

Jun 2021

Ecuador: Overview of the data protection law

On 26 May 2021, the Organic Law on the Protection of Personal Data ('the Law') was finally published in the Official Registry, establishing in Ecuador a real legal framework for the exercise of data privacy rights recognised by the Constitution of the Republic of Ecuador 2008 ('the Constitution'). Jaime Mantilla Compte, Partner at Falconi Puig Abogados, provides an overview of the Law, including the rights provided under it, the effectiveness of its scope, and the provisions on data transfers, among others.



Jörg Henninger / Essential Collection / istockphoto.com

The Law is inspired by the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), which has an extraterritorial character and sets the data subject's consent as the basis for the collection, processing, communication, or transfer of data. Below is an overview of the content of the Law, which needs to be carefully reviewed by the companies and people doing business in Ecuador.

You have 7 out of 10 free articles left for this week. Sign up for a trial to access unlimited content.



Scope of application

The Law will be applied to the processing of personal data contained in any type of support, except for cases such as domestic activities, anonymised data, journalistic activities, data related to criminal offences, and data that identifies companies. As well as this, the names, functions, addresses, and phone numbers of professionals, public servants, companies' legal representatives, and shareholders are accessible to the public and available for processing, as long as they refer to such nature.

Territorial scope

Despite the nationality of the data processor or the place where data processing takes place, the Law will be applicable when the data owner resides in Ecuador and the processing activities are related to goods or services offered to the owner, regardless of if they are required to pay, or, when the activities are referred to control of their behaviour if it takes place in Ecuador.

Consent

Personal data may be processed and communicated if there is an expression of the data subject's will to do so. This consent must be free, specific, informed, and unequivocal. Consent can be revoked at any time without a cause, for which the controller must implement mechanisms to make it as easy as it is to give consent. The withdrawal of consent shall not affect the lawfulness of processing based on consent before it was withdrawn.

Also, it is important to point out that when data processing for a plurality of purposes is based on the consent of the data owner, it will be necessary for the data processor to record that the said consent is granted for all those purposes. Consent is not required in specific situations, such as legal mandate or court order, for complying a task of public interest or when data is available in a public database.

Principles

The Law is based on: the principles of legality, loyalty, transparency, purpose and proportionality of the data processing, retention, confidentiality, relevance, minimisation, quality, accuracy, and security of the data; the proactivity of the controller; the favourable application on behalf of the owner; and impartial control by an independent authority.

Rights of the data subject

Several rights are contemplated, including the possibility of accessing digital education within the national education system as well as to make public consults to the National Registry of Personal Data Protection ('NRPDP').

You have **7 out of 10** free articles left for
the week

Signup for a trial to access unlimited
content.

Start Trial



However, within the specific and relevant rights of the data subject, the Law lists the following:

- **Information:** means that the data owner has the right to be informed of the purpose, legal basis and types of the data processing, the time of conservation, the identity and information of the data controller and the data protection officer ('DPO'), the national or international transfers of data that are intend to be made, the possibility of revoking consent, and the mechanisms to exercise other rights such as access, elimination, rectification, opposition, and update. If the data is obtained directly from the subject, this information has to be provided at the same time as when it is collected. If the data is obtained from a source accessible to the public, the owner must be informed within the next 30 days or at the time of the first communication with him/her, whichever of the two circumstances occurs first.
- **Access:** means the possibility to know and obtain all personal data without justification from the controller free of charge, who must implement mechanisms to provide it within 15 days.
- **Rectification and update:** means to justifiably obtain the rectification and update of personal data from the controller who must provide it within 15 days, as well as inform it to the data recipient, if that would be the case.
- **Erasure:** means to obtain the elimination of the data by the controller within 15 days in specific situations such as the purpose for with the data was collected or processed has been complied, the data retention period has expired, consent has been revoked, the processing does not comply with the principles of the Law, or it is not actually required to comply the purpose for which the data was collected.
- **Opposition:** means objection to data processing when it is aimed to direct marketing or in the case when consent was not necessary for data processing but due to a personal specific situation it is justifiable.
- **Portability:** means to receive personal data provided to a controller, in a structured, commonly used, and machine-readable format and have the right to transmit such data to another controller.
- **Suspension:** means to suspend data processing if the subject disputes the accuracy of the data until the issue is cleared.
- **Right not to be the subject of a decision based solely or partially on automated valuations:** this includes profiling but is not applicable when the decision is required to comply to a contract between the subject and the controller, the subject has given express consent, or there is a legal mandate or court order.

Minors under 15 years old need their legal representative to provide consent and exercise their rights, meanwhile teenagers 15 and an older can grant consent by themselves and exercise their rights directly before the Personal Data Protection Authority ('the Authority') or before the person in charge of the personal data base of the treatment.

Special categories of data left for
the week

Signup for a trial to access unlimited
content.

Start Trial


The Law establishes certain specific rules for sensitive data, health, credit information, and rights of deceased people:

- **Sensitive data:** is defined as data related to ethnicity, gender identity, cultural identity, religion, ideology, political affiliation, judicial past, immigration status, sexual orientation, health, biometric data, genetic data, and those whose improper treatment may give rise to discrimination, and its processing is forbidden in general. Exemptions are made, such as with the explicit consent of the subject, where the data has become public, in situations of public interest, or due to a court order.
- **Personal data of deceased persons:** the successors can request the controller access, rectify, update, or eliminate the personal data of the deceased.
- **Credit data:** processing this data will be legitimate when it is obtained from publicly accessible sources or from information provided by the creditor. This data may be used only for analysis purposes and cannot be communicated or disseminated, nor have any secondary purpose. Credit data cannot be communicated after five years have elapsed since the obligation to which it refers was enforceable. The subject is entitled to access his or her credit data at any time and free of charge.
- **Health data:** the National Health System is allowed to collect and process this sensitive data and must guarantee its confidentiality. Consent will not be required in cases of public interest in the field of health. Health data that is processed, whenever possible, must be previously anonymised or pseudonymised.

Transfer of personal data

Personal data may be transferred or communicated to third parties when it is carried out for the fulfilment of purposes directly related to the legitimate functions of the controller and the recipient.

Consent from the owner is required except when the data is available in publicly accessible sources, there is a Court or Administrative Authority requirement, the personal data related to health is necessary to solve an emergency that involves the vital interests of its owner and he or she is prevented from granting this, or it is necessary to carry out epidemiological studies of public interest.

If the processor accesses personal data for the provision of a service to the controller, it will not be considered a transfer or communication, however, this has to be regulated by a contract establishing that the processor will only treat data in accordance with the instructions of the controller and that it will not be used for purposes other than those indicated in the contract, nor be transferred or communicated to other people.

Once the contractual provision has been fulfilled, the personal data must be destroyed or returned to the controller. The processor will be responsible for any infringement derived from the breach of the conditions

of treatment of personal data.
You have 7 out of 10 free articles left for the week

Signup for a trial to access unlimited content.

Start Trial


When the consent of the owner is required for personal data to be communicated to a third party, it can be revoked at any time, without the need for any justification.

In cases of international transfer of personal data, the Law limits this possibility to countries that have an adequate level of protection and comply with internationally recognised standards, for which the Authority will issue a specific resolution. It is possible to make international data transfers to a country, organisation, or international economic territory that has not been qualified by the Authority to have an adequate level of protection if the controller or the processor offers adequate guarantees for the owner through the appropriate legal instrument.

The Law also establishes the possibility for controllers or processors to submit before the Authority Binding Corporate Rules ('BCR') that comply with all the requirements of the Law and include the following:

- detailed statement of the subsidiaries belonging to the same business group, including the structure and contact details of the business group;
- details of the companies in charge of processing personal data, the categories of personal data to be used, as well as the type of treatment to be carried out and its purpose;
- acceptance of the controller, the processor, or any member of their business group, of their responsibility for any violation of the BCRs;
- mechanisms in which information is provided to the owner regarding the BCRs
- the functions of any designated DPO and any other person in charge of supervising compliance of the BCRs within the business group, as well as the mechanisms and processes for the supervision and processing of claims;
- details of the mechanisms established in the business group that allow the owner to effectively verify compliance of the BCRs, including audits and methods to provide corrective actions to protect the rights of the owner;
- the mechanisms to cooperate in a coordinated manner with the Authority and the controller; and
- a declaration and commitment of the controller to promote the protection of personal data among its employees with continuous training.

Security of personal data

The controller or the processor must implement a process of verification and permanent assessment of the efficiency of the technical and organisational measures implemented to guarantee and improve the security of the personal data processing. They must demonstrate that the measures adopted adequately mitigate the risks identified.

You have **7 out of 10** free articles left for the week

Signup for a trial to access unlimited content.

Start Trial


The Law lists, as way of example, several measures such as anonymisation, pseudonymisation, or encryption of personal data and in general all actions that help maintain the confidentiality and integrity of the systems for the processing personal data.

As well as this, the principles of Data Protection by Design and Default are contemplated, stating that the controller shall implement appropriate technical and organisational measures for ensuring: (i) compliance with all data protection obligations since the conception and design of the project; and (ii) that by default, only personal data which is necessary for each specific purpose of the processing is collected and processed.

The controller and the processor must take the appropriate measures to permanently evaluate, prevent, reduce, mitigate, and control risks, threats, and vulnerabilities, for which they must consider aspects such as the particularities of the treatment and the parties involved, the nature of the personal data, and the volume of data being processed.

Additionally, an impact assessment of personal data processing by the controller is mandatory in the following cases:

- systematic evaluation of personal aspects of natural persons that is based on an automated treatment, such as the elaboration of profiles, based on which decisions are made;
- large-scale processing of special categories of data or personal data relating to convictions and criminal offences; and
- systematic large-scale observation of a public access area.

This assessment must be carried out prior to start processing personal data and could be required at any time by the Authority.

The controller must notify a security breach to the Authority and the Agency for the Regulation and Control of Telecommunications as soon as possible and, at the latest, within five days of verifying it. Meanwhile, the processor must notify the controller within two days at the latest.

A notification to the data owner should be sent by the controller within three days of verification of the breach when it involves a risk to fundamental rights and individual freedoms. The Law expressly exempts the following cases, prior to evaluation from the Authority:

- the controller has adopted appropriate protection measures for the personal data affected by the security breach that can be shown to be effective and guarantee there is no risk to fundamental rights and individual freedoms of the owner; and
- when a disproportionate effort is required to do so, in which case the data controller must make a public communication through any means in which the owners are informed of the breach of personal content.

You have 7 out of 10 free articles left for the week. Signup for a trial to access unlimited content. **Start Trial**

data security.

Obligations of the controller and processor

The controller, and the processor when applicable, have the following specific obligations, besides from implementing appropriate mechanisms and tools to comply with the Law:

- apply and implement processes of verification, evaluation, and periodic assessment of the efficiency, requirements, mechanisms, and tools implemented;
- implement personal data protection policies adequate to the processing of personal data in each particular case;
- use risk analysis and management methodologies adapted to the particularities of the treatment and of the parties involved;
- carry out evaluations of adequacy to the level of security prior to processing of personal data;
- take technological, physical, administrative, organisational, and legal measures necessary to prevent, reduce, mitigate, and control the identified risks and breaches
- notify the Authority and the data owner of the security breaches according to the corresponding procedure;
- implement the principles of Data Protection by Design and by Default;
- sign confidentiality contracts with the processor and the personnel in charge of processing personal data or that have knowledge of the personal data;
- ensure that the processor offers sufficient mechanisms to guarantee the right to the protection of personal data;
- register and keep the NRPDP updated under direction of the Authority with the following information:
 - identification of the database or the data processing;
 - name, address, and contact details of the controller and the processor;
 - characteristics and purpose of the data processing;
 - nature of the personal data processed;
 - identification, name, address, and contact details of the recipients of the personal data;
 - how to interrelate the registered information;
 - means used to implement the principles, rights, and obligations contained in the law and regulations;
 - requirements and tools implemented to guarantee the security and protection of personal data; and
 - data retention time;
- appoint the DPO, when applicable, and comply with the following:
 - ensure that the participation of the DPO is appropriate and timely and must facilitate access to the personal data processing operations; and

You have 7 out of 10 free articles left for the week. [Sign up for a trial to access unlimited content.](#) **Start Trial** 

- train and update the DPO on the matter, in accordance with the technical regulations issued by the Authority; and
- not dismiss or sanction the DPO for the correct performance of their duties; and
- allow and collaborate with audits or inspections by an auditor accredited by the Authority, when required.

DPOs

A DPO must be appointed in the following cases:

- when the data processing is carried by entities of the public sector;
- when the activities of the controller or the processor require a permanent and systematised control due to its volume, nature, scope, or purposes of the processing, as established in the Law, its regulations, or directives from the Authority; and
- large-scale processing of special categories of data.

The functions of the DPO are mainly the following:

- advise the controller, its personnel, and the processor regarding the provisions of the law its regulations or directives that may be issued by the Authority, as well as monitoring its compliance;
- advise on risk analysis, impact assessments, and evaluation of security measures, and supervise their application; and
- cooperate with the Authority and act as a point of contact with said entity.

Additionally, the Law establishes the following special considerations regarding the DPO:

- a direct relationship with the highest executive and decision-making level controller and with the processor;
- an obligation to maintain the strictest confidentiality regarding the execution of his or her functions;
- that the data owner may contact the DPO directly; and
- that, as long as there is no conflict with the responsibilities established in the Law and its regulations, the DPO may perform other functions provided by controller or the processor.

Proactive responsibility

The controller and the processor can voluntarily adhere to codes of conduct, certifications, seals, or standard clauses, without this constituting an exemption from the responsibility to comply with the provisions of the Law, its regulations, and directives from the Authority.

You have 7 out of 10 free articles left for the week

Signup for a trial to access unlimited content.

Start Trial


Direct requests and administrative procedure

In accordance with the Constitution, the Law establishes that the data owner may, at any time, submit requirements, complaints, or claims directly to the controller, related to the exercise of his or her rights, the application of principles, and the fulfilment of obligations by the controller.

This request can be submitted free of charge by physical or digital means made available by the controller to the data owner. Once the request has been presented, the controller will have ten days to reply affirmatively or negatively, notify, and execute whatever corresponds.

If the controller does not respond to the request within the legal term or responds negatively, the data owner can file an administrative complaint before the Authority according to the proceeding established by the Organic Administrative Code, the Law, its regulations, and directives. Nevertheless, the owner may also file civil, criminal, and constitutional actions.

Also, the Authority may initiate, *ex officio* or at the request of the data owner, previous actions in order to know the circumstances of the specific case and decide on the pertinence of initiating and administrative the procedure.

Corrective measures

In case of non-compliance with the provisions of the Law, its regulations, or directives, the Authority will order corrective measures in order to prevent the offence from continuing and the conduct occurring again, without prejudice to the application of the corresponding administrative sanctions.

The Law lists as examples of corrective measures that can be order by the Authority ceasing the processing under certain conditions or deadlines, the deletion of data and the imposition of technical, legal, organisational, or administrative measures to guarantee an adequate processing of personal data.

For the application of corrective measures, the following rules will be followed:

- in case of a minor infringement, if the controller or the processor are recorded in the Registry of non-compliance, the Authority will directly apply a sanction stating it in the resolution together with the applicable corrective measures;
- in case of a serious infringement, the Authority will apply corrective measures in first instance. If the corrective measures are carried out late, partially, or defectively, the Authority will apply the corresponding sanction stating it in the resolution together with the applicable corrective measures; and
- in case of a very serious infringement, the Authority will directly activate the administrative sanctioning procedure, stating within the resolution the applicable corrective measures and the sanction corresponding to the offence committed.

You have **7 out of 10** free articles left for
the week
Infringements of the controller

Signup for a trial to access unlimited
content.

Start Trial


- Minor infringements:
 - not handling requests or complaints made by the owner, or not doing it within the legal term, or to unjustifiably deny them;
 - not implementing Data Protection by Design and by Default;
 - not keeping personal data protection policies available;
 - choosing a processor that does not offer sufficient guarantees; and
 - failure to comply with the corrective measures provided by the Authority; and
- Serious infringements:
 - failure to implement administrative, technical, and organisational measures to guarantee the processing of personal data;
 - use information or data for purposes other than those declared;
 - assign or communicate personal data without complying with the requirements and procedures established in the Law, its regulations, and directives;
 - not using risk analysis and management methodologies adapted to the nature of the personal data, the particularities of the treatment, and of the parties involved;
 - not carrying out impact evaluations on data processing in cases where it was necessary to do it;
 - failure to implement organisational or technical measures of any kind, necessary to prevent, reduce, mitigate, and control risks and security breaches;
 - failure to notify the Authority and the owner of security breaches that affect fundamental rights and individual freedom of the owner;
 - not signing contracts that include confidentiality clauses and adequate treatment of personal data with the processor and the personnel;
 - failure to keep the NRPDP updated and to record the mandatory information;
 - not designating the DPO when it corresponds;
 - not allowing audits or inspections by the auditor accredited by the Authority; and
 - failure to comply with the corrective measures or comply in a late, partial or defective manner, as long as the application of a sanction for minor infraction had preceded for said cause, and repeatedly incur in minor offences.

Infringements of the processor

- Minor infringements:
 - not collaborating with the controller to comply with the obligation to respond to requests from the owner;
 - not providing access to the controller to all the information regarding compliance of the obligations established in the Law, its regulations, or directives;

You have 7 out of 10 free articles left for the week

Signup for a trial to access unlimited content.

Start Trial 

- not allowing audits or inspections from the controller or another auditor authorised by the Authority; and
- failure to comply with the corrective measures provided by the Authority; and
- serious infringements:
 - processing or communicating personal data without observing the principles and rights established in the Law, its regulations, and directives;
 - failure to process personal data in accordance with the provisions of the contract signed with the controller;
 - not signing contracts that include confidentiality clauses and adequate treatment of personal data with the personnel;
 - failure to implement mechanisms to maintain the confidentiality, integrity, availability, and resilience of personal data;
 - failure to implement preventive and corrective measures to avoid security breaches;
 - not deleting the personal data transferred to the controller, once the order has been completed;
 - failure to comply with the corrective measures or comply in a late, partial, or defective manner, as long as the application of a sanction for minor infraction had preceded for said cause; and
 - failure to notify the controller of any security breach or doing so with unjustified delay.

Sanctioning regime

- Minor infringements:
 - public servants whose action or omission caused the infringement will be sanctioned with a fine of 1 to 10 basic salaries (approx. \$400), without prejudice to the extra-contractual liability of the State; and
 - if the controller or the processor is a private law entity or a public company, a fine of 0.1% to 0.7% of the amount of sales of the infringer prior to tax reduction corresponding to the fiscal year immediately prior to the imposition of the fine; and
- serious infringements:
 - public servants whose action or omission caused the infringement will be sanctioned with a fine of 10 to 20 basic salaries (approx. \$400), without prejudice to the extra-contractual liability of the State; and
 - if the controller or the processor is a private law entity or a public company, a fine of 0.7% to 1% of the amount of sales of the infringer prior to tax reduction corresponding to the fiscal year immediately prior to the imposition of the fine.

the Authority will establish the applicable fine based on the principle of proportionality and considering the

You have **7 out of 10** free articles left for the week following.

Signup for a trial to access unlimited content.

Start Trial 

- the intentionality, which will be established based on the conduct of the offender;
- repetition of the infringer;
- the nature of the damage caused, that is, the harmful consequences for the exercise of the right to the protection of personal data; and
- recurrence of the infringement.

The Authority

the Authority is the control and surveillance body in charge of guaranteeing to all citizens the protection of their personal data and of carrying out all the necessary actions for the compliance of the principles, rights, and procedures provided in the Law, for which it has the following main attributions:


- supervise the activities carried out by the controller and the processor;
- resolve the claims filed by the owner or those initiated *ex officio*;
- applying sanctions;
- carry out or delegate technical audits to personal data processing;
- issue general or technical regulations or directives;
- create and direct the NRPDP;
- respond to inquiries regarding the protection of personal data;
- issue resolutions authorising international transfer of data;
- keep a statistical record on security breaches and identify possible security measures for each of them;
- publish periodically a guide of regulations of personal data protection; and
- control and supervise the exercise of the right of personal data protection within the data processing carried out through the NRPDP.

The person in charge of the Authority will be the Superintendent of Data Protection who will be appointed in accordance with the Constitution, from a list referred to by the President of the Republic of Ecuador, and will perform his or her duties for a period of five years.

The Superintendent must be a professional of law, information systems, communications, or technologies, with a fourth level degree and experience of at least ten years with areas related to data protection.

General dispositions

The Law has several general dispositions at the end made to organise and facilitate its application, of which the most relevant are the following:

- The Registry of non-compliant controllers and processors will be created to keep record of their infringement **the week**. This Registry will be structured in the **Regulation** to be issued for the Law. 

- The exercise of the rights recognised in the Law may be demanded immediately by the data owner regardless of the entry into force of the sanctioning regime.
- The provisions related to corrective measures and the sanctioning regime will enter into force within a period of two years.
- Any data processing carried out prior to the entry into force of the Law must comply with its provisions within a period of two years.

Jaime Mantilla Compte Partner

jmantilla@falconipuig.com

Falconi Puig Abogados, Quito

You have **7 out of 10** free articles left for the week

Signup for a trial to access unlimited content.

Start Trial
