Icaza
González-Ruiz
Alemán

PERSONAL DATA PROTECTION IN PANAMA

The protection of personal data is a fundamental guarantee and is contained in our National Constitution, which establishes in its Article 42 the following:

> *"Article 42: Every person has the right to access personal information contained in public and private databases or registries, and to request its rectification and protection, as well as its suppression, in accordance with the provisions of the Law.*
> *This information may only be collected for specific purposes, with the consent of its owner or by order of a competent authority based on the provisions of the Law."*

As demonstrated, the owner's consent must be always obtained, i.e. his or her expression of willingness to process the data and be informed of the specific purpose for which the data is collected. Law 81 establishes that consent may be obtained in a manner that allows its traceability through documentation, whether electronic or through another appropriate mechanism, and may be revoked, without retroactive effect.

Likewise, our National Constitution contemplates in its articles 43 the constitutional guarantees in which every person has the right to request information of public access or of collective interest and to request its rectification. Article 44 establishes that any person may file a habeas data action to guarantee the right of access to his or her personal information collected in data banks or official registries.

On March 29, 2021, the Personal Data Protection Law came into full force in the Republic of Panama by means of Law 81 of March 26, 2019. This Law establishes the principles, rights, obligations and procedures that regulate the protection of personal data in our country for natural and legal persons. Afterwards, Law 81 is regulated by means of Executive Decree 285 of 2021.

It is important to note that prior to the enactment of Law 81 of 2019, there were legal provisions that currently regulate the protection of personal data in Panama, by means of special laws. Among which are the Banking Law, Insurance Law, Securities Law, Trust Law, and Law regulating the Rights and Obligations of Patients, in matters of information or free and informed decision, among others.

Although there are special laws and rules that comprise the regulatory framework governing the protection of personal data, Law 81 of 2019 applies in a supplementary manner.

The regulator or regulatory authority of each sector, must establish within its regulations all the protocols, processes and procedures for treatment and secure transfer that must be complied with by the regulated subjects.

Basic Concepts of Personal Data Protection

Icaza
González-Ruiz
Alemán

What is a Personal Datum?

Personal datum is any information concerning natural persons that identifies them or makes them identifiable.

What is a sensible datum?

The Law defines sensitive data, as those which refer to the intimate sphere of the data subject, or whose improper use may give rise to discrimination or entail a serious risk for the data subject.

It is deemed as sensitive data that which may reveal aspects such as racial or ethnic origin; religious, philosophical and moral beliefs or convictions; union membership; political opinions; data related to health, life, sexual preference or orientation, genetic data or biometric data, among others.

Law 81 establishes that sensitive data cannot be transferred without the data subject's explicit consent; except when it is necessary to safeguard the data subject's life and he/she is physically or legally incapacitated, when it refers to data that is necessary for the recognition, exercise or defense of a right in a process with competent judicial authorization, when it has a historical, statistical or scientific purpose, in which case measures leading to dissociate the identity must be adopted.

Purpose, principles and application

The Law establishes the principles, rights, obligations and procedures that regulate the protection of personal data, considering its interrelation with the private life and other fundamental rights and freedoms of citizens.

The general principles that inspire and govern the protection of personal data and that are the basis for the interpretation and application of the rule, also complement some gaps in the Law 81 itself:

1. **Principle of fairness: personal data are collected without deception or misrepresentation and without using fraudulent means.**
2. **Principle of purpose: personal data must be collected for specific purposes and not be further processed for purposes other than those for which they were requested, and not be kept for a longer than necessary for the purposes of processing.**
3. **Principle of proportionality: only adequate and relevant data limited to the minimum necessary in relation to the required purpose are requested.**
4. **Principle of truthfulness and accuracy: they must be accurate and truthfully respond to the current situation of the data subject.**

5. **Principle of data security: those personal data controller must adopt measures to ensure the security of the data and inform the data subject, as early as possible, when the data have been removed without authorization or there are indications that their security has been breached.**
6. **Principle of transparency: information and communication must be expressed in clear and simple language.**
7. **Principle of confidentiality: all persons involved in the personal data processing are obliged to maintain secrecy or confidentiality with respect to such data.**
8. **Principle of lawfulness: data must be collected in a lawful manner, with the prior, informed and unequivocal consent of the data subject or by legal basis.**
9. **Principle of portability: the data subject has the right to obtain from the data controller a copy of the personal data in a generic and commonly used format.**

The scope of application of this Law extends to databases located in the territory of the Republic of Panama, which store or contain personal data of nationals or foreigners or that the data controller is domiciled in the country, are subject to the application of this Law and its regulations. The storage or transfer of personal data originated or stored within the Republic of Panama that are confidential, sensitive or restricted, that receive cross-border processing is permitted provided that the data controller or custodian of the data complies with the standards of personal data protection and obtains consent.

Executive Decree 285 of 2021, which regulates Law 81, establishes that the registration of databases transferred to third parties shall be stated in writing, by any means, including electronic means.

What exceptions apply and when can Personal Data be processed?

There are exceptions to the scope of application of the Law for those data that are expressly regulated by special laws or by regulations that develop them and that we have detailed at the beginning.
Exceptions include:

1. **Those carried out by a natural person for exclusively personal or domestic activities.**
2. **Those carried out by competent authorities for purposes of prevention, investigation or prosecution of criminal offenses or enforcement of criminal penalties.**
3. **Those carried out for the analysis of financial intelligence related to national security.**
4. **When it is data processing related to international organizations in compliance with international treaties or conventions.**
5. **Those resulting from information obtained by means of a previous anonymization procedure.**

The processing of personal data can only be carried out when: i.) The consent of the owner is

obtained, ii.) The processing is necessary for the execution of a contractual obligation, iii.) The processing is necessary for the fulfillment of a legal obligation, iv.) The processing is authorized by a special law.

Personal data controller, database custodian and Personal Data Protection Officer

The data controller is a natural or legal person, public or private, for profit or non-profit, who is responsible for the decisions related to the processing of data and determines the purposes, means and scope.

The data controller is who shall establish the protocols, processes and procedures for management and secure transfer, protecting the rights of data subjects. The National Authority for Transparency and Access to Information (ANTAI) with the support of the National Authority for Government Innovation (AIG) are the authorities that will oversee and supervise the above.

The custodian of the database, as well as anyone who has access to it, must take care of it with due diligence, and shall also be liable for any damages caused.

As a measure of accountability for compliance with the use of personal data Executive Decree 285 establishes the figure of the Protection Officer (ODP) for public entities and recommended but not mandatory for the private sector. The ODP will perform his functions independently. Its functions will be to participate in a timely manner in matters related to data protection, inform and advise the responsible and the custodian, supervise compliance with the regulations, promote the training of persons who process data, among others.

Both the personal data controller and the custodian of the database that transfers data, must keep a record of the databases and must be available to the National Authority for Transparency and Access to Information (ANTAI) when required, the database must even identify and state the period of all persons entering personal data within fifteen working days from the start of such activity.

Those data controllers and/or custodians of databases, as well as all persons involved in any phase of data processing, shall be subject to the duty of secrecy or confidentiality. This obligation shall be additional to professional secrecy, shall apply for the entire duration of the processing and shall be kept even after the employee's or official's relationship had terminated.

The data controllers and/or custodians of the databases must guarantee the compliance and are subject to the control and supervision of ANTAI through the Directorate for the Protection of Personal Data.

When is authorization not required for the processing of personal data?

Authorization is not required for the processing of personal data in the following cases:

1. **Sources in the public domain**
2. **Those collected by the public administration**
3. **Those of an economic, financial or banking nature with prior consent.**
4. **Lists of persons in organizations, professions**
5. **Those within an established business relationship**
6. **Processing of private organizations for use by associates**
7. **Medical or health emergency**
8. **Historical, statistical or scientific purposes.**

Non-waivable rights of the personal data subjects

Like many countries, our country recognizes ARCO rights, i.e. the Right of Access, Right of Rectification, Right of Cancellation, Right of Opposition and Right to Portability.

Our Law allows the personal data subject to request his information to the data controllers, and it must be provided within ten working days. The provision of information, its modification, blocking or deletion shall be free of charge.

Data must be amended when it is erroneous, inaccurate, misleading or incomplete within five working days following the request for amendment. Whoever is responsible must proceed when there is evidence of inaccuracy of the data.
If the data controller does not decide on the data subject's request within the term, the data subject may appeal to the National Authority for Transparency and Access to Information (ANTAI). In cases subject to special laws, to the regulator or regulatory authority. In the event that the sanctions for the offenses committed are not found in such laws, the regulator shall apply the sanctions established in this Law, without prejudice that the data subject may also file a complaint before the National Authority of Transparency and Access to Information (ANTAI) for the corresponding sanctions to be applied and to the courts of justice to request compensation for pecuniary and/or moral damages.

The data controller or the custodian of the database may not transfer or communicate in any case the data relating to a person after seven years have elapsed, since the legal obligation to keep it was extinguished, unless another period is agreed. These data have to be deleted or re-establish a relationship with the data subject and explain why the data are still kept and what the new purpose is.

The transfer of data is lawful if it meets at least one of the following conditions:

1. **Data subject's consent.**
2. **That the receiving country or agency provides a better level of protection.**
3. **That it is provided for in a Law or Treaty.**
4. **For prevention of medical diagnosis.**
5. **That is made to any company of the same economic group provided that they are not used for different purposes.**
6. **By virtue of a contract.**
7. **It is necessary for the safeguarding of a public interest.**
8. **For the recognition or defense of a right in a judicial proceeding.**
9. **For the maintenance or fulfillment of a legal relationship.**
10. **Required for bank or stock exchange transfers.**
11. **For international cooperation between intelligence agencies in the fight against organized crime, terrorism, drug trafficking, etc.**
12. **That the controller transferring the data adopts binding self-regulatory mechanisms.**
13. **In case of contractual clauses.**

Advisory Council and Supervisory Authority

A Council for the Protection of Personal Data is created as an advisory body on the matter which advises the National Authority for Transparency and Access to Information (ANTAI), recommends public policies related to the matter, evaluates the cases filed, provides recommendations and develops its internal regulations.

The National Authority for Transparency and Access to Information (ANTAI), through a Directorate created to deal with this matter, is empowered to sanction the data controller, as well as the database custodian ascertained to have infringed the rights of the personal data subject. The Executive Decree establishes the criteria for the graduation of the sanctions, which will depend on the intentionality, recidivism, nature and amount of the damages caused, rights affectation, adoption of corrective measures, among others.

The decisions of the Directorate may be challenged through an appeal for reconsideration and are appealed before the Director of the National Authority for Transparency and Access to Information

(ANTAI).

Infringements and Penalties

The Authority may fix penalties from B/.1,000.00 to B/.10,000.00.
Infringements are classified as minor, serious or very serious:

- **Minor: failure to submit or inform the authority of the information within the deadline and may lead to a citation from the authority.**
- **Serious: carrying out the processing without the consent of the data subject, infringement of the established principles and guarantees, breach the confidentiality commitment, restricting ARCO rights, breach the duty to inform the data subject of the data processing, storing or archiving data without security conditions, failing to comply with repeated requests and remarks of the authority, the above can lead to a fine of B/.1,000 to B/.10,000, depending on its proportionality.**
- **Very serious: to collect personal data in a fraudulent manner, not to observe the regulations, not to suspend the processing when previously requested by the authority, to store or transfer personal data internationally and to recidivate in serious offenses, which may lead to the closure of the database records and the corresponding fine, and even the suspension and disqualification of the storage and/or processing activity.**

Lastly, the Executive Decree establishes terms for the statute of limitations of the action and the penalty:

- **Statute of limitations of the action:**
  1. **Minor infringements within a period of 1 year.**
  2. **Serious infringements within a period of 3 years.**
  3. **Very serious infringements within a period of 5 years.**

- **Prescription of penalty:**
  1. **Minor penalties within a period of 3 year.**
  2. **Serious penalties within a period of 5 year.**
  3. **Very serious penalties has no statute of limitations.**

Law 81 of March 26, 2019, which was published in Official Gazette No. 28743-A, entered into full force on March 29, 2021 and Executive Decree 285 of May 28, 2021 entered into full force upon its enactment on May 28, 2021 and it was published in Official Gazette No. 29296-A.

Written by: Mariela de la Guardia Oteiza
July 1st, 2021