DATA PROTECTION LAWS OF THE WORLD

Uruguay

URUGUAY

Last modified 27 January 2020

LAW

Data Protection Act Law No. 18.331 (August 11, 2008); Decree No. 414/009 (August 31, 2009) (the Act).

DEFINITIONS

Definition of personal data

Any kind of information related to an identified or identifiable person or legal entity.

Definition of sensitive personal data

Any kind of personal data evidencing: racial or ethnic origin, political preferences, religious or moral beliefs, trade union membership or any kind of information concerning health or sexual life.

NATIONAL DATA PROTECTION AUTHORITY

Unidad Reguladora y de Control de Datos Personales (URCDP or Data Protection Authority).

REGISTRATION

Every database must be registered with the Data Protection Authority in Uruguay if the data processing is performed by a person located within the Uruguayan territory. When the person responsible for the data processing is located abroad, the database must be registered in Uruguay if:

- such processing activities occur in connection with goods / services offered to Uruguayan people;
- it is required by any contract or other international laws;
- the data is processed by means located in Uruguay; or
- the processing activities are related to the analysis of the behavior (profiling) of individuals living in Uruguay.

The database must be registered by filing mandatory forms, which must be signed by a representative of the company that owns the database.

DATA PROTECTION OFFICERS

Certain entities are required to appoint a data protection officer (in Spanish: *delegado de protección de datos*). This obligation is imposed on public entities, private entities owned by the government and private entities whose core activity is the processing of sensitive data or large amounts of data.

The data protection officer is responsible for:

- formulating, designing and implementing data protection policies;
- monitoring the compliance with local legislation and regulation; and
- serving as a link to the Data Protection Authority.

While a regulatory decree is yet to be issued, the Data Protection Authority has created an online registry for the registration of the data protection officers.

COLLECTION & PROCESSING

In order to collect personal data contained in a database, the data processor must first obtain prior, documented consent from the individual or entity whose information is being processed. Documented consent is not required in the following cases:

- Personal data obtained from public sources, for example: mass media publications
- Personal data obtained by public bodies to comply with legal obligations
- Personal data limited to:
    - corporation name, commercial name, domicile address, telephone number, tax identification number, and identification of the people in charge (in the case of legal entities), and
    - name and surname, ID number, nationality, domicile address, and date of birth (in the case of individuals)
- Personal data obtained based on a contractual or professional relationship, which is necessary to perform the contract or the development of the professional services to be rendered, or
- Personal data obtained by individuals for their personal and exclusive use

The personal data processed cannot be used for purposes, different from those that justified the initial acquisition of the information. There must be legitimate reasons (i.e. reasons which are not against the law) for the processing of the personal data. The Act further establishes that once the reasons to process the personal data are no longer present, the personal data must be deleted.

TRANSFER

Personal data can only be transferred to a third party:

- For purposes directly related to the legitimate interests of the transferring party and the transferee, and
- With the prior consent of the data subject

However, such consent may be revoked. Additionally, the data subject must be informed of the purpose of the transfer, as well as of the identity of the recipient. The prior consent of the data subject is not necessarily required when the personal data to be transferred is limited to any of the following: name, surname, identity card number, nationality, address or date of birth.

The purpose and proper identification of the transferee must be included in the request for consent addressed to the data subject. Evidence of the data subject's consent must be kept in the files of the data processor.

If the data subject's consent is not obtained within ten business days (from the receipt of the communication from the data processor asking for consent), it will be construed that the data subject did not consent to the transfer of the data.

Upon the transfer, the data processor will remain jointly and severable liable for the compliance of the recipient's obligations under the Act.

The Act forbids the transfer of personal data to countries or international entities which do not provide adequate levels of protection (according to European standards). However, the Act allows international transfers to unsafe countries or entities when the data subject consents in writing to such transfer and when contractual clauses (i.e. data transfer agreement) are in place that require an adequate level of data protection. The data transfer agreement must provide for the same levels of protection which are required under the laws of Uruguay.

In the case of an international transfer within a group of companies, Uruguayan laws establish that the international transfer is permitted without any authorization whenever the recipient branch has adopted a code of conduct that is duly registered with the local URCDP. The international transfer of personal data between headquarters and their respective branches or subsidiaries is

authorized when the headquarters and their branches have a code of conduct (such as an intercompany agreement) duly filed with URCDP.

SECURITY

Data processors must implement appropriate technical and organizational measures to guarantee the security and confidentiality of the personal data, in accordance with the notion of proactive responsibility. These measures should be aimed at preventing the loss, falsification, and unauthorized treatment or access, as well as at detecting information that may have been lost, leaked, or accessed without authorization.

It is prohibited to register personal data in databases which do not meet technical safety conditions.

BREACH NOTIFICATION

If the data processor detects a breach of security measures, the data processor should immediately report the breach and the security measures to be adopted to the affected persons and to the Data Protection Authority.

ENFORCEMENT

The URCDP is responsible for enforcement of the Act. In the context of its powers, the URCDP has broad investigatory powers, including audit and inspection, subpoena, search and seizure rights.

The URCDP has the authority to impose penalties against the data processor in the following order: warning, admonition, fines up to US$60,000, suspension of the database for five days, and closure of the database.

ELECTRONIC MARKETING

The Act will apply to most electronic marketing activities, as these activities typically involve the processing and use of personal data (*eg*, an email address is likely to be considered personal data for the purposes of the Act). The Act does not prohibit the use of personal data for the purposes of electronic marketing, but grants personal data owners / data subjects (individuals or legal entities) the right to demand the deletion or suppression of their data from the marketing database.

Personal data may be used and processed for marketing purposes when the personal data was either obtained from public documents provided by the data subject, or when prior consent has been obtained.

ONLINE PRIVACY

There are no provisions that specifically address online tracking or geolocation data. However, the general principles of the Act apply. The personal data processed cannot be used for purposes other than those that justified the acquisition of the data; when the reasons to process the personal data have expired, the personal data must be deleted.

KEY CONTACTS

Estudio Bergstein
www.bergsteinlaw.com/

Jonas Bergstein
Partner
Estudio Bergstein
T +598 2 901 2448
jbergstein@bergsteinlaw.com

Guzmán Ramírez
Estudio Bergstein
T +598 2901 2448
gramirez@bergsteinlaw.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.