Peruvian Legislation
Law 29733
Law of Data Privacy Protection

Main aspects

Introduction:

Peruvian Legislation on Personal Data Protection has recently been enacted.

The Personal Data Protection Law – Law Nº 29733 (hereinafter Law) has been partially in force since July, 4, 2011. However, the Law will be fully in force 30 days after the publication of its application rule.

It is important to note that the Draft Application Rule was issued in September 2012. Nevertheless, there is no expected date for it to be passed.

Consent:

The owner of personal information must give his/ her consent to the "processing" of personal data.

Consent must be:
- Previous.
- Informed.
- Express.
- Unequivocal.
- FOR SENSITIVE INFORMATION: ALSO WRITTEN.

Draft Application Rule provisions related to consent:
- Express: Unequivocal (a person unequivocally grants his consent for the processing of his personal information, when otherwise his behavior would have been different).
  "Click", "touch", "pad" (digital environment)
- Express and written:
  - Electronic signature.
  - Writing that is recorded in a way that can be read or printed, or by any other means which allows identifying the owner of personal data.

- Pre-established text, visible, legible and simple to understand, that the owner of personal data can accept through a written response, graphic or "click".

Processing:

Collection, recording, organization, storage, preserving, elaboration, alteration, consultation, suppression, use, disclosure by transmission or dissemination, or any other way of processing personal data to facilitate its access, ordering or interconnection.

USE OF PERSONAL DATA FOR ADVERTISEMENT PURPOSES IS PROCESSING!

Guiding Principles:

- The collection of personal data by fraudulent, unfair or illegal means is prohibited.
- The purpose of collection must be determined, explicit and legal. The processing must not be extended to a purpose other than that established unequivocally as such at the time of collection.
- Processing of personal data must be adequate, relevant and not excessive for the purpose for which the data was collected.
- Personal data must be truthful, exact, and as far as possible, updated, pertinent and adequate regarding the purpose for which it was collected.
- The data controllers and data processors must adopt technical, organization and legal measures in order to guarantee the security of the personal data.
- For cross-border data transfer, an adequate level of protection should be guaranteed, or at least comparable with the standards of the Law or the international standards.
- All personal data owners must have the administrative and judiciary means to claim in case of breach of its rights.

Exceptions to consent:

Consent is not necessary for processing personal data when:

- Data is collected by public entities during their regular activities.
- It is contained or is intended to be contained in publicly accessible sources.
- Data is related to personal credit information, according to applicable law.
- When it's related to a Law for the promotion of competition on regulated markets, as long as the information provided is not used to affect the privacy of the data owner.
- It is necessary for a contract execution where one of the parties is the owner of the personal information; or when the personal data is derived from a professional or scientific relationship of the owner of personal information and it is necessary for its development or completion.

- When personal data is related to health and is necessary, on risk circumstances, for the prevention, diagnosis and medical or surgical processing of the owner of personal information, whenever it is carried out on a health facility or by professionals under professional secrecy; or when there are public interest reasons, or reasons of public health.
- In the development of epidemiological or similar studies, when dissociation process is used.
- When processing of personal data is performed by nonprofit organizations whose goal is political, religious or of a trade union. This applies only for personal data of its members, which cannot be transferred without their consent or used outside the scope of the organization´s usual activities.
- When an anonymity or dissociation process has been applied.
- When the processing of personal data is necessary to protect legitimate interests of the owner of personal information, and is done by the data controller or the data processor.

Cross-border Data Transfer:

- Data processor and the data controller should proceed only if the destination country holds an adequate level of protection for personal data, or at least comparable with the standards of Law or International Standards.
- If the destination country does not have an adequate level of protection, the party sending the personal data across the border must guaranty that the processing of the data will take place pursuant to the provisions of the Law.

The second rule does not apply in the following situations:

- Agreements within the framework of international treaties related to the pertinent subject matter in which the Republic of Peru is a party.
- International judicial cooperation.
- International cooperation among intelligence agencies for the fight against terrorism, illicit drug traffic, money laundering, corruption, human trafficking, and other modalities of organized crime.
- When the personal data is necessary for the execution of a contract, where one of the parties is the owner of personal information, including what is necessary for activities such as the user authentication, improvement and support of the service, monitoring service quality, support for maintenance and billing of the account, and the activities that managing the contractual relationship requires.
- Banking or stock exchange transfers related to banking or stock transactions in accordance with applicable law.
- When the cross-border data transfer has been done for medical or surgical protection, prevention, diagnosis and processing for the owner of personal information, or when it is necessary in the development of epidemiological studies, or similar ones, as long as an adequate dissociation process is used.
- When an owner of personal information issues a prior, informed, express and unequivocal consent.

Owners of personal information rights:

Main rights of the Owners of personal data:

- Can withdraw their consent in any moment.
- Access the personal information about themselves that is subject to processing.
- Update, inclusion, rectification and suppression of their personal data, when:
  - Partially or totally inaccurate, incomplete or when they have noticed an omission, mistake or falseness.
  - It is no longer necessary for the purpose for which it was collected, or when the term for processing has expired.
- Be informed, in a prior, detailed, simple, express and unequivocal manner, about the following:
  - The purpose for which the personal data will be processed.
  - The identity of receivers, or potential receivers of the data.
  - The existence of the data bank in which the data will be stored, as well as the identity of the data controller and, if applicable, the data processor.
  - The obligatory or optional feature of the questions at the time of collection, with special emphasis on Sensitive Information.
  - The possibility of data transfer.
  - The consequences of providing their personal data and the refusal to do so.
  - The term which the personal data will be stored.
  - The possibility to exercise the rights granted by law, and the means to do so.
- When collecting the personal data online by means of electronic communication networks, these notice obligations could be fulfilled by means of the publication of easily accessible and identifiable privacy policies that should be previously accepted.

Sanctions for Noncompliance:

The dispositions regarding this matter are not in force yet. However, the Law establishes a scale of fines for noncompliance, ranging from S/.1,850 up to S/.370,000 (approximately US $740 up to US $148,000), with a 10% limit of annual gross income.

The National Authority of Personal Data Protection at the Ministry of Justice, may impose coercive fines that may not to exceed S/. 37,000 (approximately US$ 14,800) for breach of accessory obligations.

* * * *