PrivacyRules Special Report:

Changes in the Uruguayan personal data protection legal framework

Expert name: Jonathan Clovin
Title: Associate
Contact details
Guyer & Regules,
Plaza Independencia 811 – 11100 Montevideo – Uruguay
Email: clovin@guyer.com.uy
Phone number: (598) 2902 1515 ext.275

Expert name: María Sofía Anza
Title: Associate
Contact details
Guyer & Regules,
Plaza Independencia 811 – 11100 Montevideo – Uruguay
Email: sanza@guyer.com.uy
Phone number: (598) 2902 1515 int.271

Expert presentation

Jonathan, works in the Banking and Corporate Department. His practice includes advising financial institutions on banking transactions in general, capital markets, mergers and acquisitions. He specializes in antitrust and data protection laws.

Jonathan regularly advises clients on issues of data protection law including the registration of databases, the designation of Data Protection Officers, as well as ensuring effective data protection contractual clauses and company policies.

Expert presentation

María Sofía Anza, lawyer, works mainly in the Banking and Corporate Department since 2009.

Her practice includes advising financial institutions in banking transactions in general and those relating to project finance, capital markets, mergers and acquisitions and those related to commercial and corporate law. She also assists clients in data protection matters.

SPECIAL REPORT: CHANGES IN THE URUGUAYAN PERSONAL DATA PROTECTION LEGAL FRAMEWORK

*A: On February 21, 2020, Decree No. 64/020 (hereinafter the "**Decree**") was published in the Official Gazette, which regulates Articles 37 to 40 of Budgetary Law No. 19.670 (hereinafter the "**LRC**") regarding the protection of personal data.*

The Decree regulates the following points:

- *The territorial scope of the Personal Data Protection Law No. 18,331 (hereinafter, the "**LPDP**")*
- *The security measures and notification mechanism in case of personal data breaches;*
- *The measures of proactive responsibility to be assumed by the persons responsible and in charge of the processing;*
- *The functions and requirements for the appointment of personal data protection officers with respect to certain entities; and*
- *Applicable sanctions.*

We provide more details on the most relevant aspects of the Decree below:

A) Territorial scope of the LPDP

According to the LRC, the processing of personal data is covered by the LPDP when it is carried out by a person in charge (controller) or in charge of processing (processor) established in the Uruguayan territory where it carries out its activity. The Decree now clarifies that a data controller or processor will be understood to be established in Uruguayan territory when they carry out a stable activity in the country regardless of the legal form adopted.

In case the controller or processor is not established in the Uruguayan territory, as provided in the LRC, the LPDP is also applicable in the following cases:

(i) If the data processing is related to the supply of goods or services to inhabitants of Uruguay. For the purposes of determining the above, the Decree

establishes that elements such as the language used, the currency used and the provision of related services in Uruguay will be taken into account;

(ii) *Whether the data processing is related to the analysis of the behavior of the inhabitants of Uruguay, including the elaboration of profiles;*

(iii) *If it is provided for by the rules of public international law or a contract. The Decree clarifies that in no circumstances may the contracting parties exclude the application of national law where it should have been applicable under Uruguayan international private law rules; and*

(iv) *If the processing uses means located in the country. The Decree cites the following as examples: information and communication networks, data centers and computer infrastructure in general.*

*In these cases, data controllers or data processors must comply with the obligations set forth in the LPDP and its amendments, including the obligation to register their personal databases and provide their contact information to the Personal Data Regulation and Control Unit (hereinafter, the "**URCDP**"). The processing of data in which means located in the country are only used for transitory purposes and the data controller appoints a representative domiciled in Uruguay before the URCDP are exempt from the obligation to register their databases.*

B) Security Breaches

Security measures

The controller or processor must take technical and organizational measures to maintain the integrity, confidentiality and availability of the information in order to ensure the security of personal data at all times (in this sense the Decree implements the notion of Privacy by Design). The Decree provides that the adoption of national and international standards on information security will be assessed, such as the adoption of the Cybersecurity Framework developed by AGESIC (with principles including data minimisation, pseudonymisation, consent, etc.). Below is a link to this framework:

https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/guia-evaluacion-impacto-proteccion-datos

Security Incidents - (also known as "Data Breach")
In the event of a security incident, understood in the broadest sense, which results in, among other things, the accidental or unlawful disclosure, destruction, loss or alteration of personal data or the unauthorized communication of or access to such data, the persons responsible for and in charge of the processing must comply with the following:

(i) Data controllers or processors must implement procedures to minimize the impact of incidents within the first 24 hours;

(ii) Controllers must report the breach to the URCDP within 72 hours. To this end, processors who become aware of the occurrence of a breach must immediately inform the controllers concerned. The communication must contain relevant information such as the true or estimated date of the breach, its nature, the personal data affected and the possible impacts generated. There is currently no standard form for this communication.

(i) The persons responsible must communicate the data breach to the data subjects who have suffered a significant impact on their rights. The Decree clarifies that the communication to the data subjects only proceeds in case their rights are significantly infringed. This is a welcome precision since under the LRC the duty to communicate data breaches to the holders was not limited.

(ii) Once the data breach has been resolved, the controller must prepare a report detailing the breach and the measures taken, and the URCDP must be notified.

C) Proactive Responsibility

The principle of proactive responsibility is regulated by providing that 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 in the measures provided for by the Law. To this end, all necessary measures must be taken, must be documented, reviewed periodically and evaluated in terms of their effectiveness. The aforementioned documentation must be made available to the URCDP.

Prior to the start of the processing of the data, or with respect to the processing of data already under execution within a period

of 1 year as from the publication of the Decree, i.e. before 21 February 2021, the data controller and the data processor must carry out a personal data protection impact assessment, when:

(i) sensitive data are used as a core business;

(ii) specially protected data referred to in Chapter IV of the LPDP (e.g. health data, advertising, etc.) or data linked to the commission of criminal, civil or administrative offences are permanently or usually processed;

(iii) involve the evaluation of personal aspects of data subjects for the purpose of creating personal profiles, in particular by analyzing or predicting aspects relating to their performance at work, financial situation, health, personal preferences or interests, reliability of behavior and financial solvency, and location;

(iv) processing of data relating to groups of persons in a situation of vulnerability, in particular minors or persons with disabilities;

(v) processing of large volumes of data. With respect to the concept of large volumes of data, we point out that according to the Decree, this is understood to mean the processing of data of more than 35,000 people;

(vi) international transfers are made to countries that do not have an adequate level of protection; and

(vii) when determined by the URCDP.

In the event that the outcome of the assessment results in a potential and significant risk to the rights of the data subjects, the data controller or data processor must inform the URCDP.

In line with the above, we point out that recently the URCDP together with the Argentinean Agency of Access to Public Information published the Guide for Data Protection Impact Assessment. Below is a link to this Guide:
https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/guia-evaluacion-impacto-proteccion-datos

D) Personal Data Protection Officer

The LRC had established that: (i) public, state or non-state entities and private entities wholly or partly owned by the state; (ii) private entities that process sensitive data as their main business; and (iii) private entities that process large volumes of personal data must appoint a personal data protection officer. The Decree clarifies that large volumes of data are defined as data processing of more than 35,000 people. The Decree also establishes that in certain cases the URCDP, on its own initiative or at the request of a party, may determine the need to appoint a Personal Data Protection Officer in specific cases.

The Personal Data Protection Officer will be the link between the entity and the URCDP, and will mainly have to advise on the formulation, design and application of the data protection policies, supervising compliance with the regulations and proposing the necessary measures to adapt to the regulations and standards on the matter.

The Personal Data Protection Officer must be knowledgeable in law and be specialized in the field of personal data protection, which must be evidenced. They will be able to carry out their function through any type of contractual arrangement, whether they are employees or not.

The entities obliged to designate a Personal Data Protection Officer must communicate it to the URCDP within 90 days of the start of the processing of personal data. The remaining entities will have a period of 90 days from the entry into force of the Decree to communicate the appointment of Personal Data Protection Officer to the URCDP. Any termination or resignation of a Personal Data Protection Officer must be communicated within the same timeframe.

The Decree provides for the possibility of appointing a single Personal Data Protection Officer for a group of entities with similar tasks or activities.

E) Applicable Sanctions

It is clarified that in case of non-compliance with the provisions of the Decree, the sanctions established in the LPDP will be applied.
