Data. Protection. Adding Value.

Data Protection Laws - Peru

Legislation

Personal data protection is regulated by Law N° 29733, issued in 2011 and in full force and effect since 2013. The Law seeks to guarantee the fundamental right to the protection of personal data, defined in the Political Constitution of Peru, through its appropriate treatment, within a framework of respect for fundamental rights. Said Law is developed by the Regulation issued by Supreme Decree N° 003-2013-JUS, and there are complementary provisions regulated by Legislative Decree N° 1353 and its Regulation. There is also a guide developed by the supervisory authority contained in the Directive on Security of Information Managed by Personal Data Banks; as well as provisions on video surveillance defined by Directive N° 01-2020-JUS/DGTAIPD.

It is worth mentioning that there is a draft regulation that will amend the Supreme Decree N° 003-2013-JUS and the final version is expected to be published in the coming months. This project generates significant changes to the current regulation on consent, commercial prospecting, creation of the Personal Data Officer, incident management, among others.

Risk Level: High

Scope: The Law applies to personal data contained or intended to be contained in personal data banks of public and private administration, whose processing is carried out in the national territory. Sensitive data are subject to special protection. There are certain exceptions to the local application of the regulation listed in the regulation.

Supervisory Authority

Supervisory Authority:
The National Authority for the Protection of Personal Data (NAPPD) enforce compliance with the regulations regarding the protection of personal data. The institution registers and sanctions with fines and corrective measures for non-compliance with the Law and its related regulations.
The Ministry of Justice and Human Rights, within the framework of its specific competencies, exercises the NAPPD through the General Directorate of Transparency, Access to Public Information and Protection of Personal Data.

Registration/Approval Requirements:

The NAPPD approves the registration of personal data banks requested by companies, as well as the registration of cross-border flows and all acts related to such records, such as updates, modifications, and others.

General Data Privacy Principles

The Principles serve as an interpretative criterion for resolving questions that may arise in the application of the Law and its regulations, as well as a parameter for the development of other provisions and for filling gaps in the legislation.

- Legality
- Consent
- Purpose
- Proportionality
- Quality
- Security
- Availability of recourse
- Adequate level of protection

The draft of regulation that will amend the Supreme Decree N° 003-2013-JUS establishes the following principles: transparency and proactive responsibility.

Enforcement

Enforcement
The Law allows for the following fines to be issued:

Gravity of the infraction	UIT Fine	
	Min	Max
Minor	0.5	5
Severe	5	50
Very serious	50	100

Please be advised that UIT stands for “Unidad Impositiva Tributaria” and its amount varies annually. In 2023 its value was S/. 4,950 and in 2024 it is S/. 5,150.

Remedies for Individuals:
Individuals affected by unlawful processing of their personal data may also have access to a civil action, in order to seek compensation for damages. The Judicial Branch could also be approached for the purposes of the corresponding habeas data.
Depending on the level of exposure and involvement of personal data, there are also certain provisions provided for in the Digital Crime Law that may be punishable as crimes.

Data Processing

Legal Basis for Processing
The processing of personal data must be carried out with full respect for the fundamental rights of its owners and the rights conferred on them by the Law, as well as its principles. The same rule applies to their use by third parties.
The owner of the personal data bank or whoever is responsible for the processing, must obtain consent for the processing of personal data, which must be free, prior, express, unequivocal and informed.
The consent of the owner of personal data is not required in certain cases provided by Law. For the purposes of proving that consent has been obtained under the terms established in the Law and in these regulations, the burden of proof shall in all cases fall on the owner of the personal data bank or whoever is responsible for the processing.

Sensitive Personal Data
In the case of sensitive data, consent must be given in writing, through a handwritten signature, digital signature or any other authentication mechanism that guarantees the unequivocal will of the owner.

Other Restrictions on Processing:
The person in charge of the personal data bank is prohibited from transferring to third parties the personal data subject to the provision of processing services, unless the owner of the personal data bank who commissioned the processing has authorized it and the owner of the personal data has given his consent, in the cases where such consent is required by Law. The processing of personal data in data banks that do not meet the requirements and security conditions is prohibited.

Individual Rights

The personal data owner has the following rights:

- Right to information
- Right to access
- Right to update, inclusion, rectification and suppression of information.
- Right to impede supply
- Right of opposition
- Right to objective processing
- Right to guardianship
- Right to be indemnified

Although the right to be forgotten is not expressly regulated in the Law, there is an administrative resolution issued by the NAPPD and a resolution of the Constitutional Court recognizing this right.

Also, the draft of regulation that will amend the Supreme Decree N° 003-2013-JUS recognizes the right of portability and makes certain updates to the right of objective processing of personal data.

Security & Data Breaches

The regulation establishes that the holders of personal data banks or those who are responsible for them are required to implement information security measures, establishing a list of measures of different nature and details in the Directive on Security of Information Managed by Personal Data Banks.

The draft of regulation that will amend the Supreme Decree N° 003-2013-JUS establishes that In the event of a security incident involving personal data, the data controller must notify the NAPPD within 48 hours of becoming aware of it, establishing that the communication must contemplate a series of requirements. When the personal data security incident generates an unauthorized exposure of personal data unauthorized exposure of personal data and/or a high risk to the rights and freedoms of natural rights and freedoms of natural persons, the owner of the data bank or data controller, in addition to the owner of the data bank or data controller, in addition to notifying the NAPPD, must communicate it to the personal data owners without undue delay in a simple and clear language about the affectation of their right, as well as the measures adopted, as well as the measures taken.

Other Business Obligations

The regulation establishes that the owners of personal data banks or those responsible for their processing must implement legal, organizational and technical measures. In general terms, the measures are made up as follows:

- Legal: Obtaining informed consent, based on the principles of the regulation and according to the characteristics or limitations foreseen for this purpose. For this purpose, the privacy notices or clauses in the channels for obtaining information must be accredited. Also, regulations in contractual relationships with data processors.
- Organizational: Identification and registration of personal data banks, as well as the corresponding cross-border flows, and updates, if applicable. Also, the generation of procedures for the attention of individuals' rights, as well as training in topics related to the Law and annual audits.
- Technical: Implementation of security measures, according to the guidelines of the Security Directive, privacy policy, cookies, procedures regulating aspects of video surveillance, Privacy by design, PIA, among the main ones.

The draft regulation proposes the creation of the Personal Data Protection Officer, as well as reinforces the implementation of privacy risk assessments, among others.

Service Providers & Cross-Border Transfers

Service Provider Arrangements:
The legislation determines that this type of agreement must contain stipulations related to the responsibility of the parties for the processing, security measures, term of execution, among others.

Cross-Border Data Transfers:
For these types of transfers, a sufficient level of protection must be guaranteed for the personal data to be processed or, at least, comparable to the provisions of the Law or international standards on the matter.
Owner's consent is required on scope, security measures, etc.; there are limitations on such consent.

Other/To Watch

The NAPPD imposed fines for more than S/. 7.6 million during 2023, as well as supervised 336 entities, initiated 132 sanctioning procedures and registered 2,670 personal data banks. The primary industries sanctioned are financial, banking, technology, retail, travel, and education.

There is a regulatory project to amend the Regulations contained in Supreme Decree N° 003-2013-JUS, which aims to have an updated regulatory framework for the defense of privacy rights in the face of the challenges of e-commerce, artificial intelligence, etc. The final version will be published in the coming months, therefore, companies will have to review their privacy practices for such regulatory adaptation, improvement of their risk management and internal control system.

Let's connect to discuss how we can help:

Nancy Yong
Risk Consulting & Forensic
Partner, PwC Peru

nancy.yong@pwc.com

Guillermo Zapata
Risk Consulting & Forensic
Director, PwC Peru

guillermo.zapata@pwc.com