DATA PROTECTION LAWS OF THE WORLD

Panama

PANAMA

Last modified 28 January 2024

LAW

Panama has taken significant legislative steps in regulating data protection. Law No. 81 of March 26, 2019, supplemented by Executive Decree No. 285 of May 28th, 2021 (together the ***Ley sobre Protección de Datos Personales***; the ‘Data Protection Law’), regulates data protection in the Republic of Panama. The Data Protection Law govern the following:

- The principles, rights, obligations, and procedures applicable to the protection of personal data in Panama
- The individuals or legal entities, whether private or public, who are subject to the Data Protection Law, as well as those entities that are classified as “regulated subjects” (*ie*, banks, insurance companies, telecommunication providers, etc.)
- The data subject’s right to access, rectification, cancellation, opposition, and portability
- The fines and penalties applicable to those who violate an individual’s right to data protection

As mandated by the Data Protection Law, it’s expected that several sectoral laws will be modified to include certain data protection terms, such as Rule No. 1-2022, dated February 24th, 2022, which includes special guidelines for the protection of data processed by banks established by the Superintendency of Banks.

In addition to the Data Protection Law, the following general rules govern data protection:

- The Constitution
- The Criminal Code

DEFINITIONS

Definition of personal data

Personal Data is defined by the Data Protection Law as the personal information of an individual that identifies him or makes him identifiable.

Definition of sensitive data

Sensitive Data is defined by the Data Protection Law as the one that refers to the intimate sphere of its owner, or whose improper use could give rise to discrimination or entail a serious risk for the individual, such as information about the racial or ethnic origin, beliefs or religious, philosophical and moral convictions; union membership; political opinions; data related to health, life, sexual preference or orientation, genetic data or biometric data, among others, subject to regulation and aimed at identifying univocally a natural person.

NATIONAL DATA PROTECTION AUTHORITY

The Data Protection Regulations are enforced and overseen by:

Panama’s National Authority of Transparency and Access to Information (‘ANTA’) through the Directorate for the Protection of Personal Data
(Autoridad Nacional de Transparencia y Acceso a la Información)
Del Prado Avenue, Bulding 713, Balboa, Ancon, Panama
T (507) 527-9270 to 74
Protecciondedatos@antai.gob.pa

The National Authority for Government Innovation
(Autoridad Nacional para la Innovación Gubernamental) in matters related to Information and Communications Technology (ICT) supporting ANTAI
61st Street and Ricardo Arango Avenue, Sucre, Arias y Reyes Bulding, Floor 3
Obarrio, Panama
T (507) 520-7400
administracion@innovacion.gob.pa

REGISTRATION

The Data Protection Law does not include any registration or notification requirement prior to the processing of data before Panama’s National Authority of Transparency and Access to Information (“ANTAI”). What it does require, is for data controller’s (known in Panama as the “Responsible of the data treatment”) (*Responsable del tratamiento de datos* in Spanish) to have the data subject’s consent to the processing of said personal data, as a general principle.

DATA PROTECTION OFFICERS

Appointment of a data protection officer is optional under the Data Protection Law for private companies, but required for governmental entities. According to Rule No. 1-2022, banks established in the Republic of Panama are also required to appoint a data protection officer.

COLLECTION & PROCESSING

In Panama, personal information is protected at the constitutional level. The Constitution provides that every person has a right of access to his / her personal information contained in data banks or public or private registries and to request their correction and protection, as well as their deletion in accordance with the provisions of the law. It also states that such information may only be collected for specific purposes, subject to the consent of the person in question, or by order of a competent authority based on the provisions of the law. The disclosure of personal information without consent is also prohibited by the Panamanian Criminal Code. Criminal penalties apply to the disclosure of personal information where the disclosure causes harm to the affected individual.

As per the Data Protection Law, the data subject must consent to the processing of his data and be duly informed of the proposed use of his personal data. Prior to obtaining consent, the data controller must provide the data subject with certain basic information, such as for example: the data controller’s identity and contact information, the proposed use of the data, the data subject's right to revoke consent, recipients of the personal data where the data will be transferred abroad, how long the data will be kept. The consent must be obtained in such a way that allows its traceability with documentation, whether electronic or by any other means that are suitable to the medium of the particular case and can be revoked, without retroactive effect. If the consent of the data subject is given in the context of a sworn statement that also refers to other matters, the consent request will be presented in such a way that it is clearly distinguished from the others, in a comprehensible and easily accessible manner, using a clear and simple language, which will not be binding in any part of the declaration that constitutes an infraction of the Law and its regulation.

The Data Protection Law allows processing of personal data without the data subject's consent, if at least one of the following conditions is met:

- If necessary within an established contrctual relationship

- If needed to fullfil a legal obligation
- If authorized by a sectorial law or regulation
- If necessary to protect the vital interests of the data subject or another individual
- If required by a public entity within the exercise of the functions of the Public Administration in the field of their competences
- If necessary for the satisfaction of legitimate interests pursued by the data controller or by a third party, provided that such interests do not prevail over the interests or fundamental rights and freedoms of the interested party that require the protection of personal data, in particular when the interested party is a minor or a person with a disability
- If the personal data is derived or collected from public domain sources or accessible in public media
- If the personal data is contained in lists related to a category of people that is limited to genera background, such as the participation of a natural person to an organization, their profession or activity, their educational titles, address or date of birth
- If the processing of personal data by private organizations is for the exclusive use of their associates and the entities to which they are affiliated, for statistical purposes, for pricing or others of general benefit to them
- If the processing of information is authorized by law for historical, statistical or scientific purposes

TRANSFER

With regards to personal data, the Constitution states that individuals must give their consent in order for their personal data to be transferred or processed in any way.

The Data Protection Law clearly states that in no case may the data controller or the data processor transfer or communicate the data related to an identified or identifiable person, after seven years have elapsed since the legal obligation of kept said personal data, unless the data subject expressly requests otherwise. Data controllers can only transfer personal data when they have the prior, informed and unequivocal consent of the data subject, with the exceptions included in the Data Protection Law.

Additionally, the Data Protection Law allows for cross-border transfer of personal data, if any of the following conditions are met:

- With the data subject’s consent
- The recipient country or international or supranational organization provides an equivalent or a higher level of protection
- If necessary for the prevention or medical diagnosis, the provision of health care, medical treatment or the management of health services
- If made to any company of the same economic group of the data controller, provided that the personal data is not used for different purposes that originated their collection
- If necessary under an executed or soon to be executed contract in unambiguous interest of the data subject, by the controller and a third party
- If necessary or legally required for the safeguard of a public interest or for the legal representation of the data subject or administration of justice
- If necessary for the recognition, exercise or defense of a right in a judicial process, or in cases of international judicial collaboration
- If necessary for the maintenance or fulfilment of a legal relationship between the data controller and the data subject
- If required to conclude bank or stock transfers, relative to the respective transactions and according to the legislation that is applicable to them
- If the objective is international cooperation among intelligence agencies for the fight against organized crime, terrorism, money laundering, computer crimes, child pornography and drug trafficking
- If the data controller responsible for the data transfer and the recipient adopt mechanisms of binding self-regulation, provided that they are in accordance with the provisions of the Data Protection Law
- If carried out within the framework of contractual clauses that contain mechanisms for protection of personal data in accordance with the provisions set out in the Data Protection Law, provided that the data subject is a party

In all cases, the data controller responsible for the data transfer and the recipient of the personal data will be responsible for the legality of the data processing.

SECURITY

In matters of security, data controllers must establish protocols, safe management and transfer processes and procedures to protect the rights of data subjects under the precepts of this Law. The minimum requirements that must be contained in the privacy policies, protocols and procedures for data processing and transfer that must be met by the data controller, will be issued by the regulator of each sector in accordance with this law.

In the event that the treatment or transfer of personal data is carried out through the Internet or any other electronic, digital or physical means, the data controller or the data processor, whomever applies must comply with the standard certifications, protocols, technical and management measures appropriate to preserve the security in their systems or networks, in order to guarantee the levels of protection of personal data as established by the Data Protection Law.

BREACH NOTIFICATION

If a data controller becomes aware of a security breach, defined as any damage, loss, alteration, destruction, access and in general, any illegal or unauthorized use of personal data, even where such occurs accidentally, that represents a risk for the data’s protection, the data controller must immediately notify such breach to the regulator and affected data subjects, within 72 hours. Data processors also have the responsibility to immediately notify the data controller of any security breach.

The data controller must document any security breach and include at a minimum the following information: i) date of occurrence, ii) the reasons of the breach, iii) the facts related to the situation and its effects, iv) the definitive corrective measures immediately implemented.

The regulator will verify the seriousness of the incident and if required to safeguard the rights of the data subjects, order that the data controller adopt measures, such as the wide dissemination of the incident in the media and/or measures to reverse or mitigate the effects of the incident.

Operators that manage public networks or that provide communication services available to the public shall guarantee in the exercise of their activity the protection of personal data in accordance with the Data Protection Law. They must also adopt the appropriate technical and management measures to preserve the security in the operation of the network or in the provision of their services, in order to guarantee the levels of protection for the personal data that are required by the Data Protection Law, as well as certifications, protocols, standards and other measures established by the respective authorities.

In case there is a particular affectation or violation of the security of the network communication system, the operator that manages such network or provides the communication service will inform the data subjects about said affectation and about the measures to adopt.

ENFORCEMENT

ANTAI, through a Directorate created for this purpose, is empowered to sanction data controllers or data processors that are found to have infringed data subject’s rights, in the course of an investigation of complaints filed and proven against them. Sanctions will be subjected to ANTAI, which will set the amounts of the sanctions applicable to the respective violations, according to the seriousness of them, which they will establish from a thousand US dollars (USD 1,000.00) up to ten thousand US dollars (USD 10,000.00).

ELECTRONIC MARKETING

Law No. 51 of July 22nd, 2008, as amended by Law 82 of November 9, 2012 (“Law 51”), and its bylaws establish in the Executive Decree No. 40 of May 19, 2009 (“Decree 40”) and Executive Decree No. 684 of October 18, 2013 (“Decree 684”) regulate the electronic documents and electronic signatures, as well as the rendering of data storage services, and the certification of the electronic signatures, and adopts other dispositions for the development of e-commerce. It establishes that Companies that sell goods or services in Panama, through the Internet, will be subject to the other provisions of national legislation that apply to them based on the activity they develop, regardless of the use of electronic means for their realization.

With respect to email advertising, Panamanian law requires that all such emails:

- State that they are commercial communications
- Include the name of the sender
- Set forth the mechanism through which the recipient may choose not to receive any further communications from the particular sender

These requirements apply to other promotional offers as well.

Further, although opt-out tools are not prohibited, the client's initial opt-in consent is specifically required if an entity wishes to use the client's email for advertising purposes. Further, although no specific prohibition has been enacted with respect to the use of information for online advertising, obtaining the customer's consent is always preferable.

ONLINE PRIVACY

The existing regulatory framework does not yet address location data, cookies, local storage objects or other similar data-gathering tools.

KEY CONTACTS

Galindo, Arias & Lopez
gala.com.pa/

Ramon Ricardo Arias Porras
Galindo, Arias & Lopez
T +507 303 0303
rrarias@gala.com.pa

Beatriz Cabal
Galindo, Arias & Lopez
T +507 303 0303
becabal@gala.com.pa

Jose Luis Sosa
Galindo, Arias & Lopez
T +507 303 0303
jsosa@gala.com.pa

DATA PRIVACY TOOL

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