DATA PROTECTION LAWS OF THE WORLD

Venezuela

VENEZUELA

Last modified 12 December 2022

LAW

There is no specific legislation about data privacy or data protection in Venezuela, however, there are isolated provisions in some existing laws that regulate certain aspects related to data protection (e.g., Law on Privacy Protection of Communications, the Special Law against Computer Crimes, the Organic Law on Prevention, Conditions, and the Working Environment, and the Civil Code, Communications from the National Superintendency of Banks).

Likewise, the Constitution of the Bolivarian Republic of Venezuela (the **"Constitution")** establishes general principles that serve as a framework for the protection of information. These principles were developed by decision No. 1318 of the Supreme Court of Justice ("TSJ" for its Spanish acronyms) of August 2011, guarding the honour, privacy, intimacy, self-image, confidentiality, and reputation of individuals. The principles are:

- Principle of free will, which implies the need of a prior, free, informed, unequivocal and revocable consent for the use, and collection of personal data.

- Principle of legality, according to which the collection of personal data entails that the limitation to information self-determination
  is a result of a legal provision.

- Principle of purpose and quality, which means that the collection of personal data must respond to predetermined purposes, motives, or causes that are not contrary to constitutional and legal provisions, also a prerequisite to obtain valid consent. Data can only be extracted and treated for the fulfilment of specific, explicit, and legitimate purposes related to the activity of those who get them. This principle entails the necessary proportionality in the collection of data, which must be adequate, relevant, and not excessive.

- Principle of temporality or conservation, under which the data should be preserved until the purposes or objectives that its collection are achieved.

- Principle of accuracy and self-determination, which means that the data must be complete, accurate and up to date, in response to the real situation of the person as the data may be subject to control by the individuals whose data is collected. The interested party must have clear and expeditious procedures to obtain from the person responsible for the use or receipt of the information: the confirmation of the use of data; the purposes of such registers and its recipients; the rectification or cancellation of inaccurate, inadequate, or excessive data, and; the knowledge of such modifications by those whose wrong information has been communicated.

- Principle of foreseeability and integrity: Although the rights relating to the collection of information should be initially aimed at protecting the rights of the individuals whose information is collected, the analysis of the impact that the collection of data has on such rights cannot be isolated and without reference to data that may be collected in other

registries.

- Principle of security and confidentiality, which implies the guarantee of confidentiality, of no alteration of data by third parties, and of access to such data by the competent authorities in accordance with the law. The data must be protected from alteration, loss, accidental destruction, unauthorised access, or fraudulent use. This protection goes as far as preventing international data transfers to States whose legislation does not guarantee a level of protection similar to the one described.

- Principle of guardianship, which means that in addition to having judicial protection to enforce the right to access the information and obtain knowledge of the use of the personal data, there should be public entities that ensure the right to the protection of personal data with powers to create or implement simplified models and based on technical standards to measure the level of efficiency of the structures and procedures in place and the level of protection of the personal data.

- Principle of liability, under which a violation of the right to the protection of personal data gives rise to liability and the imposition of civil, criminal, and administrative penalties, as the case may be.

Also, Article 28 CRBV sets the right for individuals to access their personal information stored in public or private records, to know for what use such information will be recorded, and, rectify or destroy it when incorrect or when it unlawfully affects their rights. Although there is no legal regulation in this regard, the TSJ has agreed to the possibility of maintaining this information and personal data in systems or records, stored in a way that a profile of them can be done with the purpose of using the information for personal gain or for third parties, as long as the rights set in Article 28 CRBV are respected. According to this Article, a double right is guaranteed: (i) to collect information about people and their goods, and (ii) access to such information that has been collected and is reflected in the records. However, whoever collects the information or data of the individuals or their goods, shall respect the right of the people to protect their honour, privacy, intimacy, self-image, confidentiality, and reputation, all of this provided in Article 60 CRBV.

Additionally, the decision also stipulates that the particular data that someone keeps for study purposes, or for personal use or to fulfill professional objectives, which do not form a system capable of designing a total or partial profile of individuals are not subject to these principles, since they lack a general projection. However, records that, when cross-referenced with others, make it possible to outline a profile of the private life of individuals, or of their economic situation, political tendencies, etc., could be part of the records protected by the Constitution. The mere potential of intersecting and complementing the data of a registry, with the information stored in others that complete it, makes the set of records susceptible to the rights referred to in article 28 of the Constitution.

DEFINITIONS

Definition of Personal Data

There is no legal definition of “Personal Data” in Venezuelan legislation.

Nonetheless, decision No. 855 of the TSJ, of May 8, 2012, gave us the following definition of Personal Data: *“Any information related to an identified or identifiable individual”.*

Likewise, any Personal Data must be processed fairly and responsibly for particular purposes, on the basis of the data subject's consent or as a consequence of some other legitimate basis, provided by law.

Definition of Sensitive Personal Data

There is no legal definition of “Sensitive Personal Data” in Venezuelan legislation.

However, in decision No. 1335 of the TSJ, of August 8, 2011, in a case on the sensitive and personal data in a medical record, the TSJ expressed that any such data must be handled under the strictest confidentiality and privacy controls, and its content must not be disclosed.

The decision says that sensitive and personal data is a person’s most genuine and authentic assets, and, as such, is the absolute owner and holder of all that information, only that person can grant permission for its use and treatment.

Under this decision, we can conclude that any person’s intimate data can also be considered to be Sensitive Personal Data, and, as such, must be confidential, be duly guarded and only that person can grant permission for its use and treatment.

NATIONAL DATA PROTECTION AUTHORITY

There is no National Data Protection Authority in Venezuela.

REGISTRATION

There is no legal requirement to register before any National Data Protection Authority.

DATA PROTECTION OFFICERS

There is no legal requirement to appoint a Data Protection Officer.

COLLECTION & PROCESSING

The collection and processing of Personal Data must adhere to the previously explained general principles dictated by the Constitutional Chamber of the TSJ.

TRANSFER

According to the general principles dictated by the TSJ, there is a protection against the transfer of data to States whose legislation does not guarantee a level of protection similar to the one described.

In addition, in terms of labor law, the employee's consent is required to transfer personal data to third parties. There are companies that voluntarily develop their own data protection policies or apply their headquarters policies or international standards for this matter.

SECURITY

According to the general principles dictated by the Constitutional Chamber of the TSJ, there is a guarantee of confidentiality, of no alteration of data by third parties, and of access to such data by the competent authorities in accordance with the law. The data must be protected from alteration, loss, accidental destruction, unauthorised access, or fraudulent use.

BREACH NOTIFICATION

There is no legal obligation to disclose a data breach.

Mandatory Breach Notification

It is not mandatory to disclose a data breach.

ENFORCEMENT

When it comes to labor matters and records of employees, the Organic Law on Prevention, Conditions and Working Environment ("**LOPCYMAT**" for its Spanish acronym) sets forth in Article 53 the following rules on certain data and privacy protection:

- Section 10: the right of the employees to access information contained on health screenings, as well as the confidentiality of the results with respect to third parties. (According to Article 27 of the LOPCYMAT, disclosure of health results to

certain third parties is permitted with the employee's consent. Also, per Article 119 of the LOPCYMAT, failure to comply with the obligation of section 10 may result in a fine ranging from 26 to 75 tax units ("**T.U.**") for each worker exposed.

- Section 11: the confidentiality of employees' personal health data. (According to Article 120 LOPCYMAT, failure to comply with the obligation of section 11 may result in a fine ranging from 76 to 100 T.U. for each worker exposed.
- Section 16: the privacy of employee's correspondence and communications, as well as free access to all data and information relating to the employee.
- The fines or sanctions for non-compliance according to LOPCYMAT are:
    - Article 27: disclosure of health results to certain third parties is permitted with the employee's consent.
    - In addition, per Article 119, failure to comply with the obligation of section 10 may result in a fine ranging from 26 to 75 T.U. for each worker exposed.
    - Article 120: failure to comply with the obligation of section 11 may result in a fine ranging from 76 to 100 T.U. for each worker exposed.

ELECTRONIC MARKETING

Electronic Marketing is allowed, but any collection and processing of Personal Data must adhere to the previously explained general principles dictated by the TSJ.

ONLINE PRIVACY

There is no specific legislation about online privacy in Venezuela, but we advise to adhere to the previously explained general principles dictated by the TSJ if there is going to be any processing or collection of Personal Data.

KEY CONTACTS

InterJuris Abogados S.C
interjuris.com/

Maria Cecilia Rachadell
Partner
InterJuris Abogados S.C
T +13059271390
maria.rachadell@interjuris.com

Juan José Delgado
Partner
InterJuris Abogados S.C
T +13057971121
juanjose.delgado@interjuris.com

DATA PRIVACY TOOL

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