DATA PROTECTION LAWS OF THE WORLD

Peru

DLA PIPER

PERU

Last modified 26 January 2023

LAW

Article 2 of the Political Constitution of Peru sets forth certain fundamental rights that every person has, including a right to privacy regarding information that affects personal and family privacy, which was the basis for the creation of a law that specifically protects the use of personal data of any natural person and applies to both private and state entities.

The Personal Data Protection Law N° 29733 (PDPL) was enacted in June 2011. In March 2013, the Supreme Decree N° 003-2013-JUS-Regulation of the PDLP (Regulation) was published in order to develop, clarify and expand on the requirements of the PDPL and set forth specific rules, terms and provisions regarding data protection.

Together, the PDLP and its Regulation are the primary data protection laws in Peru.

It should be noted that in 2023, the NDPA published a bill for a new Regulation to the PDPL. The new Regulation is expected to be officially published in 2024 and aims to enhance the protection of personal data under the PDPL by including improvements to contribute to the defense of the protection of personal data considering the rapid development of e-commerce, artificial intelligence, and similar digital technologies.

Further, the law regulating private risk centers and the protection of the owner of the information is Law N° 27489, enacted in 2001 and later amended several times. This law establishes the applicable provisions for activities related to risk centers and companies that handle:

- Information posing higher risks to individuals (*eg*, related to financial, commercial, tax, employment or insurance obligations or background of a natural or legal person that allows evaluating its economic solvency), and
- Sensitive personal data (according to the PDPL)

DEFINITIONS

Definition of personal data

Personal data is defined as information — regardless of whether numerical, alphabetic, graphic, photographic, acoustic — about personal habits or any other kind of information about an individual that identifies or may identify such individual by any reasonable means.

Definition of sensitive personal data

Sensitive personal data includes all of the following:

- Personal data created through biometric data which by itself renders a data subject identifiable
- Personal data regarding an individual's physical or emotional characteristics, facts or circumstances of their emotional or family life, as well as personal habits that correspond to the most intimate sphere

- Data referring to racial and ethnic origin
- Economic income, opinions or political, religious, philosophical or moral convictions
- Union membership
- Information related to physical or mental health, to sexual life or other similar information that affect the data subject’s privacy

NATIONAL DATA PROTECTION AUTHORITY

The Directorate for the Protection of personal data, which is part of the General Directorate of Transparency, Access to Public Information and Protection of Personal Data (NDPA), is the primary agency in charge of enforcing data protection matters.

The NDPA’s current address is:

Scipion Llona 350
Miraflores, L-18
Lima
Peru

Website

REGISTRATION

The National Registry for the Protection of Personal Data (NRPDP) maintains information about personal databases of public or private ownership and publishes a list of such databases to facilitate individuals’ exercise of their rights of access to information, rectification, cancellation, opposition and others regulated in the PDPL and its Regulation.

In addition, the NRPDP maintains records of:

- Communications of cross-border flow of personal data, and
- The sanctions, precautionary or corrective measures imposed by the NDPA

The holders of personal databases must register in the NRPDP providing the following information:

- The name and location of the personal database
- The purposes and the intended uses of the database
- The identification of the owner of the personal database
- The categories and types of personal data to be processed
- Collection procedures and a description of the system for processing personal data
- The technical description of the security measures
- The recipients of personal data transfers

The cross-border transfer of personal data must be notified to the NDPA, including the information required for the transfer of data and registration of the database.

DATA PROTECTION OFFICERS

There is no requirement to appoint a data protection officer in the private sector (only in the public sector). However, when a company registers its personal database with the NDPA, it can report that it has a Security Manager of that database.

COLLECTION & PROCESSING

The collection and processing of personal data requires the data subject’s prior, informed, express and unequivocal consent. The consent may be expressed through electronic means.

The collection and processing of sensitive personal data requires the data subject’s prior, informed, express and unequivocal consent, and must be expressed in writing.

The data subject’s consent is not necessary if any of the following are true:

- The data are compiled or transferred for the fulfillment of governmental agency duties
- The data are contained or destined to be contained in a publicly available source
- The data are related to credit standing and financial solvency, as governed by applicable law (Law N° 27489)
- A law is enacted to promote competition in regulated markets, under the powers afforded by the Framework Law for Regulatory Bodies of Private Investmenton Public Services (Law N° 27332), provided that the information supplied does not breach the user’s privacy
- The data are necessary for a contractual, scientific or professional relationship with the data subject, provided that such data is necessary for the development and compliance with such relationship
- The data are needed to protect the health of the data subject, and data processing is necessary, in circumstances of risk, for prevention, diagnosis, and medical or surgical treatment, provided that the processing is carried out in health facilities or by professionals in health sciences observing professional secrecy
- The data are needed for public interest reasons declared by law or public health reasons (both must be declared as such by the Ministry of Health) or to conduct epidemiological studies or the like, as long as dissociation procedures are applied
- The data are dissociated or anonymized
- The data are used by a nonprofit organization with a political, religious, ortrade union purpose, and refer to the data of its members within the scope of the organization´s activities
- The data are necessary to safeguard the legitimate interest of the data subject orthe data handler
- The data are being processed for purposes linked to money laundering and terrorist financing or others that respond to a legal mandate
- In the case of economic groups made up of companies that are considered subjects obliged to inform, the data is processed in accordance with the rules that regulate the Financial Intelligence Unit, so that they may share information with each other about their respective clients to prevent money laundering and financing of terrorism (as well as in other instances of regulatory compliance, establishing adequate safeguards on the confidentiality and use of the information exchanged)
- When the treatment is carried out in a constitutionally valid exercise of the fundamental right to freedom of information
- Others expressly established by law

If the data controller outsources the processing of the personal data to a third party (*ie,* a processor), such party must also comply with the relevant requirements of the PDLP (*eg*, to maintain personal data as confidential and to use the personal data only for the purposes authorized and modify inaccurate information).

Upon termination or expiration of the outsourcing agreement, the personal data processed must be deleted, unless the data subject provides express consent to do otherwise.

The processing of personal data by cloud services, applications and infrastructure is permitted, provided compliance with the provisions of the PDPL and its Regulation is guaranteed.

TRANSFER

Where personal data is transferred to another entity, recipients must be required to handle such personal data in accordance with the provisions of the PDPL and its Regulation.

Generally, data subject consent is required.

Cross-border transfers

The transferring entity may not transfer personal data to a country that does not afford adequate protection levels (protections that are equivalent to those afforded by the PDPL or similar international standards). If the receiving country does not meet these standards, the sender must ensure that the receiver in the foreign country is contractually obligated to provide 'adequate protection levels’ to the personal data, such as via a written agreement that requires that the personal data will be protected in accordance with the requirements of the PDPL, or under one of the following circumstances:

- In accordance with international treaties in which Peru is a party
- For purposes of international judicial cooperation or international cooperation among intelligence agencies to combat
  - Terrorism
  - Drug trafficking
  - Money laundry
  - Corruption
  - Human trafficking, and
  - Other forms of organized crime
- When necessary for a contractual relationship with the data subject, or for a scientific or professional relationship
- Bank or stock transfers concerning transactions in accordance with the applicable law
- The transfer is performed to protect, prevent, diagnose or medically or surgically treat the data subject, or to perform studies of epidemiology or the like, provided a data dissociation procedure has been applied
- The owner of the personal data has given its prior, informed, express and unequivocal consent to the transfer to the inadequate jurisdiction
- Other exempt purposes established by the Regulations

For both domestic and cross-border transfers, the recipient must assume the same obligations as the transferor of the personal data. The transfer must be formalized, such as by binding written contract, and capable of demonstrating that the holder of the database or the data controller communicated to the recipients the conditions in which the data subject consented to their processing.

As an alternative to the above mentioned “adequate transfer” requirement, a Data Controller may execute with a Data Processor (or other Data Controller) the standard contractual clauses already approved by the Peruvian Data Protection Authority, which include several obligations and declarations regarding the data transfer between the parties.

SECURITY

Database holders and data handlers must adopt technical, organizational and legal measures necessary to guarantee the security of the personal data they hold. The measures taken must ensure a level of security appropriate to the nature and purpose of the personal data involved.

The Agency has passed a Directorial Resolution N° 019-2013-JUS/DGPDP (hereafter, the 'Security Directive'). This Security Directive establishes different standards depending on the features of the database, including:

- Number of data subjects whose data are contained in the database
- Number of fields of the database (eg, name, address, phone number)
- Existence of sensitive data
- Owner of the database (an individual or entity)

The following security measures must be taken with respect to the loss of a personal data bank:

- Backup copies of personal data must be made to allow recovery in case of loss or destruction
- Any recovery of personal data, from the backup, must have the authorization of the person in charge of the personal data bank
- Proof of recovery of personal data must be performed to verify that backup copies can be used if they are required

For digital information, it is important to mention that the computer systems that handle databases or process personal data must include in their operation records that keep all types of interaction with logical data, so as to identify the users, changes, consultations, starting and closing hours of a session and other actions that are carried out. These records will allow the access of competent, authorized and identified personnel only.

Further, it is necessary to establish the following:

- Security measures related to the authorized accesses to the data by procedures of identification and authentication that guarantee the confidentiality and integrity of the data

- Necessary mechanisms for correct application of the procedures for making backup copies and recovery of the data in order to guarantee the reconstruction in the status they had at the time of the loss or destruction

The applicable measures in which the information must be processed, stored or transmitted—taking into account the controls, policies, standards and recommendations related to physical and environmental security—are established in the following documents:

- Peruvian Technical Standards 'NTP- ISO/IEC 17799: 2007 EDI. Technology of Information. Code of Good Practice for the management of the security of the information. 2nd Edition'
- 'NTP ISO/IEC 27001: 2008 EDI Technology of Information. Security Techniques. Systems of Management of Information Security. Requisites.'

BREACH NOTIFICATION

The holder of a database (and processor, where applicable) is required to implement security measures to prevent the unauthorized access to personal data.

As a consequence, an implied obligation would be to adopt all corrective measures in the event of a data breach to minimize the damages it may cause to the data subjects. For that reasons, the Security Directive establishes security measures against:

- The loss of the personal database, and
- An unauthorized processing of the personal database

In this way, any case of data breach should be communicated to the data subjects as soon as it is confirmed. The database owner must inform the data subject of 'any incident that significantly affects their property or their moral rights', as soon as the occurrence of the incident is confirmed.

The minimum information to be provided in a notice includes a description of:

- The incident
- Personal data disclosed
- Recommendations to the data subject
- Corrective measures implemented

Further, it should be noted that the NDPA does not provide any terms or guidelines for submitting a mandatory or voluntary report in case of a digital security incident, nor does it contemplate any sanctions for lack of reporting.

Mandatory breach notification

Pursuant to Emergency Decree 007-2020, which approves the Digital Trust Framework, with the intent to strengthen cybersecurity ("Emergency Decree"), public administration entities, digital service providers in the financial sector, utilities (electricity, water and gas), healthcare and passenger transportation, internet service providers, and other providers of critical activities (economic and/or social activity whose interruption has serious consequences on the health and safety of citizens, on the effective functioning of essential services that maintain the economy, society and government, or affects the economic and social prosperity in general) as well as educational services must comply with the following: (a) notifying the National Centre for Digital Security (the “National Centre”) about every digital security incident; and, (b) reporting and collaborating with the NDPA in case of a digital security incident that involves personal data.

A Digital Security Incident is defined under the Emergency Decree as an “event or series of events that may compromise the trust, economic prosperity, protection of individuals and their personal data, the information, among other assets of the organization, through digital technologies”.

However, the following should be noted:

- According to the first and second final complimentary provisions of the Emergency Decree, regulations and guidelines will be issued in order to provide more information on the provisions and obligations contained in the Emergency Decree. To date no regulations have been issued.
- As previously mentioned, there are no terms or guidelines regarding the notification procedure before the National Centre, except for a brief statement on the Secretary’s website, stating that the reporting entity -when notifying a data breach- must include its identification information and all relevant information regarding the data breach that may help evaluate the incident, including supporting documents.

Considering the above, while formal content requirements for reporting breaches to the National Centre and the NDPA (as detailed above) exist, currently, due to the lack of regulations and issued guidelines, practically these are not being demanded by the relevant authorities.

ENFORCEMENT

The General Directorate of Sanctions (part of the NDPA) instructs on and resolves, in the first instance, violations and imposes sanctions as well as conducts and develops the research phase according to Article 115 of the Regulation of the PDLP.

The General Directorate for the Protection of personal data (also part of the NDPA) resolves in the second and last instance the sanctioning procedure and its decision exhausts the administrative route.

Possible sanctions for breaching data protection standards vary depending on the nature or magnitude of the offense:

- The fine applicable to minor infringement ranges from S/ 2,575 to S/ 25,750 (approximately between USD 700 and USD 7,000).
- The fine applicable to severe infringements ranges from S/ 25,750,000 to S/ 257,500 (approximately between USD 7,000 and USD 70,000).
- The fine applicable to very severe infringements ranges from S/ 257,500 to S/ 515,000 (approximately between USD 70,000 and USD 140,000).

Please note that the NDPA imposes fines considering the value of the Tax Unit for the year in which the offense is committed. The value for the Tax Unit for the current year 2024 is S/ 5,150 (approximately USD 1,400).

The NDPA is also authorized to impose additional fines up to S/ 51,150 (approximately USD 14,000), if the offender, despite being found liable and sanctioned as a consequence thereof, fails to remedy the unlawful practice. These are applicable in addition to civil and criminal liability.

ELECTRONIC MARKETING

The PDPL does not expressly regulate electronic marketing. However, the PDPL does apply to electronic marketing activities if personal data is processed as a result.

If consent is obtained through electronic media, the notice requirements can be met by publishing accessible and identifiable privacy policies with the relevant consent language and mechanism. The PDPL establishes the possibility of obtaining express consent by presenting the option to agree with the privacy policies in clickable ways (*eg*, by clicking, ticking a box).

Written consent may be provided by other options, including:

- Through an electronic signature
- A written document possible to read or print
- A mechanism or procedure that allows one to identify the subject and to receive his consent through a written text
- A pre-established text as long as it is easily visible, legible and written in simple language

The laws governing electronic signatures are:

- Law N° 27291
- The Digital Certificates and Signatures Law (Law N° 27269)

- Supreme Decree N° 052-2008-PCM

Note that expressing the will in any of the regulated forms does not eliminate the other requirements of consent referring to that consent must be informed, and freely given.

According to the article 58.1 of Consumer Protection Code Law N° 29571, the following commercial activities require prior, informed, express and unequivocal consent to promote products and services:

- Use of call centers
- Use of telephone call systems
- Bulk text messages or
- emails Telemarketing services

As to date, it is permitted to obtain personal information from public sources or by licit means in order to contact the data subjects to get their consent for the aforementioned commercial activities. Notwithstanding the foregoing, whenever the data subject does not grant its consent for commercial activities, it must not be contacted again for those purposes. Furthermore, easily accessible and free mechanisms must be implemented to allow the data subjects to revoke their consent for the commercial purposes.

However, a bill has been proposed, which would modify the aforementioned article 58.1, so that advertising could only be sent to consumers who request to receive such and grant the sender unequivocal, free, informed and express consent to be contacted for marketing purposes. So, a data subject’s information (i.e. telephone numbers and e-mails) could be used for marketing purposes only if the data subject has consented to be contacted by the sender for marketing purposes.

ONLINE PRIVACY

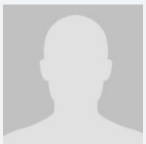
The PDPL does not expressly regulate online privacy, including cookies and location data. However, the PDPL will apply if personal data is collected and processed using these mechanisms.

This requires that the use and deployment of cookies, location data or another personal data that will be collected must comply with data privacy laws. The data subject’s consent must be obtained before cookies and/or location data can be used.

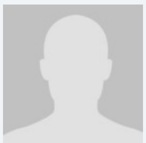
With respect to criminal law enforcement, Legislative Decree N° 1182 permits the National Police of Peru to access the location and geolocation of mobile phones or electronic devices of similar nature in cases of *flagrante delicto*.

It establishes the obligation for public communications services providers and public entities to keep the data from their users derived from telecommunication services during the first 12 months in computer systems an additional period of 24 months in an electronic storage system. Such service providers are bound to provide the location and geolocation data immediately, 24 hours a day, 365 days of the year, under warning of being liable to the responsibilities regarded by law in the event of noncompliance.

KEY CONTACTS



Ricardo Escobar
Partner
DLA Piper Pizarro Botto Escobar
T +1 511 616 1200
rescobar@dlapiperpbe.com



Daniel Flores
Associate
DLA Piper Pizarro Botto Escobar
T +1 511 616 1200
dflores@dlapiperpbe.com

DATA PRIVACY TOOL

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