COUNTRY COMPARATIVE GUIDES 2023

The Legal 500 Country Comparative Guides

Ecuador

DATA PROTECTION & CYBERSECURITY

Contributor

Robalino

Pedro Córdova

Partner | pcordova@robalinolaw.com

Maria Paula Arellano

Associate | mparellano@robalinolaw.com

This country-specific Q&A provides an overview of data protection & cybersecurity laws and regulations applicable in Ecuador.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

ECUADOR
DATA PROTECTION & CYBERSECURITY

1. Please provide an overview of the legal and regulatory framework governing data protection, privacy and cybersecurity in your jurisdiction (e.g., a summary of the key laws; who is covered by them; what sectors, activities or data do they regulate; and who enforces the relevant laws).

The regulatory framework for personal data protection in Ecuador is rather new. On May 26, 2021, the Organic Law on Personal Data Protection was enacted, establishing obligations for public and private institutions guaranteeing the rights of personal data. Although there were already some related laws, the new regulation is a big step for Ecuador in its process to comply with international standards on personal data protection.

2. Are there any expected changes in the data protection, privacy and cybersecurity landscape in 2023-2024 (e.g., new laws or regulations coming into effect, enforcement of any new laws or regulations, expected regulations or amendments)?

It is expected that by the second half of 2023, there will be important regulatory changes in the landscape of data protection, privacy, and cybersecurity in Ecuador, as the Law creates a new entity for the enforcement of the rights and obligations. This entity was supposed to start applying fines and sanctions on May 2023, but up to this date, has not been created.

3. Are there any registration or licensing requirements for entities covered by these laws, and, if so, what are the requirements? Are there any exemptions?

Among some important obligations for Data Controllers and Processors is registration of their databases before the Personal Data Protection Authority. Depending on some legal and regulatory factors to be determined by the authority's regulations, some entities shall appoint a Data Protection Officer (DPO).

4. How do these laws define personal data or personally identifiable information (PII) versus special category or sensitive PII? What other key definitions are set forth in the laws in your jurisdiction?

The Organic Law on Personal Data Protection defines personal data as any data that identifies or makes identifiable a natural person, directly or indirectly. In addition, the Law identifies sensitive data as one of the special categories of data (in addition to health data, data of minors, and data of disabled persons). According to the Law, sensitive data are data related to: ethnicity, gender identity, cultural identity, religion, ideology, political affiliation, judicial history, immigration status, sexual orientation, health, biometric data, genetic data and those whose improper treatment may give rise to discrimination, infringe or may infringe the rights and freedoms of may violate fundamental rights and freedoms.

5. What are the principles related to the general processing of personal data or PII. For example, must a covered entity establish a legal basis for processing personal data or PII in your jurisdiction, or must personal data or PII only be kept for a certain period? Please outline any such principles or "fair information practice principles" in detail.

AS GDPR, the Law defines thirteen principles for the processing of personal data. These principles consist of treatment in strict adherence to applicable law and

international instruments; loyalty regarding the owners knowledge how their data is being processed; transparency, since all data must be easily accessible; purpose that must always be explicit; relevance and minimization of Data limited to what is strictly necessary; proportionality of the treatment so it's not excessive; confidentiality and secrecy; quality and accuracy as the data must be exact, complete, precise, verifiable, clear; and duly updated.

It also embraces similar principles for Information Security, and holds principles of conservation, seeing that it must be limited to a time in which said information is required; the presence of adequate measures for protection of data in order to avoid security breaches; proactive and demonstrated responsibility, meaning that the Controller or Processor must adopt and demonstrate adequate measures for the treatment, among others.

6. Are there any circumstances where consent is required or typically used in connection with the general processing of personal data or PII?

Consent is one of the bases of legitimacy for the processing of personal data, but it is not the only one. The consent of the data subject will generally be required to process special category data, particularly health data. In addition, the consent of the data subject is required for transfers or communications to third parties.

7. What are the rules relating to the form, content and administration of such consent? For instance, can consent be implied, incorporated into a broader document (such as a terms of service) or bundled with other matters (such as consents for multiple processing operations)?

According to the Law, the consent of the data subject shall be understood as valid when it is free, specific, informed, and unambiguous, and may be revoked anytime, with no retroactive effect. When the processing of data is intended to be based on the consent of the data subject for a plurality of purposes, it is of purposes, it shall be necessary to state that such consent is granted for all of them. purposes.

8. What special requirements, if any, are required for processing sensitive PII? Are there any categories of personal data or PII that are prohibited from collection or disclosure?

The sensitive data shall be treated in a restrictive manner, i.e. it prohibits its processing, unless the holder has given an explicit consent, the processing is necessary for the fulfillment of specific obligations of the data manager or to protect vital interests of the holder, when the holder has manifestly made public their consent for processing data, by order of a judicial authority; or for archiving information relevant for the public interest, scientific, historical research or statistical purposes.

9. How do the laws in your jurisdiction address children's personal data?

Minors' data must have a wider protection than adults´ data. Government entities, educational institutions and other related entities are bound to demonstrate the treatment of these data is safe and in compliance with the Law.

Data of minors may not be processed unless expressly authorized by the owner or his/her legal representative; or when such processing is intended to safeguard an essential public interest.

10. How do the laws in your jurisdiction address health data?

Health data is also a special category of data. National Health System institutions and health professionals in general may collect and process data from their patients. But this data must always be treated with the owner's consent, except for public interest reasons, impossibility of the owner or danger for his/her life or a third party. Nonetheless, the Law also allows the anonymization or pseudonymization for treatment purposes.

11. Do the laws include any derogations, exclusions or limitations other than those already described? Please describe the relevant provisions.

Processing credit data or data of deceased people also holds special regulations.

12. Does your jurisdiction impose requirements of 'data protection by design' or 'data protection by default' or similar? If so, please describe the requirement and how businesses typically meet the requirement.

In general matters, owners/controllers or processors of personal data have the obligation to guarantee and demonstrate that the processing of personal data has been carried out following the Law´s premises. Likewise, they must register their databases and keep them updated, internally and before the National Authority´s registry. Since the regulation for applying the Law has not yet been issued, there are no premises of how companies comply with these requirements. However, law firms have been advising companies to implement the Law, making a diagnosis of the current state of compliance, and attacking the main risks.

For the protection of data by design, Ecuadorian legislation establishes that the duty of the data controller is to take into account, in the early stages of the project's conception and design, that certain types of personal data processing entail a series of risks to the rights of the data subjects. The data controller must take into account that certain types of personal data processing entail a series of risks for the rights of the data subjects, for which technical, organizational and any other type of measures must be implemented to guarantee compliance with the data protection obligations.

Data protection by default must be carried out by applying the appropriate technical and organizational measures so that, by default, only personal data that are necessary for each of the purposes of the processing are processed.

13. Are owners/controllers or processors of personal data or PII required to maintain any internal records of their data processing activities or to establish internal processes or written documentation? If so, please describe how businesses typically meet these requirements.

As a GDPR based directive, the Law holds the principle of Proactive Responsibility, that shall be demonstrated. As such, the Data Controllers and Processors must apply protection by design and by default. In that matter Data Protection principles must be taken in account since the first phases of a project, considering that certain data processing entails risks for the rights of the holders, and that for every process, the Data protection principles shall be applied and considered.

14. Do the laws in your jurisdiction require or recommend having defined data retention and data disposal policies and procedures? If so, please describe these data retention and disposal requirements.

In accordance with the principle of conservation contained in the Law, personal data will be kept for no longer than the time necessary to fulfill the purpose for which they are processed.

To ensure that personal data is not kept longer than necessary, the data controller will establish deadlines for their deletion or periodic review.

15. When are you required to, or when is it recommended that you, consult with data privacy regulators in your jurisdiction?

There are several cases in which it is mandatory to inform or obtain authorizations from the Authority. Among the most important scenarios, the following are worth emphasizing: First, the processing of anonymized health data, as the Controller must demonstrate this measure (anonymization) has been taken. Secondly, notification of Data Breaches. Thirdly, DPO´s obligation of cooperation with the authority. And finally, international transfers.

16. Do the laws in your jurisdiction require or recommend conducting risk assessments regarding data processing activities and, if so, in what circumstances? How are these risk assessments typically carried out?

The controller shall carry out an impact assessment of the processing of personal data where it has been identified that such processing, by its nature, context, or purposes, is likely to result in a substantial risk to the rights and freedoms of the data subject or where the Personal Data Protection Authority so requires.

The impact assessment shall be mandatory in case of:

a) Systematic and comprehensive evaluation of personal data based on automated processing; b) Large-scale processing of special categories of data; or c) Large-

scale systematic observation of a publicly accessible area.

17. Do the laws in your jurisdiction require appointment of a data protection officer or a chief information security officer (or other person to be in charge of privacy or data protection at the organization), and what are their legal responsibilities?

A DPO shall be appointed when the processing is carried out by public sector entities; entities with large scale processing of data, or with permanent and systematized control, special data treatments or data related to national security.

18. Do the laws in your jurisdiction require or recommend employee training? If so, please describe these training requirements.

The Law does not contain regulations concerning employee training. However, what the Law mentions regarding employees is the obligation of the data controller to sign contracts of confidentiality and proper handling of personal data with the personnel in charge of the processing or who have knowledge of the personal data.

19. Do the laws in your jurisdiction require businesses to provide notice to data subjects of their processing activities? If so, please describe these notice requirements (e.g., posting an online privacy notice).

Data subjects must be notified of the processing activities in certain scenarios. For example, when personal data has not been obtained directly from the data subject or has been obtained from a source accessible to the public, the data subject must be informed. On the other hand, when data is transferred or communicated to third parties, the owner must be notified, and his/her consent must be obtained. In addition, in the event of a breach of security of personal data, the owner must be notified.

20. Do the laws in your jurisdiction draw any distinction between the owners/controllers and the processors of personal data, and, if so, what are they? (For example, are obligations placed on processors by operation of law, or do they typically only apply through flow-down contractual requirements from the owners/controller?)

The Law does make distinctions between controllers and processors. The processing of personal data by the processor must be governed by a contract, which clearly and precisely states that the processor will process personal data only in accordance with the instructions of the controller.

In addition to the above, according to the Law, the processor has the obligation to notify the data controller about security breaches within a maximum of 2 days. Also, the Law contains a specific section regulating breaches by the processor.

21. Do the laws in your jurisdiction require minimum contract terms with processors of personal data or PII, or are there any other restrictions relating to the appointment of processors (e.g., due diligence or privacy and security assessments)?

The Law does not contain specific restrictions for the designation of data processors; however, it does establish that the controller has the obligation to ensure that the data processor offers sufficient mechanisms to guarantee the right to the protection of personal data in accordance with the provisions of the Law, other regulations on the matter and best practices at national or international level.

The obligation to perform risk, threat, and vulnerability analyses, as well as to have the necessary security measures in place for the proper processing of data, falls on the data controller and data processor alike (not as a condition for the hiring of the processor).

22. Please describe any restrictions on monitoring, automated decision-making or profiling in your jurisdiction, including the use of tracking technologies such as cookies. How are these terms defined, and what restrictions are imposed, if any?

Our country does not hold specific regulations regarding the automated decision, but the determined right not to be subjected to a decision based solely or partially on

assessments that are the product of automated processes, including profiling, that produce legal effects on him or her or that violate fundamental rights and freedoms, for which the holder may: request from the controller a reasoned explanation of the decision taken by the controller or processor, submit comments, request the assessment criteria on the automated program, request from the controller information on the types of data used and the source from which they have been obtained, and challenge the decision before the controller or processor.

23. Please describe any restrictions on targeted advertising and cross-contextual behavioral advertising. How are these terms or related terms defined?

There is currently no regulation of the matter in question.

24. Please describe any laws in your jurisdiction addressing the sale of personal data. How is "sale" or related terms defined, and what restrictions are imposed, if any?

There is currently no regulation of the matter in question.

25. Please describe any laws in your jurisdiction addressing telephone calls, text messaging, email communication or direct marketing. How are these terms defined, and what restrictions are imposed, if any?

According to the Organic Law for Consumer Protection, it is forbidden to make telephone calls, visits in person to the consumer's home, unsolicited proposals or offers, via phone, email, text messages, or any other means of communication in a persistent manner, and ignoring the consumer's request to cease this type of activity or outside working days and hours.

26. Please describe any laws in your jurisdiction addressing biometrics such as facial recognition. How are these terms defined, and what restrictions are imposed, if any?

According to the Data Protection Law, biometric data is considered sensitive data and must be treated as a special category of processing.

In addition, in 2022, the Single Authentication System (SAU) Operating Standard was issued, the purpose of which is to promote the creation and use of a single digital access credential to government services and systems portals. This standard regulates the collection of biometric data, such as validation through facial recognition.

27. Is the transfer of personal data or PII outside the jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (e.g., does a cross-border transfer of personal data require a specified mechanism? Does a cross-border transfer of personal data or PII require notification to or authorization from a regulator?)

It´s possible to execute International Transfers to countries that provide adequate levels of protection and conform to recognized international standards. If the destination country does not have an adequate level of protection, international transfers should guarantee that adequate measures are been taken to protect the Holder's rights. In addition, controllers or processors of personal data may submit binding corporate rules to comply with regulations and standards established by law.

28. What security obligations are imposed on personal data or PII owners/controllers and on processors, if any, in your jurisdiction?

In case of a Data Breach, the controller or processor must verify the categories and volume of personal data, the state of the art, best practices of integral security and the costs of application according to the nature, scope, context and purposes of the processing, as well as identifying the probability of risk, before deciding the notification.

29. Do the data protection, privacy and cybersecurity laws in your jurisdiction address security breaches, and, if so, how does the law define "security breach"?

Security measures must be on a permanent and continuous basis, to assess, prevent, impede, reduce,

mitigate, and control risks, threats, and vulnerabilities, including those that carry a substantial risk to the rights and freedoms of the data subject. The controller must notify the Authority about the breaches, as well as the processor shall notify the data controller.

30. Does your jurisdiction impose specific security requirements on certain sectors, industries or technologies (e.g., telecoms, infrastructure, artificial intelligence)?

The Central government has adopted a public policy regarding cybersecurity, by a Ministerial Agreement in 2021. According to those policies, the Government must provide cybersecurity measures and guarantees to people´s rights. As well, the Law determines the people´s rights to their digital rights, and the obligation of the government to protect them. Also, an even its not cyber security, the law establishes that information regarding strategic sectors may not be transferred outside Ecuador. These sectors are energy, telecommunications, non-renewable natural resources, transportation and refining of hydrocarbons, biodiversity, and genetic heritage.

These policies create the Cyber Defense Command, created as an operational command of the Joint Command of the Armed Forces, with the mission of executing defense operations, exploration, and response in cyberspace, to protect the critical digital infrastructure and essential services of the Country band critical digital infrastructure of the defense sector.

31. Under what circumstances must a business report security breaches to regulators, to individuals or to other persons or entities? If breach notification is not required by law, is it recommended by the regulator, and what is the typical custom or practice in your jurisdiction?

As there is no regulator, we cannot speak of a typical practice. Nonetheless, the Law holds GDPR principles regarding Data Breach reports. In that matter, the notification-term is five days since the event, unless the event will not cause an impact on the people´s rights.

32. Does your jurisdiction have any specific legal requirement or guidance regarding dealing with cybercrime, such as the payment of ransoms in ransomware attacks?

There is no public policy regarding the management of these kinds of cybercrimes.

33. Does your jurisdiction have a separate cybersecurity regulator? If so, please provide details.

The Agency of Regulation and Control of Telecommunication (ARCOTEL) is the main Regulator in the field. Also, there is a Cyber Defense Command, created as an operational command of the Joint Command of the Armed Forces, with the mission of executing defense operations, exploration, and response in cyberspace, to protect the critical digital infrastructure and essential services of the Country band critical digital infrastructure of the defense sector.

34. Do the laws in your jurisdiction provide individual data privacy rights such as the right to access and the right to deletion? If so, please provide a general description of the rights, how they are exercised, what exceptions exist and any other relevant details.

Data controllers are obliged to adopt measures for the exercise of the fundamental Privacy rights.

35. Are individual data privacy rights exercisable through the judicial system or enforced by a regulator or both?

The holder may submit requests, complaints or claims directly to the data controller, who must respond within 15 days. If the data controller does not answer the request or the request is denied, the data owner may file an administrative claim before the Data Protection Authority.

36. Does the law in your jurisdiction provide for a private right of action and, if so, in what circumstances?

The Right holders may also exercise a private right of action. The Constitution guarantees the right to exercise the rights directly, without the need of holding a determined Law. In that matter, for the Data Privacy rights, the holder may file a Habeas Data, which is a special action filed before a judge to require an

immediate solution to a possible violation of rights.

37. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection, privacy and/or cybersecurity laws? Is actual damage required, or is injury of feelings sufficient?

The Law assures the right to demand damages against the violation of their rights, against the person or enterprise that is responsible for the harm. Depending on the action, the plaintiff may demonstrate the actual damage, or sue for a moral damage repair, in which case they will have to prove the internal or “spiritual” damage caused by the breach.

38. How are data protection, privacy and cybersecurity laws enforced?

The Law creates the Superintendence of Data Protection, which will oversee holding, verifying, and controlling the accomplishment of data protection and privacy laws.

As part of the Data Protection security, they also may revise that any Data Controller or Data Processor has adequate cybersecurity measures.

39. What is the range of sanctions (including fines and penalties) for violation of data protection, privacy and cybersecurity laws?

The fines may be from 0.1 up to 1% of the total sales of the last financial period, depending on the type of infringement.

The public sector will also have to cover fines up to twenty minimum wages (US$ 450, this year).

In case a criminal offense is determined, such as any violation to intimacy rights that includes violation of data privacy rights, the sanction may be prison from one and up to three years.

40. Are there any guidelines or rules published regarding the calculation of fines or thresholds for the imposition of sanctions?

No guidelines.

41. Can personal data or PII owners/controllers appeal to the courts against orders of the regulators?

Yes, as the resolution is an administrative measure, the affected may appeal it before the court.

42. Are there any identifiable trends in enforcement activity in your jurisdiction?

As there is still no authority and no practical regulations, there is no identifiable trend.

43. Are there any proposals for reforming data protection, privacy and/or cybersecurity laws currently under review? Please provide an overview of any proposed changes and how far such proposals are through the legislative process.

Nowadays, the regulation is still pending. There is a new draft in the office, unfortunately it has not yet been published. However, during the two years that we have had time to implement the Data Protection Law, companies in Ecuador have made considerable progress, considering international standards and good practices in data protection. We are a little late, but we are also picking up the pace.

Contributors

Pedro Córdova
Partner
pcordova@robalinolaw.com

Maria Paula Arellano
Associate
mparellano@robalinolaw.com