DATA PROTECTION LAWS OF THE WORLD

Ecuador

ECUADOR

Last modified 26 January 2023

LAW

Constitution

The Constitution of Ecuador in its article 66, referring to the personal freedom rights of individuals in the Ecuadorian territory, the State recognizes and guarantees in section 19: "*The right to the protection of personal data, which includes the access and decision on information and data of this nature, as well as its corresponding protection. The collection, filing, processing, distribution or dissemination of such data or information shall require the authorization of the owner or the mandate of the law.*"

Article 92 gives the right to every person to be informed of and have access to information, documents, genetic data, personal data banks or files and reports on him/herself and his/her assets, contained in files and/or databases of public or private entities, in material and/or electronic support. The interested individual has the right to be informed of the use, purpose, origin and destination of his personal data and the time of permanence of the file of the same.

The responsible parties of the personal data banks or files may disseminate the information filed with the authorization of its owner, before which the owner of the personal data may request from the responsible party access to the file free of charge, as well as the updating, rectification, deletion or cancellation of his personal data.

In the case of sensitive data, the collection and storage must be authorized by law or by the owner. The adoption of the necessary security measures will be required. If the request is not complied with, the affected individual may appeal to the judge and may sue for the damages caused.

Personal Data Protection Organic Law

Since May 26, 2021, Ecuador adopted the Personal Data Protection Organic Law, whose main purpose is to guarantee the right to the protection of personal data, that includes the access and decision on information and personal data, as well as its corresponding protection. The law mainly refers to the conditions that must be verified for the legitimate treatment of personal data. It also refers to the ways through which the owner of the personal data may express his or her consent to the processing of his or her data.

Regulation to the Personal Data Protection Organic Law

On November 13, 2021, the President of Ecuador issued the Regulation to the Personal Data Protection Organic Law, whose main purpose is to develop aspects already provided for in the law. Among the most important aspects of the Regulation are the specifications for requests related to the exercise of data protection rights, the notification of security breaches, data processing agreements, the data protection officer, and international data transfers.

DEFINITIONS

Definition of Personal Data

The Ecuadorian data protection regime distinguishes between personal data and a sub-category of sensitive personal data, depending on the information and the harmful effects caused by its unlawful use.

Article 4 of the Organic Law on Personal Data Protection defines personal information as the information that identifies or makes identifiable a specific individual, directly or indirectly.

Definition of Sensitive Personal Data

Article 4 of the Organic Law on Personal Data Protection defines sensitive personal data as information related to: ethnicity, gender identity, cultural identity, religion, ideology, political affiliation, judicial background, immigration status, sexual orientation, health, biometric data, genetic data and those whose improper processing may give rise to discrimination, infringe or may infringe fundamental rights and freedoms.

In application of article 26 of the Organic Law for the Protection of Personal Data, the processing of sensitive personal data is prohibited unless one of the following circumstances applies:

- The owner has given his explicit consent to the processing of his personal data, clearly specifying its purposes.
- The processing is necessary for the fulfilment of obligations and the exercise of specific rights of the controller or the holder in the field of labor law and social security and protection.
- The processing is necessary to protect the vital interests of the data owner or another individual, in the event that the data owner is physically or legally incapable of giving his/her consent.
- The processing relates to personal data which the data owner has manifestly made public.
- The processing is carried out by order of a judicial authority.
- The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, which must be proportionate to the aim pursued, respect in substance the right to data protection and provide for adequate and specific measures to protect the interests and fundamental rights of the owner.
- When the processing of health data is subject to the provisions contained in this Law.

Definition of Large-Scale Data Processing

Article 4 of the Regulation to the Organic Law on Personal Data Protection defines large-scale data processing activities as the following:

- The processing of patients’ data in the normal course of activity of a hospital or health institution.
- The processing of travel data of persons using public transportation systems.
- The processing of real-time geolocation data of customers by a data controller specialized in the provision of these services.
- The processing of customer data in the normal course of business of an insurance company, brokers, agent or financial institution.
- The processing of personal data for behavioral advertising by a search engine.
- The processing of data (content, traffic, location) by telephone or Internet service providers.

Definition of Joint Controllers

Article 37 of the Regulation to the Organic Law on Personal Data Protection specifies that when two or more controllers jointly determine the same purposes of and means for the processing of personal data, they shall be considered joint controllers, who shall define their respective tasks and responsibilities regarding data protection in a transparent manner by means of a contract, insofar as these are not already defined by the law.

NATIONAL DATA PROTECTION AUTHORITY

Pursuant to the provisions of Articles 76 and 77 of the Organic Law for the Protection of Personal Data, the Authority for the Protection of Personal Data will be the Superintendence of Data Protection, which once constituted will act as the control and surveillance body in charge of guaranteeing all citizens the protection of their personal data, and of carrying out all necessary actions to ensure that the principles, rights, guarantees and procedures provided for in the Law and its implementing regulations are respected.

REGISTRATION

Article 51 of the Organic Law for the Protection of Personal Data creates the National Registry for the Protection of Personal Data, a registry that will be under the responsibility and custody of the Superintendence of Data Protection as the competent national protection authority. The person responsible for the processing of personal data shall report and keep updated the information before the Personal Data Protection Authority, on the following:

- Identification of the database treatment.
- Name, legal domicile, and contact details of the responsible and in charge individual of the processing of personal data. Characteristics and purpose of the personal data treatment.
- Nature of the personal data treatment.
- Identification, name, legal domicile, and contact details of the recipients of the personal data, including processors and third parties.
- Description of the utilized method of interrelation of the recorded information.
- Description of the means used to implement the principles, rights and obligations contained in the present Law and specialized regulations for the data protection.
- Requirements and/or technical and physical, organizational, and legal administrative tools implemented to guarantee the security and protection of personal data.
- Data retention time.

Article 87 of the Regulation to the Organic Law for the Protection of Personal Data creates the Registry of Defaulting Controllers and Processors, under the responsibility and custody of the Superintendence of Data Protection, exclusively for purposes of statistics, prevention and training.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer (DPO) if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities, provided that it does not give rise to a conflict of interests.

DPOs must exercise their duties in a "*professional manner*" for the controller or processor, though it is possible to outsource the DPO role to a service provider.

The DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalized for performing those tasks.

The specific tasks of the DPO include:

- to inform and advise on compliance with the Personal Data Protection Organic Law;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;

- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the Superintendence of Data Protection.

COLLECTION & PROCESSING

Our Personal Data Protection Law defines data processing as any operation or set of operations performed on personal data, whether by automated, partially automated or non-automated technical procedures, such as: collection, compilation, obtaining, recording, organization, structuring, conservation, custody, adaptation, modification, elimination, indexing, extraction, consultation, processing, use, possession, exploitation, distribution, assignment, communication or transfer, or any other form of enabling access, matching, interconnection, limitation, suppression, destruction and, in general, any use of personal data.

The processing of personal data shall be legitimate and lawful if any of the following conditions are met:

1. By consent of the owner for the treatment of his personal data, for a specific purpose or purposes.
2. That it is carried out by the data controller in compliance with a legal obligation.
3. That it is carried out by the data controller, by court order, in compliance with the principles of the present Law.
4. That the treatment of personal data is based on the fulfilment of a mission carried out in the public interest or in the exercise of public powers conferred on the controller, derived from a competence attributed by a regulation with the rank of law, subject to compliance with the international human rights standards applicable to the matter, to compliance with the principles of this Law and to the criteria of legality, proportionality, and necessity.
5. For the execution of pre-contractual measures at the request of the owner or for the fulfilment of contractual obligations pursued by the person responsible for the processing of personal data, person in charge of the processing of personal data or by a legally authorized third party.
6. To protect vital interests of the data subject or another natural person, such as his or her life, health, or integrity.
7. For the processing of personal data contained in publicly accessible databases; or
8. To satisfy a legitimate interest of the data controller or of a third party, provided that the interest or fundamental rights of the data subjects do not prevail under the provisions of this regulation.

Personal data may be processed and communicated when there is an explicit consent of the owner to do so. The consent will be valid when the expression of will is:

1. Free, that is, when it is absent of any consent flaws.
2. Specific, in terms of the concrete determination of the means and purposes of the data treatment.
3. Informed, so that it complies with the transparency principle.
4. Unambiguous, so that there is no doubt as to the scope of the authorization granted by the owner.

The consent of the data owner must reflect, in an unequivocal manner, his or her acceptance in relation to the processing of personal data. Silence or inaction, by itself, does not imply the consent of the data owner.

Consent may be revoked at any time without the need for a justification, for which purpose the data controller shall establish mechanisms that guarantee speed, efficiency, effectiveness, and gratuity, as well as a simple procedure, similar to the procedure by which the consent was obtained.

The processing carried out prior to the revocation of consent is lawful since it does not have retroactive effects.

When the data treatment is intended to be based on the consent of the data owner for a plurality of purposes, it will be necessary to state that such consent is obtained for all of them.

Unless proven otherwise, it shall be legitimate and lawful to process data intended to provide information on the financial or credit solvency, including information relating to the fulfilment or non-fulfilment of obligations of a commercial or credit nature that enable an assessment on the general conclusion of business, the commercial conduct or the payment capacity of the owner of the information, where such information is obtained from publicly available sources or from information provided by the creditor. Such data may be used only for the purpose of analysis and will not be communicated or disseminated, nor may they be used for any secondary purpose.

The protection of personal credit data shall be subject to the provisions of this Law, the specialized legislation on the subject and other regulations issued by the Personal Data Protection Authority.

Notwithstanding the foregoing, in no case may credit data relating to obligations of an economic, financial, banking or commercial nature be communicated after five years have elapsed since the obligation to which they refer has become due.

Pursuant to the provisions of article 29 of the Organic Law on Personal Data Protection, the holders of Credit Data have the following rights:

1. To have personal access to the information of which they are owners.
2. That the credit report allows them to know the condition of their credit history clearly and precisely; and,
3. That the sources of information update, rectify or eliminate information that is unlawful, false, inaccurate, erroneous, incomplete, or outdated.

Regarding the right of access by the Credit Data Owner, this shall be free of charge, as many times as required, with respect to the information registered about him/herself before the credit reference service providers and through the following mechanisms:

1. Direct observation through displays that the credit reference service providers will make available to such owners; and
2. Delivery of printed copies of the reports for the Credit Data Subject to verify the truthfulness and accuracy of their content, without being used for credit or commercial purposes.

Regarding the rights of updating, rectification or deletion, the Data Owner may demand these rights from the information sources by means of a written request. The information sources, within fifteen days from the date the request is submitted, shall resolve it by admitting or rejecting it with reasons. The Credit Data Owner has the right to request the credit reference service providers to indicate in the credit reports they issue, while the review process continues, that the information subject to the request is being reviewed at the owner's request.

TRANSFER

Personal data may be transferred or communicated to third parties when it is carried out for the fulfillment of purposes directly related to the legitimate functions of the controller and the recipient, when the transfer is configured within one of the grounds of legitimacy and also has the consent of the owner.

It shall be understood that the consent is informed when for the transfer or communication of personal data the data controller has provided sufficient information to the data subject to enable him/her to know the purpose for which his/her data will be used and the type of activity of the third party to whom it is intended to transfer or communicate such data.

It will not be considered a transfer or communication in the event that the processor or a third-party accesses personal data for the provision of a service to the controller of personal data. The third party who has legitimately accessed personal data in these considerations shall be considered the processor.

The treatment of personal data carried out by the processor or by a third party must be regulated by a contract, in which it is clearly and precisely established that the personal data processor or the third party will only process the information in accordance with the instructions of the owner and will not use it for purposes other than those indicated in the contract, nor transfer or communicate it even for storage to other persons.

The contract between controller and processor must contain provisions specifying at least the following:

- Object
- Duration
- Nature
- Purposes of the processing activities
- Categories of personal data
- Data owners
- Obligations and responsibilities of the processor

Once the contractual performance has been fulfilled, the personal data shall be destroyed or returned to the data controller under the supervision of the Personal Data Protection Authority.

The processor or third party shall be liable for any infringements arising from non-compliance with the conditions of personal data processing set forth in this Law.

The processor may engage a third party to supplement the provision of a service to the controller of personal data, provided that this is expressly stated in the processing agreement. Otherwise, it shall require the written authorization of the controller for the subcontracting.

SECURITY

Data controllers or the individual in charge of the treatment of personal data must abide by the principle of personal data security, for which it must consider the categories and volume of personal data, the state of the art, best comprehensive security practices. and the costs of application according to the nature, scope, context, and purposes of the treatment, as well as identifying the probability of risks.

Data controllers or the individual in charge of the treatment, must implement a process of verification, evaluation and continuous and permanent assessment of the efficiency, effectiveness, and effectiveness of the measures of a technical, organizational and any other nature, implemented to guarantee and improve the security of the processing of personal data.

The individual in charge of the treatment of personal data must demonstrate that the measures adopted and implemented adequately mitigate the risks identified.

Among other measures, the following may be included:

- Anonymization, pseudonymization or encryption measures of personal data.
- Measures aimed at maintaining the confidentiality, integrity and permanent availability of the systems and services for the processing of personal data and access to personal data, quickly in case of incidents.
- Measures aimed at improving technical, physical, administrative, and legal residence.
- Those responsible and in charge of the treatment of personal data, may avail themselves of international standards for adequate risk management focused on the protection of rights and freedoms, as well as for the implementation and management of information security systems or codes of conduct. recognized and authorized by the Personal Data Protection Authority.

BREACH NOTIFICATION

Mandatory breach notification

Data controllers or the individual in charge of the treatment of personal data must notify the breach of personal security data to the Personal Data Protection Authority and the Telecommunication Control Agency, as soon as possible, and at the latest within a term of five (5) days after the occurred breach incident, unless it is unlikely that said breach of security constitutes a risk to the rights and freedoms of its individual owners. If the notification to the Data Protection Authority does not take place within five (5) days, it must be accompanied by an indication of the reasons for the delay.

According to the Regulation to the Personal Data Protection Organic Law, the following circumstances are deemed a risk to the rights and freedoms of persons:

1. When the data have been destroyed, no longer exist or are not available in a form that is useful to the data controller.
2. When the personal data have been altered, corrupted or are no longer complete.
3. When the controller has lost control or access to the data, or the data is no longer in its possession.
4. When the processing has not been authorized or is unlawful, which includes the disclosure of personal data or access by recipients or third parties who are not authorized to receive or have access to the data, or any other form of processing that is executed contrary to the provisions of the Law.

The data breach notification must provide for the following aspects:

- The nature and type of breach.
- Data owners or interested parties affected.
- Breached systems.
- Presumed cause of the breach.
- Volume and types of compromised or exposed data.
- Response and mitigation measures.
- Risk assessment for the rights and freedoms of the data owners.

Data controllers or the individual in charge of the treatment of personal data must notify the person in charge of any violation of the security of personal data as soon as possible, and at the latest within a term of two (2) days from the date on which he becomes aware of it.

The person responsible for the treatment must notify the owner of the breach of personal data security without delay when it entails a risk to their fundamental rights and individual freedoms, within a term of three (3) days from the date on which they became aware of the risk.

ENFORCEMENT

In case of non-compliance with the provisions set forth in the Law, its regulations, guidelines and directives and regulations issued by the Personal Data Protection Authority, the Personal Data Protection Authority shall issue corrective measures with the purpose of preventing the infringement from continuing and the conduct from occurring again, without prejudice to the application of the corresponding administrative sanctions.

Corrective measures may consist of, among others:

1. The cease of the treatment, under certain conditions or deadlines.
2. The disposal of the data; and,
3. The imposition of technical, legal, organizational or administrative measures to ensure proper handling of personal data.

The Personal Data Protection Authority, within the framework of this Law, will dictate, for each case; the corrective measures, which are classified into minor infringements and serious infringements.

Penalties for minor infringements will impose an administrative sanction of a fine between 0.1% and 0.7% calculated on the turnover corresponding to the financial year immediately prior to the imposition of the fine.

Penalties for serious infringements will impose an administrative sanction of a fine between 0.7% and 1% calculated on the turnover corresponding to the financial year immediately prior to the imposition of the fine.

In addition to the previously mentioned fines, the Personal Data Protection Authority may apply provisional measures of protection or precautionary measures such as:

1. Seizure.
2. Withholding.
3. Sale Prohibitions.
4. Shutdown of establishments.
5. Activity suspension.
6. Decommissioning of products, documents, or other goods.
7. Eviction of individuals.

ELECTRONIC MARKETING

There is no specific regulation regarding data treatment on electronic marketing, to the extent that it may involve processing of personal data, is subject to the general rules applicable to such data, such as valid data subject consent, adequate privacy notices as to use and disclosure of personal data and data subject rights.

ONLINE PRIVACY

There is no specific regulation regarding processing of personal data online, therefore, this kind of processing shall be ruled by the Personal Data Protection Organic Law.

Personal data must not be available online unless there are adequate security measures to ensure that access by any unauthorized user is restricted.

The use of cookies in web pages is forbidden unless the data subject has given an authorization for usage which may be obtained by a pop-up informing the user about the privacy policy and the way to disable cookies. All the other tracking systems need proper authorization from the data subject.

Unauthorized collection of personal data will be subject to the general rules applicable to such data.

KEY CONTACTS

Bustamante Fabara
bustamantefabara.com/

José Rafael Bustamante Crespo
Partner
Bustamante Fabara
jrbc@bustamantefabara.com

Gino Ivich Jijón
Associate
Bustamante Fabara
T +593998546947
givich@bustamantefabara.com

DATA PRIVACY TOOL

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