Data. Protection. Adding Value.

Data Protection Laws - Uruguay

Legislation

The Personal Data Protection Law ("PDPL") has been enacted by the Government and published in the Official Gazette on August 18, 2008 – Law Number 18.331, regulated by Decree Number 414/009. PDPL was modified by the Laws Number 19.670, sections 37 to 40, regulated by Decree Number 64/020. In addition, Law Number 20.212 and several Resolutions of the Regulatory and Control Unit of Personal Data ("URCDP" as per its acronym in Spanish) sets some provisions regarding data protection that may be considered.

Risk Level: [Low/High/ Medium]

Scope: The protection of personal data implies the protection of natural and legal individuals (according to the Uruguayan regime companies are included) against any possible usage of their data by unauthorized parties. It applies to personal data recorded on any medium that allows them to be processed and used, both in the public and private spheres. This entails certain obligations on those who process or use personal data, as well as the right to control its use by the data owner. This applies to all processing of personal data within the national territory and also extends to individuals residing abroad. Moreover, it applies if the processing relates to the offering of goods and services in Uruguay, if contractual obligation or international law mandate it, or if means located in Uruguay are used in the processing.

Exemptions: the communication of personal data to someone other than the owner is permitted only if it serves the general interest, falls within the exceptions established in article 9 of Law Number 18.331 (data owner previous and express consent, e.g) or is necessary for health reasons, emergencies, or epidemiological studies. It is also allowed if the identity of the owner is preserved through appropriate dissociation mechanisms, or if a procedure to dissociate information has been applied, ensuring that the data owners are not identifiable. **For further details, please refer to the mentioned regulations.**

Supervisory Authority

Supervisory Authority: The URCDP, created and regulated by the PDPL, is a decentralized body of the Agency for the Development of the Government of Electronic Management and the Information and Knowledge Society ("AGESIC"). According to its institutional location and the assigned powers, the URCDP has technical autonomy and is in charge of controlling compliance with the legal regime regarding the protection of personal data and its principles, being able to carry out tasks of advice, registration, inspection and imposition of sanctioning measures.

Registration/Approval Requirements: All personal data protection treatment protocols, policies and databases must be registered and approved before the URCDP. Also, Data Protection Officer and Protection Impact Assessments (EIPD in Spanish) must be registered before URCDP.

General Data Privacy Principles

Personal data treatment is based on the following principles, under the PDPL:

- **Legality**: Any database will be legal once it is duly registered in the URCDP, unless it is only for domestic use.
- **Truthfulness:** Personal data must be truthful, adequate, equitable and not excessive in relation to the purpose for which it was collected.
- **Purpose:** The personal data processed may not be used for purposes other than or incompatible with those for which it was collected.
- **Prior informed consent:** The data controller must obtain the free, prior and express consent of the data subjects.
- **Data Security**: The person responsible of the database must adopt the necessary measures to guarantee the security and confidentiality of the personal data.
- **Reserve:** Data treatment must be carried out exclusively for the usual operations of the business activity, and any dissemination of the personal data collected to third parties is prohibited
- **"Proactive" responsibility / accountability:** The person responsible for the database or the data treatment and the person in charge, if applicable, will be responsible for the violation of the provisions of this law and must take all the measures to comply with it.

These general principles will also serve as interpretive criteria to resolve questions that may arise in the application of the relevant provisions.

Enforcement

Enforcement (Fines, Criminal Penalties): In case a data controller, a data processor or any individual or legal entity violates the regulations regarding data protection, they will be subject to the sanctions provided for in the article 35 of Law No. 18,331, which stablish the following sanctions from lowest to highest: i) Observation ii) Warning iii) Fine of up to 500,000 indexed units (usd 75.000 aprox) iv) Suspension of the database for up to 5 days v) Closure of the database

Investigations - and eventual penalties- can be initiated by the URCDP or by a complaint from the data owner. In addition, the data owner may initiate civil action if considers that has suffered a prejudice due to the improper use of his or her data.

Data Processing

Legal Basis for Processing: The personal data treatment will only be legal if at least one of the following conditions is met: i) the data owner gave express consent; ii) the data usage is necessary for the execution of a contract in which the data owner is a party or for the implementation at the request of the data owner of pre-contractual measures; iii) the data usage is necessary to protect the vital interests of the data owner or of another natural person; iv) It is necessary for the fulfillment of a mission carried out in the public interest or in the exercise of public powers conferred on the controller; v) the data processing is necessary for the satisfaction of legitimate interests pursued by the controller or by a third party, provided that such interests are not overridden by the interests or fundamental rights and freedoms of the data owner that require the protection of personal data, in particular when the data owner is a child.

In all cases, the legal basis in which the processing is carried out must be identified and documented. .

pwc

Sensitive Personal Data: This is the type of Personal Data that reveal racial and ethnic origin, political preferences, religious or moral convictions, union membership, information regarding the health or sexual life of people, genetic data, biometric data processed solely to identify a human being. The express written consent of the data owners is required to treat and storage this type of personal data. Special conditions may also apply to the processing for specific personal data such as biometric data, video- surveillance data, personal data of minors among others.

Data owners Rights

Data owners, that previously proves their identity, have the following rights under the PDPL (arts. 13 to 17)

- **Right of access:** is the right to have access to all information someone has about itself.
- **Right to update and of rectification:** is the right to modify data that is inaccurate or incomplete
- **Right of inclusion:** is the right of the data owner to be included with the corresponding information in a database proving a well-founded interest.
- **Right of deletion:** is the right of the data owner to have data whose use by third parties turns out to be illegitimate, or which turns out to be inadequate or excessive, to be deleted.
- **Right to challenge personal assessments:** implies that people have the right not to be subjected to a decision based on automated data processing.
- **Rights relating to the communication of data:** The personal data subject to processing may only be communicated for the fulfillment of purposes directly related to the legitimate interest of the issuer and the recipient

Security & Data Breaches

Security Requirements: The controller and data processor must adopt the necessary technical and organizational measures to maintain the integrity, confidentiality and availability of the information, in order to guarantee its security. For these purposes, it is considered important to assess the adoption of national and international standards on information security, such as the Cybersecurity Framework developed by AGESIC.

Data Breaches: Once the existence of a security incident is confirmed, those responsible and in charge of processing the data must initiate the planned procedures necessary to minimize the impact of such incident within the first 24 hours of their occurrence.

Notification to Supervisory Authorities: Also the URCDP and AGESIC must be informed of the security incident within a maximum period of 72 hours of becoming aware of the breach.

Notification to data owners: The data controller must communicate the breach of data in clear and simple language to the data owners who have suffered a significant impact on their rights.

Other Obligations

In addition to the obligations described in the present report, those who process or use personal data must, when certain requirentes are met, a **Data Protecction officer**. The DPO must be a person whose functions are to advise on the formulation, design and application of personal data protection policies, supervise compliance with the regulations on said protection, propose all the measures that they deem relevant to adapt to it and the international standards on the matter.

Data Protection Impact Assessment (EIPD in Spanish) must be developed in certain treatment activities, such as when minors personal data is collected, when data treatment activity involves more than 35.000 data owners, when cross-border transfers are carried out, among other hypothesis.

Transparency Requirements

Data owner must be informed if and to what extent their personal data is being processed. This is also required if the data processor has obtained the data through a third party.

Service Providers & Cross-Border Transfers

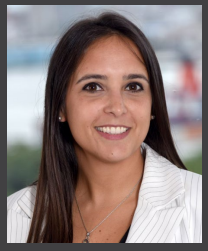
Cross-Border Data Transfers: Uruguayan regulations prohibits the transfer of personal data to countries or international organizations that do not provide adequate levels of protection according to the international standards. Adequate countries and organizations are established on URCDP Resolution Number 63/023. There are certain exceptions when it comes to: international judicial cooperation, exchange of medical data, bank or stock transfers, agreements within the framework of international treaties to which Uruguay is a party, international cooperation between intelligence agencies for the fight against organized crime, terrorism and drug trafficking, among others. Finally, URCDP Resolution Number 70/023 established some other requirements in case of international data transfer to certain organizations within the Data Privacy Framework of US.

Express authorization from URCDP: The URCDP may authorize an international data transfer or a series of international data transfers to a country or jurisdiction that does not guarantee an adequate level of protection, when the data controller offers sufficient guarantees (for example throughout some contractual clauses) regarding the protection of life, fundamental rights and freedoms, as well as with respect to the exercise of the respective rights.

Other/To Watch

The European Commission ratified, through a report published and adopted on January 15th, 2024, the recognitions of all countries that had been declared appropriate during the validity of Directive 95/46/EC, predecessor of the European General Data Protection Regulation (GDPR). This report includes Uruguay as a appropriate country in the treatment of personal data.

Let's connect to discuss how we can help:



Andrea Chanquet

Tax and Legal Manager, PwC Uruguay

+598 (2) 916 0463

andrea.chanquet@pwc.com