Jurisdiction	*Uruguay*
Date	*June, 2022.*
Law Firm	*Guyer & Regules*
Name and Position of the person in charge	*Florencia Castagnola, Partner*
Contact Information	*fcastagnola@guyer.com.uy*

* We are planning to put the information on our website so that the viewers can reach out to you, directly, and if you don't mind, we will include the above contact information in the report. You may have more than one contact person.

Questionnaire

I. Law concerning protection of personal information

i. Does your country have a general law concerning the protection of personal information in the **private sector** at the present or in the near future?

Yes.

Law No. 18.331("Ley de Protección de Datos Personales y Acción de Habeas Data") which entered in force on August 18, 2008, and its regulatory Decree No. 414/009, dated August 31, 2009, established in Uruguay a general legal framework with the purpose of assuring the fundamental right to protection of personal data and intimacy/privacy.

Furthermore, new provisions have recently been incorporated by Budget Law No. 19.670 (articles 37 to 40) dated October 25, 2019 and its regulatory Decree No. 64/020 dated February 21, 2020.

ii. Does your country have a general law concerning protection of personal information in the **public sector** at the present or in the near future?

Yes.

According to Article 3 of the Law No. 18.331, the regime applies to personal data recorded on any medium that makes it susceptible to processing, and to any form of subsequent use of such data by the public or private sector.

iii. Does your country have laws concerning protection of personal information **which apply in individual (specific) sectors** at the present or in the near future? (If yes, please describe outline.)

No, no specific sectorial rules.

Where all of the answers to the question of I.(i), (ii) and (iii) is "no", please skip to IV.

II. The basic information of the regulation concerning protection of personal information.

i. Please fill in the blanks below about <u>all</u> the law concerning personal information mentioned at I..(please add a reply column as necessary,)

The title of the law： *Personal Data Protection and Habeas Data Act ("Ley de Protección de Datos Personales y Acción de Habeas Data")*

① The definition of "Personal Information"	*According to Article 4 of Law No. 18.331, personal data is information of any kind relating to specific or determinable natural or legal persons.*
② The scope in which the law applies	*As mentioned above, the law is applicable to personal data recorded on any medium that makes them susceptible to processing, and to any form of subsequent use of such data by the public or private spheres. Notwithstanding the fact that article 3 of said law establishes that the same shall not apply to databases maintained by natural persons in the exercise of exclusively personal or domestic activities; to those whose purpose is public security, defense, State security and its activities in criminal matters, investigation and repression of crime; and to those databases created and regulated by special laws.*
③ The territorial scope	*Law 18.331 is generally applicable to anyone doing business in Uruguay. Decree No. 64/020 has clarified this somehow broad territorial scope:* *"it shall be understood that the controller or processor is established in Uruguayan territory when it carries out a stable activity therein, regardless of the legal form adopted for such purpose.* *In the event that the controller or processor is not established in Uruguayan territory, Law No. 18.331 of August 11, 2008 and this regulation shall also apply if:* *a) The data processing activities are related to the offer of goods or services directed to inhabitants of the Republic which will be appreciated through elements such as the use of the language, the reference to payment in national currency or the provision of related services -not necessarily rendered by the responsible or processor- in Uruguayan territory.* *b) The data processing activities are related to the analysis of the behavior of the inhabitants of the Republic, including those aimed at profiling, being applicable to this effect in particular the provisions of Article 16 of Law No. 18.331 of August 11, 2008.* *c) As provided for by rules of public international law or a contract. In no case may*

	the contracting parties exclude the application of national law, when applicable. *d) The processing uses means located in the country, such as information and communication networks, data centers and computer infrastructure in general."*
④ URL (please provide the URL officially posted by the government, English page is preferred, if available)	*https://www.impo.com.uy/bases/leyes/18331-2008* *(English not available, the official language of the republic is Spanish)*
⑤ The **effective** date *	*18/08/2008, with further amendments effective 01/1/2020*

* If the law has been amended, please fill in the effective date of the amended law.

ii. If there are any special instructions about the laws, please describe them.

-NA

III. OECD Privacy Principles

i. If there are any provision of law which embody each OECD Privacy Principle in your country, please describe the outlines.

https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Article 5 of Law No. 18.331 provides for 7 guiding principles:

1) *Legality: All databases shall be properly registered and shall observe the principles provided for by applicable regulations.*
2) *Veracity: Personal data collected must be truthful, adequate, fair and not excessive regarding the purpose for which it has been obtained. Personal data collection may not be made by unfair, fraudulent, abusive, extortive means or in a manner contrary to applicable regulations.*

   Personal data must be accurate and updated, if necessary.
3) *Purpose: Personal data may not be used for other purposes than those that motivated its collection. Personal data must be removed when it is no longer necessary or relevant to the purposes for which it was collected.*
4) *Prior and Informed Consent: The treatment and processing of personal data must be preceded by the person's (""data subject") free, prior, express and informed consent, which must be documented. There are some exceptions to this principle.*

5) *Security of Data: All the steps necessary to guarantee the security and confidentiality of personal data shall be taken.*
6) *Confidentiality: Persons who legitimately obtained information from a database shall be obliged to use it in a reserved manner, and exclusively for their regular course of business.*
7) *Proactive responsibility: The data controller or the data processor shall assume a proactive role in view of the nature of the data, the processing carried out and the risks involved.*

We outline below how these principles may correspond to the 8 OECD guiding principles.

(a) Collection Limitation Principle

This principle means that there should be limits on the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Article 9 of Law No. 18.331 provides that the processing of personal data is unlawful unless the owner has given his free, prior, express and informed consent. Such consent, together with other statements, must be expressly and prominently displayed.

(b) Data Quality Principle

This principle means that personal data should be relevant to the purposes for which they are to be used, and, to the minimum extent necessary for such purposes, should be accurate, complete and kept up-to-date.

Article 8 of Law No. 18.331 establishes the principle of purpose, which implies that the data being processed may not be used for purposes other than or incompatible with those for which they were collected. Furthermore, the data must be deleted when they are no longer necessary or relevant to the purposes for which they were collected.

In addition, article 7 stipulates the principle of truthfulness, according to which personal data stored for processing must be truthful, adequate, fair and not excessive in relation to the purpose for which they were collected.

(c) Purpose Specification Principle

This principle means that the purposes for which personal data are collected should be specified not later than at the time of the data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

This principle is reflected in Articles 8 and 9 of Law No. 18.331, which were mentioned above.

(d) Use Limitation Principle

This principle means that personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with I Purpose Specification Principle, except:

i) with the consent of the data subject; or

ii) authorized by law.

Article 9 of Law No. 18.331 refers to this principle, and establishes the following exceptions where prior consent is not required:

A) The data comes from public sources of information, such as records or publications in mass media.

B) The data is collected for the exercise of the functions of the State authorities or by virtue of an obligation of the State.

C) In the case of lists whose data is limited in the case of natural persons to names and surnames, first and last names and surnames, identity document, nationality, address and date of birth. In the case of legal persons, company name, fantasy name, sole taxpayers' registry, address, telephone number and identity of the persons in charge of the same.

D) They derive from a contractual, scientific or professional relationship of the owner of the data, and are necessary for its development or fulfillment.

E) It is carried out by individuals for their exclusive personal, individual or domestic use.

(e) Security Safeguards Principle

This principle means that personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access,

destruction, use, modification or disclosure of data.

Article 10 of Law No. 18.331 includes this principle, which establishes that the person responsible for or user of the database must adopt the necessary measures to guarantee the security and confidentiality of personal data.

(f) Openness Principle

This principle means that there should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and address of the data controller.

Article 12 of the Personal Data Protection Law No. 18.331, stipulates the principle of responsibility, according to which the person responsible for the database or processing and the person in charge, as the case may be, are responsible for the violation of the dispositions of the aforementioned law. In order to actively comply with such responsibility, they must adopt appropriate technical and organizational measures.

(g) Individual Participation Principle

This principle means that an individual should have the right:

i) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller holds data relating to him;

ii) to have communicated to him, data relating to him within a reasonable time;

at a charge, if any, that is not excessive;

in a reasonable manner; and

in a form that is readily intelligible to him;

iii) to be given reasons if a request made under subparagraphs (i) and (ii) is denied, and to be able to challenge such denial; and

iv) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Article 14 of Law No. 18.331 provides that any holder of personal data shall have the right to obtain any information about himself/herself contained in

public or private databases, provided that he/she previously proves his/her identification. The information must be provided within five working days of being requested, and must be provided in a clear form, free of codifications and, if necessary, accompanied by an explanation.
In the same way, Article 15 regulates the right of rectification, inclusion or suppression, providing that any individual or legal entity shall have the right to request the rectification, updating, inclusion or suppression of the personal data included in a database, when an error or falsehood or exclusion in the information of which he/she is the owner is detected.

(h) Accountability Principle

This principle means that a data controller should be accountable for complying with measures which give effect to the principles stated above.

As previously stated, Article 12 of Law No. 18.331 establishes the principle of liability. This principle states that the data controller of the database or processing and the person in charge, as the case may be, will be responsible for the violation of the provisions of the law. In exercising a proactive responsibility, they must adopt the appropriate technical and organizational measures: privacy by design, privacy by default, data protection impact assessment, among others, in order to ensure proper processing of personal data and demonstrate its effective implementation.
Moreover, we have the Regulatory and Control Unit of Personal Data, created by Article 31 of this law. The powers of such Unit are regulated in Article 34.

ii. If there are any sectors in which any laws exclude the application of each OECD Privacy Principle, please describe the outline.

(a) Collection Limitation Principle

(b) Data Quality Principle

(c) Purpose Specification Principle

(d) Use Limitation Principle

(e) Security Safeguards Principle

(f) Openness Principle

(g) Individual Participation Principle

(h) Accountability Principle

In the Uruguayan legal system, there are no sectors excluded from the application of the aforementioned principles, since the 7 principles set forth in Article 5 are of general application and are expressly intended to inform the interpretation of the rest of the law.
Nevertheless, some exceptions to the general rules may be provided for in certain situations:
For example, Article 22 of the law refers to data relating to commercial or credit activity, and expressly authorizes the processing of data intended to provide information on creditworthiness or credit solvency.
Another example is the article 23, paragraph D, which provides that the international transfer of data shall be authorized exceptionally when it is necessary or legally required for the safeguard of an important public interest, or for the recognition, exercise or defense of a right in a judicial proceeding. proceedings.

IV. Data Localization and Government Access

In your country, are there any systems having an impact on the rights of data subjects such as **comprehensive government access (e.g., limitation on the authorities' access to personal data for investigation purposes, and the safeguard is the attorney-client privilege)** to personal data or **Data Localization (e.g., rules requiring domestic installation and storage of servers and data)**? If yes, please describe them.

The generally applicable principle is that of confidentiality, regulated in article 11 of the law, and which states that "Those natural or legal persons who legitimately obtain information from a database that provides them with data processing, are obliged to use it in a reserved manner and exclusively for the usual operations of their line of business or activity, any dissemination of the same to third parties is forbidden.
The persons who, due to their work situation or any other form of relationship with the person in charge of a database responsible for a database, have access or intervene in

any phase of the processing of personal data, are obliged to keep them in strict to maintain strict professional secrecy with regard to such data (article 302 of the Code), when they have been collected from sources that are not accessible to the public. The above shall not apply in cases of orders of the competent court, in accordance with the rules in force in this matter or if there is consent of the owner.
This obligation shall subsist even after the termination of the relationship with the database manager."

Pursuant to Article 26 of Law No. 18.331, there are exceptions to the rights of access, rectification and cancellation of personal data. In this sense, those responsible for databases containing personal data may deny access, rectification or cancellation based on the dangers that may arise for the defense of the State or public safety, the protection of the rights and freedoms of third parties or the needs of the investigations being carried out.
Likewise, the persons in charge of the public finance databases may deny the exercise of the rights of the interested parties when the same hinders the administrative actions aimed at ensuring compliance with the obligations.
However, the owner of the data who is totally or partially denied the exercise of the rights referred to in the exercise of the rights mentioned above may bring it to the attention of the Control Organ, which shall ascertain whether or not the appropriateness or inappropriateness of the refusal.

V. The Data Protection Authority

If there is the data protection authority, please write down the name and address of the authority

Name: *The Personal Data Regulatory and Control Unit (Unidad Reguladora y de Control de Datos Personales) (the "URCDP").*
Address: *Liniers 1342 4th floor.*
Telephone: *2901 0065 ext. 3*
Website: *https://www.gub.uy/unidad-reguladora-control-datos-personales/*
Other information if any: *The URCDP is a decentralized agency from the Agency for the Development of the Electronic Management Government and the Information Society of Knowledge (Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información del Conocimiento) (the "AGESIC"), an entity which is in charge of advising governmental entities in connection with issues related to IT.*