

DATA PROTECTION LAWS OF THE WORLD

Uruguay



Downloaded: 11 July 2017

URUGUAY



Last modified 24 January 2017

LAW

Data Protection Act Law No. 18.331 (11 August 2008); Decree No. 414/009 (31 August 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 as well as any kind of information concerning health or sexual life.

NATIONAL DATA PROTECTION AUTHORITY

('URCDP', *Unidad Reguladora y de Control de Datos Personales* ('Data Protection Authority')).

REGISTRATION

Every database must be registered with the Data Protection Authority in Uruguay if the information contained in the database is gathered or obtained through means, mechanisms or sources located in Uruguay.

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

DATA PROTECTION OFFICERS

There is no requirement to appoint a data protection officer.

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
- personal data obtained by public bodies to comply with legal obligations
- personal data limited to domicile address, telephone number, ID number, nationality, tax number, corporation name

- 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 or corporations for their personal and exclusive use.

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

However, the prior consent of the data subject is not necessarily required when the personal 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 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 (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 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 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 provide for 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 recipient branch has adopted a conduct of code duly registered with 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 code of conduct (such as an inter-company agreement) duly filed with URCDP.

SECURITY

Data processors must implement appropriate technical and organisational measures to guarantee the security and confidentiality of the personal data. These measures should be aimed at preventing the loss, falsification, and unauthorised treatment or access, as well as at detecting information that may have been lost, leaked, or accessed without authorisation.

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

BREACH NOTIFICATION

In case the data processor detects a breach of security measures, and if the consequences of the breach could substantially affect the rights of the data subject and/or the rights of any other agent or person involved, the data processor should report the breach to the affected persons.

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 rights, and subpoena, search and seizure authority.

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 database for five days, 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 '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 gathered.

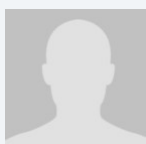
ONLINE PRIVACY

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; and when the reasons to process the personal information have expired, the personal information must be deleted.

KEY CONTACTS

Estudio Bergstein

www.bergsteinlaw.com/

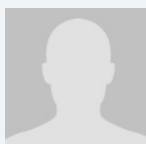


Jonas Bergstein

Partner

T +598 2 901 2448

jbergstein@bergsteinlaw.com



Guzmán Ramírez

T +598 2901 2448

gramirez@bergsteinlaw.com

DATA PRIVACY TOOL

You may also be interested in our [Data Privacy Scorebox](#) to assess your organisation's level of data protection maturity.

Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2017 DLA Piper. All rights reserved.