Peru

Erick Iriarte Ahon and Cynthia Tellez
Iriarte & Asociados

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

Data protection in Peru is governed by Law No. 29733, the Law on Personal Data Protection published in the Official Gazette on 3 July 2011 (the Law), and Supreme Decree No. 003-2013-JUS, which approved the Regulations under Law on Personal Data Protection published in the Official Gazette on 22 March 2013 (the Reguations).

The Law entered into force on 4 July 2011; however, many of the provisions and its Regulations became effective on 8 May 2013.

The Constitutional Procedural Code recognises the habeas data process, which defends the constitutional right to personal data protection.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the powers of the authority.

The authority responsible for overseeing the data protection law is 'the National Data Protection Authority'; this entity is attached to the Ministry of Justice.

The National Data Protection Authority has functions such as:

- the administration and maintenance of the National Register of Personal Data Protection;
- the investigation of complaints lodged by data subjects and the issuing of provisional or corrective measures as established in the Regulation;
- the supervision of the personal data processing carried out by data controllers and data processors and, in the case of illegal acts, order the appropriate actions pursuant to the Law;
- starting investigations, ex officio or following a complaint from a party for presumed acts contrary to the provisions of the Law and apply the corresponding administrative sanctions;
- answering questions about personal data protection and the meaning of the current rules;
- issuing corresponding guidelines for the better application of the Law and its Regulation; and
- cooperating with foreign data protection authorities and generating bilateral and multilateral cooperation mechanisms for mutual assistance and help when required.

3 Breaches of data protection

Can breaches of data protection lead to criminal penalties? How would such breaches be handled?

There is no obligation on any entities to give notice in the event of a data security breach.

Scope

4 Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The Law applies to all entities that perform the processing of personal data in the country.

However, the Law does not apply to personal data or data intended to be contained in personal data banks created by natural persons exclusively for purposes related to their private life or family or are intended to be contained in a bank's data administration, national defence, public safety and the development of activities in criminal matters for investigation and enforcement.

5 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

The Law provides that communications, telecommunications, computer systems or their instruments, be they public or private, can only be opened, seized or intercepted by order of the judge with permission from the owner, with the guarantees provided in the law. The personal data obtained in violation of this mandate has no legal effect.

The marketing of personal data must adhere to the principles laid down in the Law.

6 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

- The Law regulating private risk information registries and providing protection to the owners of information (Law No. 27489 and modified by Law No. 27863).
- Article 154-A of the Criminal Code penalises the illicit traffic of personal data.
- Article 156 of the Criminal Code penalises the disclosure of personal and family privacy.
- Article 157 of the Criminal Code penalises the misuse of computer files.
- Article 9 of the Computer Crimes Act, Law No. 30096, penalises the impersonation of identity.

7 PII formats

What forms of PII are covered by the law?

The Law protects all personal data regardless of whether it is intended to be contained in computerised data banks or not.

8 Extraterritoriality

Is the reach of the law limited to data owners and data processors established or operating in the jurisdiction?

No. The law only states that contractual clauses are established to determine the same level of protection as in Peruvian law.

9 Covered uses of PII

Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide services to owners?

The data controllers and data processors must also comply with the guiding principles (legality, consent, purpose, proportionality, data quality, security, recourse and adequate protection).

The personal data processing may be performed by a third party other than the party delegated to do the processing, through an agreement or contract between the two. The subcontractor assumes the same obligations as are prescribed for the processor in the Law, the Regulations and other applicable provisions.

Legitimate processing of PII

10 Legitimate processing – grounds

Does the law require that the holding of PII be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

Personal data may be processed with the consent of the data subject.

The personal data may be processed without consent if the processing is necessary to fulfil a contract to which the data subject is a party, and if the processing is necessary to enable the public entities to fulfil a legal obligation.

11 Legitimate processing – types of data

Does the law impose more stringent rules for specific types of data?

Sensitive data is subject to special protection. It includes personal data consisting of biometric data that can be used to identify the individual; data referring to racial or ethnic origin; income; political, religious, philosophical or moral convictions; trade union membership; or information related to health or sexual life.

Written express consent is required for sensitive data. The creation of these personal databases can only be justified if its purpose, as well as being legitimate, is concrete and consistent with its actions or explicit purpose (eg, a bank holder's personal data).

Data handling responsibilities of owners of PII

12 Notification

Does the law require owners of PII to notify individuals whose data they hold? What must the notice contain and when must it be provided?

The PII owners have the obligation to notify the data subject of the possession of personal data when the data subject explicitly requested the information. The PII owners must respond to a such a request for information within a maximum of 8 working days from the day of receipt of the request.

If the data subject requested his or her right of access to information, the maximum response time will be 20 working days.

13 Exemption from notification

When is notice not required?

There are no exemptions from the requirement to notify.

14 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

The data subject has the right to access personal data that is subject to processing databases and obtain information about the way the data was compiled, the reasons for its compilation, at whose request it was compiled, and the transfers carried out or to be carried out.

15 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

The personal data being processed must be truthful, accurate, and, as far as possible, up to date, necessary, relevant, and adequate for the purpose for which it was collected.

Personal data collected directly from the data subject is considered to be accurate.

16 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

The law does not restrict the amount of PII that may be held.

Personal data should be held for only as long as is necessary to fulfil the purposes for which it was collected.

17 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

In accordance with the finality principle, personal data must be collected for a specific, explicit and legal purpose. In particular, the purpose should be clearly and objectively described, leaving no room for confusion.

18 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

The processing of personal data must not be used for another purpose that has not been unequivocally established at the time of its collection, excluding activities with historical, statistical or scientific value when used with a dissociation or anonymisation procedure.

Security

19 Security obligations

What security obligations are imposed on data owners and entities that process PII on their behalf?

Data controllers must adopt technical, organisational and legal measures to guarantee the security of personal data and avoid their alteration, loss, unauthorised processing or unauthorised access.

The environments in which the information is processed, stored, or transmitted must be equipped with appropriate security controls, based on the recommendations for physical and environmental security contained in the current edition of the 'NTP ISO/IEC 17799 EDI Information Technology Code of Good Practices for the Management of Information Security'.

The Directive on Information Security, Directorial Resolution No. 019-2013-JUS/DGPDP, provides guidance on the conditions, requirements and technical measures that should be taken into account in compliance with Law No. 29733 and its Regulations, security of personal data banks.

20 Notification of security breach

Does the law include obligations to notify the regulator or individuals of breaches of security?

No.

Internal controls

21 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

The Directive on Information Security provides the existence of the security officer who coordinates and monitors the implementation of security measures in a personal database.

22 Record keeping

Are owners of PII required to maintain any internal records or establish internal processes or documentation?

The data controller or the party responsible for the processing has the burden of proof to demonstrate that consent has been obtained in accordance with the Law and Regulations.

Registration and notification

23 Registration

Are owners and processors of PII required to register with the supervisory authority? Are there any exemptions?

The owners and processors of PII are not required to register with the supervisory authority.

However, personal data banks should be recorded with the supervisory authority.

24 Formalities

What are the formalities for registration?

Not applicable.

25 Penalties

What are the penalties for a data owner or processor for failure to make or maintain an entry on the register?

Not applicable.

26 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

Not applicable.

27 Public access

Is the register publicly available? How can it be accessed?

The register is not publicly available.

28 Effect of registration

Does an entry on the register have any specific legal effect?

Not applicable.

Transfer and disclosure of PII

29 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

The provision of personal data by a data controller to a data processor is not considered to be a transfer of personal data.

Outsourcing providers should not be permitted to gain ownership of data banks connected to the processing services that they provide;

30 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

The data processor is prohibited from transferring the data to a third party except when authorised by the controller.

31 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

The transfer of PII outside the jurisdiction is permitted only if the destination country maintains an adequate level of protection according to the Law. If the destination country does not provide adequate protection, the recipient must guarantee that the processing of personal data will conform to the requirements of the Law.

32 Notification of transfer

Does transfer of PII require notification to or authorisation from a supervisory authority?

The transfer of PII requires notification from a supervisory authority.

33 Further transfer

If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

Authorisation for cross-border transfers is not required.

However, the data controller and the data processor may request the opinion of the supervisory authority.

Rights of individuals

34 Access

Do individuals have the right to see a copy of their personal information held by PII owners? Describe any limitations to this right.

The data subject has the right to access personal data that is subject to processing in databases and to obtain information about the way the data was compiled, the reasons for the compilation, at whose request the compilation was made, and the transfers carried out or to be carried out.

The responsible may deny access to protect the rights and interests of third parties; where it would prevent pending judicial or administrative proceedings; where it is related to the investigation of compliance with tax or social security obligations, the performance of health and environmental control functions, or the verification of administrative violations; or when so ordered by law.

35 Other rights

Do individuals have other substantive rights?

The data subject has the right to access, rectify, object to and delete personal data that is subject to processing in databases.

36 Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

The data subject has the right to be indemnified under the Law in the event he or she is affected as a result of data violation.

37 Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

These rights are exercisable through the judicial system or by the supervisory authority.

Exemptions, derogations and restrictions

38 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

No.

Supervision

39 Judicial review

Can data owners appeal against orders of the supervisory authority to the courts?

Yes, they can.

Update and trends

The supervisory authority has published formats for the registration of personal databases on the National Register of Personal Data Protection and also the forms used to make complaints to the authority. The supervisory authority also issued the Directive of Information Security for personal databases with recommendations for compliance with security measures required by Law 29733.

In the criminal penal code article and computer crime law to criminalise the unauthorised marketing of personal data, illicit collection of sensitive data and identity theft through the use of ICT was modified. The crime of 'data trafficking' contained in the law of cybercrime was eliminated here for its inclusion in the Penal Code, besides allowing this crime to be prosecuted by the public exercise of criminal action and not private action as it is for other offences against privacy.

40 Criminal sanctions

In what circumstances can owners of PII be subject to criminal sanctions?

According to article 154-A of the Penal Code, when they have created or misused a database for marketing purposes or to facilitate commercialisation.

41 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

Not regulated.

42 Electronic communications marketing

Describe any rules on marketing by e-mail, fax or telephone.

Electronic communications marketing is not regulated.

I & A

IRIARTE & ASOCIADOS

Erick Iriarte Ahon **eiriarte@iriartelaw.com**
Cynthia Tellez **ctellez@iriartelaw.com**

Miro Quesada 191, Of 510
Cercado De Lima
Lima
Peru

Tel: +511 2035400
Fax: +511 2035400
www.iriartelaw.com
www.datospersonales.pe