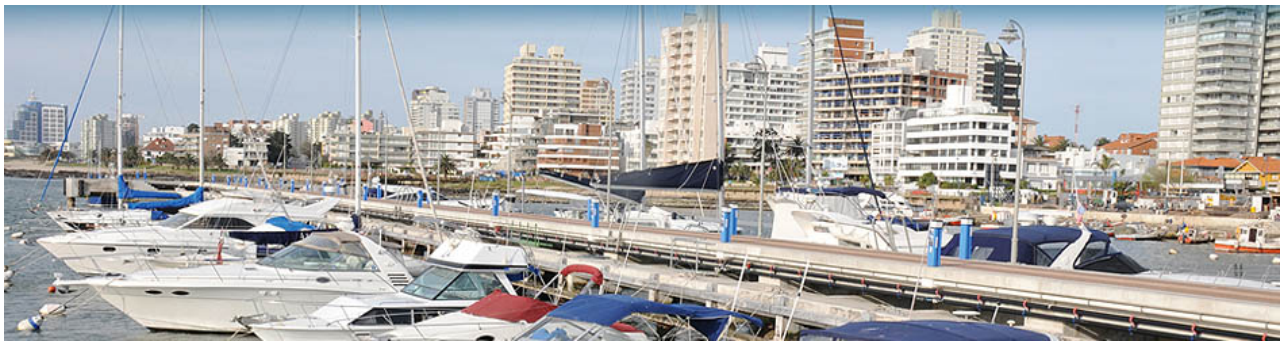
DATA PROTECTION LAWS OF THE WORLD

Uruguay

URUGUAY



Last modified 28 January 2024

LAW

Data Protection Act Law No. 18.331 (11 August 2008); Decree No. 414/009 (31 August 2009), Arts 47 to 40, Act Law No. 19.670 (15 October 2018), Decree No. 64/2020 (17 February 2020) and Arts 62 and 63, Act No. 20.075 (20 October 2022). .

DEFINITIONS

Definition of personal data

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

Definition of sensitive personal data

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

NATIONAL DATA PROTECTION AUTHORITY

(“**URCDP**”), *Unidad Reguladora de Control y Actos Personales* (“**Data Protection Authority**”).

REGISTRATION

The Uruguayan legal system requires the registration of all databases containing personal data of individuals or legal entities (Articles 24, 28, and 29 of the Act and Articles 15 to 20 of the Decree 414/009).

The Law applies when the processing of personal data is performed by controllers located in Uruguay.

The Act has extraterritorial effects in the following cases:

- if the activities are related to the offer of goods or services to individuals residing in Uruguay, or intended to monitor their behaviour;
- if private international laws or contractual agreements so establish it; and
- if the processing is made by using means located in Uruguay, with the exceptions of the cases in which those means are used for the sole purpose of transit, and there is a person responsible for the processing with residency in Uruguay, appointed by the controller before the URCDP.

The register must be updated every three months (Article 20 of the Decree 414/009).

DATA PROTECTION OFFICERS

The appointment of a Data Protection Officers (DPO) is mandatory in the following cases: (i) public state or non-state entities, (ii) private or partially state-owned entities, (iii) private entities which process sensitive data as a core activity, and (iv) private entities which process large scales of data.

Decree 64/2020 clarifies that large scales of data means the data processing of more than 35,000 subjects.

The DPO must meet the conditions required for the correct performance of his/her duties. He/she must act autonomously in technical matters.

The appointment of a DPO must be submitted before the URCDP for its approval. If the legal and technical requirements are not met, the Regulator is entitled to deny or revoke (as the case may be) the filing/authorisation to the appointed DPO.

COLLECTION & PROCESSING

In order to collect the information which is contained in the database, the data processor should 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;
- personal data obtained by public bodies to comply with legal obligations;
- personal data limited to domicile, telephone number, ID number, nationality, tax number, corporation name;
- personal data obtained in base of a contractual or professional relationship, which is necessary to perform the contract or the development of the professional services to be rendered; and
- personal data obtained by individuals or corporations for their personal and exclusive use.

The personal data processed cannot be used for purposes different from those that have justified the acquisition of the information. It is understood that legitimate reasons (i.e. reasons which are not against the law) must pre exist and underlay the processing of the personal information. The Data Protection Act further establishes that once the reasons to process the personal information have disappeared, the personal information must be deleted.

Data subjects have the right to be informed by the data processor about how their information is and has been used, and may exercise this right at all times.

TRANSFER

Personal data can only be transferred to a third party:

- for the compliance of purposes directly related to the legitimate interest of the transferring party and the transferee; and
- with the data subject's prior consent. Such consent may be revoked. Additionally, the data subject must be informed of the purpose of the transfer, the identity of the transferee, and the purposes for which the personal data will be used

The data subject's prior consent is not necessary if the individual’s data to be transferred is limited to: name, surname, identity card number, nationality, address, and date of birth.

The purpose and proper identification of the transferee must be included in the consent communication that would be 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 (counted from the receipt of the communication from the data processor asking for the 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 transferee obligations under the Data Protection Act.

The Data Protection Act forbids the transfer of personal data to countries or international entities which do not provide adequate levels of data protection (according to URCDP). However, the Data Protection Act allows international transfer to unsafe countries or entities, when the data subject consents to the transfer (such consent must be given in writing), or when the

guarantees of adequate protection levels arise from “contractual clauses”, and “self regulation systems”. The international data transfer agreement must establish the same levels of protection which are effective under the laws of Uruguay.

In the case of a cross‑border transfer within a group of companies, Uruguayan laws establish that the international transfer will be lawful without any authorisation whenever the branch has the same conduct code duly registered before the local URCDP.

The international transfer of personal data between headquarters and their respective branches or subsidiaries is authorised when the headquarters and their branches have a conduct code duly filed before URCDP.

SECURITY

The data processor must implement appropriate technical and organisational measures to guarantee the security and confidentiality of the personal data. These measures should be aimed at avoiding the loss, falsification, non‑authorised treatment or inquiry, as well as at detecting information that may have been leaked, performed by human intervention or not.

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

BREACH NOTIFICATION

Data breaches and data incidents must be reported to the URCDP and to the Data Subject.

Once the DPO or the Data Controller confirms the occurrence of a security breach, it must be notified to the URCDP within 72 hours.

Notification to data subjects must be done once the DPO or the Data Controller confirms the occurrence of a security breach. The Uruguayan Data Privacy Act requires the notification to be effected “as soon as practicable”, but fails to spell out a precise time frame for such notice.

Legal requirement of the data breach/incident

- Notification to the Regulator must contain relevant information, including the:
  - certain or estimated date of the occurrence of the breach;
  - main characteristics of the breach;
  - details of the data affected; and
  - the possible impacts.
- The regulation does not state any formalities to the communication to the Data subject. However, it states that such notification must be clear and simple.

After the first notification to the Regulator within the first 72 hours after the Data Breach/incident, a second communication must be done by the DPO or the Data Controller to the Regulator. The second report must indicate all the details of what happened and the measures that were adopted and carried out so that such violation/incident has been mitigated and does not occur again. The Act does not state a time frame for execution of the second report.

ENFORCEMENT

The URCDP is responsible for the enforcement of the Data Protection Act. In the context of its powers, the URCDP is entitled to:

- request the data processor the exhibition of books, documents and files, electronic or not;
- summon the data processor before the URCDP in order to provide information;
- intervene in the documents and files inspected;
- adopt security or protection measures in order to preserve the documentation, including copying the files;
- seize or impound the documents and files for six days;
- carry out inspections on data processor’s offices;
- summon third parties to appear before the URCDP.

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

ELECTRONIC MARKETING

The Act will apply to most electronic marketing activities, as these activities likely involve the processing and use of personal data (e.g. an email address is likely to be "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 with the right to demand the elimination or blocking of their data from the data base.

Personal data can be used and processed for marketing purposes when it has been taken from public documents, when it has been provided by the personal data owner or when prior consent has been gathered.

ONLINE PRIVACY

There are no express provisions for online privacy, but the general data privacy principles fully apply. In this regard, key principles such as prior informed consent, the purposes of collection and use, and the right to information are particularly relevant. These principles state that in order to use cookies, the data subject's prior consent must be obtained and the data subject must be informed about the purposes of collection and use; personal data collected through cookies may only be processed as necessary to fulfill the purposes for which it was collected and must be deleted when the purpose ceases.

KEY CONTACTS

Bergstein Abogados
www.bergsteinlaw.com/

Jonás Bergstein
Partner
Bergstein Abogados
jbergstein@bergsteinlaw.com

Ignacio Torres Negreira
Senior Associate
Bergstein Abogados
itorresnegreira@bergsteinlaw.com

Guzman Ramírez
Senior Associate
Bergstein Abogados
T (598) 2 901 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.