, unambiguous, specific, informed and given beforehand. When collecting personal data, the subjects shall be informed expressly and clearly beforehand, to evidence the data subject's authorization in favor of the controller for the processing of his/her personal data. Consent must be obtained for each of the purposes of the processing.
Exceptions to the consent	Are there exceptions to the voluntary consent of a data subject? If so, please list the exceptions.	Yes	Consent will not be necessary when: 1. Data was collected from public sources. 2. Data must be provided to administrative or judicial authorities. 3. Data processing is a free and legal relationship between the data controller and the data subject to the extent that it is limited to the purpose that justifies it. 4. Data is communicated between Public Administrations, and is intended for further processing for historical, statistical or scientific purposes, provided that the data are duly dissociated. 5. Personal data relates to health emergency that involves vital interests and the data subjects unable to give his consent. 6. Health-related data are processed for epidemiological studies of public interest, preferably anonymized. 7. The processing of health data when it is necessary for reasons of essential public interest and must be proportionate to the objective pursued. 8. The treatment is necessary for reasons of public interest in the field of public health, or to ensure levels of quality and health safety.
Content and scope of the information to be validated by the data subject.	What should be the content of the consent? (For example, data use or destination, international data transfer, etc.)	Yes	Consent will be valid when the manifestation of the will is: ► Free , i.e., it is exempt from defects of consent. ► Specific , regarding the concrete determination of means and purposes of data processing. ► Informed , complying with the principle of transparency and allows the exercise of the right to transparency. ► Unambiguous , without doubts on the scope of the authorization granted by the data subject. ► Revocable , so that it can be withdrawn at any time, without justification being required. However, processing carried out before consent being withdrawn is lawful.

Matter	Concept	Yes / No / NA	Observations / comments
Transfer of personal data	Are there requirements or restrictions on the transfer of personal data? Are there requirements that apply to the international transfer of data? (Example: model clauses, Supervisors' authorization, etc.)	Yes	<ul style="list-style-type: none"> ▶ National transfer: Personal data may be transferred or communicated to third parties for purposes directly related to the legal functions of the data controller and the recipient, when the transfer is part of legitimacy causes, and when the data subject has given his consent. ▶ The consent is informed when, to transfer or communicate personal data, the data controller has provided enough information to the data subject to help him understand the purpose of the data processing and the type of activity of the third party who may receive the data. ▶ International transfer: It will be possible when the following considerations are observed: <ul style="list-style-type: none"> a. Personal data may be transferred, organizations and legal entities in general that provide adequate levels of protection. b. In the event of an international transfer of data to a country, organization or international economic territory that has not been qualified by the ADPDP as having an adequate level of protection, a binding legal instrument must be issued, which guarantees: <ul style="list-style-type: none"> i. Compliance with principles, rights and obligations in the processing of personal data at a standard equal or higher than the Ecuadorian regulations. ii. Permanent availability of administrative or judicial actions. iii. The right to request full reparation, if applicable. c. For other cases, authorization must be obtained from the APDPD, registering the information on international transfers in the National Registry for the Protection of Personal Data by the data controller. d. Ex officio or upon request, the Personal Data Protection Authority will determine, through a reasoned resolution, the countries, organizations, or legal entities that have adequate levels of protection for the transfer of personal data.
BCR	Do they have binding corporate rules (BCR)?	Yes	<p>Personal data controllers and processors may submit binding, specific corporate regulations applied to their activity to the Personal Data Protection Authority.</p> <p>Any business group or union of companies engaged in a joint economic activity will have the ability to invoke binding corporate rules authorized for their international transfers of data to third countries, provided that such corporate rules incorporate all applicable principles of personal data processing and rights, as well as adequate security guarantees for the transfer of personal data.</p>
Sensitive data	What is understood by sensitive data? How is sensitive data processed, if applicable?	Yes	<p>Sensitive data are those related to ethnics, gender identity, cultural identity, religion, ideology, political association, criminal record, migration status, sexual orientation, health, biometric data, genetic data, and information whose improper processing may cause discrimination, threatens, or may threaten human rights or the dignity and integrity of people. The Personal Data Protection Authority will determine other categories of sensitive data.</p> <p>The OLPDP allows the processing of sensitive personal data when any of the following circumstances apply:</p> <ol style="list-style-type: none"> 1. The subject grants his explicit consent. 2. The processing is necessary for the fulfillment of obligations and exercise of rights in the field of labor law and/or social security and protection. 3. The processing is necessary to protect vital interests of the data subject where the data subject is not capable of giving his consent. 4. The processing relates to personal data which the data subject has manifestly made public. 5. The processing is carried out by order of a judicial authority. 6. The processing is necessary for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes.

Matter	Concept	Yes / No / NA	Observations / comments
Database registration or periodic reporting to the corresponding authority	Is it mandatory to register (e.g., with the corresponding enforcement body) a database and/or a database ownership, processing and/or use? Is it mandatory to submit any type of information or report periodically to the enforcement authority?	Yes	<p>The data controller shall report and keep updated the information with the Personal Data Protection Authority on the following:</p> <ol style="list-style-type: none"> 1. Identification of the database or processing. 2. Legal address and contact details of the data controller and data processor. 3. Characteristics and purpose of the processing. 4. Nature of the personal data processed. 5. Address and contact details of the recipients of the personal data. 6. Mode of interrelation of recorded information. 7. Means used to implement the LOPDP. 8. Requirements and tools implemented to guarantee the security and protection of personal data. 9. Data retention time.
Data security	Are there technical measures to guarantee the security and confidentiality of personal data? If so, what are they?	Yes	<p>The data controller or processor must implement a permanent and continuous evaluation process of efficiency, efficacy and effectiveness of the technical, organizational and measures of any other kind, which may include:</p> <ol style="list-style-type: none"> 1. Anonymization, pseudonymization or encryption of personal data. 2. Measures aimed at maintaining the confidentiality, integrity and availability of systems and services at all times. 3. Measures aimed at improving technical, physical, administrative, and legal resilience. 4. International standards for implementing information security systems or codes of conduct recognized and authorized by the PDPA. adopt technical and organization measures to guarantee the security and confidentiality of personal data and avoid their unauthorized change, loss, or consultation or processing.
Rights of the data subjects	What are the data subjects' rights? (Example: correction, update, or deletion). Please list and explain.	Yes	<p>The data subject has the following rights:</p> <ul style="list-style-type: none"> ▶ Right to information. ▶ Right of access. ▶ Right to rectification and update. ▶ Right to deletion. ▶ Right to oppose. ▶ Right to portability. ▶ Right to suspension of processing. ▶ Right not to be subjected to a decision based solely on automated assessments. ▶ Right of children and adolescents not to be the subject of a decision based solely or partially on automated assessments. ▶ Right to consultation. ▶ Right to digital education.
Actions by the data subjects	How can they exercise them?	Yes	<p>Direct and administrative claims.</p> <p>If data controllers do not address the claims within the set term, or the answer were negative, data subjects may file the administrative claims with the Personal Data Protection Authority.</p> <p>Without precluding the above, data subjects may file civil, criminal, and constitutional claims which they consider they are involved in.</p>
Assignment of personal data	What are the requirements for the assignment of personal data?	Yes	Express consent of the holder.

Matter	Concept	Yes / No / NA	Observations / comments
Data processing	Can the services be provided through a third party (data processing)? If so, please explain the procedure and exceptions, if applicable.	Yes	Personal data processing rendered by third parties, shall be regulated by an agreement in which it is clearly and precisely stated that it will process the data in accordance with the instructions of the data controller and will not use the data for purposes other than those stipulated in the agreement. The third party shall not transfer or communicate the personal data for retention. The third party shall be liable for any infringements arising from the breach of the conditions of processing of personal data.
Data retention	Is it mandatory to retain/conserve the data collected or processed for a specific term? If so, what is the term?	No	Personal data will be retained for a time no longer than necessary to fulfill the purpose of the data processing. To ensure that data will be retained no longer than necessary, data controllers shall establish deletion or periodic review terms. Extended retention during the personal data processing will only occur when data is stored for public interest, scientific research, historical or statistical purposes, provided that timely and necessary security and personal data protection measures are established.
Data elimination	Is there an obligation to eliminate the data collected or processed? If so, under what conditions and for what term?	Yes	Data subjects have the right for data controllers to delete their personal data when: 1. The data processing does not comply with legal principles. 2. The data processing is not necessary or relevant for the purpose. 3. Personal data fulfilled the purpose for which it was collected or processed. 4. The personal data retention term expired. 5. The data processing affects fundamental rights or individual liberties. 6. Data subjects revoke the consent given or state that they did not give any consent without justification. 7. There is a legal obligation. Data controllers will implement methods and techniques to definitely and securely delete or make personal data unreadable or unrecognizable within fifteen (15) days after receiving the request made by data subjects. This request is for free.
Privacy impact assessment	Are privacy impact assessments mandatory?	Yes	Data controllers will assess the impact of personal data processing when they identify that such processing imposes high risks for the rights and liberties of data subjects due to its nature, background or purposes, or when the Personal Data Protection Authority requires it. Data processing impact assessments are mandatory in the cases established by law and must be conducted prior to the commencement of personal data processing. Data controllers must use the criteria set out in the Regulation to determine when there is a need for a systematic and comprehensive assessment of personal aspects, large-scale processing of special categories of data, data related to criminal convictions and offenses, or systematic large-scale observation of a public access area. In case of doubt, the data controller may submit a consultation to the Data Protection Authority to determine whether an impact assessment is required. The Data Protection Authority must respond to this consultation within a maximum period of five (5) days from the receipt of the inquiry.
Incidents	Is it mandatory to report security incidents or breaches or the related legal provisions?	Yes	The data controller shall notify the breach of personal data security to the PDPA and the Telecommunications Regulation and Control Agency as soon as possible and no later than 5 days after becoming aware of the breach. If this term is not complied with, the reasons for the delay must be specified. The data processor shall notify the data controller of any breach of security as soon as possible, and at the latest within 3 days from the date on which he/she becomes aware of it. Similarly, the data controller must notify the data subject without delay of the breach when it involves a risk to his/her fundamental rights and freedoms, within 3 days from the date on which he/she became aware of the breach.
Sanctions	Are there sanctions for failures to comply with this obligation? If so, please list them along with the corresponding sanction or penalty amounts.	Yes	<ul style="list-style-type: none"> ▶ Minor infringements: Public officers: fines of one (1) to ten (10) unified basic worker wages in general, without precluding the extra-contractual liability of the State. ▶ Serious infringements: Public officers: fines of ten (10) to twenty (20) unified basic worker wages in general. <p>Regarding the private sector: fines between 0.7% and 1%, calculated on their business volume corresponding to the economic year immediately prior to the year when the fine was imposed.</p>

Matter	Concept	Yes / No / NA	Observations / comments
Legal actions	Are there any legal actions for personal data protection? Who has the right to exercise/request them?	Yes	<p>Data subjects may file requirements, petitions, or claims directly to data controllers at any time, freely and by physical or digital means provided by data controllers.</p> <p>Regarding administrative claims, without precluding the above, data subjects may file civil, criminal, and constitutional claims which they consider they are involved in.</p>
Personal data protection officer or controller.	Is there a Data Protection Officer (DPO) or similar position? If so, is their appointment mandatory? Must they be appointed locally?	Yes	<p>The law defines the DPO as a natural person in charge of informing the controller or processor about its legal obligations, supervising compliance with regulations concerning the protection of personal data, and cooperating with the PDPA, serving as a point of contact between the PDPA and the entity responsible for data processing.</p> <p>The law does not establish a requirement to appoint a data protection officer. However, the officer will be appointed when:</p> <ol style="list-style-type: none"> 1. The data processing is carried out by the public sector. 2. A permanent and systematized control is required, due to the volume, nature, scope, or purposes of the processing of personal data. 3. Data refers to national security. 4. Data processing refers to a high processing volume of special data categories. <p>The Data Protection Authority may define new conditions under which a Data Protection Officer must be appointed.</p> <p>The Data Protection Officer (DPO) can be employed by the data controller under an employment relationship or through a service contract.</p> <p>Business groups have the option to appoint a single DPO for the entire group.</p>
Investigations	Can a competent authority officially act and/or investigate breaches of personal data protection?	Yes	<p>At its own initiative or at data subjects' request, the Personal Data Protection Authority may initiate prior procedures to understand the circumstances of the specific case or the convenience of initiating or not, an administrative procedure.</p>
Processing Records	Are there any mandatory requirements for maintaining processing records under the applicable laws? Specifically, what information must be included in these records, and are there any particular conditions or circumstances under which data controllers or processors are obliged to keep detailed records of their data processing activities?		<p>The data controller with one hundred or more employees must keep a record of all personal data processing activities under their responsibility. This record must be maintained in writing or electronically. Controllers must make the records of activities available to the Data Protection Authority upon request.</p> <p>The obligation to maintain records of processing activities also applies to controllers with fewer than one hundred employees if they meet any of the following conditions:</p> <ul style="list-style-type: none"> ► The processing may pose a risk to the rights and freedoms of data subjects, according to risk, threat, and vulnerability analysis, in accordance with the law. ► The processing is not occasional. ► It includes special categories of personal data.
Similarities with the GDPR	Per your understanding, do you believe that the regulation contemplates all the requirements set by similar international regulations (e.g., Example: GDPR)? What relevant differences did you find?	Yes	<p>The Organic Law of Personal Data Protection considers all the requirements received from the international regulations by adopting the Protection Standards (GDPR, Personal Data for Ibero-American States, and the Bill of laws on Personal Data Protection issued by the OEA).</p>
Other obligations	Are there other additional considerations/requirements or legal obligations on data protection that must be met?	Yes	<p>As of May 2023, the sanctioning regime began.</p> <p>By Decree "904", the General Regulation of the Organic Law on Personal Data Protection was issued, published in the third supplement of Official Registry No. 435 on November 13, 2023.</p>

A scenic landscape of a river flowing through a lush green valley, with a range of mountains in the background under a blue sky with scattered clouds.

Mexico



Matter	Concept	Yes / No / NA	Observations / comments
Regulations	Does the country have a personal data protection law? If so, please name the applicable regulation.	Yes	<p>Mexico has the following regulations on this matter, which apply to individuals or private entities:</p> <ul style="list-style-type: none"> ► The Federal Law of Personal Data Protection Held by Private Parties (2010) ("LFPDPP" from Spanish). ► The Rules of the Federal Law of Personal Data Protection Held by Private Parties (2011) ("Rules of the LFPDPP"). ► Guidelines of the Privacy Notice (2013) ("LAV" from Spanish). ► Parameters for the Correct Development of Binding Self-Regulation Systems (2013) ("PAPDP"). ► Rules of Procedure of the Registry of Binding Self-Regulation Systems (2015) ("ROREAV"). <p>It is worth mentioning that Mexico also has regulations on the protection of personal data held by the public sector, and specifically the General Law on Protection of Personal Data Held by Bound Parties (2017) ("LGPDPPSO"), whose analysis is not included in this document.</p>
Enforcement Authority	Who is the enforcement authority? If applicable, please provide their website link	Yes	<p>The enforcement authority is the National Institute of Transparency, Access to Information and Personal Data Protection ("INAI" from Spanish).</p> <p>http://inicio.ifai.org.mx/SitePages/ifai.aspx</p>
Scope of Application	Which is the regulation's scope of application? I.e., is it a strictly national or cross-border concept?	Yes	<p>The regulations will be applicable, as established in Sections 2, 3, para. ix) of the LFPDPPP and Sections 3, 4 and 49 of the LFPDPPP Rules, to any private party, whether individual or entity, that carries out personal data processing under the following assumptions:</p> <ol style="list-style-type: none"> 1. Any processing conducted at any data controller establishment located in Mexico. 2. Any processing conducted by a data processor regardless of their location, on behalf of a data controller established in Mexico. 3. When the data controller is not located in Mexico but is subject to Mexican laws, derived from the signing of a contract or in terms of international law; and 4. When the data controller is not located in Mexico and uses means located there, except if those means are used only for transit purposes and do not involve processing. <p>The foregoing, with the understanding that any processing of personal data on physical or electronic means, which makes it possible to access personal data according to certain criteria, regardless of the form or method of its creation, type of support, processing, storage and organization, will be subject to regulation, including the data processing that is carried out by a data controller, be it an individual or corporation, who alone or together with others processes personal data on behalf of the data controller.</p>
Data collection	Which are the requirements or processes for personal data collection? (For example, data subject consent, information on purpose of data use and subject's rights, etc.)	Yes	<p>Any party responsible for data collection (data controller) will have the obligation to inform the subjects of the data of the information that is collected from them and for what purposes, information regarding data transfers to be made, if applicable, and which are the rights of the data subject, as well as the means to exercise them, through the "privacy notice".</p> <p>This notice may be in the form of a physical document, an electronic document, or any other format generated by the data controller, and must be made available to the data subject before their personal data is processed.</p> <p>The privacy notice must comply with the provisions of Section 3, sub-section I, 15-17 of the LFPDPPP, the LAV.</p> <p>In the same line, the LAV are based on the concept of the principle of information. It is also important to note that any personal data processing will be subject to the subject's consent, whether implied or explicit, as applicable, except through the exceptions stated by the LFPDPPP.</p>
Legal concept of "personal data"	What are personal data	Yes	<p>Personal data is any information relating to an identified or identifiable individual. An individual is considered to be identifiable when their identity might be directly or indirectly determined through any information.</p> <p>Section 3, para. V, LFPDPPP.</p>

Matter	Concept	Yes / No / NA	Observations / comments
Personal data categories	Are there different personal data categories? Please explain each category, if applicable.	Yes	<p>Mexican regulations classify data into three categories:</p> <ul style="list-style-type: none"> Personal data: Any information concerning an identified or identifiable individual. An individual is considered to be identifiable when their identity might be directly or indirectly determined through any information. Capital or financial data. Sensitive personal data: Data related to the subject's private sphere, whose use may cause discrimination or a serious risk to its subject. In an illustrative but not exhaustive manner, sensitive data are all those personal data that may reveal aspects such as racial or ethnic origin, present or future state of health, genetic information, religious, philosophic, and moral beliefs, political opinions, and sexual preference. <p>For the processing of capital or financial and sensitive data, the data controller must obtain the express and written consent of the subject through his handwritten signature, electronic signature, or any authentication mechanism established for that purpose. Since these are sensitive data, sensitive databases may only be created when there is a legal mandate, it is justifiable in terms of Section 4 of the LFPDPPP or when the data controller requires it for legitimate, specific purposes and in accordance with the activities or explicit purposes that it pursues.</p> <p>Section 3, para. v) and vi), 8, 9, 13, and 16 LFPDPPP and Section 15 para. II and III, 56 and 62 of the LFPDPPP Rules.</p>
Situation of the corporations and other legal entities.	Does the regulation sufficiently protect the personal data of the corporations or entities?	No	
Data subject consent	Is the data subject's consent required to collect the data? If so, are there conditions to obtaining the data subject's consent? (For example, prior information that must be provided to the data subject).	Yes	<p>Yes, if the consent is required and must be as set out in Sections 3, para. iv), 6, 8, 9 and 12 of the LFPDPPP and Sections 9, 11-21 of the LFPDPPP Rules (free, specific, and reported, in addition to unequivocal when referring to express consent). Any processing of personal data will be subject to the subject's consent, except for the stipulated exceptions (see next question). For the purposes of demonstrating that consent was obtained, the burden of proof will fall in all cases on the data controller.</p> <p>The consent will be explicit when the will is expressed verbally, in writing, through electronic means, optical means or any other technology, or through unequivocal signals.</p> <p>It will be understood that the subject gives implied consent to the processing of their data when a privacy notice has been made available to them and they do not express their opposition.</p> <p>Consent to the processing of personal data is not required when:</p> <ol style="list-style-type: none"> 1. Is provided by law. 2. The data is contained in publicly available sources. 3. The personal data are subjected to a disassociation process. 4. Has the purpose of fulfilling obligations arising from a legal relationship between the subject and the data controller. 5. There is a situation of emergency that could potentially harm an individual or their assets. 6. It is indispensable for medical attention, the prevention, diagnostic, rendering of health assistance, medical treatment or health service management, as long as the data subject is not in condition to give consent in the terms established by the applicable legislation, and this data processing is conducted by a person subject to professional confidence obligations or their equivalent. 7. A resolution is issued by the competent authority. <p>The data subject may revoke their consent for the processing of their personal data at any time, for which the data controller must establish the mechanisms and procedures in the privacy notice.</p> <p>Sections 3, para. iv), 6, 8, and 9 LFPDPPP.</p> <p>Sections 9- 21 LFPDPPP Rules.</p>
Exceptions to the consent	Are there exceptions to the voluntary consent of a data subject? If so, please list the exceptions.	Yes	The data controller will not be under the obligation to gather the subject's consent to process their personal data when any of the exceptions stated in Sections 10 and 37 of the LFPDPPP and Section 17 of the LFPDPPP Rules is present.

Matter	Concept	Yes / No / NA	Observations / comments
Content and scope of the information to be validated by the data subject.	What should be the content of the consent? (For example, data use or destination, international data transfer, etc.)	Yes	Consent per se should not have specific content (it can be given tacitly, through a simple handwritten signature or other electronic mechanisms), since the privacy notice on which consent is granted is the one that must meet the requirements established by law, so that the consent is valid. The requirements of the privacy notice are described in the items "Data Collection".
Transfer of personal data	Are there requirements or restrictions on the transfer of personal data? Are there requirements that apply to the international transfer of data? (Example: model clauses, Supervisors' authorization, etc.)	Yes	<p>Any transfers of personal data, whether national or international, are subject to the subject's consent, except under the exceptions mentioned in Section 37 of the LFPDPPP. These must be reported to the data subject through a privacy notice and be limited to the purpose that justifies them.</p> <p>The processing of the data will be done in accordance with what was agreed in the privacy notice, which will contain a clause that states whether the subject accepts the transfer of their data; likewise, the third-party recipient will assume the same obligations that correspond to the person in charge who transferred the data.</p> <p>International data transfers must be made per the provisions of Sections 67-70, 74-76 of the LFPDPPP Rules.</p> <p>Sections 36 and 37, LFPDPPP; Arts. 67-71, 73-76, LFPDPPP Rules.</p> <p>In this sense, it should be noted that the communication of personal data between the data controller and the data processor, inside or outside Mexico, is not classified as a "transfer", but as a referral, in terms of Section 2 para. IX. of the LFPDPPP Rules. National and international remissions of personal data between a data controller and data processor does not need to be reported to the subject or have their consent. The data processor is the individual or entity, public or private, not related to the data controller organization, that alone or in conjunction with others, processes personal data on behalf of the data controller, as a result of the existence of a legal relationship that connects him with the latter and outlines the scope of his actions as part of the service rendering.</p> <p>Section 2 and 53 of the LFPDPPP Rules.</p>
BCR	Do they have binding corporate rules (BCR)?	Yes	<p>Individuals or entities may agree with each other or with civil or governmental organizations, both national and foreign, any binding self-regulation systems on this matter that complement the provisions of the LFPDPPP. These systems must have the mechanisms to measure their efficacy in protecting data, consequences, and corrective measures in case of breach.</p> <p>Self-regulatory systems may be translated into deontological codes or good professional practice codes, privacy policies, seals of confidence or other mechanisms and will contain specific rules or standards that allow harmonizing the data processing performed by those adhering to them and facilitate exercising the rights of the subjects.</p> <p>When a data controller adopts and complies with a self-regulation system, this circumstance will be taken into consideration to determine the reduction of the corresponding sanction, in the event that a breach of the LFPDPPP and LFPDPPP Rules is verified by the INAI. Likewise, the INAI may determine other incentives to adopt self-regulation systems, as well as mechanisms that facilitate administrative proceedings with these.</p> <p>For transfers of personal data between controlling entities, subsidiaries or affiliates under common control of the same group as the controller, or a parent or any corporation in the same group as the controller, the mechanism to guarantee compliance with the provisions of LFPDPPP, the LFPDPPP Rules and any applicable set of regulations could be the existence of internal regulations for personal data protection, whose observance may be binding and aligned with the provisions of the applicable regulations.</p> <p>Section 44 of the LFPDPPP and Sections 70 and 79 to 86 of the LFPDPPP Rules.</p>

Matter	Concept	Yes / No / NA	Observations / comments
Sensitive data	What is understood by sensitive data? How is sensitive data processed, if applicable?	Yes	<p>Sensitive data is data related to the subject's intimate sphere, or data whose inadequate use may cause discrimination or involve a serious risk to its subject. In an illustrative but not exhaustive manner, sensitive data are all those personal data that may reveal aspects such as:</p> <ul style="list-style-type: none"> ▶ Racial or ethnic origin. ▶ Present or future state of health. ▶ Genetic information. ▶ Religious, philosophic, and moral beliefs. ▶ Political opinions. ▶ Sexual preference. <p>Its processing must occur per the provisions of Sections 9, 13 and 16 of the LFPDPPP, Sections 15 and 56 of the LFPDPPP Rules.</p> <p>Sections 9, 13, 16 and 64 paras. iv) LFPDPPP; Sections 15, 56 and 62 of the LFPDPPP Rules.</p>
Database's registration or periodic reporting to the corresponding authority	Is it mandatory to register (e.g., with the corresponding enforcement body) a database and/or a database ownership, processing and/or use? Is it mandatory to submit any type of information or report periodically to the enforcement authority?	No	<p>There is no obligation to register a database with the enforcement authority.</p>
Data security	Are there technical measures to guarantee the security and confidentiality of personal data? If so, what are they?	Yes	<p>The data controller, and when applicable the data processor must establish and maintain administrative security such as:</p> <ul style="list-style-type: none"> ▶ Administrative: the segregation of permissions based on roles and responsibilities -always granting least privilege. ▶ Physical: such as the implementation of technology capable of ensuring that data remains available, complete and confidential, and, where appropriate. ▶ Technical: such as the implementation of controls to identify and track any unauthorized changes made by users or encrypted storage, to protect the personal data, regardless of the processing system. <p>Section 2, paras. v), vi) and vii) of the LFPDPPP Rules explains what these measures consist of. Likewise, the data controller or third parties that intervene in any phase of the processing of personal data must always maintain confidentiality over the data, and even after their relationship with the subject or controller, as applicable, is over.</p> <p>Security measures must be implemented based on a risk analysis of the personal data processed, taking into account the sensitivity of the personal data, its quantitative or qualitative value, as well as technological developments, and on a gap analysis of existing security measures.</p> <p>The controller should consider actions with the purpose of establishing and maintaining the security of personal data, including but not limited to:</p> <ul style="list-style-type: none"> ▶ Having an inventory of personal data and repositories (physical and electronic). ▶ Having traceability of personal data throughout its life cycle (collection, storage, use, transfer, blocking and deletion) in the various processing activities. ▶ Define training and awareness plans and programs for personnel involved in the processing of personal data. ▶ Establish a list of the security measures that the controller has in place to ensure the protection of personal data. <p>The responsible party shall update the security measures for their continuous improvement, or in case of any substantial modification in the processing or violation/assault of personal data.</p> <p>The LFPDPPP rules develop the regulatory framework for security measures in Sections 57, 59-62.</p> <p>Sections 19 and 21, LFPDPPP; Sections 2 para. v), vi) and vii), 48 paras. ix), 57, 59, 60-62, LFPDPPP Rules.</p>
Rights of the data subjects	What are the data subjects' rights? (Example: correction, update, or deletion). Please list and explain.	Yes	<p>The rights of data subjects, according to Mexican regulations, are the right of access, rectification, cancellation, and opposition (ARCO Rights, from Spanish). The exercise of any of them is not a requirement and does not impede the exercise of another right.</p> <p>Sections 3, para. iii), 22-25, 31 and 33, LFPDPPP; Sections 2 para. ii) and 87, LFPDPPP Rules.</p>

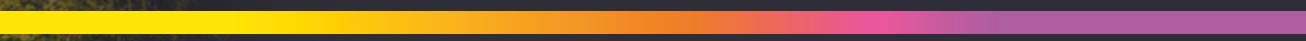
Matter	Concept	Yes / No / NA	Observations / comments
Actions by the data subjects	How can they exercise them?	Yes	<p>ARCO rights must be exercised per the provisions of Sections 22-26, 28, 29, 31-33 and 35 of the LFPDPPP. Sections 87-90, 92-98 y 101-106 and 109 of the LFPDPPP Rules.</p> <p>Sections 22-26, 28, 29, 31-33 and 35 of the LFPDPPP Rules. Sections 89, 90, 92, 93, 95-98, 101, 102-106 and 109 of the LFPDPPP Rules.</p>
Assignment of personal data	What are the requirements for the assignment of personal data?	N/A	<p>Data protection regulations do not regulate the institute of personal data assignment.</p> <p>They only refer to the national or international transfer of personal data, as well as the remission.</p>
Data processing	Can the services be provided through a third party (data processing)? If so, please explain the procedure and exceptions, if applicable.	Yes	<ul style="list-style-type: none"> ▶ The data processor is the individual or entity, public or private, not related to the data controller organization, that alone or in conjunction with others, processes personal data on behalf of the data controller, as a result of the existence of a legal relationship that connects him with the latter and outlines the scope of his actions as part of the service rendering. They must comply with the obligations established in Section 50 of LFPDPPP Rules. ▶ When a third party, at the request of a data controller, processes personal data, the latter must ensure compliance with the principles of personal data protection and must adopt the necessary measures for their application. These principles are legality, consent, information, quality, end, loyalty, proportionality, and responsibility. ▶ The data controller will oversee compliance with the principles of protection of personal data established by the LFPDPPP and must adopt the measures necessary for their application. The above will apply even when the data is processed by a third party per request by the data controller. The data controller must take the necessary and sufficient measures to guarantee that the privacy notice made known to the subject is respected at all times by him or by third parties with whom he has a legal relationship. ▶ the third party that intervenes in any phase of the processing of personal data must maintain confidentiality over them, and this obligation will subsist even after the end of their relations with the subject or, where appropriate, with the data controller. ▶ The data controller must inform the third party of any requests for rectification or cancellation so that they can proceed accordingly. ▶ When there are data transfers, whether national or international, privacy notices and the ends for which the subject their data to processing must be communicated to the third party so that they can assume the same obligations as those that apply to the data controller transferring the data. <p>Sections 6, 14, 25 and 36 LFPDPPP, Sections 49, 50 and 51, LFPDPPP Rules.</p>
Data retention	Is it mandatory to retain/conserve the data collected or processed for a specific term? If so, what is the term?	Yes	<p>The periods of conservation of personal data must not exceed those that are necessary for the fulfillment of the ends that justified the processing and must comply with the provisions applicable to the matter in question, and take into account the administrative, accounting, tax, legal and historical aspects. Once the ends of the processing have been fulfilled, and when there is no legal or regulatory provision that establishes otherwise, the data controller must proceed to cancel the data in his possession after blocking them, for their subsequent deletion.</p> <p>The subject will always have the right to cancel their personal data.</p> <p>The cancellation of personal data will result in a blocking period after which the data will be deleted. The data controller may conserve them exclusively for the responsibilities created in the processing. The blocking period will be equivalent to the statute of limitations of the actions derived from the legal relationship of the processing per the terms of the applicable Law.</p> <p>After the data has been canceled, the subject will be notified.</p> <p>When the personal data had been transmitted prior to the date of rectification or cancellation and they continue to be processed by third parties, the data controller must inform them of said request for rectification or cancellation, so that it can also be carried out.</p> <p>Section 11, LFPDPPP; and Sections 37-39 of the LFPDPPP Rules.</p>

Matter	Concept	Yes / No / NA	Observations / comments
Data elimination	Is there an obligation to eliminate the data collected or processed? If so, under what conditions and for what term?	Yes	<p>Once the personal data is no longer necessary for the purposes set forth in the privacy notice and the applicable legal provisions, they must be canceled.</p> <p>Furthermore, the data subject will always have the right to cancel their personal data, in which case the data subject will be notified of the effective cancellation of the data.</p> <p>See previous section.</p> <p>Section 11 and 25 LFPDPPP; and Sections 37-39 of the LFPDPPP Rules.</p>
Privacy Impact Assessment	Are privacy impact assessments mandatory?	Yes	<p>Although the LFPDPPP does not impose an obligation to conduct impact assessments, it advises data controller to have a risk analysis for personal data as a security measure over personal data.</p> <p>Likewise, said regulation has a Chapter "On Binding Self-regulation" (Chapter VI), through which it encourages both individuals and entities to acquire self-regulation systems, which complement the related relevant provisions and attempt to promote the commitment of the data controllers, advising the implementation of risk assessments, among others.</p> <p>Sections. 57,59-61, para. iii) and 80 paras. viii), LFPDPPP Rules Section 10 PAPDP.</p>
Incidents	Is it mandatory to report security incidents or breaches or the related legal provisions?	Yes	<p>The data controller must inform the subject of breaches that significantly affect their economic or moral rights, as soon as it is confirmed that the breach occurred and that the data controller has begun to take the actions aimed at triggering a process of exhaustive review of the magnitude of the breach, so that the affected subjects can take the corresponding measures to defend their rights. This obligation must be fulfilled per Sections 20 LFPDPPP, Sections 58,63-66 of the LFPDPPP Rules.</p>
Sanctions	Are there sanctions for failures to comply with this obligation? If so, please list them along with the corresponding sanction or penalty amounts.	No	<p>The regulation does not stipulate specific sanctions for failing to comply with the obligation to report a breach. Nevertheless, Section 58 of the LFPDPPP Rules state that INAI may also consider the compliance with its recommendations to determine a potential reduction of the corresponding sanction. The Sections 63-65 of the LFPDPPP Rules establish other relevant provisions regarding security breaches.</p> <p>In this regard, the LFPDPPP describes in Sections 64, 66-69 the type of sanctions that will apply when there are breaches to personal data.</p> <p>Sections 64, 66-69 of the LFPDPPP; Sections. 58, 63-65 of the LFPDPPP Rules.</p>
Legal actions	Are there any legal actions for personal data protection? Who has the right to exercise/request them?	No	<p>There is no specific legal action protecting this right. However, subjects may always exercise their "ARCO Rights", additionally, the law provides a personal data protection procedure that must be carried out before the INAI.</p> <p>Chapter VII of the LFPDPPP and Chapter VIII of the Regulations of the LFPDPPP.</p>
Personal data protection officer or controller.	Is there a Data Protection Officer (DPO) or similar position? If so, is their appointment mandatory? Must they be appointed locally?	No	<p>Section 30 of the LFPDPPP states that all data controllers must designate a person or personal data department to process the subjects' requests to exercise their rights. It will also promote the protection of personal data within the organization.</p>
Investigations	Can a competent authority officially act and/or investigate breaches of personal data protection?	Yes	<p>The Federal Institute for Access to Information and Data Protection may initiate "Verification Procedure" either officially or at the request of a party. The official verification will apply when there is a breach of the resolutions issued as a result of rights protection procedures or it is presumed (in a founded manner) that there were violations of the provisions of current regulations on data protection.</p> <p>Any person may report to the Institute the alleged violations of the provisions set forth in the LFPDPPP and other applicable regulations, as long as they do not rely on the assumptions of origin of the rights protection procedure. In this case, the Institute's Plenary will determine, in a founded and motivated manner, the applicability of initiating the corresponding verification.</p> <p>The right to file a complaint expires one year from the day following the events or omissions that are the subject of the complaint. When the facts or omissions are of a consecutive nature, the term will begin to run from the business day following the last event that took place.</p> <p>Through the procedure, the Institute will have access to the information and documentation that it deems necessary, per the related resolution.</p> <p>Federal public officers are under the obligation to maintain confidentiality over the information they discover as a result of the corresponding verification.</p> <p>Sections 59 and 60, LFPDPPP; Sections 128 and 129, LFPDPPP Rules.</p>

Matter	Concept	Yes / No / NA	Observations / comments
Processing Records	Are there any mandatory requirements for maintaining processing records under the applicable laws? Specifically, what information must be included in these records, and are there any particular conditions or circumstances under which data controllers or processors are obliged to keep detailed records of their data processing activities?	Yes	<p>To ensure the proper handling of personal data, the controller must adopt certain measures, prioritizing the interests of the data subject and their reasonable expectation of privacy. Among the measures the controller may implement are technical procedures that enable tracking of personal data during its processing.</p> <p>In this regard, it is essential to emphasize that, to establish and maintain the security of personal data, the controller must, among other things, maintain an inventory of personal data and the processing systems/repositories (both physical and electronic).</p> <p>Art. 61 of the LFPDPPP; and Art. 48 of the LFPDPPP Regulation.</p>
Similarities with the GDPR	Per your understanding, do you believe that the regulation contemplates all the requirements set by similar international regulations (e.g., Example: GDPR)? What relevant differences did you find?	No	<p>Matters that the Mexican laws do not contemplate:</p> <ul style="list-style-type: none"> ▶ Extraterritorial application of Mexican laws when processing personal data of Mexican nationals. ▶ More assumptions or ways of processing personal data without the consent of data subjects. ▶ Specific requirements on profiling and decisions based on automated processing (Sections 4.4 and 22 of the GDPR). ▶ Other Data Protection rules, such as the "obligation to host in the national territory" (Sections 88 and 89 of the GDPR).
Other obligations	Are there other additional considerations/requirements or legal obligations on data protection that must be met?	Yes	<p>Relevant consideration when the ends of the personal data processing will include sending advertisements and/or other purposes related to marketing (Section 30 of the LFPDPPP Rules and Sections 24, 36 and 40 of the LAV).</p> <p>Special requirements on advertising and marketing Section 30 of the LFPDPPP Rules, and in relation to the use of cookies (Article 14 of the Regulations of the LFPDPPP and Articles 3 and 31 of the LAV).</p>



Panama

A scenic landscape of a river flowing through a dense tropical forest, with mountains in the background under a blue sky with white clouds.

Matter	Concept	Yes / No / NA	Observations / comments
Regulation	Does the country have a personal data protection law? If so, please name the applicable regulation.	Yes	Law No. 81 of 2019 on Data Protection, regulated by Executive Decree No. 285 of May 28, 2021.
Enforcement Authority	Who is the enforcement authority? If applicable, please provide their website link	Yes	National Authority for Transparency and Access to Information (NATAI). https://www.antai.gob.pa/
Scope of Application	Which is the regulation's scope of application? I.e., is it a strictly national or cross-border concept?	Yes	The rule allows cross-border application, allows that always the data storage controller or its custodian complies with the personal data protection standards required by Law or shows that it complies with the personal data protection standards and rules that are equal to or stricter than those required by the Laws of the Republic of Panama.
Data collection	Which are the requirements or processes for personal data collection? (For example, data subject consent, information on purpose of data use and subject's rights, etc.)	Yes	All processing of personal data shall be subject to prior, informed, and unequivocal consent by a means that allows the data controller to prove the traceability of such consent. Consent must be given in writing, or by any other electronic means that guarantees the identity of the subject of the personal data so that there is certainty as to his or her identity that identifies him or her or makes him or her identifiable.
Legal concept of "personal data"	What are personal data	Yes	Personal Data: Any information regarding individuals that identifies them or makes them identifiable.
"Personal data" categories	Are there different personal data categories? Please explain each category, if applicable.	Yes	<ul style="list-style-type: none"> ▶ Confidential Data: Data that because of its nature should not be of public knowledge or known by unauthorized third parties, including data that is protected by law, by confidentiality or non-disclosure agreements to safeguard information. In Public Administration cases, it is data whose processing is limited to the purposes of that Administration or, if it has express consent from its subject, without limiting the provisions of special laws or rules that develop them. Confidential data will always have restricted access. ▶ Anonymous Data: Data whose identity cannot be established by reasonable means or by the connection between such means and the individual to which it refers. ▶ Expired Data: Data that has not been updated by provisions of Law, by the compliance of the condition, or by the expiration of its designated term of validity or, if there is no express rule, by the change of facts or circumstances that it consigns. ▶ Personal Data: Any information regarding individuals that identifies them or makes them identifiable. ▶ Dissociated Data: Data that cannot be associated to the subject or that because of its structure, content, or degree of disaggregation, the identity of the individual cannot be allowed. ▶ Sensitive Data: Refers to the private sphere of its subject or whose improper use may cause discrimination or severe risk to its subject. Sensitive personal data includes, but is not limited to, data that could reveal aspects such as racial or ethnic origin; religious, philosophical, and moral beliefs or convictions; union membership; political opinions; data related to health, life, sexual preference or orientation, genetic or biometric data, among others, subject to regulation or intended to unequivocally identify a person.
Situation of the corporations and other legal entities.	Does the regulation sufficiently protect the personal data of the corporations or entities?	Yes	The scope of this law is applicable to every individual or company that processes personal data.
Data subject consent	Is the data subject's consent required to collect the data? If so, are there conditions to obtaining the data subject's consent? (For example, prior information that must be provided to the data subject).	Yes	For the processing of personal data to be legal, it shall be collected and processed with the previous, informed, and unequivocal consent of its subject or with legal basis. Likewise, it must be obtained in a way that allows its traceability. For the treatment of sensitive data, it must also be irrefutable and expressly given. In order to comply with the principle of transparency, all information or communication to the subject must be in simple and clear language and keep him/her informed of all the rights that protect him/her as subject of the data, as well as the possibility of exercising the ARCO rights.

Matter	Concept	Yes / No / NA	Observations / comments
Exceptions to the consent	Are there exceptions to the voluntary consent of a data subject? If so, please list the exceptions.	Yes	<p>Exceptions to the scope of this Law include processing that is expressly regulated by special laws or by rules that develop them, in addition to the following personal data processing:</p> <ol style="list-style-type: none"> 1. Processing made by an individual exclusively for personal or local activities. 2. Processing by competent authorities for the prevention, investigation, detection, or prosecution of criminal offenses or execution of criminal sanctions. 3. Processing for financial intelligence analysis and that refers to national security as per the international laws, treaties, or conventions that regulate these matters. 4. When the data processing relates to international organisms in compliance with the provisions of treaties and conventions in effect that are ratified by the Republic of Panama. 5. Processing of information obtained through a previous procedure of dissociation or anonymization so that the result cannot be associated to the personal data subject.
Content and scope of the information to be validated by the data subject.	What should be the content of the consent? (For example, data use or destination, international data transfer, etc.)	Yes	<ul style="list-style-type: none"> ▶ Contact Identification and data of the data controller. ▶ Purpose or purposes of the processing. ▶ The condition that legitimizes the processing. ▶ The recipients of personal data. ▶ Intention to transfer personal data to a third country. ▶ Data retention period. ▶ Procedures to exercise the rights of access, rectification, cancellation, opposition and portability. ▶ Existence of automated decisions (including profiling). ▶ Contact information of the personal data protection officer.
Transfer of personal data	Are there requirements or restrictions on the transfer of personal data? Are there requirements that apply to the international transfer of data? (Example: model clauses, Supervisors' authorization, etc.)	Yes	Only that data storage controller or custodian complies with the personal data protection standards required by Law or shows that it complies with the personal data protection standards and rules that are equal to or stricter than those required by the Laws of the Republic of Panama.
BCR	Do they have binding corporate rules (BCR)?	No	
Sensitive data	What is understood by sensitive data? How is sensitive data processed, if applicable?	Yes	<p>Sensitive Data: Data that refers to the private sphere of its subject or whose improper use may cause discrimination or severe risk for its subject.</p> <p>Sensitive personal data includes, but is not limited to, data that could reveal aspects such as racial or ethnic origin; religious, philosophical, and moral beliefs or convictions; union membership; political opinions; data related to health, life, sexual preference or orientation, genetic or biometric data, among others, subject to regulation or intended to unequivocally identify a person.</p>
Database registration or periodic reporting to the corresponding authority	Is it mandatory to register (e.g., with the corresponding enforcement body) a database and/or a database ownership, processing and/or use? Is it mandatory to submit any type of information or report periodically to the enforcement authority?	No	Only by request of the authority or if there is a data safety breach or incident.
Data security	Are there technical measures to guarantee the security and confidentiality of personal data? If so, what are they?	Yes	<p>The national and international rules or standards on the matter, as well as the binding self-regulation mechanisms or any other established mechanism adequate for such purposes, will be used as reference.</p> <p>Any other established by the control authority.</p>

Matter	Concept	Yes / No / NA	Observations / comments
Rights of the data subjects	What are the data subjects' rights? (Example: correction, update, or deletion). Please list and explain.	Yes	<ul style="list-style-type: none"> ▶ Access. ▶ Rectification. ▶ Cancelation. ▶ Opposition. ▶ Portability.
Actions by the data subjects	How can they exercise them?	Yes	<ul style="list-style-type: none"> ▶ Access right: enables the subject to obtain its personal data that is stored or subject to processing in public or private institution databases, in addition to knowing the origin and object for which such data has been collected. ▶ Rectification right: enables the subject to request the correction of its incorrect, irrelevant, incomplete, outdated, inexact, false, or impertinent personal data. ▶ Cancelation right: enables the subject to request the elimination of its incorrect, irrelevant, incomplete, outdated, inexact, false, or impertinent personal data. ▶ Opposition right: enables the subject, for well-founded and legitimate reasons related to a particular situation, to refuse to provide its personal data or that is data be subjected to a specific processing, as well as to revoke its consent. ▶ Portability right: right to obtain a structured copy of its personal data, in a generic and common use format, that enables its operation by different systems and/or its transfer to another controller when: <ul style="list-style-type: none"> a. The subject has directly delivered its data to the data controller. b. It is a relevant volume of data that has been processed in an automated manner. c. The subject has given its consent to be processed or the data is required for the execution or compliance of a contract. <p>The subject of the personal data may exercise these rights at all times, as these rights are inalienable, except for the exceptions established in special laws.</p>
Assignment of personal data	What are the requirements for the assignment of personal data?	Yes	Only with granted consent.
Data processing	Can the services be provided through a third party (data processing)? If so, please explain the procedure and exceptions, if applicable.	Yes	<p>The controller that processes personal data stored in databases will establish the protocols, processes, management, and safe transfer procedures protecting the rights of the data subjects under the provisions of this Law.</p> <p>This will be audited and supervised by the National Information Transparency and Access Authority with the support of the National Government Innovation Authority when dealing with aspects related to Information Technologies and Communication (TICs).</p> <p>The minimum requirements to be included in the privacy policies, protocols, processes, and safe processing and transfer procedures to be complied by the data processing controller will be issued by the regulator of each sector in accordance with this Law.</p>
Data retention	Is it mandatory to retain/conserve the data collected or processed for a specific term? If so, what is the term?	Yes	Seven (7) years, except if the competent authority requests a longer term for special cases.
Data elimination	Is there an obligation to eliminate the data collected or processed? If so, under what conditions and for what term?	Yes	In no event may the personal data processing controller and/or database custodian transfer or communicate data that relates to an identified or identifiable person after seven years have elapsed since the legal conservation obligation expired, except if the personal data subject expressly requests otherwise.

Matter	Concept	Yes / No / NA	Observations / comments
Privacy impact assessment	Are privacy impact assessments mandatory?	Yes	<p>The data protection impact assessment is defined as the data controller's documentation containing a description of processes with personal data that may generate risks for individual and social rights and obligations, as well as measures, safeguards, and risk mechanisms.</p> <p>Depending on the seriousness of the risk presented by the processing of personal data, as well as the novelty of the technology used, the Supervisory Authority may order the submission of a data protection impact assessment report.</p> <p>The report must include, at a minimum, a description of the types of data collected, the methodology used for data collection and security assurance of the information, and the data controller's analysis regarding the measures, safeguards, and risk mitigation mechanisms adopted.</p> <p>The supervisory authority may request entities to publish the data protection impact assessment reports they carry out and suggest the adoption of standards and best practices for the processing of personal data.</p>
Incidents	Is it mandatory to report security incidents or breaches or the related legal provisions?	Yes	To the corresponding authority, in this case NATAI.

Matter	Concept	Yes / No / NA	Observations / comments
Sanctions	Are there sanctions for failures to comply with this obligation? If so, please list them along with the corresponding sanction or penalty amounts.	Yes	<p>The National Information Transparency and Access Authority will set the amounts of the sanctions that are applicable to the respective infractions depending on the severity of such infractions that will be set from one thousand balboas (B/.1,000) to ten thousand balboas (B/.10,000) and will regulate the corresponding procedure.</p> <p>A minor infraction will be:</p> <ol style="list-style-type: none"> 1. To not remit and/or inform the National Information Transparency and Access Authority within the established terms the information as requested by this Law, its regulations, or any other regulating provision. <p>Section 40. Severe infractions are:</p> <ol style="list-style-type: none"> 1. To process personal data without having received the consent of its subject, as set forth in this Law, its regulations, or any other regulating provision that refers to this Law. 2. To violate the principles and guarantees established in this Law or its regulations. 3. To violate the confidentiality commitment related to personal data processing. 4. To restrict or hinder the application of the access, rectification, cancellation, and opposition rights. 5. To not comply the duty to inform the affected subject of its personal data processing when the data has not been obtained from its subject. 6. To store or file personal data without having the adequate security conditions established by this Law or its regulations. 7. To not address the reiteration of the formally notified requirements or observations, or to not provide the documents or information formally requested by the National Information Transparency and Access Authority. 8. To hinder or not cooperate with the National Information Transparency and Access Authority when it exercises its inspection duties. <p>Section 41. Very severe infractions are:</p> <ol style="list-style-type: none"> 1. To collect personal data in a fraudulent manner. 2. To not follow the established regulations regarding sensitive data processing. 3. To not suspend personal data processing when there is a previous requirement from the National Information Transparency and Access Authority to do so. 4. To intentionally store or transfer personal data violating what is set forth in this Law. 5. To repeat severe infractions. <p>Section 42. The sanctions imposed by the National Information Transparency and Access Authority to database controllers and other subjects to whom this law and regulations apply, will be adjusted depending on the severity of the infraction.</p> <p>Section 43. Infractions to this Law will be sanctioned as follows:</p> <ol style="list-style-type: none"> 1. Minor infraction, summons before the National Information Transparency and Access Authority for matters regarding registrations or faults. 2. Severe infractions, penalties according to its proportionality. 3. Very severe infractions: <ol style="list-style-type: none"> a. Closure of the records in the database, without prejudice to the corresponding fine. To carry out this action, the National Authority for Transparency and Access to Information must have the formal opinion of the Personal Data Protection Council, without prejudice to the remedies granted by the Law to the affected party. b. Temporary or permanent suspension and disqualification of the storage and/or processing of personal data activities, without prejudice to the corresponding fine.
Legal actions	Are there any legal actions for personal data protection? Who has the right to exercise/request them?	Yes	Whoever is affected by the violation of their personal data.

Matter	Concept	Yes / No / NA	Observations / comments
Personal data protection officer or controller.	Is there a Data Protection Officer (DPO) or similar position? If so, is their appointment mandatory? Must they be appointed locally?	Yes	Mandatory appointment.
Investigations	Can a competent authority officially act and/or investigate breaches of personal data protection?	Yes	Among the legal powers granted to the General Directorate of Data Protection is the authority to oversee and supervise the proper implementation of the law by data controllers and custodians of databases.
Processing Records	Are there any mandatory requirements for maintaining processing records under the applicable laws? Specifically, what information must be included in these records, and are there any particular conditions or circumstances under which data controllers or processors are obliged to keep detailed records of their data processing activities?	Yes	<p>The responsible parties and/or custodians of databases that transfer personal data stored in databases to third parties shall maintain a record of these transfers and must make it available to the National Authority for Transparency and Access to Information if requested to fulfill its powers under the Law.</p> <p>The record mentioned in the previous paragraph shall include, for each of these databases, the identification of the database and its responsible party, the nature of the personal data it contains, the legal basis for its existence, the procedures for obtaining and processing the data, the destination of the data and the natural or legal persons to whom it may be transferred, a description of the universe of persons involved, security measures, protocols, and a technical description of the database, the manner and conditions under which individuals can receive or access the data concerning them, the procedures for rectification and updating of the data, the retention period of the data, and any changes to the indicated elements, as well as the identification and period of all individuals who have accessed the personal data within fifteen business days from the start of such activity.</p>
Similarities with the GDPR	Per your understanding, do you believe that the regulation contemplates all the requirements set by similar international regulations (e.g., Example: GDPR)? What relevant differences did you find?	Yes	Indeed, Panamanian regulations largely incorporate the principles of the GDPR, recognizing the ARCO rights.
Other obligations	Are there other additional considerations/requirements or legal obligations on data protection that must be met?	No	Even though the figure of a compliance officer is not mandatory, the appointment will be considered as a criterion for the graduation of penalties.



Paraguay



Matter	Concept	Yes / No / NA	Observations / comments
Regulations	Does the country have a personal data protection law? If so, please name the applicable regulation.	Yes	<p>Personal data protection in Paraguay is regulated by several direct or transversal regulatory provisions. Law No. 6,534/2020 on "Personal Credit Data Protection" was enacted on October 27, 2020, derogating Law No. 1,682/2001 and its modifications and establishing a new personal information and data protection regime in Paraguay. This regulatory framework is supplemented mainly by other rules such as:</p> <p>Constitution of the Republic of Paraguay (1992). (Art. 135 "Habeas Data", Art. 28 "Right to Information", Section 33 "Intimacy Right", Section 35 "Rights to identification documents", Section 36 "Documental Estate and Private Information Inviolability", Section 45 "Of the Rights and Guarantees or statements").</p> <ul style="list-style-type: none"> ▶ Law No. 4,868/2013 on "Electronic Commerce", and its supplementary provisions. ▶ Law No. 6,822/2021 On Trust Services for Electronic Transactions, Electronic Document and Electronic Transmissible Documents, and its supplementary provisions. ▶ Law No. 861/1996 "General Law of Banks, Financial Entities, and other Credit entities". ▶ Law No. 5,830/2017 "That Prohibits the unauthorized advertisement of mobile telephone service owner users". ▶ Law No. 5,282/2014 "Of the free access to Public Information and Government Transparency by the citizens". ▶ Paraguayan Penal Code No. 1,160/1997 and its complementary provisions. ▶ Resolution No. 3/2023 of the Central Bank of Paraguay 'Regulation of Credit Information Bureaus (BIC from Spanish) and Protection of Personal Credit Information under Law No. 6,534/2020 on the Protection of Personal Credit Data.' This Resolution establishes the guidelines and obligations applicable to BICs and Credit Information Users, as well as mechanisms for the effective exercise of data subject rights. ▶ Resolution SDCU No. 1.502/2022 'Regulating Articles 6, 9, and 20 of Law No. 6,534/2020 on the Protection of Personal Credit Data.' <p>The object of Section 1, Law No. 6,534/20 is to ensure the credit data protection of every person, regardless of their nationality, residency, or domicile. It also regulates credit information data collection and access, as well as the incorporation, organization, operation, rights, obligations, and extinction of companies that engage in the collection and provision of credit information with the object of preserving the fundamental rights, intimacy, information self-determination, liberty, security, and fair treatment of persons, as established by the Constitution, its provisions, and international instruments on the matter that have been ratified.</p> <p>Law No. 6,534/20 further emphasizes the processing of data linked to the processing of personal credit data and credit information of every person by credit bureaus and credit information users. However, it also includes the definitions of personal data and sensitive personal data, highlighting the specific considerations required for their processing.</p> <p>The provisions contained in the Constitution of the Republic, along with the previously mentioned regulations, are part of the complementary sources related to personal data protection in the country. It is important to note that, according to Section 45 of the Constitution, the enumeration of rights and guarantees included in the Constitution shall not be understood as the denial of others' rights that, being inherent to the human personality, are not explicitly stated in it. The lack of a regulatory law cannot be invoked to deny or undermine any right or guarantee.</p>
Enforcement Authority	Who is the enforcement authority? If applicable, please provide their website link.	Yes	<p>In the framework of Law No. 6,534/20, the Central Bank of Paraguay (BCP from Spanish): https://www.bcp.gov.py/ and the Secretary of Defense of the User and Consumer (SEDECO from Spanish) Under the Ministry of Industry and Commerce (MIC): http://www.sedeco.gov.py/ are appointed as control organs and authorities to enforce its provisions.</p> <p>In turn, and as a complementary measure, within the framework of Law No. 4,868/13, Law No. 5,830/17, and Law No. 6,822/21, the MIC, through its respective departments, is designated as the enforcement authority.</p>
Scope of Application	Which is the regulation's scope of application? I.e., is it a strictly national or cross-border concept?	Yes	<p>Law No. 6,534/20 establishes that it is mandatory to enforce personal data processing in public or private registries collected or stored in the Paraguayan territory.</p>

Matter	Concept	Yes / No / NA	Observations / comments
Data collection	Which are the requirements or processes for personal data collection? (For example, data subject consent, information on purpose of data use and subject's rights, etc.)	Yes	<p>Law No. 6,534/20 warrants to every person the right to be expressly and clearly informed about the object to be given to its required data and thus be able to expressly state its consent to collect and use its data.</p> <p>Consent for personal data processing shall be given in a free, specific, unequivocal, and informed manner by means of a statement or a clear affirmative action. It shall be written, electronical, digital, or by any other reliable mechanism. In other words, consent must be given under conditions that do not admit any doubts about its granting.</p> <p>Likewise, the right to informative self-determination recognized in this law establishes that the data subject must know the use given to such data of the information and data about themselves contained in official or private public records or in entities that provide information on economic solvency and financial status or its object and demand its access, rectification, cancelation, and opposition (the exercise of the so called "ARCO Rights").</p>
Legal concept of "personal data"	What are personal data	Yes	<p>Law No. 6,534/20 defines personal data as the "Information of any kind, that refers to specific or identifiable companies or individuals". Identifiable is understood as the company or individual that may be identified through any identifier or by one or more characteristic elements of physical, physiological, genetic, psychic, economic, cultural, or social identity of said company or individual. Personal data protection rights and guarantees will be extended to companies when applicable.</p>
Personal data categories	Are there different personal data categories? Please explain each category, if applicable.	Yes	<p>In the framework of Law No. 6,534/20, the following data categories are established:</p> <ul style="list-style-type: none"> ▶ Personal Data: Information of any kind related to identified or identifiable natural or legal persons. A person is considered identifiable if they can be identified through an identifier or one or more characteristic elements of their physical, physiological, genetic, psychological, economic, cultural, or social identity. Data protection rights and guarantees will extend to legal persons insofar as they are applicable. ▶ Sensitive data: Data that refers to the private sphere of the subject or whose improper use may cause discrimination or severe risk for its subject. Personal data that may reveal aspects such as racial or ethnic origin; religious, philosophical, and moral beliefs or convictions; union membership; political opinions; data related to health, life, sexual preference or orientation, genetic or biometric data whose object is to unequivocally identify an individual is considered sensitive data. ▶ Personal Credit Data or credit information: Positive or negative information related to the credit history of individuals or companies about credit and commercial activities or activities of a similar nature to correctly and unequivocally identify the person, their domicile, commercial activity, determine their debt level, compliance of its obligations, and, in general, their credit risks in a specific moment.
Situation of the corporations and other legal entities.	Does the regulation sufficiently protect the personal data of the corporations or entities?	Yes	<p>Within the framework of Law No. 6,534/20 applies to data related to specific or identifiable artificial legal individuals or companies.</p>
Data subject consent	Is the data subject's consent required to collect the data? If so, are there conditions to obtaining the data subject's consent? (For example, prior information that must be provided to the data subject).	Yes, partially in what	<p>In the framework of Law No. 6,534/20, the subject must know the object to be given to their data to be able to grant or refrain their consent for its processing. The consent must be granted in a free, specific, unequivocal, and informed manner through a statement or a clear affirmative action. It may be expressly and freely revoked in the same conditions. This action does not generate a retroactive effect.</p> <p>Regarding the informed consent granted by the final consumer to a provider, SDCU Resolution No. 1,502/22 that regulates Articles 6, 9, and 20 of Law No. 6,534/20 on Personal Credit Data Protection, establishes that informed consent only authorizes the provider who obtained it directly. Therefore, other providers must obtain a new authorization or informed consent from the final consumer. In this sense, the Resolution indicates that the consent granted by a final consumer to a provider cannot be considered as implicitly authorizing third party providers that were not part of the first authorization or informed consent.</p> <p>On the other hand, and by way of example, Law 4,868/13 on Electronic Commerce and its regulatory standards require that Providers of Goods and Services must obtain the express consent of the consumer or user to collect their personal data. They must also provide a simple and free procedure to oppose the use of data for promotional purposes, implement express confirmation mechanisms, and disclose the purpose and processing of the consumer's or user's personal data, among other requirements.</p> <p>Furthermore, Law No. 6,822/21 stipulates that trusted service providers may only collect personal data directly from the person to whom the data pertains. Individuals must give express and informed consent for these purposes. The collection and processing of personal data are to be conducted only to the extent necessary for providing the trusted service. Personal data cannot be processed for any purpose other than that agreed upon without the express consent of the data subject.</p>

Matter	Concept	Yes / No / NA	Observations / comments
Exceptions to the consent	Are there exceptions to the voluntary consent of a data subject? If so, please list the exceptions.	Yes	<p>The consent will not be needed when the data is obtained from public access sources or when such data has to be revealed by a competent authority because of a judicial order or the data is collected to exercise duties that are specific to the State.</p> <p>Law No. 6,534/2020, expressly stipulates that third party credit information processing controllers or processors and whoever intervenes in any collection, processing, storage, use, or circulation stages have to keep the information as secret, except if a competent authority orders otherwise.</p>
Content and scope of the information to be validated by the data subject.	What should be the content of the consent? (For example, data use or destination, international data transfer, etc.)	Yes	See data collection answer.
Transfer of personal data	Are there requirements or restrictions on the transfer of personal data? Are there requirements that apply to the international transfer of data? (Example: model clauses, Supervisors' authorization, etc.)	Yes	<p>Law No. 6,534/20 establishes that personal data transfers will be possible provided that there is consent and a clear statement about the objects and uses to be given to such data. Consequently, it is prohibited to transfer personal data to other persons or companies against the rules established by the provisions in effect.</p> <p>The law establishes the prohibition to transfer personal data of any kind to countries or international or supranational organisms that do not provide the known guarantees, requirements, or exceptions established in the Law or that do not provide appropriate protection levels. These situations are infractions with respect to the laws and cause the application of sanctions by the competent authorities.</p> <p>Currently, there is no list of jurisdictions that do not comply the requirements stated above.</p> <p>References are not contemplated in the currently regulation, with respect to contract models to be used in international data transfers to countries that are not appropriate, both in the case of assignment of data as in the assumptions of the provision of services.</p> <p>As a better practice, it may be interesting to consider the guidance provided by the Ibero-American Network of Data Protection (RIPD), specifically, the Implementation Guide for Model Contract Clauses for the International Transfer of Personal Data. Paraguay is a member of the Network.</p>
BCR	Do they have binding corporate rules (BCR)?	No	No.
Sensitive data	What is understood by sensitive data? How is sensitive data processed, if applicable?	Yes	<p>Pursuant to Law No. 6,534/20, sensitive personal data is understood as those relating to the intimate sphere of the data subject, or whose improper use may lead to discrimination or pose a serious risk to them. These include data that reveal aspects such as:</p> <ul style="list-style-type: none"> ▶ Racial and ethnic origin. ▶ Political opinions. ▶ Religious, philosophical, or moral convictions. ▶ Union membership. ▶ Information about health or sex life. ▶ Genetic or biometric data with the intent to unequivocally identify an individual. <p>It is prohibited to advertise or broadcast sensitive personal data that is explicitly individualized or identifiable.</p>
Database registration or periodic reporting to the corresponding authority	Is it mandatory to register (e.g., with the corresponding enforcement body) a database and/or a database ownership, processing and/or use? Is it mandatory to submit any type of information or report periodically to the enforcement authority?	No	To this date, by law there is no Database Registration in Paraguay.

Matter	Concept	Yes / No / NA	Observations / comments
Data security	Are there technical measures to guarantee the security and confidentiality of personal data? If so, what are they?	Yes.	<p>The Law No. 6,534/20 establishes that the credit personal data controller must warrant the adoption and implementation of the technical, organizational, and security measures needed to safeguard the access and integrity of personal data to avoid its unauthorized alteration, loss, consult, merchandising, or access.</p> <p>Likewise, there is an express obligation for Credit Information Bureaus to process information with the highest ethical, confidentiality, and security standards. Personal data collection, storage, and transmission by third parties through unsafe mechanisms or by any means that do not warrant data security and unchangeability, as well as incomplete, late, or defective notice to the data protection authorities of information related to personal data security violations are infractions established by the Law No. 6,534/20.</p>
Rights of the data subjects	What are the data subjects' rights? (Example: correction, update, or deletion). Please list and explain.	Yes	<p>In the framework of Law No. 6,534/20, the data subject has the following rights:</p> <ul style="list-style-type: none"> ▶ Access right. ▶ Update and/or rectification right. ▶ Suppression right. ▶ Opposition right. ▶ Portability right. ▶ Right to be forgotten. <p>Additionally, we remit to complementary regulations, such as the Electronic Commerce Law, as well as the concept of Habeas Data and the Right to Information as provided in the Constitution, among others.</p>
Actions by the data subjects	How can they exercise them?	Yes	<p>According to Law No. 6,534/20, any data subject or their legal representative may at any time request the data controller to provide access to, update, rectify, delete, oppose, or enable the portability of their personal data. The data controller must implement straightforward, quick, accessible, and free procedures for the data subject to exercise these rights.</p> <p>If requests or claims are not resolved as stipulated by law and regulations, the data subject may appeal to the Consumer Financial Protection Office of the Superintendence of Banks or SEDECO (as applicable) and, ultimately, seek judicial protection from the competent magistrate.</p> <p>The constitutional guarantee of the Habeas Data guarantee, that ensures that every person has the right to judicially request the update, rectification, or destruction of personal data that is incorrect or that illegitimately affects its rights stored in official or private registries of a public nature (of public access, such as Credit Information Bureaus).</p> <p>The relief action is another legal tool established in the National Constitution [protecting Section 33 or Section 36 and]. This procedure is not specifically contemplated in the legal framework of reference but would be viable in accordance with Section 45 of the Constitution.</p> <p>It would also be potentially viable to file an unconstitutional action against any judicial resolution or legal rule that infringes the recognized principles and guarantees of every person.</p>
Assignment of personal data	What are the requirements for the assignment of personal data?	Yes	<p>In the framework of Law No. 6,534/20, personal data processing and assignment would be possible provided that the subject gives their consent and there is a reliable notice regarding the purpose of such data. The law defines the Data Processor as the individual or company, authority or other organism, that processes personal data on behalf of the Data Controller, the latter, is the individual or company, authority or organism, that on its own or with others determines data processing objects and means.</p>
Data processing	Can the services be provided through a third party (data processing)? If so, please explain the procedure and exceptions, if applicable.	Yes	<p>In the framework of Law No. 6,534/20, it is possible provided that consent is granted, and the data is not applied or used for a purpose different than the one stated in the contract. Please remit to the comments on Data Controller and Processor.</p>
Data retention	Is it mandatory to retain/conserve the data collected or processed for a specific term? If so, what is the term?	Yes	<p>Law No. 6,534/20, the right to be forgotten regulates the credit data. Data about an individual or company stored in a registry and that could affect to the data subject, may be kept up to five (5) years to be counted as of the date of occurrence of the registered facts, except by special regulatory provision that establishes another term or if the parties agree on a lesser term. If the information must be retained beyond the maximum period, the data subject's personal information must be disassociated from it.</p> <p>On the other hand, the Resolution 3/23 of the BCP, states that positive credit-related personal data must be retained and published for a minimum of 10 (ten) years.</p>

Matter	Concept	Yes / No / NA	Observations / comments
Data elimination	Is there an obligation to eliminate the data collected or processed? If so, under what conditions and for what term?	Yes.	<p>Data must be eliminated when it has expired, in accordance with Articles 9 and 19 of Law No. 6,534/20 of credit-related personal data protection and in accordance with Resolution 3/23 regulated by the law in question regarding the right to be forgotten. Likewise, when they are no longer necessary or relevant for the purposes for which they were collected.</p> <p>The fact of unjustifiably refusing to delete or rectify Personal Data or Credit Information of a person who has so requested by a clear and unequivocal means constitutes an infraction in light of the regulations in force, and both BCP and SEDECO are entitled to implement sanctions.</p> <p>We reiterate that, in the framework of guarantees recognized by the Constitution, every person may request by means of Habeas Data or Legal Protection, the destruction of its data when its rights have been illegally affected.</p>
Privacy impact assessment	Are privacy impact assessments mandatory?	No	<p>It is not established in the law.</p>
Incidents	Is it mandatory to report security incidents or breaches or the related legal provisions?	Yes	<p>In the framework of law No. 6,534/20, the credit personal data processing controller must warrant the adoption and implementation of the technical, organizational, and security measures needed to safeguard the access and integrity of personal data to avoid its unauthorized alteration, loss, consult, merchandising, or access. Incomplete, delayed, or defective notification to the data protection authority regarding information related to a personal data security breach constitutes an infraction.</p>
Sanctions	Are there sanctions for failures to comply with this obligation? If so, please list them along with the corresponding sanction or penalty amounts.	Yes	<p>In the framework of Law No. 6,534/20, both the BCP and SEDECO may impose the following sanctions to those who violate the Law. The sanctions range from warnings, fines, suspensions, and temporary closings to disqualifications.</p> <ol style="list-style-type: none"> 1. Fine of up to 15,000 minimum wages (approximately USD 204,000), that is doubled in the event of a recurrence (30,000 minimum wages, equivalent to approximately USD 408,000); and may reach 50,000 minimum wages (approximately USD 680,000) when an individual or company has annual invoicing above Gs. 6,000,000,000 (approximately USD 760,000). 2. Suspension of data processing related activities for up to six months, stating the corrective measures to be applied. 3. Disqualification to perform a job, position, or commission within the financial and credit system and in Credit Information Bureaus for six months to five years. 4. Temporary closing of data processing related operations once the suspension term has elapsed and the corrective measures ordered by the control authority have not been adopted. 5. Immediate and final closing of Sensitive Data processing operations. <p>The administrative sanctions that may be adjusted by the competent enforcement authority depending on the severity and are independent from the corrective or precautionary measures issued by said authorities to safeguard the public interest protected by Law No. 6,534/20. The sanctions may be challenged by administrative legal procedures.</p> <p>To date, there are several administrative resolutions from SEDECO through which fines, sanctions, and corrective measures have been imposed on companies that have violated provisions of the Credit Personal Data Protection Law.</p> <p>On the other hand, and as a complementary measure, other regulatory provisions, such as the e-commerce law, establish fines for violations related to the misuse or improper handling of personal data in contravention of the law.</p>
Legal actions	Are there any legal actions for personal data protection? Who has the right to exercise/request them?	Yes	<p>The action for the exercise of the rights recognized in the area of personal data protection may be exercised by the data subject or through their representative. In the case of a deceased person, their heirs or legatees may exercise the corresponding rights.</p>
Personal data protection officer or controller.	¿Existe la figura del delegado de protección de datos (DPO) o similar? En dicho caso, ¿su designación es obligatoria?, ¿debe ser designado localmente?	No	<p>The applicable regulations do not establish explicitly the concept of a data protection official delegate.</p> <p>However, the provisions related to the processing of credit-related personal data and the requirements imposed on BICs and Credit Information Users are a clear example of a trend toward the eventual establishment of a data protection area and/or the outsourcing of advisory services in this context, which demands an appropriate level of expertise in the subject matter commensurate with the complexity of data processing.</p> <p>Please remit to comments regarding "Other obligations".</p>
Investigations	Can a competent authority officially act and/or investigate breaches of personal data protection?	Yes	<p>The enforcement authorities have broad powers under the Law and their complementary provisions and must coordinate efforts to ensure compliance with the law.</p>

Matter	Concept	Yes / No / NA	Observations / comments
Processing Records	Are there any mandatory requirements for maintaining processing records under the applicable laws? Specifically, what information must be included in these records, and are there any particular conditions or circumstances under which data controllers or processors are obliged to keep detailed records of their data processing activities?	No	Paraguayan regulations do not explicitly provide for this.
Similarities with the GDPR	Per your understanding, do you believe that the regulation contemplates all the requirements set by similar international regulations (e.g., Example: GDPR)? What relevant differences did you find?	No	Paraguayan regulations do not include all the requirements established by international regulations. In May 2021, a bill called "Law for the Protection of Personal Data in Paraguay" was presented and is currently being studied by the Paraguayan Congress, the provisions of which provide for the comprehensive regulation of the processing of personal data. To date, several sessions have been held in Congress to study the bill in question, the last one in October 2024.
Other obligations	Are there other additional considerations/requirements or legal obligations on data protection that must be met?	Yes	<p>BCP Resolution 3/23 provides that BICs are required to:</p> <ul style="list-style-type: none"> ▸ Establish Departments of Attention to the holders of the information that have the necessary internal means and procedures to provide efficient and timely attention to requests for updating, rectification, opposition, deletion and portability of personal credit data, all this, within the legal deadlines. ▸ Determine the appropriate communication and coordination mechanisms with the sources and users from whom the information is collected. ▸ Submit for approval by the Superintendence of Banks (SIB) of BCP, the Performance Protocol that establishes Codes of Conduct of professional practice, parameters for the treatment of personal credit data that tend to ensure and improve the operating conditions of information systems, policies of good practices of Corporate Governance. ▸ Regarding information security, implement the provisions of the Information Technology Governance and Control Manual (Resolution SB SG. No. 00124/2017). ▸ Obligations to report to the SIB. ▸ Among others. <p>Likewise, Credit Information Users are obliged to:</p> <ul style="list-style-type: none"> ▸ Process the queries and claims formulated in the terms indicated in Res. 3/2023. ▸ Adopt an internal manual of policies and procedures to ensure proper compliance with Law No. 6,534/20 and its regulations. ▸ To have the express consent of the holders in order to process their data, even in those cases in which their data had already been processed before the Resolution came into force. ▸ Inform the holder of the personal data about the consultation to be made on their credit information. ▸ Among others. <p>It is expressly prohibited for users of credit information to use or provide credit data to third parties for employment decisions, hiring, promotion, transfer, or dismissal of personnel. Furthermore, the use of credit information to deny or restrict access to prepaid medical care, as well as to deny or restrict access to emergency medical attention for any individual, is also explicitly prohibited.</p> <p>As additional information and as previously indicated, within the framework of regulation on Electronic Commerce, the Regulatory Decree No. 1,165/14 of the Electronic Commerce Law, provides that: The supplier of goods and services by electronic means at a distance, must make the consumer or user aware of the purpose and the treatment that will be given to their personal data, in accordance with the Law in force regarding the matter.</p> <p>Likewise, it must communicate the recipient of the data provided and the person responsible for the custody or storage of the information provided. The supplier of goods and services will use secure systems to prevent the loss, alteration and access by unauthorized third parties to the data provided by the consumer or user.</p> <p>In July 2022, the BCP issued Resolution BCP 10/2022 "Regulations for the Use of Cloud Computing Services", which establishes the minimum guidelines and obligations to be met by supervised entities that choose to outsource their processes and activities of cloud computing services. It provides that the entities must comply with the legislation and regulations in force regarding the protection of personal and credit data in the processes of cloud computing services, in order to ensure adequate protection of the personal data of its customers.</p>



Peru



Matter	Concept	Yes / No / NA	Observations / comments
Regulation	Does the country have a personal data protection law? If so, please name the applicable regulation	Yes	<p>The personal data protection regime includes the following regulations:</p> <ul style="list-style-type: none"> ▶ Political Constitution of Peru (1993), Article 2 N°6. ▶ Law 29,733 - known as Personal Data Protection Law ("PDPL"). ▶ Supreme Decree No. 003-2013-JUS, that regulates PDPL. ("Supreme Decree").* * Supreme Decree 016-2024-JUS, which approves the New Regulation of the Peruvian Personal Data Protection Act, was published on November 30, 2024 and will come into effect on April 1, 2025. ▶ Directorial Resolution 019-2013-JUS/DGPDP, Security Directive for Information Managed by Personal Data Banks. ▶ Directorial Resolution 080-2019-JUS/DGTAIPD, Duty to Inform Guide. ▶ Directive 01-2020-JUS/DGTAIPD, about Personal Data Processing through Video Surveillance Systems approved by Board Resolution 02-2020-JUS/DGTAIPD. ▶ Emergency Decree 007-2020, Digital Trust Framework Law ▶ Ministerial Resolution 326-2020-JUS, Methodology to Calculate Fines in Personal Data Protection Matters. ▶ Directorial Resolution 074-2022-JUS/DGTAIPD approving the Model Contractual Clauses for the International Transfer of Personal Data.
Enforcement authority	Who is the enforcement authority? If applicable, please provide their website link	Yes	<p>Personal Data Protection National Authority, body ascribed to the Ministry of Justice and Human Rights.</p> <p>Web portal: https://www.gob.pe/anpd</p>
Scope of application	What is the regulation's scope of application? Is it a strictly national or cross-border concept?	Yes	<p>The scope of application is territorial (Section 3 of the PDPL), in other words, refers to personal data processing in the national territory. However, there are cross-border clauses in Section 5 of the Supreme Decree. For example, when the data controller is not located in Peru but (i) the Peruvian regulations are applicable by contractual provisions or due to international laws, or (ii) when it uses means or support that are located in Peru.</p>
Data collection	Which are the mandatory legal requirements or processes for personal data collection? (for example, data subject consent, information on purpose of data use and subject's rights, etc.)	Yes	<p>Personal data processing requires the consent of its subject.</p> <p>Personal data must be collected for a specific, explicit, and legal purpose. As stated in Section 33 paragraph 5 of the PDPL, personal data may only be processed with the consent of its subject, except when the law provides otherwise. As established in Section 12 of the Supreme Decree, the consent must be free, previous, informed, express, and unequivocal.</p> <p>Likewise, as established in Section 14 of the Supreme Decree, in the case of sensitive data (for example, data related to health or economic income) the consent must also be in writing (this includes digital means with some authentication mechanisms).</p>
Legal concept of "personal data"	What is understood by personal data?	Yes	<p>The PDPL in its Section 2, defines personal data as all the information about an individual that identifies them or makes them identifiable by means that may be reasonably used.</p> <p>In turn, Section 2 paragraph 4 of the Supreme Decree, defines personal data as numeric, alphabetic, graphic, photographic, acoustic information about personal habits or of any other kind regarding individuals that identifies them or makes them identifiable by means that may be reasonably used.</p>
"Personal data" categories	Are there different personal data categories? Please explain each category, if applicable.	Yes	<p>In addition to the general concept of personal data, the PDPL and the Supreme Decree recognize two specific types of personal data:</p> <ul style="list-style-type: none"> ▶ Sensitive data: biometric data that by itself may identify the subject; data that refers to racial or ethnic origin; economic income; political, religious, philosophical, or moral opinions or convictions; union membership; and information related to health or sex life. (PDPL Section 2 paragraph 5). ▶ Health related personal data: Is information about past, present, or predicted physical or mental health, including its degree of disability and its genetic information. (Supreme Decree Section 2 paragraph 5).
Situation of the corporations and other legal entities	Does the regulation sufficiently protect the personal data of the corporations or entities?	No	<p>The PDPL does not include companies or their representatives (who act on behalf of such legal entities).</p>

Matter	Concept	Yes / No / NA	Observations / comments
Data subject consent	Is the data subject's consent required to collect the data? If so, are there conditions to obtaining the data subject's consent? (For example, prior information that must be provided to the data subject.)	Yes	Consent must be given in a free, previous, express, unequivocal and informed manner as set forth in Section 18 of the PDPL and Section 12 of the Supreme Decree. As stated in Section 14 of the Supreme Decree, in the case of sensitive data (for example, data related to health or economic income) the consent must also be in writing.
Exceptions to the consent	Are there exceptions to the voluntary consent of a data subject? If so, please list the exceptions.	Yes	<p>The consent to process personal data is not required from its owner in the events established in Section 14 of the PDPL. For example:</p> <ol style="list-style-type: none"> 1. When the personal data processing is executed by public entities when performing their duties. 2. When the personal data is needed to prepare, hold, and execute a contractual relation in which the personal data subject is a party. 3. When said information is included in sources accessible to the public (public records, newspapers, webpages, etc.).
Content and scope of the information to be validated by the data subject	What should be the content of the consent? (For example, data use or destination, international data transfer, etc.)	Yes	<p>As established in Section 18 of the PDPL, the personal data subject has the right to be informed in a detailed, simple, express, unequivocal manner and before such data has been collected, mainly regarding:</p> <ol style="list-style-type: none"> (i) The purpose for which its personal data will be processed. (ii) The recipients of such data (national or international transfer). (iii) The existence of personal data banks. (iv) The identity and domicile of its subject, and if such is the case, the name of the personal data processor. (v) The term during which its information will be kept. (vi) The possibility to exercise their rights.
Transfer of personal data	Are there requirements or restrictions on the transfer of personal data? Are there requirements that apply to the international transfer of data? (Example: model clauses, control authority's authorization, etc.)	Yes	<p>For personal data cross-border flow, the owner and personal data processor may perform the personal data cross-border flow only if the recipient country has proper protection levels as required by the PDPL.</p> <p>In the event that the recipient country does not have proper protection levels, the issuer of the personal data cross-border flow must ensure that the personal data processing is performed as established in the law.</p> <p>Likewise, as established in Section 25 of the Supreme Decree, to formalize cross-border flows (international transfer of personal data) contractual clauses or other legal instruments may be used to establish the obligations of both parties (issuing country and recipient country).</p> <p>On this point, precisely by Directorial Resolution 074-2022-JUS/DGTAIPD, the Model Contractual Clauses for the International Transfer of Personal Data were approved, the text of which is part of the Implementation Guide for Model Contractual Clauses for the International Transfer of Personal Data of the Iberoamerican Data Protection Network.</p>
BCR	Do they have binding corporate rules (BCR)?	No	Notwithstanding this, the Supreme Decree in its Section 21 establishes, through the concept named "code of conduct", an assumption voluntary (not mandatory) in the event of personal data transfers within company groups, affiliated or linked subsidiary companies under the common control of the same group as the personal data bank owner or controller.
Sensitive data	What is understood by sensitive data? How is sensitive data processed, if applicable?	Yes	Sensitive data is defined in numeral 5 of Section 2 of the PDPL and in numeral 6 of Section 2 of the Supreme Decree. Sensitive data is defined as data that refers to biometric information, racial and ethnical origin, economic income, religious, philosophical, or moral opinions or convictions, union membership, health and sex life. Consent must be granted in writing, by using its written signature, digital signature, or any other authentication mechanism that ensures the unequivocal will of the owner as set forth in Section 14 of the Supreme Decree.
Database registration or periodic reporting to the control authority	Is it mandatory to register (e.g. with the corresponding enforcement body) a database and/or a database ownership, processing, and/or use? Is it mandatory to submit any type of information or report periodically to the enforcement authority?	Yes	<p>The National Personal Data Protection Registry is an administrative registry managed by the National Personal Data Protection Authority whose object is to record cross-border communications of personal data banks in a separate manner and nationally, and also register the respective sanctions. Not recording personal data banks in the National Personal Data Protection Registry constitutes a minor infraction as established in literal e), numeral 1 of Section 132 of the Supreme Decree.</p> <p>The registration of a personal data bank must be updated at all times. Any modification that affects the content of the registration must be previously communicated to the National Personal Data Protection Registry Office, through the corresponding approved formats.</p>

Matter	Concept	Yes / No / NA	Observations / comments
Data security	Are there technical measures to guarantee the security and confidentiality of personal data? If so, what are they?	Yes	<p>The information systems that manage personal data banks must include for its operation what is established in Section 39 of the Supreme Decree:</p> <ol style="list-style-type: none"> 1. Personal data information access control. 2. Generate and keep records that evidence interactions with logical data and once said data is not useful anymore, keep evidence of its destruction, transfer, storage, among others. <p>Likewise, the Information Security Directive Managed by Personal Data Banks, approved by Directorial Resolution 019-2013-JUS/DGPDP, is a facilitating and guiding document that contains details of the conditions, requirements and technical measures that must be considered to comply with the PDPL and the Supreme Decree.</p> <p>On the other hand, according to Section 42 of the Supreme Decree, non-automated documents (files or folders) must be located in areas where access is protected with access doors whose opening system requires a key or similar device. Said areas must remain closed when access to the documents included in the personal data banks is not needed.</p>
Rights of the data subjects	What are the data subjects' rights? (Example: correction, update or deletion). Please list and explain.	Yes	<p>The data owner has the following rights, established in Sections 18 to 25 of the PDPL:</p> <ul style="list-style-type: none"> ▶ Right to information ▶ Right of access. ▶ Right to update, include, rectify, and suppress information. ▶ Right to hinder its provision. ▶ Right of opposition. ▶ Objective processing right. ▶ Protection right. ▶ Right to be compensated. <p>Chapter II (special provisions) of the Supreme Decree regulates the procedure to exercise the "right to information" (Section 60) and the so called "ARCO rights":</p> <ul style="list-style-type: none"> ▶ Access right (Section 61). ▶ Rectification right (Section 65). ▶ Cancellation right (Section 67). ▶ Opposition right (Section 71).
Actions by the data subjects	How can they exercise them?	Yes	<p>The procedure to exercise data subject rights is established in Sections 47 to 75 of the Supreme Decree.</p> <p>Section 50 of the Supreme Decree establishes that to exercise any of the aforesaid rights a request must be filed with the following information:</p> <ol style="list-style-type: none"> 1. Names and last names of the personal data subject. 2. Specific request, clear description of the personal data linked to the exercise of the right, and express statement of the right intended to be exercised. 3. Documents that support the request. 4. Address to receive corresponding communications. 5. Date and signature. If the right is exercised by means of a representative, its representation must be accredited. <p>Section 55 of the Supreme Decree establishes specific response terms. For example, for right of information requests the term is eight (8) days and for rectification, cancellation, and opposition right requests the term is ten (10) working days. The response term for access right requests is twenty (20) working days. These terms may be extended one time for an equal period, provided there are justifying circumstances.</p>

Matter	Concept	Yes / No / NA	Observations / comments
Assignment of personal data	What are the requirements for the assignment of personal data?	Yes	<p>When personal data is transferred to another entity, the recipients are required to handle such personal data as provided for in the PDPL and the Supreme Decree.</p> <p>For example, the third paragraph of Section 18 of the PDPL establishes that if a transfer of personal data is made after the consent because of a merger, portfolio acquisition, or similar situations, the new data bank owner must establish an efficient information mechanism for the personal data subject.</p>
Data processing	Can the services be provided through a third party (data processing)? If so, please explain the procedure and exceptions, if applicable.	Yes	<p>Section 30 of the PDPL, establishes that when personal data processing services are provided on behalf of third parties, these services cannot be applied or used for an object different than the one indicated in the signed contract or agreement and cannot be transferred to other persons, even for its safekeep.</p> <p>Section 36 of the Supreme Decree states that the personal data bank processor is prohibited from transferring to third parties' personal data object of the processing services provision, unless the personal data bank owner that requested such processing has authorized it and the personal data subject has provided its consent. The term to store personal data will be two (2) years to be counted as of the conclusion of the last requested data processing.</p> <p>As stated in Section 37 of the Supreme Decree, personal data processing may be performed by a third party different than the data processor by means of an agreement or contract signed between them (subcontracting).</p>
Data retention	Is it mandatory to retain/conserve the data collected or processed for a specific term? If so, what is the term?	No	<p>Although the PDPL and the Supreme Decree do not set a specific term to withhold/keep personal data, numeral 6.13 of Directive 01-2020-JUS/DGTAIPD about Personal Data Processing by means of Video Surveillance Systems provides that personal data (images) obtained from video surveillance cameras must be stored for a minimum period of 30 working days and a maximum period of 60 working days, except for sectorial regulations that establish otherwise. In the case of educational institutions, the maximum period to preserve images captured by video surveillance systems is 30 business days.</p>
Data elimination	Is there an obligation to eliminate the data collected or processed? If so, under what conditions and for what term?	Yes	<p>The only regulated assumption on the obligation to eliminate personal data (images) is in numeral 6.15 of Directive 01-2020-JUS/DGTAIPD about Personal Data Processing by means of Video Surveillance Systems.</p> <p>This numeral establishes that, once the period to keep the information has elapsed and there is no requirement from any competent authority to deliver or visualize the recorded content, the files with the personal data must be eliminated within a maximum term of two (2) working days.</p> <p>This maximum term will not be applicable when there is a purpose or legitimate interest that justifies its conservation (numeral 6.16 of the aforementioned Directive). For example, when the personal data (image) has been considered as evidence in a police investigation or administrative and/or judicial proceeding.</p>
Privacy Impact Assessment	Are Privacy Impact Assessments required and/or mandatory?	No	<p>It is not established in the PDPL or the Supreme Decree.</p>
Incidents	Is it mandatory to report security incidents or breaches or the related legal provisions?	Yes	<p>Item e) of numeral 9.1 of the Digital Trust Framework Law establishes that digital service providers are required to report and collaborate with the National Personal Data Protection Authority when a DIGITAL security incident involving personal data is verified.</p> <p>Although PDPL and the Supreme Decree do not impose any obligation over data controllers or personal data owners to report security incidents before the National Personal Data Protection Authority, they do recommend as a good practice that said incidents be reported to the interested parties as soon as the incident has been confirmed.</p>
Sanctions	Are there sanctions for failures to comply with this obligation? If so, please list them along with the corresponding sanction or penalty amounts.	Yes	<p>In general terms, Section 38 of the PDPL classifies minor, severe, and very severe infractions that are classified in Section 132 of the Supreme Decree.</p> <p>Section 39 of the PDPL establishes that:</p> <ul style="list-style-type: none"> ▶ Minor infractions are sanctioned from 0,5 UITs (Tax Units) to 5 UITs. ▶ Severe infractions are sanctioned from more than 5 UITs to 50 UITs. ▶ Very severe infractions from more than 50 UITs to 100 UITs. <p>For the year 2024, the UIT is S/ 5,150 equivalent to approximately UDS 1,392.</p> <p>Infraction classification and descriptions are indicated in Section 132 of the Supreme Decree.</p>

Matter	Concept	Yes / No / NA	Observations / comments
Legal actions	Are there any legal actions for personal data protection? Who has the right to exercise/request them?	Yes	Section 24 of the PDPL establishes that in the event of a refusal from the personal data subject to exercise its rights, said subject may appear before the National Personal Data Protection Authority by means of a claim (administrative scope) or before the Judicial Power to file the corresponding habeas data action (legal scope).
Personal data protection officer or controller.	Is there a Data Protection Officer (DPO) or similar position? If so, is their appointment mandatory? Must they be appointed locally?	No	There is no requirement to appoint a data protection officer (DPO). However, the Safety Directive issued by the National Personal Data Protection Authority establishes, as a specific provision of security measures, that the personal data bank owner must appoint a personal data bank security controller (who has the capacities and authority needed to develop its duties). When there is no such appointment, it is understood that the role of the personal data bank security controller corresponds to the personal data bank owner (that is to say, to the highest ranking or representative body of the entity).
Investigations	Can a competent authority officially act and/or investigate breaches of personal data protection?	Yes	Auditing and sanctioning procedures are initiated by the National Personal Data Protection Authority or by a claim from such authority before the presumptive perpetration of acts against the provisions of the PDPL or the Supreme Decree. The investigating organ is the Auditing and Instruction Administration. The organ that initiates the sanctioning procedure is the Personal Data Protection Administration (first administrative instance). Against resolutions issued by the latter, an appeal may be filed and resolved by the General Transparency, Public Information Access, and Personal Data Protection Administration (second administrative instance).
Processing Records	Are there any mandatory requirements for maintaining processing records under the applicable laws? Specifically, what information must be included in these records, and are there any particular conditions or circumstances under which data controllers or processors are obliged to keep detailed records of their data processing activities?	No	Currently, there are no mandatory requirements in the applicable Peruvian laws that require data controllers (responsible for processing) and/or data processors (in charge of processing) to maintain detailed records of their data processing activities in general. Nevertheless, as a best practice, it is advisable for data controllers or processors to keep processing records to demonstrate the traceability (as a security measure) of personal data in the event of any potential oversight or information request from the National Authority for Data Protection.
Similarities with the GDPR	Per your understanding, do you believe that the regulation contemplates all of the requirements set by similar international regulations (e.g., the GDPR)? What relevant differences did you find?	No	There are some matters that the Peruvian regulations do not regulate. For example, different than the GDPR, it does not establish rights to processing limits and to data portability. It does not refer either to regulations in the matter of "cookies". Also, it does not regulate the concept of shared responsibility of personal data processing (this concept is given in assumptions of collaborative agreements or participation associations). Finally, the Peruvian framework does not establish a minimum or maximum term to keep personal data and, before the occurrence of a personal data incident, does not obligate the data controller or personal data bank owner to report said incident before the National Personal Data Protection Authority. On the other hand, it is worth mentioning that Peruvian law, in contrast to the GDPR, does regulate the obligation for data controllers to register and keep their personal data banks updated before the National Authority for the Protection of Personal Data.
Other obligations	Are there other additional considerations/requirements or legal obligations on data protection that must be met?	Yes	Section 13 of the Supreme Decree establishes the obligation to publish the Privacy Policy (adjusted to the Peruvian regulations) to be understood as a form of information duty compliance. This obligation is included in the webpages for personal data collected online (Section 18 of the PDPL).



Uruguay



Matter	Concept	Yes / No / NA	Observations / comments
Regulations	Does the country have a personal data protection law? If so, please name the applicable regulation.	Yes	<p>In Uruguay there is extensive regulation on data protection matters. The following is the most relevant:</p> <ul style="list-style-type: none"> ▶ Law No. 18,331 "Personal data protection and Habeas Data action" ("Law 18,331"). ▶ Regulatory Decree No. 414/009 ("Dec. 414/900"). ▶ Law No. 19,670 - Sections 37 to 40 ("Law 19,670"). ▶ Law No. 19,030 ("Law 19,030"). ▶ Regulatory Decree No. 64/020 ("Dec. 64/020"). ▶ Regulatory Decree No. 664/008 ("Dec. 664/008"). ▶ Regulatory Decree No. 242/017 ("Dec. 242/017"). ▶ RPDCU Resolution No. 1,647/010. ▶ RPDCU Resolution No. 23/021. ▶ RPDCU Resolution No. 41/021. ▶ RPDCU Resolution No. 58/021. ▶ RPDCU Resolution No. 63/023. ▶ RPDCU Resolution No. 70/023.
Enforcement Authority	Who is the enforcement authority? If applicable, please provide their website link	Yes	<p>The enforcement authority, named Regulatory and Personal Data Control Unit ("RPDCU"), managed by the Executive Director of the Agency for the Electronic Management Government Development and the Information and Knowledge Office ("AGESIC" from Spanish) and by two members appointed by the Executive Power.</p> <p>The RPDCU is a decentralized body of the AGESIC.</p> <p>Link: https://www.gub.uy/unidad-reguladora-control-datos-personales/</p>
Scope of Application	Which is the regulation's scope of application? I.e., is it a strictly national or cross-border concept?	Yes	<p>The scope of application of the regulations is territorial. However, Section 3 of the Regulatory Decree No. 414/009 makes a special distinction on data processing practiced as follows:</p> <ol style="list-style-type: none"> 1. Data processing by a database controller or processing established in the Uruguayan territory, being Uruguay the place where its activity is performed, whichever its form of business organization. 2. The database or processing controller is not established in the Uruguayan territory but uses for data processing means located within the country. In this case it is equally covered by the Uruguayan regulations. <p>Exceptions to these regulations are cases where the cited means are exclusively used for transit purposes, provided that the database or processing controller appoints a representative with domicile and permanent residence in the national territory.</p> <p>Section 3, Dec. 414/009: As of the effective date of Law 19,670, are the regulations that will also govern beyond the borders of the country when the controller or processor is not established in the Uruguayan territory if the following situations exist:</p> <ol style="list-style-type: none"> 1. In the event that data processing activities are related to the offer of goods and services for inhabitants of Uruguay or 2. In the event that the data processing activities are related to behavior analysis of the inhabitants of the Republic. 3. If provided for public international law regulations or in a contract. 4. If means located in the country are used for data processing; means such as communication and information networks, data centers and, in general, information technology infrastructure. <p>Therefore, Law 18,331 extends its scope of application beyond the territory of Uruguay.</p> <p>Section 37, Law 19,670 and Section 1 and 2, Dec. 64/020.</p>

Matter	Concept	Yes / No / NA	Observations / comments
Data collection	Which are the mandatory requirements or processes for personal data collection? (For example, data subject consent, information on purpose of data use and subject's rights, etc)	Yes	<p>The update of database controllers must adjust to certain general principles, among them, the veracity of data. This principle establishes a series of requirements to collect data:</p> <ol style="list-style-type: none"> 1. Data collection cannot be performed by unfair, fraudulent, abusive or extorsive means or in a manner that goes against the provisions of this law. 2. Data must be exact and updated if needed. 3. When it has been verified that data is inaccurate or false, the processing controller as soon as it knows of such circumstances must suppress, replace, or complete such data with exact, true, and updated data. <p>Likewise, data that has expired in accordance with the provisions of this law shall be deleted.</p> <p>Regarding consent, personal data processing is legal when the owner has granted its free, previous, express, and informed consent. This consent must be documented. The Law establishes certain cases where previous consent is not needed.</p> <p>On the other hand, the law also establishes the right of information regarding data collection stating that when personal data is collected its owners must be previously informed in an express, exact, and unequivocal manner of the object for which the collected data will be processed.</p> <p>Section 7, 9 and 13, Law 18,331.</p>
Legal concept of "personal data"	What are personal data?	Yes	<p>Personal data is understood as information of any kind that refers to specific or identifiable individuals or companies.</p> <p>Section 4 para. D), Law 18,331.</p>
Personal data categories	Are there different personal data categories? Please explain each category, if applicable.	Yes	<p>As set forth in Section 4, para. D) and E) and Section 18 of Law 18,331, the regulations on the matter make a distinction between personal data and sensitive data.</p> <p>The law also makes a distinction between:</p> <ul style="list-style-type: none"> ► Health-related data. ► Telecommunication related data. ► Database related data used for advertising. ► Commercial activity or credit related data. ► Internationally transferred data. <p>All this data is considered "especially protected data" by the Law.</p> <p>Sections 4 para. D) and E), 18, 19, 20, 21, 22, and 23 Law 18,331.</p>
Situation of the corporations and other legal entities	Does the regulation sufficiently protect the personal data of the corporations or entities?	Yes	<p>To the extent applicable, the personal data protection right will also be applied to companies.</p> <p>Section 2, Law 18,331.</p>
Data subject consent	Is the data subject's consent required to collect the data? If so, are there conditions to obtaining the data owner's consent? (For example, prior information that must be provided to the data subject.)	Yes	<p>Data processing is legal when the subject has granted its free, previous, express, and informed consent and such consent must be documented.</p> <p>The granted consent must be express and clear.</p> <p>Likewise, when collecting personal data, certain information must be provided to the owner as set forth in Section 13 of Law 18,331.</p> <p>Sections 9 and 13, Law 18,331.</p>
Exceptions to the consent	Are there exceptions to the voluntary consent of a data subject? If so, please list the exceptions.	Yes	<p>Previous consent will not be needed when any of the assumptions listed in Section 9 of Law 18,331 exist. In its turn, Section 17 of the same Law refers to assumptions where the consent of the owner is not needed to inform about collected data.</p>

Matter	Concept	Yes / No / NA	Observations / comments
Exceptions to the consent	Are there exceptions to the voluntary consent of a data subject? If so, please list the exceptions.	Yes	Previous consent will not be needed when any of the assumptions listed in Section 9 of Law 18,331 exist. In its turn, Section 17 of the same Law refers to assumptions where the consent of the owner is not needed to inform about collected data.
Content and scope of the information to be validated by the data subject	What should be the content of the consent? (For example, data use or destination, international data transfer, etc.)	Yes	<p>The owner that grants consent for data collection and processing shall be informed in an unequivocal manner of the object to be given to such data and the type of activity developed by the database controller to whom consent was granted. Otherwise, the consent will be void.</p> <p>Likewise, one of the assumptions that allows the international transfer of data is the unequivocal consent of the interested party for such a transfer to be performed, as established in Section 23, literal A of Law 18,331. Section 5, Dec. 414/009.</p>
Transfer of personal data	Are there requirements or restrictions on the transfer of personal data? Are there requirements that apply to the international transfer of data? (Example: model clauses, control authority's authorization, etc.)	Yes	<p>Regulations issued on the matter of international transfer of data. As a matter of principle, such transfer is prohibited to countries and international organisms that do not provide proper protection levels as per the standards of International or Regional Laws on the matter. However, this prohibition will not apply when the assumptions listed in Section 23 of Law 18,331 (numerals 1 to 5 and literals A to F) exist.</p> <p>It is important to keep in mind that Resolution No. 6/023 of the RPDCU modifies Resolution No. 23/021 and 4/019 of the RPDCU and establishes that all countries that, to the opinion of the Unit, have proper protection regulations and means to ensure its effective application are deemed appropriate for the international transfer of data. Particularly appropriate countries are the members of the European Union and of the European Economic Area, Principality of Andorra, Republic of Argentina, the private sector of Canada, Guernsey, Isle of Man, Faroe Islands, State of Israel, Japan, Jersey, New Zealand, United Kingdom of Great Britain and Northern Ireland, and the Swiss Confederation, the Republic of Korea, and to transfers to organizations included in the "Data Privacy Framework" published by the U.S. Department of Commerce.</p> <p>Regarding the Data Privacy Framework, it emerged in response to the invalidation of the "Privacy Shield" by the Court of Justice of the European Union. Previously, resolution No. 23/021 of the RPDCU it eliminated the organizations included in the "Privacy Shield" framework of the United States of America of adequate countries for the international transfer of data. By virtue of this resolution, the international transfer of data to the United States of America must be justified by the consent of the interests' parties or by any of the exceptions set forth in Section 23 of Law No. 18,331.</p> <p>By virtue of this resolution, the international transfer of data to the United States of America must be justified by the consent of the interested parties or by any of the exceptions set forth in Section 23 of Law No. 18,331.</p> <p>In response to the invalidation of the "Privacy Shield," the U.S. Department of Commerce prepared the "Data Privacy Framework" which was approved by the European Commission on July 10, 2023. Thus, as previously mentioned, Resolution URCDP No. 63/023 allowed for international data transfers to organizations included in the new "Data Privacy Framework" published by the U.S. Department of Commerce and approved by the European Commission on July 10, 2023.</p> <p>Subsequently, Resolution URCDP No. 70/023 stated that data controllers and processors seeking to carry out international transfers to these organizations must submit an explicit declaration to the URCDP prior to the registration of the database or transfer. This declaration must indicate that the importing organization has extended the application of the safeguards of the Data Privacy Framework to the data transferred from Uruguay. If such a declaration is not made, transfers to the mentioned organizations may proceed based on contractual clauses presented by the controllers or processors that have been previously authorized by the URCDP, or other legally established grounds.</p> <p>Through the RPDCU Resolution No. 41/021 recommended the implementation of a series of clauses regarding international transfers of personal data to unsuitable territories. The purpose of these clauses is to clearly establish the responsibilities of the parties involved in order to effectively safeguard the data protection of the parties involved.</p> <p>Finally, Resolution URCDP No. 70/2023 added certain additional requirements that the data controller or processor must communicate to the data subjects in cases of international data transfers:</p> <ol style="list-style-type: none"> 1. The destination of their data. 2. The role of the importer. 3. The term of the transfer. 4. The legal basis for the transfer. 5. The processing operations performed by the importer.

Matter	Concept	Yes / No / NA	Observations / comments
BCR	Do they have binding corporate rules (BCR)?	Yes	The Uruguayan regulations in Section 36 defines it as "Code of conduct". Section 35 and 36, Law 18,331.
Sensitive data	What is understood by sensitive data? How is sensitive data processed, if applicable?	Yes	Sensitive data is personal data that reveals racial and ethnical origin, political preferences, religious, or moral convictions, union membership, and information regarding health or sex life. This is indicated in Section 4, para. E) and 18 of Law 18,331. Public, state, or non-state entities, entities that are fully or partially private and owned by the state, private entities that process sensitive data as its main business, and entities that process large volumes of data must appoint a data protection delegate. The duties of said delegate will be counselling, supervision, and control, among others. Section 4 para. E) and Section 18, Law 18,331. Section 40, Law 19,670.
Database registration or periodic reporting to the control authority	Is it mandatory to register (e.g. with the corresponding enforcement body) a database and/or a database ownership, processing and/or use? Is it mandatory to submit any type of information or report periodically to the enforcement authority?	Yes	It is mandatory to register all public and private data before the RPD CU Registry. It is required that such registration abides by the provisions of Section 29 of Law 18,331 and with the updating obligation set forth in Section 20 of Dec. 414/009. Likewise, Resolution No. 1,647/010 of October 15, 2010, regulates the content and form of presentation of database updates stating that quarterly updates of registered Database information must only be filed if any of the following conditions apply: 1. That there is a quantitative alteration of 20% of the data indicated in the registration request, or 2. That there are structural modifications in the registered database such as the adding or elimination of a field, changes in the object, or any other modification that significantly alters the information initially declared in the registration request. Section 29, Law 18,331; Arts. 15 and 20, Regulatory Decree No. 414/009; Regulatory Decree No. 664/008 and Resolution No. 1,647/010.
Data security	Are there technical measures to guarantee the security and confidentiality of personal data? If so, what are they?	Yes	The Law regulates the principle of data security by means of which the database controller or user must adopt the measures needed to ensure the security and confidentiality of personal data. The object of such measures is to avoid its unauthorized tampering, loss, consult, or access, and to detect information deviations that are intentional or unintentional whether risks arise from human actions or from the technical means used. In the matter of security measures, Section 3 of Dec. No. 64/2020 establishes that the data controllers and processors must adopt the technical and organizational measures needed to safeguard the integrity, confidentiality, and availability of information to ensure the security of personal data. Section 10, Law 18,331 and Section 3, Dec. 64/020.
Rights of the data subjects	What are the data subjects' rights? (Example: correction, update or deletion). Please list and explain.	Yes	The regulations on the matter of personal data establish the following rights for data subjects: ▶ Right of information regarding data collection. ▶ Right of access. ▶ Rectification, update, inclusion, and suppression right. ▶ Right to challenge personal assessments. ▶ Rights that refer to the communication of data. These rights are established in Sections 13 -17 of Law No. 18,331 and in Sections 9-14 of Dec. 414/009.
Actions by the data subjects	How can they exercise them?	Yes	These rights may be exercised as set forth in Sections 13-17 of Law 18,331.
Data retention	Is it mandatory to retain/conserve the data collected or processed for a specific term? If so, what is the term?	No	Although the law does not establish said data withholding or conservation, the Regulatory Dec. No. 414/009 in its Section 37 establishes a Procedure for the authorization to keep data for historical, statistical, or scientific purposes. Data must be eliminated when it is no longer needed or pertinent for the purposes for which it was collected. Section 8, Law 18,331 and Section 39, Dec. 414/009.
Data elimination	Is there an obligation to eliminate the data collected or processed? If so, under what conditions and for what term?	Yes	Data must be eliminated when it is no longer needed or pertinent for the purposes for which it was collected. Section 8, Law 18,331, and Section 39, Dec. 414/009.

Matter	Concept	Yes / No / NA	Observations / comments
Privacy Impact Assessment	Are Privacy Impact Assessments required and/or mandatory?	Yes	When exercising a proactive responsibility, certain technical and organizational measures must be adopted including an impact assessment of the protection of data to ensure a proper processing of personal data and show its effective implementation. The impact assessments must be executed following the standards established in Sections 6 and 7 of Dec. 64/020. Section 12, Law 18,331. Section 6 and 7, Dec. No. 64/020.
Incidents	Is it mandatory to report security incidents or breaches or the related legal provisions?	Yes	Dec. No. 64/020 includes a Chapter on security vulnerabilities. Sections 3 and 4 of this Decree, details everything related to security vulnerabilities. On the other hand, Law 19,670 establishes that when the database controller or processor learns that the database security has been breached, it will immediately report it to the data subject and to RPDCU and will also inform any measures adopted. The RPDCU will coordinate the steps to be followed with the National Response Center for Computer Security Incidents of Uruguay (CERTuy). In addition, Article 80 of Law 20,212 established the National Cybersecurity Incident Registry. Public entities and private entities linked to critical services or sectors in the country must report cybersecurity incidents to AGESIC within 24 hours of becoming aware of them and provide the necessary information for effective registration as soon as possible. Furthermore, Article 83 of Law 20,212 created the Cybersecurity National Strategy Management Committee, composed of various state agencies, with the primary task of supporting and collaborating with AGESIC in implementing and monitoring the national cybersecurity strategy. Sections 3 and 4, Dec. 64/020. Section 38, Law 19,670. Article 80 and Article 82 of Law No. 20,212.
Sanctions	Are there sanctions for failures to comply with this obligation? If so, please list them along with the corresponding sanction or penalty amounts.	Yes	Law No. 18,331 in its Section 35 establishes sanctions for the personal data controllers or processors and other subjects to which the legal regime applies when the regulations or modifications of this law have been violated. These sanctions are established by the severity, repetition, or recurrence of the committed infraction. Furthermore, Section 39 of Law No. 19,670 replaces the old Section 12 of Law No. 18,331 on Personal Data Protection. The new section imposes modifications to the "principle of responsibility" establishing that both the database controller and the processor are responsible for the violation of the provisions of the law. The regulations also stipulate that data controllers and processors must implement appropriate technical and organizational measures (such as privacy by design, privacy by default, and data protection impact assessments) to ensure the security of personal data. Article 35 of Law No. 18,331 and Article 39 of Law No. 19,670.
Legal actions	Are there any legal actions for personal data protection? Who has the right to exercise/request them?	Yes	The Habeas Data action by means of which every person has the right to file a judicial action to know about its personal data and its object and use, of data recorded in public or private databases and, in the event of error, falsehood, processing prohibition, discrimination, or outdated data, to demand its corresponding rectification, inclusion, suppression. Sections 37 - 40, Law 18,331.
Personal data protection officer or responsible party.	Is there a Data Protection Officer (DPO) or similar position? If so, is their appointment mandatory? Must they be appointed locally?	Yes	Public, state, or non-state entities, partially or wholly private entities owned by the state, and private entities that process sensitive data as a main business and entities that process large volumes of data (for example, more than 35,000 individuals) must appoint a data protection delegate. The duties of the data protection delegate are indicated in Section 40 of Law 19,670. Section 10 - 15, Dec. 64/020.
Investigations	Can a competent authority officially act and/or investigate breaches of personal data protection?	Yes	The RPDCU, in the course of its duties or at the request of any interested party, has the power to act in matters related to the protection of personal data. Section 9-Bis, 34, 45, Law 18,331.

Matter	Concept	Yes / No / NA	Observations / comments
Processing Records	Are there any mandatory requirements for maintaining processing records under the applicable laws? Specifically, what information must be included in these records, and are there any particular conditions or circumstances under which data controllers or processors are obliged to keep detailed records of their data processing activities?		<p>The regulations do not specifically mandate the documentation of the processing activities carried out by the data controller or processor. However, Article 5 of Decree 64/020 states that data controllers and processors must document the accountability measures they implement, periodically review these measures, and evaluate their effectiveness. This process should consider the state of the art, the cost of implementation, and the nature, scope, context, and purposes of the processing, as well as the diverse probability and severity risks involved for individuals' rights.</p> <p>The Article 5 of said Decree determines that, depending on the nature of the data, the processing being carried out and the risks involved, appropriate technical and organizational measures must be implemented, such as the privacy impact assessment, privacy by design and privacy by default, without prejudice to others that may be implemented, in order to guarantee adequate processing of personal data and demonstrate its effective implementation.</p> <p>These measures must be documented, including at least the form, means, and purpose of the processing, the procedures aimed to comply with regulations, the planned mechanisms to respond to security breaches, and the role of the data protection officer when applicable.</p> <p>This documentation must be available upon request from the Regulatory and Control Unit for Personal Data.</p>
Similarities with the GDPR	Per your understanding, do you believe that the regulation contemplates all of the requirements set by similar international regulations (e.g., the GDPR)? What relevant differences did you find?	Yes	<p>As evidence, in 2013 Uruguay approved Convention No. 108 of the European Council with the enactment of Law No. 19,030, and Uruguay was declared by the European Union as a country with an adequate level of protection in personal data protection matters, as per Directive 95/46/CE.</p> <p>As of the recent reforms in the Uruguayan laws regarding personal data (Law 19,670 and Dec. 64/020), it is possible to say that an alignment of the local regulations with the GDPR standards has been made.</p>
Other obligations	Are there other additional considerations/requirements or legal obligations on data protection that must be met?	Yes	<p>With Dec. 242/017, Uruguay regulated the electronic exchange and processing of personal data by public and private institutions with competences in health matters, and by the National Clinical History Electronic System.</p> <p>Section 181 of Law 19,996 created the "Do not call" Registry with the purpose of protecting holders or users of telecommunications services from abuses of the contact procedure, advertising, offer, sale and gift of goods or services not requested through them.</p> <p>Decree No. 132/022 regulated the procedure for the registration and deregistration of users in said base, as well as the conditions for contacting consumers.</p> <p>For such purposes, it is established as an obligation of the companies to consult the registry prior to the contact, the conservation of the proof of the consultation for a term of 4 years, and the making of calls from a visible number or indicating the call center company making the contact, the brand name and the commercial reason for the contact. This requirement is exempted in cases where there is a consent or a contractual relationship in force with the user, provided that the contact refers to the object of such relationship. Regarding these calls considered as "permitted", it is provided that the free, express and informed consent of the registered user must be obtained, being documented and preserved by the entity carrying out the campaign.</p>

EY LAW | LATAM

Contactos

Argentina	Brasil	Chile	Colombia
Jorge Garnier <i>Partner</i> jorge.garnier@ar.ey.com	Ligia Augusto <i>Partner</i> ligia.augusto@br.ey.com	Pedro Lluch <i>Partner</i> pedro.lluch@cl.ey.com	Camila González <i>Partner</i> camila.gonzalez@co.ey.com
Pablo Bisogno <i>Associate Partner</i> pablo.bisogno@ar.ey.com	Gustavo Poggio <i>Associate Partner</i> gustavo.poggio@br.ey.com	Felipe Fernández <i>Associate Partner</i> felipe.fernandez@cl.ey.com	Ana María Castellanos <i>Manager</i> ana.m.castellanos.vargas@co.ey.com
Laila Yu <i>Manager</i> laila.yu@ar.ey.com	Sandra Avella <i>Manager</i> sandra.avella@br.ey.com		
Mercedes García <i>Staff</i> mercedes.garcia.gomez@ar.ey.com			
Costa Rica	Ecuador	México	Panamá
Fernando Vargas Winiker <i>Partner</i> fernando.vargas.winiker@cr.ey.com	Fernanda Checa <i>Partner</i> fernanda.checa@ec.ey.com	Carina Barrera <i>LATAM Law Leader</i> carina.barrera@mx.ey.com	Ana Clement <i>Senior Manager</i> ana.clement@pa.ey.com
Walter Contreras <i>Senior Manager</i> walter.contreras@cr.ey.com	Gina Ruiz <i>Manager</i> gina.ruiz@ec.ey.com	Bárbara Fernandez <i>Associate Partner</i> barbara.fernandez@mx.ey.com	Víctor Del Busto <i>Senior</i> victor.del.busto@pa.ey.com
	Daniela Orozco <i>Supervisor</i> daniela.orozco@ec.ey.com	Alejandro Guevara <i>Manager</i> alejandro.guevara@mx.ey.com	Diego Varela <i>Staff</i> diego.varela@pa.ey.com
Paraguay	Perú	República Dominicana	Uruguay
Gustavo Colman <i>Partner</i> gustavo.colman@py.ey.com	María del Pilar Sabogal <i>Partner</i> maria.sabogal@pe.ey.com	Julio Muñoz <i>Senior Manager</i> julio.munoz.rodriguez@ey.com	María Inés Eibe <i>Associate Partner</i> ines.eibe@uy.ey.com
Nabila Larroza <i>Manager</i> nabila.larroza@py.ey.com	Bruno Mejía <i>Senior Manager</i> bruno.mejia@pe.ey.com	José Miguel <i>Senior</i> jose.miguel@do.ey.com	Germán Gómez <i>Manager</i> german.gomez.bonaglia@uy.ey.com
		Mariam Labour <i>Staff</i> mariam.labour@do.ey.com	

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws.

For more information about our organization, please visit ey.com.

© 2024 EYGM Limited.
All Rights Reserved.

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content. This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com