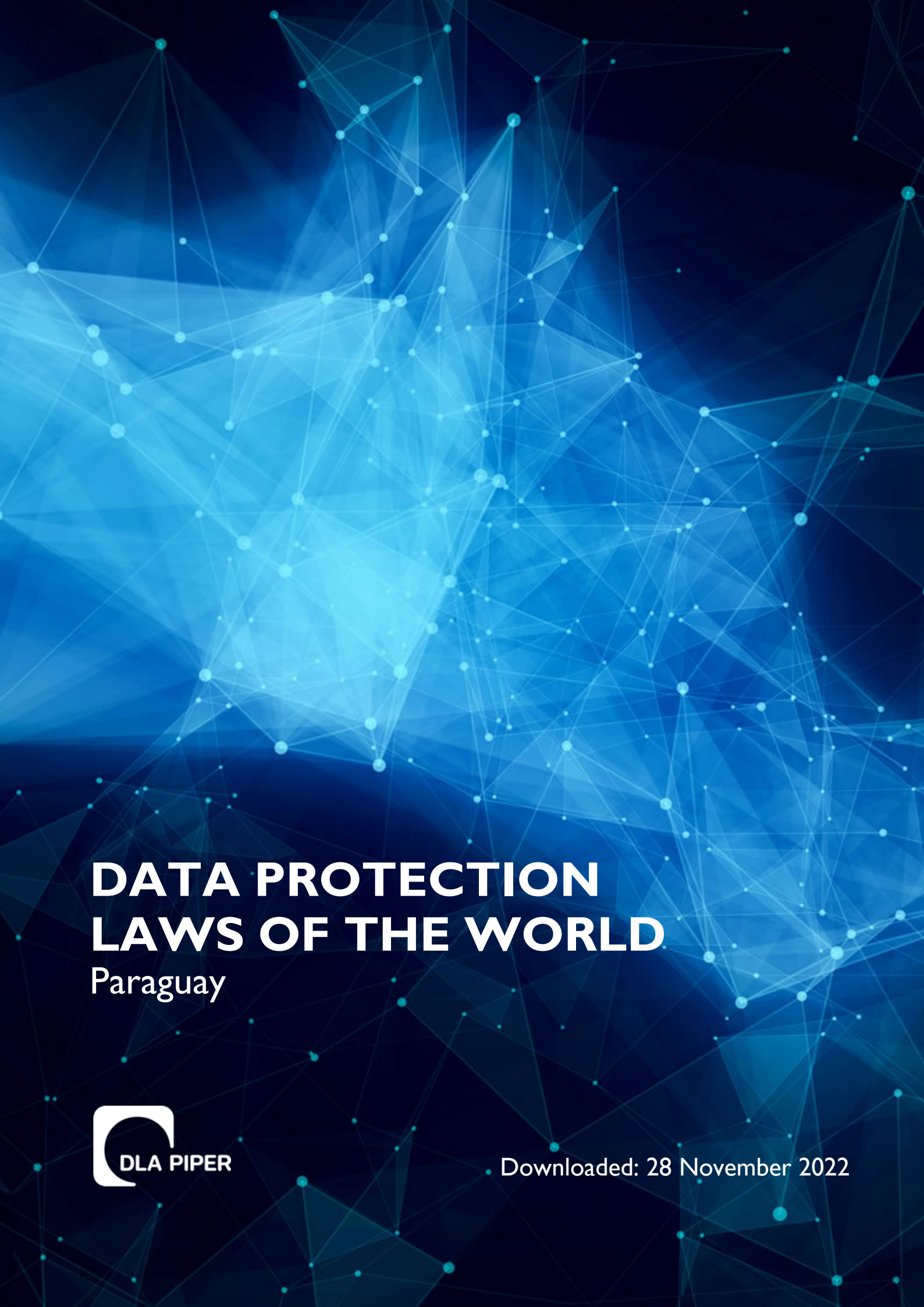
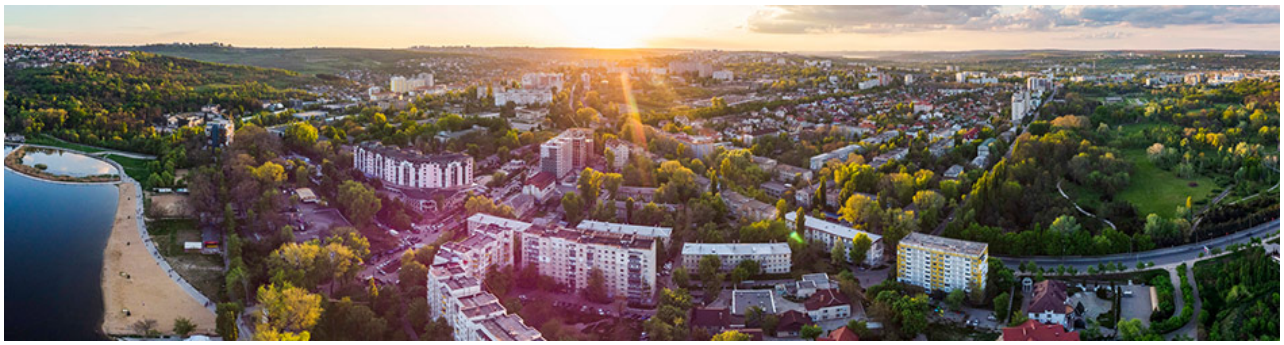


DATA PROTECTION LAWS OF THE WORLD

Paraguay

DLA PIPER

PARAGUAY



Last modified 24 January 2022

LAW

Legal framework

- National Constitution, art. 135, Habeas Data: Any person may file an action to have access to (i) personal data about such person or its property; and (ii) information about the use of such data and purpose for which it is kept, whether it is stored in public or private data registries. Additionally, any person may request the suppression, correction, confidentiality or updating of the data where inaccurate or discriminatory;
- Criminal Code, art. 174 (Unlawful access to computer systems) and art. 175 (Sabotage of computer systems): individuals or entities that unlawfully access or alter personal data contained in databases (computer systems) are criminally liable;
- Law No. 6534/2020 "of protection of personal credit data" ("**Personal Credit Data Protection Law**" or "**Law**"). The previous data protection regulatory regime lead by Law No. 1682/2001 "which regulates the use of private information" as amended by laws No. 1969/2002 and 5543/2015 is no longer in force and was replaced in full by the Personal Credit Data Protection Law (Art. 30 of the Law); and
- Law No. 4868/2013 "Electronic Commerce" **("Electronic Commerce Law")** and its regulatory decree No. 1165/2014 **("Regulatory Decree of the Electronic Commerce Law").**

DEFINITIONS

Definition of personal data

Art. 3 of Personal Credit Data Protection Law defines Personal Data or Personal Information as "information of any type that refers to legal entities or natural persons that are identified or identifiable. An identifiable person shall mean any person who can be identified by means of an identifier or by one or more elements that characterize the physical, physiological, genetics, mental, economic, cultural, or social identity of the data subject. The rights and guarantees of personal data protection shall be extended to legal entities, insofar as they are applicable".

Definition of sensitive personal data

Sensitive Personal Data is defined as information that refers to the intimate sphere of the data subject, or data that, if misused, may give rise to discrimination or entail a serious risk for the data subject. Personal data is considered sensitive when it reveals aspects such as racial and ethnic origin; religious, philosophical and moral beliefs or convictions; trade union memberships; political opinion; data related to health, life, sexual preference or orientation, genetic or biometric data aimed at uniquely identifying a natural person.

Personal Credit Data Protection Law further defines Credit Data as 'information, positive and negative, related to the credit history of natural persons and legal entities, in relation to credit, commercial and other activities of similar nature, that serves to identify, correctly and unequivocally, the data subject, his/her address, business activity, determine his/her level of indebtedness, compliance with his/her financial obligations and, in general, of his/her credit risks, at any given time'.

NATIONAL DATA PROTECTION AUTHORITY

There is no National Data Protection Authority in Paraguay.

For activities that are considered to be "electronic commerce" as provided by the Electronic Commerce Law, the national authority is the General Direction of Digital Signature and Electronic Commerce – Ministry of Industry and Commerce **("Electronic Commerce Direction").**

REGISTRATION

Under the current legislation, no registration is required in order to process or store personal data.

Even though the Electronic Commerce Law does not establish a registration requirement, according to Art. 7 of the Regulatory Decree of the Electronic Commerce Law, the Electronic Commerce Direction has the faculty to gather information from companies that render services via electronic means (such as electronic storage data companies) regarding:

- their commercial activity;
- their identity; and
- other data established in current regulations.

Such companies have the duty to collaborate with the Electronic Commerce Direction and comply with all information requirements (Art. 8, Regulatory Decree of the Electronic Commerce Law).

DATA PROTECTION OFFICERS

Under current legislation, the appointment of Data Protection Officers is not required.

COLLECTION & PROCESSING

Under the current legal regime, it is prohibited to publicize or diffuse sensitive data of people that are explicitly identified or identifiable (Art. 4 of Personal Credit Data Protection Law).

The current regulatory regime allows for private use the collection, storage and processing of personal information when it is lawful, exact, complete, true and updated for the specific purpose for which the data was collected (Art. 7 of the Law). However, the data subject has to give consent to the collection and use of their personal information, to that effect, the data subject has to be informed, clearly and expressly, about the purposes their collected personal data will be processed for. The data subject's consent may be revoked at any time under the same conditions as it was granted (Art. 6 of the Personal Credit Data Protection Law).

The Personal Credit Data Protection Law specifically regulates personal credit data collection and processing by Credit Data Bureaus. Such bureaus have to be fully authorized and registered by the Central Bank in order to be able render credit reference services (*ie,* provision of data related to personal credit information of persons or entities) and may only provide services to specific users (*eg,* financial entities, banks, credit agencies, etc.) (Arts. 3, 12, 13 and 14 of the Law).

Furthermore, the Personal Credit Data Protection Law establishes that a Credit Data Bureau may process personal data related to financial solvency and credit of persons or entities provided that:

- the data was provided by the data subject; or
- the data subject provided express and written consent; or
- the information is related to information that private or governmental entities have the duty to publish; or
- the information is public (Art. 13 of the Law).

The Personal Credit Data Protection Law also establishes a duty to the person/entity responsible for collecting and/or storing the data, to permanently update (when necessary) any personal information regarding the financial situation, solvency and/or the fulfilment of commercial and financial obligations (Arts. 9 and 11 of the Law). It also provides that the users of Credit Data

Bureaus have the obligation to regularly provide to them, updated data on their credit portfolio clients, especially information related to the compliance with credit obligations, which must be notified within twenty four (24) hours of its cancellation (Art. 14 of the Law).

In addition, the Law establishes that Personal Credit Data which may affect a data subject cannot be stored (and/or publicized) for more than five (5) years from the date of the recorded event (Art. 9 of the Law).

A data subject has the right to:

- access the information and data about themselves, their dependents and/or property;
- know the use and purpose of such data; and
- where data is incorrect, inexact or misleading, request access, prompt correction, rectification, to withdraw consent and object to the processing (Art. 5 of Personal Credit Data Protection Law).

In addition, the Regulatory Decree of the Electronic Commerce Law establishes that the data subject's express consent is required in order to obtain any personal information (Art. 13). Accordingly, electronic collection, storage and processing data companies (and other companies that render services via electronic means who collect personal data), have the duty to inform to the data subject about:

- the purposes for which the personal data are collected; and
- how the personal data colelcted will be processed.

TRANSFER

The Personal Credit Data Protection Law establishes that international transfers of personal data to a recipient that is in a third country (as defined under the Law), or to an international organization where the guarantees, requirements and/or exceptions established in the Law are not met, is a violation of applicable data protection law and, thus, can be subject to sanctions (Art. 21.x. of the Law).

Under current legislation, there are no other specific provisions that regulate the transfer of private information. However, the transfer of private information is considered as a form of data processing, so the same rules than for collection and processing personal data applies (Art. 3.e. of the Law – definition treatment of data).

SECURITY

Under current legislation, there are no specific security requirements regarding the protection of private information. However, Art. 10 of the Law establishes that the person or entity responsible of the treatment of personal credit data shall guarantee the adoption and implementation of the necessary technical, organization, and security measures to protect the access and integrity of personal data in order to prevent its alteration, loss, commercialization and not authorized access.

The Regulatory Decree of the Electronic Commerce Law also establishes that companies that render services via electronic means (that also collect or process personal or private data), have the duty to:

- inform to the recipient of such data, of the person in charge of its custody and storage; and
- implement secure systems to avoid the unauthorized loss, alteration and/or third party access to such data (Art. 11).

Additionally, such companies have the duty to inform consumers and users (in a transparent, clear and simple manner) regarding the specifics of:

- the level of security and the applicable privacy policy covering the permanent protection of personal data; and
- security measures and technology used to protect the means of payment and the transfer, processing and/or storage of financial data (Art. 12).

BREACH NOTIFICATION

No data breach notification obligation exists under the current data protection regime.

ENFORCEMENT

The current legal regime contemplates the following enforcement mechanisms:

- Without the need of a court order, a data subject has the right to (i) access the information and data about themselves, their dependents and/or property and know how such data is used; and (ii) request the correction and suppression of the information Art. 5 and 8 of Personal Credit Data Protection Law). Data controllers and processors must establish simple, fast, accessible and free of charge procedures, to enable data subjects to exercise their rights. However, where the data subject's efforts in obtaining the above are unsuccessful, it may bring court actions to compel access to personal data and request the correction, suppression or updating of such data; and
- Violations against obligations established under the Personal Credit Data Protection Law and the Electronic Commerce Law are subject to fines.

The enforcement authorities for the enforcement of the Personal Credit Data Protection Law are the Central Bank of Paraguay ('**BCP**') and the National Secretariat of Consumer and User Defense ('**SEDECO**'). The BCP has authority to further regulate, interpret and enforce the Law (Art. 20 of Personal Credit Data Protection Law).

ELECTRONIC MARKETING

The Electronic Commerce Law requires that all marketing communications and promotional offers:

- state that they are commercial communications;
- include the name of the sender; and
- provide a mechanism through which the recipient may choose not to receive any further communications from the particular sender.

Additionally, the communication shall state that the recipent's private data was obtained without violating privacy rights.

Electronic Marketing is also subject to general marketing and advertising related provisions of the Consumer's Protection Law.

ONLINE PRIVACY

Art. 30.3. of the Electronic Commerce Law requires suppliers of goods and services ,which use data storage and recovery devices, to clearly and thoroughly inform users and consumers about the use of and purposes regarding the collected data and provide data subjects the ability to object to the use(opt-out) of their personal data through a simple procedure and free of charge.

Other than the rule mentioned above, the current legal framework does not specifically address location data, cookies, local storage objects or other similar data-gathering tools.

KEY CONTACTS

Jorge Angulo
Junior Partner
Fiorio, Cardozo & Alvarado Law Firm
jorge.angulo@fca.com.py

Francisca Peroni
Associate
Fiorio, Cardozo & Alvarado Law Firm
francisca.peroni@fca.com.py

DATA PRIVACY TOOL

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